Tennessee State University
Digital Scholarship @ Tennessee State University

Tennessee State University Alumni Theses and Dissertations
Tennessee State University Alumni

8-1995

On Single Equational-Axiom Systems for Abelian Groups

Sonsauhray C. Price-Sampson

Follow this and additional works at: https://digitalscholarship.tnstate.edu/alumni-etd

Part of the Mathematics Commons

ON SINGLE EQUATIONAL-AXIOM SYSTEMS FOR ABELIAN GROUPS

SONSAUHRAY C. PRICE-SAMPSON

TENNESSEE STATE UNIVERSITY
NASHVILLE, TENNESSEE
AUGUST, 1995

TENNESSEE STATE UNIVERSITY
LIBRARY

ON SINGLE EQUATIONAL-AXIOM SYSTEMS FOR ABELIAN GROUPS

A Thesis

Submitted to the Graduate School

of

Tennessee State University

in

Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in Mathematical Sciences

Graduate Research Series No. 2891

Sonsauhray C. Price-Sampson

August 1995

TENNESSEE STATE UNIVERSITY
LIBRARY

August 1995

To the Graduate School :

We are submitting a thesis written by Sonsauhray C. Price-Sampson entitled "On Single Equational-Axiom systems for Abelian Groups." We recommend that it be accepted in partial fulfillment of the requirements for the degree, Master of Science in Mathematical Sciences.

M. Rajagopalan

Chairperson

Sandra H. Scheick

Committee Member

Committee Member

D. K. Chaudhuri

Guest Examiner

Sandra H. Scheick

Major Adviser

Accepted for the Graduate School :

Dean of the Graduate School

ON SINGLE EQUATIONAL-AXIOM SYSTEMS FOR ABELIAN GROUPS

A Thesis

Submitted to the Graduate School

of

Tennessee State University

in

Partial fulfillment of the Requirements

for the Degree of

Master of Science

in Mathematical Sciences

Sonsauhray C. Price-Sampson
August 1995

421190

DEDICATION

This Project is dedicated to my loving mother Cynthia Price, my grandparents William and Margret Price, My uncle Bishop Joesph Price and my husband Steven D. Sampson, who have been my mainstay and support during my academic years and throughout my life. I thank them for everything they have given me; their love and support and hope they are proud of me as I am proud of them. I will also like to dedicate this project to my sister, I know she is will be successfull in completing college.

S.C.S.

ACKNOWLEDGMENT

I would like to thank Dr. M. Rajagopalan whose academic support and supervision made the completion of this project possible. I would like also to especially express my deepest gratitude to Dr. Scheick for all the academic and financial support she gave me. I would also like to express my appreciation to Dr. Richardson, Dr. Atkinson, and Dr. Dean for their help and support. This thesis was suported by a National Security Agency Grant with number MDA-904-93-H-2002.

S.C.S.

ON SINGLE EQUATIONAL-AXIOM SYSTEMS
FOR ABELIAN GROUPS

An Abstract

Submitted to the Graduate School

of

Tennessee State University

in

Partial fulfillment of the Requirements

for the degree of

Master of Science

in Mathematical Sciences

Sonsauhray C. Price-Sampson
August 1995

ABSTRACT

SONSAUHRAY C. PRICE-SAMPSON. On Single Equational-Axiom Systems for Abelian Groups (under the direction of **DR. M. RAJAGOPALAN).** It is a facinating problem in the axiomatics of any mathematical system to reduce the number of axioms, the number of variables used in each axiom, and the length of the various identities, to a minimum. In this thesis it is shown that a general Abelian group (G, +) can be defined as a set G with a binary operation '*' which satisfies only one equation of length 6. Six equations in '*' are given in this thesis each of which defines a general Abelian group. It is also shown that among all possible equations in '*' with length less that or equal to 6, these are the only equations that defines a general Abelian group.

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

Let G be a set with a binary operation '•' satisfying the conditions : -

1. $a \bullet (b \bullet c) = (a \bullet b) \bullet c \ \forall a,b,c \in G$

2. $\exists \ e \in G$ such that $e \bullet a = a \ \ \forall a \in G$

3. $a \bullet e = a \ \ \forall a \in G$

4. $\forall \ x \in G \ \exists \ x^{-1} \in$ such that G $x \bullet x^{-1} = e$

5. $\forall \ x \in G, \ x^{-1} \bullet x = e$

We say that a group G is an Abelian (or communitive) group if in addition we have $a \bullet b = b \bullet a \ \ \forall \ a,b \in G$. If a group G is Abelian we often denote the group operation by '+' instead '•'. To define an Abelian group we need six equations, and three operations, binary, unary, and o-ary. We define a binary operation. Given two elements a,b in G then multiply them together and we get some element c, this multiplication of two elements is a binary operation. So a binary operation in G is a function $f : G \times G \rightarrow G$. We define an unary operation. Given $x \in G$ we get $x^{-1} \in G$. If we multiply the two we will get e. Therefore an unary operation is the inverse of x. So here an unary operation in G is the function $f : G \rightarrow G$ given by $f(x) = x^{-1} \ \forall \ x \in G$. We define an o-ary operation. $\exists \ e \in G$ such that $e \bullet a = a \ \forall \ a \in G$. Now e exists in G. Interpret that you get e in G starting from nothing given in G. So a zero-ary operation is a function $f : \varnothing \rightarrow G$ which is an element of G.

In general given a set G and a cardinal number k, a k-ary operation in G can be defined as a function from G x G x G x........x G taken k-times into G. So using the language of operations and equation we can say that a group is a set G with 3 operations, one binary, one unary, and one o-ary satisfying 5 equations. An Abelian group can be thought of as a set G with 3 operations, one binary, one unary, and one o-ary satisfying 6 equations.

Now we ask :

"What is the least number of equations and operations needed to define a group?"

(ie. What is the minimum number of equations needed to get exactly all groups?)

If we take group operation only then we can not get the operation "inverse" from the group operation '•' only using the repetition of '•' any number of times. The reason is that, if we can derive "inverse" from group operation only then we should be able to write the number "-1" from the set Z^+ of integers ≥ 0 by using '+' only, but that is not possible since (Z^+, +) is not a group. However if we take an Abelian group (G, +) and write a * b = a - b ∀ a,b ∈ G, then we can recapture the operation '+' from the operation '*' as follows : a + b = a * ((a * a) * b). (which is the same as saying a + b = a - ((a - a) - b)). Then we can write a single equation in '*' so that the recaptured group operation '+' from '-' defined as a + b = a * ((a * a) * b) ∀ a,b ∈ G will make G an Abelian group. So we can define a general Abelian group as a set G with only one binary operation '*' satisfying only one equation. We also study the possible equations of the least length that will define a general Abelian group.

This statement can also be written in the language of variety as follows : "The variety of an Abelian group with one binary, one unary, and one o-ary operation, satisfies an axiom system of equations. It can also be written as a variety with only one operation satisfying only one equation."

CHAPTER 2

VARIETIES AND ALGEBRAIC SYSTEMS

DEFINITION 2.1

Let X be a set. An operation in X is defined to be a function $f : X^J \rightarrow X$ where J is a set. If J is empty we call f a nullary operation. If $|J| = 1$ we call f a unary operation in X. If $|J| = 2$ we call f a binary operation in X in general if $|J| = \alpha$ then f is called an α-ary operation in X.

NOTE 2.1

A o-ary operation in X chooses a fixed element of X.

DEFINITION 2.2

Let G be a set with a collection of operations. A monomial in G is a finite composite of finitely many operations in G. A monomial is also called a formula.

EXAMPLE 2.1

Let (G, *) be a group. Let us call the binary operation x * y as f(x,y). Let us call the unary operation x^{-1} as g(x). Let us call nullary operation as 'e'. Then the expression $(x\ y^{-1})\ x^2$ is a monomial in G. For$((x\ y^{-1})\ x^2 = f\,(f\,(x,\ g(y),\ f\,(x,x))$.

DEFINITION 2.3

Let X be a set. Let J also be a set. For every $\alpha \in J$ let there be a cardinal K_α and an α-ary operation in X. An equation in X is an expression of the form m = n where m,n are

DEFINITION 2.3

Let X be a set. Let J also be a set. For every $\alpha \in J$ let there be a cardinal K_α and an α-ary operation in X. An equation in X is an expression of the form m = n where m,n are monomials in X. An equation is also called a law or an identity.

EXAMPLE 2.2

Suppose that X is a set, with two binary operations '+' and '•' then $(x_1 + x_2) \bullet x_3 = (x_1 \bullet x_3) + (x_2 \bullet x_3)$ is an equation in X. $x_1 + x_2 \bullet x_3 = (x_1 + x_2) \bullet x_3$ is not in equation X, because on the left hand side the operations are not well defined.

DEFINITION 2.4

A variety is a set X with a finite collection of operations, satisfying a finite set of equations.

Examples of varieties :

1. Groups.
2. Abelian Groups.
3. Rings.
4. Communitive Rings.
5. Lattices.

DEFINITION 2.5

Let V be a variety. We say that V can be expressed as a single equation system if the following holds : -

For each G in V we can find an operation '*' in G and one equation 'S' in '*' so that we have the following : -

1. The operation '*' is obtained as a formula in G, with it's operations in V. That is, '*' is obtained as a composite of finitely many operations in V.
2. The equation 'S' for the operation '*' should be derivable from G, with it's operations and equations as a member of the variety V.
3. The operations in G as a member of V should be formulas in '*'.
4. The equations in V that G satisfies should be derivable from G with '*' and 'S'.

In the introduction we raised the question "Can an Abelian group be defined by a single operation and a single equation?" Since that is the theme of this chapter we explain below what we mean by "An Abelian group can be defined by a single operation and a single equation." We say that an Abelian group (G, +) can be defined by a single operation and a single equation if the following holds : -

For any Abelian group (G, +) an operation '$*_+$' can be defined on G, where the operation '$*_+$'

('$*_+$' depends on all the operations binary, unary, and nullary defined in (G,+)) is defined by a formula involving the operations in (G,+) so that we have :

1. All the operations '+' (Binary), '-' (Unary), and '0' (Nullary) in (G,+) can be expressed as formula in '$*_+$'.

2. (G,$*_+$) satisfies one equation S.

3. For every (G,$*_+$) satisfying S the associated (G,+) (which is obtained from '*' as in 1) is an Abelian group.

THEOREM 2.1

Let (G,+) be an Abelian group. Put $a * b = a - b = a + (-b)\ \forall\ a,b \in G$. Then '*' is a binary operation in (G,+) defined by using the binary operation '+' and unary operation '-' in (G,+).

We don't give the proof since the statement is clear.

THEOREM 2.2

Let (G,+) be an Abelian group. Let '*' be the associated binary operation in G defined in theorem 2.1. Then we have : -

1. $x * (z * (y * (x * z))) = y\ \forall\ x,y,z \in G$.
2. $(x *(z * y)) * (x * z) = y\ \forall\ x,y,z \in G$.
3. $(x * ((x * z) * y)) * z = y\ \forall\ x,y,z \in G$.
4. $(x * z) * ((x * y) * z) = y\ \forall\ x,y,z \in G$.

PROOF :

Using the fact that $(a * b) = a - b \; \forall \; a,b \in G$ we get $x * (z * (y * (x * z)) = x - (z - (y - (x - z)) = y$ which is 1. 2,3,4 follow likewise.

LEMMA 2.1

Let (G,+) be an Abelian group. Let '*' be the operation defined in theorem 2.1 as $a * b = a - b \; \forall \; a,b \in G$. Then we have : -

1. $a * a = 0$ where $a \in G$.

2. $a * ((a * a) * b) = a + b \; \forall \; a,b \in G$.

3. $(a * a) * a = -a \; \forall \; a \in G$.

Thus the binary operation '+', unary operation '-', and nullary operation '0' (identity of (G,+)) can be obtained as formulas from (G,*).

DEFINITION 2.6

Let (G,+) be a set G with a binary operation '*'. We put $a \bullet b = a * ((a * a) * b) \; \forall \; a,b \in G$. If $(G, \bullet)$ is an Abelian group then (G, *) is called an a•a•group (a•a•group stands for associated Abelian group).

<u>THEOREM 2.3 (PADMANABHAN [P])</u>

Let G be a set with a binary operation '*'. Then the following are equivalent : -

1. (G, *) is an a • a • group.
2. x * (z * (y * (x * z))) = y ∀ x,y,z ∈ G.
3. (x *(z * y)) * (x * z) = y ∀ x,y,z ∈ G.
4. (x * ((x * z) * y)) * z = y ∀ x,y,z ∈ G.
5. (x * z) * ((x * y) * z) = y ∀x,y,z ∈ G.

<u>PROOF:</u>

We prove that 1⇒ 2 .

Let x,y,z ∈ G

Now

x * (z * (y *(x * z)))

= x * (z * (y * (x - z))) (for a * b = a-b if (G, *) is an a • a • group).

= x * (z * (y- (x - z)))

= x * (z * (y - x + z))

= x * (z - (y - x + z))

= x * (z - y + x - z)

= x * (x - y)

= x - (x - y)

= y.

We prove that $2 \Rightarrow 3$.

PROOF:

Now by 2 we have $x * (z * (y * (x * z))) = y \; \forall \; x,y,z \in G$. Let $x,y,z \in G$ put $z = z * (y * x)$ and $y = y$ and $x = x$ in 2. We get

$$x * (z * (y * x)) * (y * (x * (z * (y * x)) = y \text{----------A.}$$

Note

$$y * (x * (z * (y * x) \; = z \text{ by equation 2.}$$

So equation A reads

$$x * (((z * (y * x))) * z) = y \text{-----------B.}$$

Note that x,y,z are arbitrary in equation B, so B can be written as

$$a * ((c * (b * a)) * c) \; = b \;\; \forall \; a,b,c \in G \text{----------C.}$$

Put $a = x * (z * y)$ and $b = y$ and $c = z$ in C. We get

$$((x *(z * y)) * ((z * (y * (x * (z * y)))) * z) = y \text{----------D.}$$

Now $(z * (y * (x * (z * y))) = x$ by 2. Therefore D becomes

$$(x * (z * y)) * (x * z) = y \text{ which is 3.}$$

Prove that $3 \Rightarrow 4$.

PROOF:

Notice that if we assume 3 then $(G, *)$ is left cancellative (ie. if $a,b,c \in G$ and $a * b = a * c$ then $b = c$). For let $a,b,c \in G$ and let $a * b = a * c$----------E. Choose some $d \in G$. Then $(d * (a * b) * (d * a)) = (d * (a * c)) * (d * a)$ by E. But $((d * (a * b)) * (d * a)) = b$ by 3. Similarly $(d * (a * c)) * (d * a) = c$, so E gives $b = c$. Therefore $(G, *)$ is left cancellative. So we have the equation

$$(a * (c * b)) * (a * c) = b \ \forall \ a,b,c \in G\text{----------}3$$

and the left cancellative law namely $a * b = a * c \Rightarrow b = c \ \forall \ a,b,c \in G$.

Let $d \in G$ put $a = c * (b * d)$ in 3. We get

$$((c * (b * d)) * (c * b)) * ((c * (b * d)) * c) = b.$$

Now by 3 we have $(c * (b * d)) * (c * b) = d$.

Therefore $d * ((c * (b * d)) * c) = b$----------F.

Therefore $d * ((a * (b * d)) * a) = d * ((c * (b * d)) * c$.

Therefore $(a * (b * d)) * a = c * (b * d)) * c \ \forall \ a,b,c,d \in G$----------H, by left cancellation of '*'. Now let $s \in G$. Put $a = b * (d * s)$ in H. We get

$$((b * (d * s)) * (b * d)) * (b * (d * s)) = (c * (b * d)) * c.$$

Using 3 we get

$$s * (b * (d * s)) = (c * (b * d)) * c \ \forall \ b,c,d,s \in G\text{----------I.}$$

Put $s = c * (b * d)$ in I. We get

$$(c * (b * d)) * (b * (d * (c * (b * d)))) = (c * (b * d)) * c \forall \ b,c,d \in G\text{----------J.}$$

By cancellative law '*' we get from J

$$b * (d * (c * (b * d))) = c \ \forall \ b,c,d \in G\text{----------K (which is equation 2).}$$

Replace $b = y$, $d = t$, and $c = x$ in K. We get

$$y * (t * (x * (y * t))) = x \ \forall \ x,y,t \in G\text{---------L (which is equation 2).}$$

Now let $r,z \in G$. Put $t = r * (z * (y * r))$ in L. We get

$y * t = z$ by 2. Furthur we have

$$y * ((r * (z * (y * r))) * (x * z)) = x.$$

Put $x = (y * y)$ in last equation. We get

$$y * ((r * (z * (y * r))) * ((y * y) * z)) = y * y.$$

So $(r * (z * (y * r))) * ((y * y) * z) = y$.

So $(r * (z * (y * r))) * ((z * z) * z) = y$.

Put $r = z * z$ in last equation. We get

$$((z * z) * (z * (y * (z * z)))) * ((z * z) * z) = y.$$

So using 3 we get y

$$y * (z * z) = y\text{----------O.}$$

So $x * (x * z) = (x * (z * z)) * (x * z) = z$ by 3. We get

$$x * (x * z) = z\text{----------P.}$$

Now using 3 we get

$$(x * ((x * z) * y)) * (x * (x * z)) = y.$$

So $(x * ((x * z) * y)) * z = y$ which is equation 4.

Now we prove that $4 \Rightarrow 5$.

So we assume that $(x * ((x * z) * y)) * z = y \ \forall \ x,y,z \in G$.

Put $z = (x * y) * t$ in 4 where $t \in G$. We get

$$(x * ((x * ((x * y) * t)) * y)) * ((x * y) * t) = y.$$

Using 4 we get

$$(x * t)) * ((x * y) * t) = y \text{ which is equation 5.}$$

Now we prove that $5 \Rightarrow (G, *)$ is an a•a •group.

So we assume that

$$(x * z) * ((x * y) * z) = y \ \forall \ x,y,z \in G\text{----------}5.$$

Put $z = x * y$ in 5 we get

$$(x * (x * y)) * ((x * y) * (x * y)) = y\text{---------}A_1.$$

Replace x by $x * y$ in A_1. We get

$$((x * y) * ((x * y) * y)) * (((x * y) * y) * ((x * y) * y)) = y.$$

Using 5 we get

$$y * (((x * y) * y) * ((x * y) * y)) = y\text{----------}A_2.$$

Put $((x * y) * y) * ((x * y) * y) = e(y,x)$----------$A_3$. We get

$$y * e(y,x) = y\text{----------}A_4.$$

Now put $y = e(x,y)$ and $z = e(x,y)$ in 5. We get

$$(x * e(x,y)) * ((x * e(x,y)) * e(x,y)) = e(x,y).$$

So using A_4 we get

$$x * x = e(x,y) \text{----------} A_5.$$

So e(x,y) is independant of 'y'. So we will write $e(x,y) = e(x)$-----------A_6.

So A_4 gives that $y * e(y) = y$----------A_7.

Now

$$\begin{aligned} x * x &= e(x,y) \text{ (from } A_5) \\ &= ((y * x) * x) * ((y * x) * x) \text{ (from } A_3) \\ &= ((y * x) * x) * ((y * x) * e(y * x)) * x) \text{ (from } A_7) \\ &= e(y * x) \text{ from } 5 \\ &= (y * x) * (y * x) \text{ (from } A_6 \text{ and } A_5) \\ &= (y * x) * ((y * e(y)) * x) \text{ (from } A_7) \\ &= e(y) \text{ from } 5. \end{aligned}$$

So $x * x = e(y) = y * y$----------A_8.

So e(x) does not depend on x.

So e(x) is a constant.

We put $e(x) = e$----------A_9, so we get

$$y * e = y \text{----------} A_{10} \text{ (from } A_7 \text{ and } A_9)$$

And

$$x * x = e \text{----------} A_{11} \text{ (from } A_8).$$

Put z = e in 5. We get

$$(x * e) * ((x * y) * e) = y \text{------------} A_{12}.$$

Using A_{10}. We get

$$x * (x * y) = y \text{--------------} A_{13}.$$

Put x * y for y in 5. We get

$$(x * z) * ((x * (x * y)) * z) = x * y \text{----------} A_{14}.$$

Using A_{13} . We get

$$(x * z) * (y * z) = x * y \text{----------} A_{15}.$$

Now we give our own proof of the fact that $5 \Rightarrow 1$ which is new. We go through the following steps.

Now in A_{15} put $z = x$. We get

$$(x * x) * (y * x) = x * y.$$

So

$$e * (y * x) = x * y \text{----------} A_{16} \text{ (from } A_8).$$

Putting $y = e$ we get from A_{16} that

$$e * (e * x) = x * e = x \text{----------} A_{17}.$$

Now recall that the associated group operation '•' in G is defined by

$$x \bullet y = x * ((y * y) * y) \ \forall\ x,y \in G \text{----------} A_{18}.$$

So we have that

$$\begin{aligned} x \bullet e &= x * ((e * e) * e) \\ &= x * (e * e) \text{ (from } A_{11}) \\ &= x * e \\ &= x \text{ (from } A_{10}). \end{aligned}$$

Similarly

$$\begin{aligned} e \bullet x &= e * ((x * x) * x) \\ &= e * (e * x) \text{ (from } A_{11}) \\ &= x * e \text{ (from } A_{16}) \\ &= x \text{ (from } A_{10}). \end{aligned}$$

So

$$x \bullet e = e \bullet x = x \ \forall\ x \in G \text{----------} A_{19}.$$

Clearly $x \bullet y \in G \ \forall\ x,y \in G$----------$A_{20}$.

If $x \in G$ then put $x^{-1} = e * x$----------A_{21}.

Then

$$\begin{aligned} x \bullet x^{-1} &= x * ((x^{-1} * x^{-1}) * x^{-1}) \\ &= x * (e * x^{-1}) \text{ (from } A_{11}) \\ &= x * (e * (e * x)) \text{ (from } A_{21}) \\ &= x * (x * e) \text{ (from } A_{16}) \\ &= x * x \text{ (from } A_{10}) \\ &= e \text{ (from } A_{11}). \end{aligned}$$

So

$$x \bullet x^{-1} = e \ \ \forall\ x \in G\text{-----------}A_{22}$$

Now

$$\begin{aligned} (x^{-1})^{-1} &= e * x^{-1} \text{ (from } A_{21}) \\ &= e * (e * x) \text{ (from } A_{21}) \\ &= x \text{ (from } A_{13}). \end{aligned}$$

So

$$\begin{aligned} x^{-1} \bullet x &= x^{-1} \bullet (x^{-1})^{-1} \\ &= e \text{ (from } A_{22}). \end{aligned}$$

So

$$x \bullet x^{-1} = x^{-1} \bullet x = e \ \ \forall\ x \in G\text{-----------}A_{23}.$$

Now we have that

if $x,y,z \in G$ and $x * y = z * z$ then $y = z$.

For if $(x * y) = x * z$ then $x * (x * y) = x * (x * z)$

Hence $y = z$ (from A_{13}).

So

$$\text{"}x * y = x * z\text{"} \Rightarrow \text{"}y = z\text{"-----------}A_{26}.$$

Now let x,y,z $\in$ G.

Let y * x = z * x.

Then

$$e * (x * y) = e * (x * z) \text{ (from } A_{16}).$$

So

$$x * y = x * z \text{ so } y = z \text{ (from } A_{26}).$$

So

$$\text{"}y * x = z * x\text{"} \Rightarrow \text{"}y = z\text{"----------}A_{25}.$$

Now let x,y,z $\in$ G.

Then (x * z) * ((x * y) * z) = y (from 5).

We also have (x * z) * ((x * z) * y) = y (from A_{13}).

So

$$(x * z) * ((x * y) * z) = (x * z) * ((x * z) * y).$$

So

$$(x * y) * z = (x * z) * y \ \forall\ x,y,z \in G \text{ (from } A_{24}).$$

Thus we have

$$(x * y) * z = (x * z) * y\text{----------}A_{27}.$$

Now let x,y $\in$ G.

Then

$$\begin{aligned} x \bullet y &= x * (e * y) \\ &= e * ((e * y) * x) \text{ (from } A_{16}) \\ &= e * ((e * x) * y) \text{ (from } A_{27}) \\ &= y * (e * x) \text{ (from } A_{16}) \\ &= y \bullet x \text{ (from definition of '}\bullet\text{').} \end{aligned}$$

So

$$x \bullet y = y \bullet x \text{----------} A_{28}.$$

Now let $x, y, z \in G$.

Then

$$\begin{aligned}(x * y) * (x * z) &= (x * (x * z)) * y \text{ (from } A_{27}) \\ &= z * y \text{ (from } A_{13}).\end{aligned}$$

So

$$(x * y) * (x * z) = z * y \ \forall \ x, y, z \in G \text{----------} A_{29}.$$

Now let $x, y, z \in G$.

Then

$$\begin{aligned}x \bullet (y \bullet z) &= x * (e * (y \bullet z)) \text{ (from definition of '} \bullet \text{')} \\ &= x * (e * (y * (e * z))) \\ &= x * (e * z) * y)) \text{ (from } A_{16}) \\ &= ((e * z) * ((e * z) * x)) * ((e * z) * y) \text{ (from } A_{13}).\end{aligned}$$

So

$$\begin{aligned}x \bullet (y \bullet z) &= ((e * z) * ((e * z) * x)) * ((e * z) * y) \\ &= y * ((e * z) * x) \text{ (from } A_{29}).\end{aligned}$$

So

$$x \bullet (y \bullet z) = y * ((e * z) * x)) \text{----------} A_{30}.$$

Now

$$\begin{aligned}(x \bullet y) \bullet z &= (x * (e * y)) \bullet z \\ &= (x * (e * y)) * (e * z) \\ &= (((e * z) * ((e * z) * x)) * (e * y)) * (e * z) \text{ (from } A_{13}) \\ &= (((e * z) * ((e * z) * x)) * (e * z)) * (e * y) \text{ (from } A_{27}) \\ &= (((e * z) * ((e * z) * x) * ((e * z) * e)) * (e * y) \text{ (from } A_{10}) \\ &= (e * ((e * z) * x)) * (e * y) \text{ (from } A_{29}) \\ &= y * ((e * z) * x)) \text{ (from } A_{27}).\end{aligned}$$

So

$$(x\bullet\ y)\bullet\ z = y * ((e * z) * x)\text{----------}A_{31}.$$

So from A_{30} and A_{31} we get

$$x\bullet\ (y\bullet\ z) = (x\bullet\ y)\bullet\ z\text{----------}A_{32}.$$

So we get from A_{11}, A_{21}, A_{23}, A_{19}, A_{32}, A_{28} and A_{18} that (G, •) is an Abelian group. Thus we have proved that 5 ⇒ (G, *) is an a • a • group.

Hence we have proved theorem 2.3.

The equations A_1 to A_{32} are new and to our knowledge are not found in any previous publication. Thus we supply in part, our own proof of Padmanabhan's Theorem (see [P]) which is theorem 2.3.

<u>THEOREM 2.4 (Sholander) [Sh]: -</u>

Let G be a set with a binary operation ' *'. Then (G, *) is an a • a • group if and only if we have $x * ((x * z) * (y * z)) = y \ \forall\ x,y,z \in G$.

<u>PROOF : -</u>

Let (G, *) be an a• a • group then a * b = a - b in the associtated group theoritic language. So $x * ((x * z) * (y * z)) = x - ((x - z) - (y - z)) = y \ \forall\ x,y,z \in G$. Conversely, suppose that $x * ((x * z) * (y * z)) = y \ \forall\ x,y,z \in G$. Then we notice that given $x,y \in G$ there is an element $u \in G$ so that $x * u \in G$. For, we have to only put $u = ((x * z) * (y * x))$ and use the given equation $x * ((x * z) * (y * z)) = y \ \forall\ x,y,z \in G$.

Let us put

$$x * ((x * z) * (y * z)) = y \text{ as equation S.}$$

Then we have

$$(x * ((x * z) * (y * z)) * z = y * z\text{----------}S_1.$$

Put $u = y * z$ in S_1. We get

$$(x * ((x * z) * u)) * z = u \ \forall \ x,y,z \in G\text{----------}S_2.$$

But S_2 is same as equation 4 of Theorem 2.3. So by theorem 2.3 we get that (G, *) is an a • a •group.

THEOREM 2.5

Let (G, *) be a set G with a binary operation '*'. Then (G, *) is an a• a• group if and only if $x * ((z * y) * (z * x)) = y \ \forall \ x,y,z \in G$.

PROOF : -

Let (G, *) be an a• a• group. Then $a * b = a - b$ in the associated group theoretic language for all $a,b \in G$. So $x * ((z * y) * (z * x)) = x - ((z - y) - (z - x)) = y \ \forall \ x,y,z \in G$. Conversely let $x * ((z * y) * (z * x)) = y \ \forall \ x,y,z \in G$. We put the equation $x * ((z * y) * (z * x)) = y$ as (H-N). Now suppose that $a,s,t \in G$ and $a * s = a * t$.

Then we have that

$$a * ((a * s) * (a * a)) = s\text{----------}(H\text{-}N_1) \text{ (by using H-N).}$$

Similarly we have

$$a * ((a * t) * (a * a)) = t\text{----------}(H\text{-}N_2).$$

So s = t since a * s = a * t. So '*' is left cancellative. Futhur, we see that if x,y ∈ G are given then putting u = (x * y) * (x * x) and using (H-N), that x * u = y.

Now let x,y,z ∈ G. then we have

x * ((z * y) *(z * x)) = y----------(H-N).

So

z * (x * ((z * y) * (z * x))) = z * y----------(H-N_3).

Put z * y = u. then

z * (x * (u * (z * x))) = u----------(H-N_4).

This is same as equation 2 of theorem 2.3. So (G,*) is an a • a • group by theorem 2.3.

NOTE 2.1

Sholander [Sh] proved theorem 2.4. G. Higman and B.H. Neumann [H-N] proved theorem 2.5. We did not access their papers. Our proof for theorems 2.4 and 2.5 based on Padmanabhan's theorem 2.3 is new. The proof of the part that 5 ⇒ 1 in Padmanabhan's theorem 2.3 is also new. Padmanabhan used theorem 2.4 of Sholander to show that 5 ⇒ 1 in theorem 2.3. The proof given here for that part of theorem 2.3 is fairly elementary and self contained and does not use Sholander's theorem 2.4.

NOTE 2.2

In the theorems 2.1, 2.2, and 2.3 the operation '*' in (G, *) was defined from the operations of group (G, +) as a * b = a - b ∀ a,b ∈ G. But we can define many binary operations in G starting from a group (G, +). For example we can put a * b = b - a ∀ a, b ∈ G. Now we can ask, if we are given a binary operation '$*_2$ ' in G using '+' and '-' in G then whether we can find a single equation S in $*_2$ so that (G, $*_2$) with equation S will define a general Abelian group similar to the case of (G, *) as in theorem 2.1, or theorem 2.2, or theorem 2.3.

More generally we can ask the question "What are all the binary operations # that can be defined in G as formulas in the operations of a general Abelian group (G, +) so that a single equation in (G, #) will define a general Abelian group as was the case of (G, *) in theorem 2.1. So the following deep theorem of B.H. Neumann is significant (See B.H. Neumann topics in algebra, universal algebra 1962).

THEOREM 2.6 (B.H. Neumann)

Let (G, +) be a general Abelian group. Let # be a binary operation in G defined as a formula using the operations in the Abelian group (G, +). Suppose that there is a single equation S in (G, #) so that (G, #) with S defines a general Abelian group canonically. (that is the operation of (G, +) are formulas in (G, #)) and (G, +) is an Abelian group). Then a # b = a - b ∀ a,b ∈ G or a # b = b - a ∀ a,b ∈ G.

We do not give here the proof of this theorem.

NOTE 2.3 : -

Earlier we saw that if (G, +) is a general Abelian group and '*' is the binary operation defined in theorem 2.4 as a formula in the operations of (G, +) then a single equation S in '*' defines (G, +). Theorems 2.1, 2.2, and 2.3 together give 6 such equations in '*' each of which defines the operation of (G, +) as formulas in '*' and (G, +) so defined is an Abelian group. We can ask the following questions.

QUESTION 1

Let (G, +) be any Abelian group and '*' a binary operation in G defined as a formula in (G, +). Suppose that '*' defines all the operations of the group (G, +) as formulas in '*'. Then what are all the equations S in (G, *) so that if (G, *) satisfies S then the associated (G, +) is an Abelian group?

QUESTION 2

Let (G, +) be a general Abelian group. Let '*' be a formula in (G, +) as in question 1. What are all the equations S in the binary operation '*' defined on the set G so that S is in some sense the shortest equation in '*' and the associated (G, +) as in question 1 is an Abelian group?

We answer question 2 in the next chapter completely. We make the meaning of question 2 more precise and prove that the six equations of theorems 2.1, 2.2, and 2.3 are the only shortest equations in (G, *) that define a general Abelian group.

CHAPTER 3

THE EQUATIONS IN '*' THAT MAKES THE ASSOCIATED (G, +) AN ABELIAN GROUP.

DEFINITION 3.1

Let '*' be a binary operation in a set G. Let $f(x_1,x_2 .... x_n)$ be a monomial or a formula in (G, *) in the variables $x_1,x_2,.........,x_n$. We call the formula f as a word in $x_1,x_2,.........,x_n$ in (G, *).

DEFINITION 3.2

Let (G, +) be an Abelian group. Let '*' be a binary operation in G defined as $x * y = x - y$ $\forall$ $x,y \in G$, where '-' is the inverse in G. We call (G, *) as having been defined canonically by (G, +). We say that (G, +) is defined canonically by (G, *) if all the operations of the Abelian group (G, +) are words in (G, *) and the (G, +) so obtained from (G, *) is an Abelian group and '*' coincides with the binary operation '#', defined canonically by the group (G, +) obtained from (G, *).

DEFINITION 3.3

Let (G, *) be a set G with a binary operation '*'. Let $f(x_1,x_2,.........,x_n)$ be a word in (G, *) in the variables $x_1,x_2,........,x_n$. Then the length of the word f is the total number of times the variables $x_1,x_2,........,x_n$ appear in f.

EXAMPLE 3.4

Let (G, *) be a set with a binary operation '*'. Then the word $(x_1 * x_2) * x_1$ is a word in x_1,x_2 but of length 3 since the total number of occurrences of the variables x_1,x_2 in that word is 3.

DEFINITION 3.5

Let (G, *) be a group in the binary operation '*'. Let 'w' be a word in (G, *) in the variables $x_1,x_2,\ldots\ldots,x_n$. Then the sum of the powers of all the variables in w is called it's degree.

EXAMPLE 3.6

Let (G, *) be a group. Let w be the word $x_1 * x^{-1}_2 * x_1$ in G in the variables x_1,x_2. Then it's degree is 1 + (- 1) + 1 = 1. The degree of $x_1^2 * x^{-3}_2 * x_1$ is 0.

DEFINITION 3.7

Let (G, *) be a set G with a binary operation '*'. An equation in (G, *) or an identity in (G, *) or a law in (G, *) is an equation of the form m = n where m,n are words in some variables $x_1,x_2,\ldots\ldots,x_n$ of G.

EXAMPLE 3.8

Let (G, *) be a set with a binary operation '*'. Then $(x_1 * x_2) * x_1 = x_3$ is an equation in the variables x_1, x_2, x_3 in (G, *). Notice that we do not demand the occurrence of every variable in both sides. Similarly $x_1 * (x_2 * x_1) = x_3$ is also and equation or identity or law in (G, *) in the variables x_1, x_2, x_3. However $x_1 * x_2 * x_1 = x_3$ is not an equation in (G, *) since without brackets the left hand side is not well defined and hence is not a word in (G, *).

DEFINITION 3.9

Let (G, *) be a set G with a binary operation '*'. Let m = n be an equation in G. Then the length of this equation is (length of m) + (length of n).

DEFINITION 3.10

Let (G, *) be a set G with a binary operation '*'. Let S be an equation in '*'. The triple (G, *, S) is called a single equational system. It is said to define a general Abelian group if the following hold : -

1. There exist formulas f_1, f_2 in (G, *) so that f_1 is a binary operation, f_2 is an unary operation in G. We put $f_1(x,y) = x + y \ \forall x,y \in G$.

2. (G, +) is an Abelian group with $f_1(x)$ as inverse of x $\forall x \in G$.

3. The operation '*' coincides with taking difference in (G,). That is $a * b = a - b \ \forall a,b \in G$. Thus the law S should be satisfied in every Abelian group G where '*' is taken as '-'.

4. For every Abelian group (H, +) the equation S is satisfied in (H, *) if we interpret $a * b = a - b \quad \forall a,b \in G$.

We say some times that S defines a general Abelian group if we know (G,*).

We give some single equation systems which do not define a general Abelian group.

EXAMPLE 3.11

The equation $x_1 = x_2$ in set G with a binary operation '*' does not define a general Abelian group. For if we start with any Abelian group (G, +) and take '*' as '-' then the equation $x_1 = x_2$ is not true $\forall x_1, x_2 \in G$ unless G is a singleton.

EXAMPLE 3.12

The equation $x * x = x$ in (G, *) does not define a general Abelian group where (G, *) is as in example 3.11. For we do not have $x - x = x$ for all x in every group G.

EXAMPLE 3.13

The equation x * x = y * y in (G, *) does not define a general Abelian group where (G, *) is as in example 3.11. For take an infinite set G with the operation '*' defined as x * y = a ∀ x,y ∈ G. Where 'a' is a fixed element of G. Clearly it is not possible to find a group operation '+' in G so that x - y = a ∀ x,y∈ G. Hence (G, *, S) can not define a general Abelian group.

NOTE 3.14

The single equational systems (G, *, S) defines a general Abelian group where S is one of the equations in theorem 2.1 or theorem 2.2 or theorem 2.3.

THEOREM 3.15

Let (G, *, S) be a single equational system that defines a general Abelian group. Let the equation S be $f(x_1,x_2,....x_n) = g(x_1,x_2,....x_n)$ where f,g are words in the variables $x_1,x_2,....x_n$. Then either $f(x_1,x_2,....x_n) = x_i$ for some i = 1,2,........,n or $g(x_1,x_2,..,x_i ...x_n) = x_i$ for some i = 1,2,......,n. In other words both the sides of the equation f = g can not have length strictly greater than 1.

PROOF : -

Suppose that both sides of the equation $f = g$ have length at least 2. Take an infinite set X. Fix some element 'a' in X. Put $x * y = a \ \forall \ x,y \in X$. Then (X, *) satisfies equation S. But clearly the '*' for this X cannot be the operation '-' in some Abelian group operation '+' on X. Hence the theorem.

THEOREM 3.16

Let (G, *, S) be a single equational system that defines a general Abelian group. Let 'S' be of the form $f(x_1,x_2,\ldots\ldots x_n) = x_i$ for some $i = 1,2,\ldots\ldots\ldots,n$. Then f cannot be independant of x_i . That is x_i should be present in the monomial f.

PROOF : -

Suppose 'x_i' is not present in f. Take an infinite Abelian group G. Fix some element a in G. Put $x_1 = a_1$, $x_2 = a_2$, $x_{i-1} = a_{i-1}$, $x_{i+1} = a_{i+1}$ ....$x_n = a_n$ and x_i arbitrary in the equation $f(x_1,x_2,\ldots\ldots\ldots,x_n) = x_i$. We get $f(a_1,a_2,\ldots\ldots a_n) = x_i$. So x_i is a constant where $x_i \in$ G. That is G is a singleton which is not the case. So x_i should occur in G.

THEOREM 3.17

Let (G, *, S) be a single equational system which defines a general Abelian group. Let S be of the form $f(x_1,x_2,.....x_n) = x_i$ where f is a word in variables $x_1,x_2,.....x_n$ and i = 1,2,.......,n. Then x_i cannot be either the first or last variable in f.

PROOF : -

Suppose that x_i is first variable of f. Take an infinite set G with a binary operation * defined by $x * y = x \ \forall\ x,y \in G$. Then the equation $f(x_1,x_2,.....x_n) = x_i$ is satisfied in (G, *). But we cannot have an Abelian group structure '+' on G so that when '*' is interpreted as '-' of G then $x - y = x \ \forall\ x,y \in G$. so $f(x_1,x_2,.....x_n) = x_i$ cannot define a general Abelian group. The same kind of argument applies to the case when x_i is last variable in f.

THEOREM 3.18

Let (G, *) be a set G with a binary operation '*'. Let f be a monomial in an even number of variables $x_1,x_2,.....x_{n^n}$. Then the equation $f(x_1,x_2,.....x_{n^n}) = x_i$ cannot define a general Abelian group where $1 \leq i \leq 2k$. Similarly if g is a monomial in $x_1,x_2,.....x_n$ and degree of $g \neq 1$ then "$g = x_i$" cannot define a general Abelian group for any i = 1,2,.......,n.

TENNESSEE STATE UNIVERSITY
LIBRARY

PROOF : -

Suppose that $f(x_1,x_2,.....x_{2n}) = x_i$ defines a general Abelian group where $1 \leq i \leq n$. Then the degree of f is even. But degree of x_i is 1. So $f(x_1x_2,.....x_{2n}) = x_i$ cannot define a general Abelian group. The statement on g is proved similarly.

THEOREM 3.19

Let (G, *) be a set with a binary operation '*'. Let $f(x_1,x_2,......,x_n) = x_i$ define a general Abelian group where f is a word in (G, *) and $1 \leq i \leq n$. Then f cannot be of length one or two or three.

PROOF : -

Suppose that f is of length 1. Then f can contain only one variable. Let us call it x_1. then $f(x_1) = x_1$ since x_1 is the only monomial in x_1 of length 1. So the equation $f(x_1,x_2,........,x_n) = x_1$ becomes $x_1 = x_1$ in this case. Obviously (G, *) with the equation $x_1 = x_1$ cannot define a general Abelian group as is seen by taking the set N of natural integers {1,2,.....n....} with usual addition as the operation '*'.

Suppose that f is of length 2. Then f cannot have more than 2 variables in it. Since f is also a monomial we have that either

1. $f = x_1 * x_2$ or 2. $f = x_2 * x_1$

suppose that $f = x_1 * x_{.2}$ Then the equation $f = x_1$ (with $i = 1$ or 2) is either

1a. $x_1 + x_2 = x_1$ or 1b. $x_1 + x_2 = x_2$

neither 1a nor 1b can define as a general Abelian group by theorem 3.17 (or we can use theorem 3.18 also). Similarly 1b also cannot define a general Abelian group.

Now suppose that f has length 3.

Then f cannot have more that 3 variables in it. Let us write down all the possible words of length 3 in (G, *) which contain 3 variables. We have that the only possible such f's are (except for a permutation): -

I. $f = (x_1 * x_2) * x_3$

II. $f = x_1 * (x_2 * x_3)$

Notice that other formulas for f obtained from I and II by permuting x_1, x_2, x_3 do not give any essentially new cases for f to discuss. In case I the equation $f = x_i$ is possible only for $i = 1,2,3$. So in case I we can have only the following 3 equations for $f = x_i$ namely : -

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

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

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

Now we can argue in different ways why none of the equations Ia, Ib and Ic above can define a general Abelian group. We give below some of those different arguments because they will be used again and again to discuss possible equations $f = x_i$ with f having length greater than 3.

ARGUMENT 1

We calculate the degree of $(x_1 * x_2) * x_3$ which is f. So we should write $(x_1 * x_2) * x_3$ in group theoretic terms and calculate the degree of the monomial we get in group theoretic language corresponding to $(x_1 * x_2) * x_3$. To avoid confusion in the calculation of degree it is better to think $a * b = ab^{-1}$ instead of $a * b = a - b$. So $(x_1 * x_2) * x_3$ becomes $(x_1 x^{-1}_2) x^{-1}_3$ in group theoretic language. So it's degree, which is the sum of the exponents, is '-1'. so theorem 3.18 gives that none of the equations Ia, Ib, Ic can define a general Abelian group.

ARGUMENT 2 (Reducing variables in f)

Neither equation Ia or equation Ic can define a general Abelian group by theorem 3.17. so we discuss the equation Ib only. Assume that the equation Ib defines a general Abelian group. Then Ib should be true in all Abelian groups when we write a - b for a * b $\forall$ a,b $\in$ G. Now Ib becomes $(x_1 - x_2) - x_3 = x_2$ in group theoretic language. We have the freedom to make some pairs of the variables x_1, x_2, x_3, equal. So if we want $(x_1 - x_2) - x_3 = x_2$ in an Abelian group for all x_1, x_3, and x_2 then x_1 must be equal to x_3. But then the equation $(x_1 - x_2) - x_3 = x_2$ reduces to the equation $-x_2 = x_2$. (notice we have removed x_1, x_3, from f). Clearly $-x_2$ cannot be equal to x_2 for all x_2 in a general Abelian group. So Ib also cannot define a general Abelian group.

We come to the other case II namely $f = x_1 * (x_2 * x_3)$. As we did in case I and following the, steps in this case also we show that II cannot give an equation in (G, *) that defines a general Abelian group.

STEP I

Lis all possible equations $f = x_i$ where $f = x_1 * (x_2 * x_3)$ as in case II. At this step we get that the only possible equations for $f = x_i$ are the following : -

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

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

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

STEP II

(This consists of the following : - Take one equation at a time. Apply theorem 3.17 or theorem 3.18 to possibly eliminate it. If they do not help, then go to the group theoretic form of that equation and reduce the number of variables by making some pairs of variables equal and decide). Now IIa and IIc cannot define a general Abelian group by theorem 3.17. Now IIb becomes $x_1 - (x_2 - x_3) = x_2$ in group theoretic terms. This cannot be true for all x_1, x_2, x_3 in all Abelian groups unless $x_1 = x_2 = x_3$. But then the equation IIb reduces to $x_1 = x_1$ which cannot define a general Abelian group. (we saw earlier, a proof of this fact). So in case II also we see that none of the equations $f = x_i$ can define a general Abelian group.

REMARK 3.20

We want to discuss whether any of the equations of the form $f = x_i$ in (G, *) can define a general Abelian group with f having length 4 or 5. We follow the same pattern of discussion in these cases as we did the theorem 3.19 for the cases when f has length 1,2, or 3. Note that the proof of theorem 3.19 started with giving all the possible formulas for f in case the length of f is 1,2 or 3. We do the same for the discussing the equation $f = x_i$ with length of f being 4 or 5. So we prove the following theorem.

THEOREM 3.21

Let (G, *) be a set with a binary operation '*'. Let f be a monomial in (G, *) of length 4. Let g be a monomial in (G, *) of length 5. Then f has to be one of the following F - 1 to F - 5 below and g has to be one of G - 1 to G - 14, upto a permutation of the variables.

$f = ((x_1 * x_2) * x_3) * x_4$----------F - 1

$f = (x_1 * x_2) * (x_3 * x_4)$----------F - 2

$f = (x_1 * (x_2 * x_3)) * x_4$----------F - 3

$f = x_1 * ((x_2 * x_3) * x_4)$----------F - 4

$f = x_1 * (x_2 * (x_3 * x_4))$----------F - 5

$$g = (((x_1 * x_2) * x_3) * x_4) * x_5 \text{----------} G - 1$$

$$g = ((x_1 * x_2) * x_3) * (x_4 * x_5) \text{----------} G - 2$$

$$g = ((x_1 * x_2) * (x_3 * x_4)) * x_5 \text{----------} G - 3$$

$$g = (x_1 * x_2) * ((x_3 * x_4) * x_5) \text{----------} G - 4$$

$$g = (x_1 * x_2) * (x_3 * (x_4 * x_5)) \text{----------} G - 5$$

$$g = ((x_1 * (x_2 * x_3)) * x_4) * x_5 \text{----------} G - 6$$

$$g = (x_1 * (x_2 * x_3)) * (x_4 * x_5) \text{----------} G - 7$$

$$g = (x_1 * ((x_2 * x_3) * x_4)) * x_5 \text{----------} G - 8$$

$$g = x_1 * ((x_2 * x_3) * x_4)) * x_5) \text{----------} G - 9$$

$$g = x_1 * ((x_2 * x_3) * (x_4 * x_5)) \text{----------} G - 10$$

$$g = (x_1 * (x_2 * (x_3 * x_4))) * x_5 \text{----------} G - 11$$

$$g = x_1 * ((x_2 * (x_3 * x_4)) * x_5) \text{----------} G - 12$$

$$g = x_1 * (x_2 * ((x_3 * x_4))* x_5)) \text{----------} G - 13$$

$$g = x_1 * (x_2 * (x_3 * (x_4 * x_5))) \text{----------} G - 14$$

<u>PROOF : -</u>

The proof is given by a complete exhaustion method of all possible parenthesis schemes using the given variables to get the possible formulas.

THEOREM 3.22

Let (G, *) be a set G with a binary operation '*'. Let f be a nominal of length 4 in (G, *). Then no equation of the form $f(x_1,x_2,x_3,x_4) = x_i$ can define a general Abelian group where i = 1,2,3,4.

PROOF : -

Take an equation of the form $f(x_1,x_2,x_3,x_4) = x_i$ where f is of length 4 and i = 1,2,3,4. Then f is one of F - 1 to F - 5 of theorem 3.21. Now the degree of each of the F - 1 to F - 5 is -2 or 0 or 2. So, an application of theorem 3.18 shows that none of the equations of the form $f(x_1,x_2,x_3,x_4) = x_i$ with i = 1,2,3,4 and f having length 4 can define a general Abelian group.

REMARK 3.23 : -

Now we discuss the question of which equations of the form $f = x_i$ in (G, *) can define a general Abelian group when (G, *) is as in theorem 3.22 where f is a word of length 5 in '*'.

NOTATION 3.24

Let (G, *) be as in theorem 3.22. We put P-1, P-2, P-3, P-4, Sh and HN as follows : -

$$x * (z * (y * (x * z))) = y \ \forall \ x,y,z \in G \text{----------P-1}$$

$$(x * (z * y)) * (x * z) = y \ \forall \ x,y,z \in G \text{----------P-2}$$

$$(x * ((x * z) * y)) * z = y \ \forall \ x,y,z \in G \text{----------P-3}$$

$$(x * z) * ((x * y) * z) = y \ \forall \ x,y,z \in G \text{----------P-4}$$

$$x * ((x * z) * (y * z)) = y \ \forall \ x,y,z \in G \text{----------Sh}$$

$$x * ((z * y) * (z * x)) = y \ \forall \ x,y,z \in G \text{----------HN}$$

NOTE 3.25

Let (G, *) be a set G with a binary operation '*'. Then there is no equation of the form $f(x_1,x_2,\ldots\ldots.,x_n) = x_i$ where f is a monomial of length strickly less than five and which defines a general Abelian group. This was shown in theorem 3.22 and theorem 3.19, we also saw that Padmanabhan [P], Sholander [Sh] and Higman-Neumann [HN] showed that each of the equations P-1, P-2, P-3, P-4, Sh and HN defines a general Abelian group and the left hand side of each of the above equations is a word in (G, *) of length equal to 5. Now we are going to show that P-1, P-2, P-3, P-4, Sh and HN are the only equations in (G, *) of the form $f(x_1,x_2,\ldots\ldots.,x_n) = x_i$ which define a general Abelian group and also such that f is a word in (G, *) of length 5. We prove two theorems before we give the final theorem on finding all equations of the form $f = x_i$ with f having length 5 and also defining a general Abelian group.

THEOREM 3.26

Let (G, *) be a set with a binary operation '*'. Let f be a word in (G, *) in the variables $x_1, x_2, \ldots\ldots, x_n$. Let 'i' be an integer so that $f = x_i$ defines a general Abelian group $1 \leq i \leq n$. Then there exist two variables besides x_i which do not occur as y * y in f. In other words if variables except x_i and one more variable occur only as y * y in f then $f = x_i$ cannot define a general Abelian group.

PROOF : -

Suppose that $f = x_i$ defines a general Abelian group. Furthur assume that all variables 'y' other that x_i and one more variable, say x_2, occur only as y * y in f. Without loss of generality we can take $x_i = x_1$. So f is of the form $f(x_1, x_2, x_3 * x_3, \ldots, x_n * x_n)$. Note that y * y = x * x for all x,y in G because f defines a general Abelian group. Now take the system Σ_2 of equations

(i). $f(x_1, x_2, x_2 * x_2, x_2 * x_2, \ldots\ldots, x_2 * x_2) = x_1$

(ii). $x * x = y * y$

In (G, *). Then Σ_2 is logically equivalent to the single equation $f = x_i$. But each equation in Σ_2 has no more than 2 variables. This is not possible which is a result of Mckinsey and Diamond[M-D]. So we have theorem 3.26.

THEOREM 3.27

Let (G, *) be as in theorem 3.26. Let i be an integer and $1 \leq i \leq 5$. Let $f(x_1,x_2,x_3,x_4,x_5) = x_1 * ((x_2 * (x_3 * x_4)) * x_5)$. Then $f = x_i$ cannot define a general Abelian group.

PROOF : -

Suppose that the equation $x_1 * ((x_2 * (x_3 * x_4)) * x_5) = x_i$ defines a general Abelian group for some i = 1,2,3,4,5. Now the group theoretic form of $x_1 * ((x_2 * (x_3 * x_4)) * x_5)$ is $x_1 + x_2 + {}_3 - x_4 - x_5$. So if the equation $x_1 + x_2 + x_3 - x_4 - x_5 = x_i$ holds for all x_1,x_2,x_3,x_4,x_5 and in all Abelian group then i = 3. In this case we must have one of the following cases: -

(i). $x_1 = x_4$ and $x_2 = x_5$

(ii). $x_1 = x_5$ and $x_2 = x_4$

In case (i) the given equation $f = x_i$ becomes

$$x_1 * ((x_2 * (x_3 * x_4)) * x_5) = x_3$$

Now take the set P = {0,1,2,3,4,5,6,7} put $a * b = 3(a - b) \bmod 8 \ \forall\ a,b \in P$. Then the identity

$$x_1 * ((x_2 * (x_3 * x_4)) * x_5) = x_3$$

is satisfied in p. But $x * (y * y) = 3x \neq x \ \forall\ x,y \in P$. So $f = x_i$ does not define a general Abelian group in case (i). Suppose we have case (ii). So the equation $f = x_i$ becomes

$$x_1 * ((x_2 * (x_3 * x_4)) * x_5) = x_3.$$

Take the system S^* where

$$S^* = \begin{cases} 1.\ (x * y) * x = (x * x) * y \\ 2.\ x * x = y * y \\ 3.\ (x * x) * (y * x) = x * y \\ 4.\ x * (x * y) = y \end{cases}$$

Then S^* is equivalent to the equation

$$x_1 * ((x_2 * (x_3 * x_4)) * x_5) = x_3$$

But each equation in S^* is defined using at most 2 variables which contradicts the theorem of Mckinsey and Diamond[M-D] mentioned in theorem 3.26. Thus we have the theorem 3.27.

THEOREM 3.28 (Main theorem)

Let f be a word of length five in (G, *) where (G, *) is as in theorem 3.26. Suppose that the equation $f = x_i$ defines a general Abelian group for some integer 'i'. Then the equation $f = x_i$ has to be one of P-1, P-2,P-3,P-4, Sh, and HN of notation 3.24.

PROOF : -

Let f and $f = x_i$ satisfy hypothesis of theorem. The f cannot be a function of more than five variables. So $f = x_i$ should look like $f(x_1,x_2,x_3,x_4,x_5) = x_i$. Furthur f should be one of G-1 to G-14 of theorem 3.21. We argue case by case. f cannot be G-12 by theorem 3.27. Now the degree of G-1,G-2,G-3,G-5,G-6, G-9,G-11,and G-13 is not 1.

So f cannot be G-1,G-2,G-3,G-5,G-6,G-9,G-11,or G-13. Thus we have eliminated f being any of G-1,G-2,G-3,G-5,G-6,G-9,G-11,G-12, or G-13. So the only possible candidates for f are G-4,G-7,G-8,G-10, or G-14. We discuss each of these possibilities one at a time.

<u>Case 1</u> f = G-4.

Then the equation f = x_i becomes

$$(x_1 * x_2) * ((x_3 * x_4) * x_5) = x_i\text{----------}S.$$

In group theoretic terms the above equation becomes

$$(x_1 - x_2) - x_3 + x_4 + x_5 = x_i\text{----------}Y$$

Now Y should be true for all Abelian groups and all variables x_1,x_2,x_3,x_4,x_5. That is possible only if $x_i = x_1$ or $x_i = x_4$ or $x_i = x_5$. Now x cannot be equal to x_1 or x_5 by theorem 3.17. So $x_i = x_4$. So the equation S should be

$$(x_1 * x_2) * ((x_3 * x_4) * x_5) = x_4\text{----------}S_1$$

Furthur the equation Y can become true for all Abelian groups and all x_1,x_2,x_3,x_4,x_5 only in the following cases : -

Case a:

$x_1 = x_2$ and $x_3 = x_5$

Case b:

$x_1 = x_3$ and $x_2 = x_5$

Now case 'a' cannot be possible by theorem 3.26. So the case 'b' is the only case possible.

Then equation S becomes

$$(x_1 * x_2) * ((x_1 * x_4) * x_2) = x_4$$

which is equation P-4 of note 3.24.

Now we discuss

<u>Case 2</u> f = G-7.

Then the equation $f = x_i$ becomes

$$(x_1 * (x_2 * x_3)) * (x_4 * x_5) = x_i \text{----------} S_2$$

In group theoretic terms S_2 become

$$x_1 - x_2 + x_3 - x_4 + x_5 = x_i \text{----------} Y_2$$

This is possible only if $x_i = x_1$ or $x_i = x_3$ or $x_i = x_5$. Now the case $x_i = x_1$ and $x_i = x_5$ are not possible by theorem 3.17. So $x_i = x_3$. So the equation Y_2 becomes

$$x_1 - x_2 + x_3 - x_4 + x_5 = x_3 \text{---------} Y_3$$

Now Y_3 is possible only in the following cases: -

Case a_1:

$x_1 = x_2$ and $x_4 = x_5$

Case b_1:

$x_1 = x_4$ and $x_2 = x_5$

Now case a_1 is not possible by theorem 3.26. So the only case possible is b_1 and the equation S_2 becomes

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

which is nothing but equation P-2 of note 3.24.

Now we discuss the case 3

<u>Case 3</u> f = G-8.

Then the equation f = x_i becomes

$$(x_1 * ((x_2 * x_3) * x_4)) * x_5 = x_i\text{----------}S_3$$

in group theoretic terms S_3 becomes

$$x_1 - x_2 + x_3 + x_4 - x_5 = x_i\text{----------}Y_3$$

Y_3 is possible only if $x_i = x_1$ or $x_i = x_3$ or $x_i = x_4$. Now "$x_i = x_1$", is not possible by theorem 3.17. So $x_i = x_3$ or $x_i = x_4$. Suppose that $x_i = x_3$. Then Y_3 becomes

$$x_1 - x_2 + x_3 + x_4 - x_5 = x_3$$

Then we should have either $x_1 = x_2$ and $x_4 = x_5$ or $x_1 = x_5$ and $x_2 = x_4$. If we have $x_1 = x_2$ and $x_4 = x_5$ then S_3 becomes

$$(x_1 * ((x_1 * x_3) * x_4)) * x_4 = x_3\text{----------}S_4$$

S_4 gives

$$x_1 * ((x_1 * ((x_1 * x_3) * x_4)) * x_4) = x_1 * x_3\text{----------}S_5$$

Putting $x_1 * x_3 = u$; we see that S_5 is equivalent to

$$x_1 * ((x_1 * (u * x_4)) * x_4) = u\text{----------}S_6$$

By theorem 3.27 we see that S_6 cannot define a general Abelian group. So the case $x_1 = x_2$ and $x_4 = x_5$ is not possible. So we must have $x_1 = x_5$ and $x_2 = x_4$. Then the equation S_3 becomes

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

This is also not possible by an argument similar to the case above. So x_i cannot be equal to x_3. So $x_i = x_4$. Then Y_3 becomes

$$x_1 - x_2 + x_3 + x_4 - x_5 = x_4$$

This is possible only if we have either

A:

$$x_1 = x_2 \quad \text{and} \quad x_3 = x_5$$

B:

$$x_1 = x_5 \quad \text{and} \quad x_2 = x_3$$

We cannot have B by theorem 3.26. So we must have $x_1 = x_2$ and $x_3 = x_5$ Then equation S_3 becomes

$$(x_1 * ((x_1 * x_3) * x_4)) * x_3 = x_4$$

which is equation P-3 of notation 3.24.

Now we discuss the possibility that f = G-14.

In this case the equation $f = x_i$ becomes

$$x_1 * (x_2 * (x_3 * (x_4 * x_5))) = x_i \text{----------} S_4$$

In group theoretic terms S_4 becomes

$$x_1 - x_2 + x_3 - x_4 + x_5 = x_i \text{----------} Y_4$$

No Y_4 can hold only if $x_i = x_3$ by theorem 3.17. So Y_4 should be

$$x_1 - x_2 + x_3 - x_4 + x_5 = x_3 \text{----------} Y_5$$

Now Y_5 can hold only in the following cases: -

C:

$$x_1 = x_2 \quad \text{and} \quad x_4 = x_5$$

D:

$$x_1 = x_4 \quad \text{and} \quad x_2 = x_5$$

Now the case C cannot hold by theorem 3.26. So we must have $x_1 = x_4$ and $x_2 = x_5$. So the equation S_4 becomes

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

which is equation P-1 of notation 3.24.

So now we come to the last possibility namely f = G-10.

Then the equation $f = x_i$ becomes

$$x_1 * ((x_2 * x_3) * (x_4 * x_5)) = x_i \text{----------} S_5$$

Again writing S_5 in group theoretic terms we get

$$x_1 - x_2 + x_3 + x_4 - x_5 = x_i \text{----------} S_6$$

This can hold only in the following two cases: -

<u>Case a</u>

$$x_i = x_3$$

<u>Case b</u>

$$x_i = x_4$$

We discuss case a "$x_i = x_3$": -

Then S_6 becomes

$$x_1 - x_2 + x_3 + x_4 - x_5 = x_3 \text{----------} Y$$

This can hold only in the following cases, for all Abelian groups and all variables x_1, x_2, x_3, x_4, x_5.

Case a_1

$x_1 = x_2$ and $x_4 = x_5$

Case a_2

$x_1 = x_5$ and $x_2 = x_4$

Case a_1 cannot hold by theorem 3.26. So we must have $x_1 = x_5$ and $x_2 = x_4$. The equation S_5 becomes

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

Which is nothing but equation HN of notation 3.24. Now we study case b which is "$x_i = x_4$".

Now S_6 becomes

$$x_1 - x_2 + x_3 + x_4 - x_5 = x_4 \text{----------} Y_7$$

Y_7 can hold for all Abelian groups and all variables x_1, x_2, x_3, x_4 only in the following cases: -

Case b_1:

$x_1 = x_2$ and $x_3 = x_5$

Case b_2:

$x_1 = x_5$ and $x_2 = x_3$

Case b_2 cannot hold because of theorem 3.26. So we must have $x_1 = x_2$ and $x_3 = x_5$. Then the equation S_5 becomes

$$x_1 * ((x_1 * x_3) * (x_4 * x_3) = x_4$$

Which is nothing but equation Sh of notation 3.24. Thus we have proved the theorem 3.28 (main theorem).

REFERENCES

[M-D] J.C.C Mckinsey and A.H. Diamond., Algebras and their Subalgebras, Bull. Amer. Math. Soc 53 (1947). 959-962.

[H-N] G. Higman and B.H. Neumann; Groups as Groupoids with one Law, Publ. Math. Debrecen 2 (1962). 215-221.

[P] R. Padmanabhan, On single-Equational-Axiom Systems for Abelian Groups, J. Austral. Math. Soc 10. (1969). 143-151.

[Sh] M. Sholander, Postulates for Commutative Groups; Amer. Math. Monthly 66. (1959). 93-95.

ABW-7973 SC
L
TENNESSEE STATE UNIVERSITY LIB.
5 0103 00346200 0
TENNESSEE STATE UNIVERSITY
LIBRARY