NEW ALGEBRAIC PROPERTIES OF MIDDLE BOL LOOPS

BY

DAVID SUNDAY PETER

B.Sc. (Ed.) Mathematics (IFE)

A THESIS SUBMITTED IN PARTIAL

FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE (M.Sc.) IN MATHEMATICS OF THE

OBAFEMI AWOLOWO UNIVERSITY, ILE-IFE, NIGERIA

2015

ABSTRACT

The objectives of this study were to establish some new algebraic properties of a middle Bol loop; investigate the relationship between a middle Bol loop, right (left) Bol loops and some inverse property loops like WIPLs, CIPLs, AIPLs, SAIPLs, RIPLs and IPLs; establish some new algebraic properties of translations, autotopisms and anti-autotopisms of a middle Bol loop and study the holomorphic structure of a middle Bol loop. This was with a view to preparing a good ground for the reformulation of the 1994 Syrbu's question on the equivalence of the universal elasticity condition (UEC) and the middle Bol identity (MBI).

Existing literature on the algebraic study of middle Bol loops were surveyed and all accessible materials relevant to the concepts of loops, Moufang loops and Bol loops were also acquired, particularly those that relate them with the concepts of parastophes, extra loop, groups and isotopy. Existing results on middle Bol loops, middle inner mapping T_x and algebraic properties of middle Bol loops by Grecu and Syrbu were employed. The middle Bol identity was judiciously used to investigate the characterizations of middle Bol loops $(Q\cdot,\backslash,/)$. The middle inner mapping T_x was used to produce new algebraic properties of middle Bol loops $(Q\cdot)$. The parastrophes of a middle Bol loop were also used to explore new algebraic properties. The anti-autotopic form of a middle Bol loop was also used to investigate the algebraic properties of autotopisms of middle Bol loops. The structure of the holomorph of a middle Bol loop was also explored.

The result established some new algebraic properties of a middle Bol loop among which were the following near-balanced identities: $yx\backslash x = x\backslash(y\backslash x)$, $xz\backslash x = x\backslash(x/z)$, $(yz)\backslash y = y\backslash(y/z)$,

$(yz)\backslash z = z\backslash(y\backslash z)$, $x(z\backslash x) = (x/z)x$ and $(x/yz)x = (x/z)(y\backslash x)$. It was also established that WIP, RIP, LIP and IP were equivalent in a middle Bol loop. Furthermore, commutative WIP, commutative RIP, commutative LIP and commutative IP were equivalent in a middle Bol loop. Two middle Bol loops using a right Bol loop and a ring were constructed. A new method of constructing a middle Bol loop using a non-abelian group and a subgroup of it was developed. The holomorph of a loop was shown to be a middle Bol loop if and only if the loop was a middle Bol loop. For some special autotopisms, it was found that commutativity (flexibility) was a necessary and sufficient condition for holomorphic invariance under the existing isostrophy between middle Bol loops and the corresponding right (left) Bol loops. The right(left) combined holomorph of a middle Bol loop and its corresponding right (left) Bol loop were shown to be equal to the holomorph of the middle Bol loop.

The study concluded that the Syrbu's open problem can be solved using the algebraic properties of middle Bol loops in this work. And that the following two statements $(yx)u = x \Leftrightarrow y(xu) = x$ and $(xz)u = x \Leftrightarrow (xu)z = x$ which were found to be true in a middle Bol loop were useful for cryptosystems.

Keywords: Cryptosystems / Bol loops/Syrbu/Algebraic

Supervisor: Dr. T. G Jaiyeola

Number of pages: xi, 126p

INTRODUCTION

1.1 Introduction

The diverse areas where loop theory started and in which it moved in the early part of its 70 years of history can be geographically, chronologically and conceptually mapped and fitted It is not possible to compare 300 years of differential calculus to 70 years of loop theory. Loop theory is a new subject when it is juxtaposed with differential calculus and it is misinterpreted always.

For instance, when somebody asks this question: ' what is a loop?' It can be simply explained to mean, "a group without associativity". This is actually true and correct. However, this is not the whole truth It is very important to reiterate here that loop theory is a discipline of its own and not just a generalization of group theory, originating from and still moving within four basic research areas ; algebra, geometry, topology and combinatorics.

In the first 50 years of loop history, we can see that each decade set in motion a brand new and important stage or phase in its development. These distinct periods are briefly discussed below

1.1.1 1920s–The First Glimmering of Non-Associativity

Cases abound in the history of science where at particular times certain revolutionary ideas were, so to speak, "in the air" until these revolutionary ideas came to manifestation in different places, sometimes independently and in different forms.

Two such prominent cases have occurred in mathematics and physics in the last two centuries. Hyperbolic geometry was discovered almost simultaneously by Lobatschevski and

Bolyai in the 1820s, and would afterward combine with Riemannian geometry (announced in

1866) to form the field of Non-Euclidean Geometry. Similarly, around the turn of the century , a completely new conception of Space-Time came out of the Lorentz transformation of 1895, which took the place of earlier Galilean notions, and Einstein's Special Relativity of 1905. We now realise that these two ideas, Non-Euclidean Geometry and Curved Space-Time, are totally related and both assisted to prepare the ground for the notion of non-associativity.

The oldest non-associative operation used by mankind was plain subtraction of natural numbers. The first example of an abstract non-associative system was Cayley numbers; the Cayley numbers constructed by Arthur Cayley in 1845. Dickson later generalised these Cayley numbers to what is known as Cayley-Dickson algebras. These became the subject of serious study in the 1920s because of their important role in the structure theory of
alternative rings.

Another level of non-associative structures was systems with one binary operation. The paper *On a Generalization of the Associative Law* (1929) by Anton K Suschkewitsch, who was a Russian professor of mathematics in Voronezh was one of the earliest publications dealing with binary systems that clearly mentioned non-associativity.

In his paper, Suschkewitsch comments that, in the proof of the Lagrange's theorem for groups, one does not make any use of the associative law. He guesses rightly that it is possible to have non-associative binary systems which satisfy the Lagrange property. There are two types of such so called 'general groups', that Suschkewitsch constructed that satisfy his Postulate A or Postulate B. In Suschkewitsch's approach, some early attempts in the direction of modern loop theory as a generalization of group-theoretical notions can be seen. His 'general groups' seem to be the predecessors of modern quasigroups as isotopes of groups.