Algebras

Riley Chien

April 27, 2015

1. Introduction

By the time of undergraduate study one typically has an intuitive grasp on elementary algebra. Next, one often learns linear algebra in which vector spaces are studied. In abstract algebra, algebraic structures such as groups, rings, fields, and Boolean algebras are studied. Through further abstraction, more algebraic structures can be obtained. Throughout this paper, various algebraic structures will be explored, some will be familiar and some may not be however an attempt will be made to relate these unfamiliar ones back to better-known structures. When possible, relationships between structures will be explored.

2. Algebra Defined

Definition: An algebra, A, is a nonempty set of elements, S, under a set of operations.

Definition: An n-ary operation, f, on S takes n elements of S, $(a_1...a_n)$, to a single element, b, of S, denoted

$$f(a_1...a_n) = b.$$

A 0-ary, or nullary, operation on S takes zero elements of S to a single element of S. 1-ary, 2-ary, 3-ary operations are known as unary, binary, and ternary operations respectively. Most of the common algebras have operations of arity no higher than 2, however we will discuss some algebras with higher arity.

3. Groups and Rings

In order to gain some persepective on the algebras that will be discussed later on, we will begin by briefly examining the familiar structures of groups and rings. A group, G consists of a set of elements, C, along with a single binary operation. In the context of the previously stated definition of an algebra, the inverse of an element can be interpreted as a unary operation. We will explore groups in greater detail later on.

A ring, R, consists of a set of elements, L, along with a pair of binary operations, addition and multiplication. There also exists an additive inverse of each element and in some rings, there is also a multiplicative inverse, so there can also be one or two unary operations as well.

4. Ternary Boolean Algebras

The Boolean algebra we are familiar with is one set, B, with two binary operations, join($\vee$) and meet($\wedge$), one unary operation, complement($'$), and two nullary operations, known as the smallest element(O) and largest element(I). It is necessary that B along with join and meet form a distributive lattice and that the operations of the Boolean algebra satisfy the following relations:

$$x \wedge O = O \tag{1}$$

$$x \vee I = I \tag{2}$$

$$x \vee x' = I \tag{3}$$

$$x \wedge x' = O \tag{4}$$

We can obtain an interesting structure, which we will call ternary Boolean algebra, by defining an algebra by the set K along with the ternary operation, which we will denote

$$a^b c \text{ for } a, b, c \in K,$$

and the largest element, smallest element, and complement operations from traditional Boolean algebra.

This ternary operation will satisfy the relations:

$$a^b(c^d e) = (a^b c)^d (a^b e)) \tag{5}$$

$$a^b b = b^b a = b \tag{6}$$

$$a^b b' = b'^b a = a \tag{7}$$

The relations we have defined are already enough to begin to prove some theorems about this ternary Boolean algebra. We will use these relations to prove that each element has a unique complement, that the idempotent holds, and that the ternary operation is associative and commutative.

Theorem 4.1: Each element $a \in K$ has a unique complement a'.

Proof: Suppose $a \in K$ has two distinct complements a'_1 and a'_2.

$$\begin{aligned} a'_1 &= (a'_1)'^a a'_2 \text{ by (7)} \\ &= a'_2 \end{aligned}$$

By contradiction, a' is unique.

Theorem 4.2: $(a')' = a$

Proof:

$$\begin{aligned} (a')' &= (a')'^{a'} a \text{ by (7)} \\ &= a \end{aligned}$$

Theorem 4.3: The idempotent law holds, that is $a^b a = a$.

Proof:

$$\begin{aligned} a^b a &= (a^b b')^b (a^b b') \text{ by } (6) \\ &= a^b (b'^b b') \text{ by } (5) \\ &= a^b b' \text{ by } (7) \\ &= a \text{ by } (7) \end{aligned}$$

Theorem 4.4: The ternary operation is associative, that is $a^b(c^b d) = (a^b c)^b d$.

Proof:

$$\begin{aligned} a^b(c^b d) &= (a^b c)^b (a^b d) \\ &= [(a^b c)^b a]^b [(a^b c)^b d] \\ &= [(a^b c)^b (a^b b')]^b [(a^b c)^b d] \\ &= [a^b (c^b b')]^b [(a^b c)^b d] \\ &= [(a^b c)^b [(a^b c)^b d] \\ &= [(a^b c)^b b']^b [(a^b c)^b d] \\ &= (a^b c)^b d \\ a^b(c^b d) &= (a^b c)^b d \end{aligned}$$

Theorem 4.5: $a^b a' = b$.

Theorem 4.6: The ternary operation is commutative such that any two elements can be interchanged.

Proof:
(a)

$$\begin{aligned} a^b c &= a^b (a^c a') \\ &= (a^b a)^c (a^b a'). \\ &= a^c b \end{aligned}$$

(b)

$$\begin{aligned} a^b c &= a^b(b^c b') \\ &= (a^b b)^c (a^b b'). \\ &= b^c a \end{aligned}$$

(c) By (a) and (b),

$$a^c b = b^c a.$$

From these six theorems it is clear that an operation with arity higher than two can still posses properties similar to those held by some of the binary operations.

We will now show a further relationship between ternary Boolean algebra and the typical Boolean algebra.

Theorem 4.7: Let p be a fixed element of K. Define

$$\begin{aligned} a \wedge b &= a^p b \\ a \vee b &= a^{p'} b^{\cdot} \end{aligned}$$

The algebra consisting of K along with the $\wedge$ and $\vee$ operations, known as $B(p)$, forms a Boolean algebra with p as its largest element and p as its smallest element.

There are further relationships to be made between Boolean algebra and this ternary Boolean algebra which will not be covered, but we have shown that there are interesting results to be discovered in algebras with higher arity operations and we will continue to show this in the next section.

5. Polyadic Groups

We have previously discussed a group as a set of elements and a binary operation but similarly to Boolean algebras, interesting structures can be obtained by allowing the operation to be of a higher arity.

Definition: Given a set of elements C, and an operation $f(a_1 a_m)$, we say that the elements of C constitute an m-adic group, G, under f if the following conditions are satisfied:
(1) If any m of the $m+1$ symbols in the equation of the form

$$f(a_1 ... a_m) = a_{m+1} \tag{8}$$

represent elements of C, then the remaining symbol is also an element of C and is uniquely determined by this equation.

(2) The elements of C satisfy the associative law under f such that

$$f(f(a_1...a_m)a_{m+1}...a_{2m-1}) = f(a_1 f(a_2...a_{m+1})a_{m+2}...a_{2m-1}) = ... = f(a_1...f(a_m...a_{2m-1})). \quad (9)$$

Whereas 2-adic groups(or simply groups) have an identity element, higher-adic groups can also have identity. For these higher-adic groups however, the higher arity of the operation leads to more complex identities.

Definition: If the equation

$$f(a_1...a_{m-1}s) = s \quad (10)$$

is true for some $s \in C$, then the equation is true $\forall s \in C$ and the sequence or $(m-s)$-ad, $(a_1...a_{m-1})$, is a left identity of G. If the equation

$$f(sb_1...b_{m-1}) = s \quad (11)$$

is true for some $s \in C$, then the equation is true $\forall s \in C$ and the $(m-1)$-ad, $(b_1...b_{m-1})$, is a right identity of G.

Theorem 5.1: Every left identity of$G$ is also a right identity of G and every right identity of G is also a left identity of G. They will now be referred to simply as identities of G.

Theorem 5.2: If the $(m-1)$-ad, $(a_1...a_{m-1})$, is an identity of G, then any cyclic permutation, $(a_{i+1}...a_{m-1}a_1...a_i)$ is also an identity of G.

Proof: Consider the identity equation

$$f(a_1a_2...a_{m-1}a_1) = a_1$$

where $a_1...a_{m-1} \in C$ and $(a_1...a_{m-a})$ is an identity of G. It is clear that $(a_2...a_{m-1}a_1)$ is also an identity of G.

Now, consider the identity equation

$$f(a_2a_3...a_{m-1}a_1a_2) = a_2.$$

Again, it is clear that $(a_3...a_{m-1}a_1a_2)$ is an identity of G as well. Repeating this series of steps shows that $(a_4...a_{m-1}a_1...a_3)$ is an identity and so on such that $a_{i+1}...a_{m-1}a_1...a_i)$ is an identity of G for $i < m-1$. Thus any cyclic permutation of an identity of G is also an identity of G.

In a 2-adic group, an inverse of an element, $a \in C$, is an element, a, such that aa is equal to the identity element. In $m > 2$-adic groups, an identity is obtained from multiplying an element, a, with $(m-2)$ other elements to create the $(m-1)$-ad necessary for an identity. Thus the inverse of an element, a, is a $(m-2)$-ad. We can also define inverses for i-ads for arbitrary $i < m-1$.

Definition: Consider an i-ad, $(a_1 a_i)$, where $i < m-1$, its inverse is the $(m-1-i)$-ad, $(a_1 a_{m-1-i})$, such that $(a_1 a_i a_1 a_{m-1-i})$ is an identity.

Next, we will discuss the idea of equivalent i-ads.

Definition: If for a pair of i-ads, $(a_1...a_i)$ and $(b_1...b_i)$, and an $(m-1)$-ad, $(s_1...s_k...s_{m-i})$, we can write an equation

$$f(s_1...s_k a_1...a_i s_{k+1}...s_{m-1}) = f(s_1...s_k b_1...b_i s_{k+1}...s_{m-1}), \tag{12}$$

$a_1...a_i)$ and $b_1...b_i)$ are equivalent i-ads.

Definition: An m-group, G, is abelian if the dyads $(s_1 s_2)$ and $(s_2 s_1)$ are equivalent for ever pair of elements $s_1, s_2 \in G$.

All of these results should feel familiar because they are extensions of the basic ideas of identity, inverse, and equivalence from the standard 2-adic group. For all of these ideas, we obtain exactly the same definitions of identity, inverse, and equivalence by setting $m = 2$.

References

[1] Burris, Stanley, Sankappanavar, H.P.*A Course in Universal Algebra*

[2] Grau, A.A. *Ternary Boolean Algebra.* Bulletin of the American Mathematical Society. July 4, 2007.

[3] Judson, Thomas W. *Abstract Algebra Theory and Applications.* GNU Free License Document, abstract.pugetsound.edu. 2014.

[4] Post, Emil L. *Polyadic Groups.* Transactions of the American Mathematical Society. 1940