

Boolean Groups

Anellis, Irving H.

Veröffentlicht in:
Abhandlungen der Braunschweigischen
Wissenschaftlichen Gesellschaft Band 33, 1982,
S.85-97



Verlag Erich Goltze KG, Göttingen

Boolean Groups

By Irving H. Anellis, Duluth/USA

Abstract

Abstract groups are constructed as equivalence classes from elements of Boolean algebra $(A, \cup, \cap, \rightarrow, \dashv)$ associated to the elements of the sequence of natural numbers whose model is $N = \langle 0, \omega, +, \cdot \rangle$, where a partition modulo- m is a subclass defined on the Boolean equivalence and congruence relation I^N defining $N_m \subset A/p$ with I^N associated with identity. This gives a Boolean algebra \mathfrak{B} , whose groups, then, are not multiplicative sets, but classes of m -partition subclasses of the model N of the Boolean universe V_ω^N defining the algebra \mathfrak{B} . Thus, a Boolean group for \mathfrak{B} with universe V_ω^N may be either an additive or a multiplicative class. These Boolean groups are closely related to the \mathcal{L} -groups constructed in Birkhoff's *Lattice Theory*.

AMS 1970 **subject classifications**. Primary: 02J05, 06A40, 20F99;
Secondary: 06A55, 06A60, 20E40, 02H15.

Key words and phrases. Boolean algebra, ordered lattices, ordered groups, infinite groups.

0. Introduction

Groups are defined as multiplicative sets. Thus, for some group G , $G = (S, *)$, where $\{S\}$ is a set and $*$ is a productive operation on the elements of $\{S\}$, such that, for all $x, y \in S$, $x * y \in S$ and $x * y$ is a unique product of x, y . We then say that all groups satisfy the condition $Cl(x * y)$. Here, we define groups as equivalence classes of Boolean elements closed under $*$ defined as group addition.

We have, then, abstract groups constructed as equivalence classes from elements of the Boolean algebra $(A, \cup, \cap, \rightarrow, \dashv)$ associated to the elements of the sequence of natural numbers whose model is $N = \langle 0, \omega, +, \cdot \rangle$, where a partition modulo- m is a subclass defined by the Boolean equivalence and congruence relation I^N defining $N_m \subset A/p$ with I^N associated with identity. This gives a Boolean algebra \mathfrak{B} , whose groups, then, are not multiplicative sets, but classes of m -partition subclasses of the model N of the Boolean universe V_ω^N defining the algebra \mathfrak{B} . Thus, a Boolean group for \mathfrak{B} with universe V_ω^N may be either an additive or (by the usual characterization of groups) a multiplicative class. We also note that Boolean groups are abelian (but leave the routine proof to the reader).

Boolean groups are closely related to the \mathcal{L} -groups of [1], which are defined as po-groups in which any two elements have l.u.b. and g.l.b.. There, according to

Lemma 2, the algebra $(A, +, \vee)$ is an \mathcal{L} -group iff it is a group under $+$, a join-semilattice under \vee , and the distributive laws hold for $a, b, x, y \in A$ for $+$, \wedge , and \vee .

The apparatus for construction of Boolean groups has long been available, but group-theorists prefer to use a set-theoretic approach, usually through ZF. Willie Brown suggested that it might be possible to construct such groups, but that no one had yet made the attempt. I wish to thank him here for his suggestion.

1. Boolean Lattices

A Boolean algebra is abstract, and is constructed on a domain U , composed of a family of sub-domains Q of U such that each domain defines a class. For U we obtain the intersection of all subdomains of Q . Thus, if $Q \neq \emptyset$, $U \neq \emptyset$. A Boolean algebra based on a nonempty family of subdomains Q of U is a **lattice**. For two classes $A, B \in Q$, $A \cup B \in Q$ and $A \cap B \in Q$, and if $A \in Q$, $\bar{A} \in Q$. A simple Boolean algebra is closed, then, under the binary operations of union and intersection. The algebra (A, \cup, \cap) with these two binary operations is a lattice if, for all $a, b, c \in A$, the following equations hold:

$$\begin{array}{ll} a \cup b = b \cup a & a \cap b = b \cap a \\ a \cup (b \cap c) = (a \cup b) \cap c & (a \cap b) \cap c = a \cap (b \cap c) \\ (a \cup b) \cap c = b \cap c & a \cup (a \cap b) = a \end{array}$$

Thus, we obtain immediately as theorems

Theorem 1.1. If (A, \cup, \cap) is a lattice, then for all $a, b \in A$, $a \cup b = b$ iff $a \cap b = a$.

Theorem 1.2a. If (A, \cup, \cap) is a lattice, then for all $a, b \in A$, we obtain the relation \leq on A , defined as $a \leq b$ iff one of the equations of Theorem 1.1 holds, and \leq is the lattice ordering on A .

Theorem 1.2b. For the ordered class (A, \leq) we obtain $a \cup b = \sup\{a, b\}$, $a \cap b = \inf\{a, b\}$ on the elements $\{a, b\}$.

Theorem 1.3. The ordered class (A, \leq) is a lattice. Proof is obtained where (A, \leq) contains a nonempty subclass ∇ of the class A and ∇ is a filter where, for all elements $a, b \in A$, $a \cap b \in \nabla$ if $a \in \nabla$ and $b \in \nabla$.

Proof. Let (A, \cup, \cap) be a lattice. Then the following conditions, all of which are equivalent, hold

1. $a \cap b \in \nabla$ iff $a \in \nabla$ and $b \in \nabla$.
2. if $a \in \nabla$ and $b \in \nabla$, then $a \cap b \in \nabla$,
if $a \in \nabla$ and $a \leq b$, then $b \in \nabla$.
3. if $a \in \nabla$ and $b \in \nabla$, then $a \cap b \in \nabla$,
if $a \in \nabla$ and $b \in \nabla$, then $a \cup b \in \nabla$.

Then clearly (A, \leq) is a lattice equivalent to the lattice (A, \cup, \cap) . We may also note that, if the lattice has the greatest element V , then $\{V\}$ is a filter. ■

Examples. All of the following are filters

1. If (A, \cong) is a lattice, then $(a_0) = \{a \in A : a_0 \cong a\}$ is a filter (the filter generated by a_0).
2. If (A, \cong) is a lattice and $B \subset A$, then $\nabla(B) = \{a \in A : (\exists b_1, \dots, b_n \in B) (b_1 \cap \dots \cap b_n \cong a)\}$ is a filter (the filter generated by B).
3. If (A, \cong) is a lattice, ∇_0 is a filter and $a \in A$, then $\nabla(\nabla_0, a) = \{x \in A : (\exists b \in \nabla_0) (b \cap a \cong x)\}$ is a filter.

Proof: Let $x, y \in \nabla(\nabla_0, a)$. Then $a \cap b_1 \cong x$ and $a \cap b_2 \cong y$ for some $b_1, b_2 \in \nabla_0$. Therefore $(a \cap b_1) \cap (a \cap b_2) \cong x \cap y$. But $(a \cap b_1) \cap (a \cap b_2) = a \cap (b_1 \cap b_2) = a \cap b$, where $b = b_1 \cap b_2 \in \nabla_0$. Then $x \cap y \in \nabla(\nabla_0, a)$. ■

Theorem 1.4a. A lattice (A, \cup, \cap) is distributive if, for all $a, b, c \in A$, $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$.

The proof is easy and left to the reader.

Theorem 1.4b. If (A, \cong) is distributive, then every maximal filter is prime.

Proof. We begin with definitions of maximal and prime filters.

Definition 1.4b1. A filter ∇ is **prime** if it is proper (i. e. there is an element $a \in A$ such that $a \notin \nabla$ for the lattice (A, \cup, \cap)).

Definition 1.4b2. A filter ∇ is **maximal** provided it is proper and is not a proper subclass of any proper filter.

Definition 1.4b3. A filter ∇ is **prime** if it is proper and $a \cup b \in \nabla$ implies either $a \in \nabla$ or $b \in \nabla$.

Now assume that ∇ is maximal but not prime. Then there exist $a, b \in A$ such that $a \cup b \in \nabla, a \notin \nabla$ and $b \notin \nabla$. But consider $\nabla_1(\nabla, a)$. $\nabla_1(\nabla, a) = A$, so $b \in \nabla_1(\nabla, a)$. Thus, $x \cap a \cong b$ for $x \in \nabla$. Therefore, $(x \cap a) \cup b = b = (x \cup b) \cap (a \cup b) \in \nabla$; and we obtain a contradiction. ■

Principle 1.5. Every relatively pseudo-complemented lattice is distributive.

An abstract algebra $(A, \cup, \cap, \rightarrow)$ is a **relatively pseudo-complemented lattice** if (A, \cup, \cap) is a lattice and for all $a, b, x \in A$, the condition $a \cap x \cong b$ iff $x \cong a \rightarrow b$ is satisfied.

Let (A, \cup, \cap) be a lattice and $B \subset A$. Then assume $\sup(B) = a$ iff $[(\forall b \in B) (b \cong a)] \& (\forall b \in B) (b \cong c) \rightarrow (a \cong c)$, and \underline{a} is the g.l.b. of B . Then note, by the condition for a relatively pseudo-complemented lattice, that $a \rightarrow b$ is the upper bound for $\{x \in A : a \cap x \cong b\}$.

An abstract algebra $(A, \cup, \cap, \rightarrow, \dashv)$ is pseudo-Boolean if $(A, \cup, \cap, \rightarrow)$ is a relatively pseudo-complemented lattice and satisfies the condition

$$\text{for any } a \in A, \bar{a} = a \rightarrow \Lambda$$

where Λ is the least element of a lattice and $\{\Lambda\}$ is an ideal. We note then that a pseudo-Boolean algebra has a greatest element V and a filter $\{V\}$ insofar as it is relatively pseudo-complemented, and a least element Λ and an ideal $\{\Lambda\}$. The algebra

(A, \cup, \cap) is a **complete lattice** if it is a lattice and, for all $B \subset A$, $\sup(B)$ and $\inf(B)$ are defined.

Principle 1.6. An abstract algebra $(A, \cup, \cap, \rightarrow, -)$ is a Boolean algebra if it satisfies the conditions

- a. $(A, \cup, \cap, \rightarrow, -)$ is a pseudo-Boolean algebra
- b. $a \cup -a = V$ for all $a \in A$.

Theorem 1.6.1. If $(A, \cup, \cap, \rightarrow, -)$ is a Boolean algebra, the following conditions are equivalent

1. ∇ is a maximal filter
2. ∇ is a prime filter
3. for all $a \in A$, exactly one of the elements $a, -a$ belong to ∇ .

Principle 1.7. For a Boolean algebra $(A, \cup, \cap, \rightarrow, -)$, $p \supset A^2$ is an equivalence relation and p is a congruence relation on $(A, \cup, \cap, \rightarrow, -)$ if, for $x_1 p y_1$ and $x_2 p y_2$, then $(x_1 \cup x_2) p (y_1 \cup y_2)$, $(x_1 \cap x_2) p (y_1 \cap y_2)$, $(x_1 \rightarrow x_2) p (y_1 \rightarrow y_2)$, and $(-x_1) p (-y_1)$.

Theorem 1.7.1. Let $(A, \cup, \cap, \rightarrow, -)$ be a Boolean algebra and ∇ a filter. Let $p \subset A^2$ be a relation defined by $a p b$ iff $a \rightarrow b \in \nabla$ and $b \rightarrow a \in \nabla$. Then

- and
- a. p is an equivalence relation
 - b. p is a congruence relation.

Corollary 1.7.2. p is a congruence relation defined as $a p b$ iff $a \rightarrow b \in \nabla$ and $b \rightarrow a \in \nabla$.

We denote A/p as the set of all equivalence classes of p .

2. The Number-theoretic Boolean Algebra \mathfrak{N} .

We now prove that the sequence N of natural numbers belongs to a subclass of the Boolean algebra $(A, \cup, \cap, \rightarrow, -)$. We do so by showing that \mathfrak{N} is a Boolean algebra with elements $n \in N$ of the ordered sequence N .

We know that \mathfrak{N} is a Boolean algebra iff it is a relatively pseudo-complemented lattice and that the sequence N is defined by $N = \langle 0, \omega, +, \cdot, >$.

Theorem 2.1. N can be ordered and (N, \cong) is an ordered class if, for any $x, y \in N$, $x \cong y$.

The proofs are routine. It is also easy to prove the stronger theorem (Zermelo) that every set can be well-ordered.

Thus, (N, \cong) is a lattice.

It follows that, where $\inf\{0\}$ and $\sup\{\omega\}$ on the elements of N , for any $n \in N$, $0 \leq n$ and $n \leq \omega$. Thus, for all $n \in N$, \mathfrak{N} is a lattice having a least element 0 associated to Λ and a greatest element V associated to ω . We note that singleton $\{\emptyset\}$ is defined as having a value 0 ; then $\{\emptyset\}$ is an ideal and $\{\omega\}$ is a filter.

Definition 2.2. Let R^N be an operation of \mathfrak{N} such that $R^N = \bigcap_{\alpha_i \leq \omega} N_{\alpha_0} \dots N_{\alpha_i} R$, where every $N_{\alpha_i} \subseteq N$. Then R^N is the *closure* of N .

Definition 2.3. Identity Id is the **universal closure** of a Boolean subalgebra $\mathfrak{B} \subseteq \subseteq(A, \cup, \cap, \rightarrow, \dashv)$.

Theorem 2.4. I^N is the **identity relation of the Boolean subalgebra \mathfrak{B}** . Therefore I^N is a **congruence relation and equivalence relation**.

Proof. First we denote by Id_N the number-theoretic identity on N , and associate the operator I^N to Id_N . We obtain Id_N where, for all $x, y \in N$, $x \cap y \rightarrow y \cap x$, $y \cap x \rightarrow x \cap y$, $x \cup y \rightarrow y \cup x$, $y \cup x \rightarrow x \cup y$. Next we note that, by Theorem 2.1, (N, \subseteq) is an ordered class. Thus, we define Id_N for (N, \subseteq) according to the usual rules for the arithmetic identity relation $=$ and note that Id_N gives closure for all $\alpha \in N$ where $\alpha^2 = \alpha$ satisfying the conditions

$$\alpha \cap \alpha = \alpha, \quad \alpha \cup \alpha = \alpha$$

where $\alpha \cap \alpha = \alpha + \{1\}$, $\alpha \cup \alpha = \alpha + \{\emptyset\}$ defined for all ordered pairs $\langle x, y \rangle \in N$ such that

$$\langle x, y \rangle = \{\{x\}, \{x, y\}\} \longleftrightarrow x \text{Id}_N y = \{\langle x, y \rangle : x = y\}$$

under the condition $\langle x, y \rangle = \langle y, x \rangle$.

Let $a, b, c \in N$. Then I^N is an equivalence relation if the following conditions hold

- For $a I^N a$, $a \cap a \rightarrow a$, $a \cup a \rightarrow a$ (reflexivity)
- For $a I^N b$, $a \cap b \rightarrow b \cap a$, $a \cup b \rightarrow b \cup a$ (symmetry)
- For $a I^N b I^N c$, $a \cap b \cap c \rightarrow a \cap b \cap c$,
 $a \cup b \cup c \rightarrow a \cup b \cup c$ (transitivity).

Then $x I^N y$ defines an equivalence relation on $x, y \in N$ where $x I^N y$ determines the conditions of reflexivity, symmetry, and transitivity of elements $x, y \in N$. Moreover $x I^N y$ is a congruence relation if it satisfies the following additional conditions

- For $a I^N b$ and $a, b \in N$, if $a \subseteq b$, $b \subseteq a$, then $|a| = |b|$
(Schröder-Bernstein Theorem)
- If $x I^N y$, for all $x, y \in N$, then $a \cap c I^N b \cap c$ for all c
- $a I^N b \rightarrow a' I^N b'$ for all $a, b \in N$.

It is clear that I^N satisfies all of these conditions for N . ■

We have next to show that the following theorem holds.

Theorem 2.5. \mathfrak{B} is a Boolean algebra whose elements are given by the sequence N .

We do so by showing first that the two following conditions hold

- \mathfrak{B} is pseudo-Boolean
- $n_n \cup \neg n_n = V^N$ for all $n \in N$.

Proof. First note that conditions a and b are exactly those of Principle 1.6. Thus, if \mathfrak{B} satisfies these, it satisfies all subconditions for lattices and relatively pseudo-complemented lattices.

We also note that the algebra \mathfrak{N} is closed under addition and multiplication for $N = \{0, 1, \dots, n\}$, $n \leq \omega$, and that $\mathfrak{N} = \langle 0, \omega, +, \cdot \rangle$.

a. \mathfrak{N} is pseudo-Boolean if it is a relatively pseudo-complemented lattice and satisfies the condition that, for any $n \in N$, $\neg n = n \rightarrow \Lambda$, where Λ is the least element of a lattice and $\{\Lambda\}$ is an ideal.

Let $0 \in N$ be defined as \emptyset . We note that for any $n, m \in N$, where $m = n + n$, there is associated a zero to any m such that $m = n$ where $n + n = n$. Then \emptyset is a zero element for a sequence N if $\neg \emptyset = \emptyset$, such that \emptyset is the least element of a lattice V^N for N . If V^N is a lattice for the structure \mathfrak{N} whose elements are $N = \{0, 1, \dots, \omega\}$, then $\{\emptyset\}$ is an ideal. \square

b. Let $a = \neg\neg a$. If $a \cup b = V$ and $a \cap b = \Lambda$, then $b = \neg a$. For $a \rightarrow b$, we obtain $a \cup \neg a$. Then $a \cup \neg a = V$. Now assume $V^N \subseteq V$. Then $V^N \models \{n_n : n \leq \omega, n \in V\}$. Let $n_0, n_1, \dots, n_\omega \in N$. Select any $n_n \leq n_\omega$ and any $n_m \neq n_n$. Then $n_m \cap n_n$. Now let $a = n_m$ and $b = n_n$. Then for $a \cup b = V$, we obtain $n_m \cup \neg n_n = V^N$. Then $n_m \cup \neg n_m = V^N$. Now note that $a \cup b = \sup\{a, b\}$. Then $n_m \cup n_n = \sup\{n_m, n_n\}$. Then for $V^N = \{n_n : n \leq \omega\}$, $n_m \cup \neg n_m = V^N$. \square

The other conditions for \mathfrak{N} being Boolean follow. \blacksquare

If \mathfrak{N} is a Boolean algebra, then $N \subset A/p$.

Theorem 2.6. $N \subset A/p$, for A/p the set of all equivalence relations of p .

Proof. Follows directly from Theorems 2.4 and 2.5 (from I^N being an equivalence and congruence relation on N , and from \mathfrak{N} being Boolean).

Note that $N \subset A/p$ iff A/p is true only where $N \subseteq I^N$.

3. Boolean Groups

Boolean groups may be constructed directly by applications of some equivalence relation E modulo- m ($m < \omega$) of the set of elements of V_ω^N of the Boolean algebra \mathfrak{N} . It is important to define the group operations as Boolean.

We remind the reader that, by Principle 1.7, for a Boolean algebra $(A, \cup, \cap, \rightarrow, \neg)$, $p \subset A^2$ is an equivalence relation, and p is a congruence relation on $(A, \cup, \cap, \rightarrow, \neg)$ if, for $x_1 p y_1$ and $x_2 p y_2$, the following conditions hold

- a. $(x_1 \cup x_2) p (y_1 \cup y_2)$
- b. $(x_1 \cap x_2) p (y_1 \cap y_2)$
- c. $(x_1 \rightarrow x_2) p (y_1 \rightarrow y_2)$
- d. $(\neg x_1) p (\neg y_1)$

Also recall Theorem 1.7.1 and Corollary 1.7.2, whereby we find that $p \subset A^2 \stackrel{\text{df}}{=} (a p b \text{ iff } a \rightarrow b \in \nabla \text{ and } b \rightarrow a \in \nabla)$ such that p is an equivalence relation. By Theorem 2.4, we have I^N , the identity of number theory, the congruence and equivalence relation of Boolean algebra \mathfrak{N} .

We now prove that a group G is Boolean if it is defined on a lattice \mathfrak{L}^n whose structure is $\langle G, * \rangle$, for $*$ group addition, where elements of G are elements of a Boolean algebra. Here, all elements of G are elements of \mathfrak{A} . We begin by proving that E_m and E'_m , $m < \omega$ are values for the equivalence and congruence I^N .

First we offer some definitions.

Definition 3.1. The arithmetic operations of addition and multiplication may be defined as Boolean operations such that

- a. $\alpha + \beta = [(\alpha \cap -\beta) \cup (-\alpha \cap \beta)] = \alpha \cup \beta$
- b. $\alpha \cdot \beta = \alpha \cap \beta$

where $\alpha \cap \alpha = \alpha + \{1\}$ and $\alpha \cup \alpha = \alpha + \{\emptyset\}$ (see proof of Theorem 2.4).

Note that multiplication may be defined in terms of addition.

Definition 3.2. E_m and E'_m are modulo- m equivalence relations for I^N_m such that

- a. $E_m(\alpha, \beta) = \alpha \cup \beta / m$
- b. $E'_m(\alpha, \beta) = \alpha \cap \beta / m$

where $\alpha I^N_m \beta = \alpha \cup \beta / m$ if $\alpha I^N_m \beta = \alpha + \beta / m$ and $\alpha I^N_m \beta = \alpha \cap \beta / m$ if $\alpha I^N_m \beta = \alpha \cdot \beta / m$

Definition 3.3. (Samuel [3]). $\sup(x, y) = x + y + xy$, i.e. $(x \cup y)$, and $\inf(x, y) = x \cdot y$, where, for inverse (complement) of x , $x^{-1} = y$, $\sup(x, y) = 1$, $\inf(x, y) = 0$.

Theorem 3.4. E_m (E -mod m), $m < \omega$ is an equivalence and congruence relation if $E_m = I^N_{m=(k+l)} \leq \omega$.

Proof. We use well-known theorems of Gauss. Suppose $n, m, l, k \in \mathbb{N}$, and let $m = k + l$. Now let $\alpha, \beta \in \mathbb{N}$, and let $m + k = n$. Then if $\gamma, \delta \in \mathbb{N}$, and $m + \alpha = \gamma$ or $m + \beta = \delta$, then either $\alpha = \beta = k$, $\gamma = \delta = n$, and $I^N_{m=(k+l)} \leq \omega$ defines an identity mod- m or $\gamma \neq \delta \neq n$. Assume $G \subseteq \mathbb{N}$. Suppose $\alpha \in G$, $\alpha = k$. Then $\gamma \in G$, $\gamma = n$, and $m + \alpha = n$. Thus, α, k are equivalent mod- m , and γ, n are equivalent mod- m . And if we have a mod- m system, m is zero, $m + m = m$, $m + \alpha = \alpha$ for any α . Now consider the relation E_m on the elements of the algebra \mathfrak{A} . Let $\{N\} = \{\langle 0, 1, 2, \dots, n \rangle\}$ and let $n \leq \omega$, $m < n$. For any $p, x, y, z \in \{N\}$, E_m defines a partition p if $x + m = z/p$, $y + m = z/p$. Then E_m is an equivalence and congruence relation mod- m , and partitions elements of $G \subseteq \mathbb{N}$ into congruent classes such that, for any $x, y \in G$, there is a $z \in G$, if $m + x = z/p$, $m + y = z/p$, then x, y are congruent mod- m . Then E_m defines x, y elements of the same equivalence class. ■

The relation E_m can be understood as a group-theoretic identity, where E_m is just $I^N_{m=(k+l)} \leq \omega$, which partitions elements of \mathbb{N} into equivalence classes.

Theorem 3.5. Let $e, a, b, c, \dots, c+n, m-n, m-l \in G \subseteq \mathbb{N}$, $(c+n)(m-n) = m$. Then if $*$ is addition for E_m , we obtain a modulo- m additive group for E_m if $m = e$ and for all $k, l \in G$,

$$\begin{aligned} E_m \{ \langle e, e \rangle = e, \langle e, k \rangle = k, \dots, \langle c+n, m-n \rangle = c+m = e, \dots, \\ \langle a, m-l \rangle = m = e, \dots, \langle k, l \rangle = k+l, \dots, \langle m+k, l \rangle = k+l \}. \end{aligned}$$

Proof. The proof is by Theorem 3.4. ■

Corollary 3.5.1. If $x, y \in G$ and G is a group, then $Cl_m(x*y)$ where $*$ is group addition.

Proof. Let $x*y = z$. Then either $z \in G$ or $x*y \neq z$.

Case I: Let $x*y \neq z$. Then $z - x \neq y$, $z \in G$, and $x \notin G$ or $y \notin G$. But by definition, $x, y \in G$. Contradiction.

Case II: Let $x*y = z$. Then $z - x = y$, so if $x, y \in G$, $-x, z \in G$. Note that $a + (-b) = a - b$. Then $z + (-x) = z - x$. Moreover, $z - x = y$ and $y \in G$; and if $x \in G$ then $-x \in G$, the inverse $-x$ of $x \in G$ is an element of G , since $x - x = 0$, and by Theorem 3.5, $E_m(\langle x, -x \rangle = m) | E_m(m, -x) = -x$, where by $a \cup -a = V$, and $n_n \cup -n_n = V^N$ Theorem 2.5 b). ■

Corollary 3.5.2. For $x, y \in G$ and $Cl_m(x*y)$, G has a zero element e such that, for some $a \in G$, $a*m = e$.

Proof. The proof is by Theorems 3.4, 3.5, and Corollary 3.5.1. We know that $E_m(m, m^{-1}) = e$ by I_m^N -addition. Now choose some a such that $a = m^{-1}$. Then by group addition mod- m , $a*m = e$ and e is the zero for group addition mod- m where $e = m$. ■

Modulo- m group G whose elements are the elements of the Boolean algebra \mathfrak{A} satisfies the conditions of closure under group addition and of having a zero element. Thus, G is minimally an \mathcal{L} -group, as defined by [1]. Then E_m is group addition for $*$ in G . But it would be possible also to present a relation E'_m under which $*$ is group multiplication mod- m and defines a multiplicative group G whose elements are exactly those of the additive group $G \text{ mod-}m$. We then obtain

Theorem 3.6. Let $e, a, b, c, c+n, m-n, m-l \in G \subseteq N$, $(c+n)(m-n) = m$. Then if $*$ is group multiplication under E'_m , we obtain a mod- m multiplicative group for E'_m if $m+e$, and for all $k, l \in G$,

$$E'_m \{ \langle c, e \rangle = e, \langle e, k \rangle = e, \dots, \langle c+n, m-n \rangle = e, \dots \langle l, k \rangle = (k-l \cdot l) + l, \dots, \langle k, k \rangle = (l-l \cdot k) + k, \dots \}$$

where any group product divisible by an m -quotient $(c+n)$, $(m-n)$ is e , $e = m$, or a remainder $e-r$, $r \in G$ if $r \neq e$ or an m -quotient of e , and for all $x \in G$, $E'_m(x, m) = m$, $E'_m(e, m) = e$, e the zero.

Proof. The proof is easy that multiplicative sets are groups under group multiplication. If, for $(x, y)_m / E'_m$, $m, x, y \in G$, $x*y \in G$, then $m*x, m*y \in G$, provided m is a partition element of G . Then for some $a \in G$, $a/x = m$ and $m \in G$, or $a/m = x$ and m is a partition element of G . Then $m \in G$. We prove that e is a zero for $G \text{ mod-}m$ in $Cl_m(x, m)$ for $x, m \in G$, and $x*m \in G$ for $*$ group multiplication mod- m . We can also show that $e = m$. ■

E_m and E'_m define group addition and group multiplication for a group G on a partition m on the elements of Boolean algebra \mathfrak{A} , where m gives the least element of \mathfrak{A} and thus $m = 0$ for Λ^N . Then if I^N is the congruence and equivalence relation for \mathfrak{A} , E_m and E'_m define the equivalence classes for mod- m group G . Thus, if I_m^N denotes the mod- m equivalence classes defined by E_m and E'_m , then I_m^N is the congruence and

equivalence relation for G . Also note that G is a Boolean group if elements of G are elements of a Boolean algebra, and if, for $x, y \in G$, we obtain $Cl_m(xI_m^N y)$ and the conditions of Principle 1.7 hold. Then we obtain

Corollary 3.6.1. G is a Boolean group if, for $\alpha, \beta, \gamma, \delta \in G$, $m | \alpha - \beta$ ($\alpha \equiv \beta \pmod{m}$), $m | \gamma - \delta$ ($\gamma \equiv \delta \pmod{m}$), the following conditions hold

- a. $\alpha + \gamma \equiv \beta + \delta \pmod{m}$
- b. $\alpha\gamma \equiv \beta\delta \pmod{m}$
- c. $\alpha \rightarrow \gamma \equiv \beta \rightarrow \delta \pmod{m}$
- d. $-\alpha \equiv -\delta \pmod{m}$
- e. For all τ , if $\tau \in G$, τ is a zero element for G if $\tau \equiv m$.

The first four of these conditions are equivalent to the conditions of Principle 1.7. The first two follow directly from Theorems 3.5 and 3.6, as does the last one. The remaining ones follow routinely and are easy to prove. Thus, if I_m^N is \mathfrak{p} for the subalgebra \mathfrak{A} , x_1, x_2, y_1, y_2 are elements of \mathfrak{A} , and I_m^N defines mod- m groups for \mathfrak{A} , we obtain the following, equivalent, conditions

- a'. $(x_1 \cup x_2)I_m^N(y_1 \cup y_2)$
- b'. $(x_1 \cap x_2)I_m^N(y_1 \cap y_2)$
- c'. $(x_1 \rightarrow x_2)I_m^N(y_1 \rightarrow y_2)$
- d'. $(-x_1)I_m^N(-y)$
- e'. For all $z \in G$, if $z = m$, then $(z \cap x_1)I_m^N(z)$ and $(z \cup x_1)I_m^N(x_1)$, and z is the zero for G .

We next extend the structure for G to obtain a structure $\langle L, *, \cdot \rangle$ for a lattice \mathfrak{L}^n which includes Z . Then the group L for \mathfrak{L}^n is Boolean and cyclic. We begin with definitions of lattices \mathfrak{L}^n and \mathfrak{L}^z .

Definition 3.7. \mathfrak{L}^n is any lattice with n -many elements, $n \leq \omega$, and \mathfrak{L}^z is a lattice whose elements are the integers such that for \mathfrak{L}^z , L is equinumerous with Z .

It follows from this definition that if Z is the group for \mathfrak{L}^z and L is the group for \mathfrak{L}^n , $L \subseteq Z$ or $L \subset Z$, and that if $L \subset Z$, L is isomorphic to Z by the paradox of the infinite.

Theorem 3.8. L is a cyclic group.

Proof. Consider a lattice \mathfrak{L}^z defined by a structure $\langle Z, *, \cdot \rangle$, where, for every $z \in Z$, $z \leq \omega$ and Z is a Boolean ring defined on the set of integers constructed from the set N of natural numbers, addition and negation. Then for the algebra $(A, \cup, \cap, \rightarrow, -)$, if elements of A are elements of N , we obtain Z where, for all $a \in A$, if $a \cup -a = V^N$, $-a \cup -a = V^{N^+}$, and if $a \cap -a = \Lambda^N$, $-a \cap -a = \Lambda^{N^+}$. Then $-a \cap -a \leq \emptyset$ and $\{\Lambda^{N^+}\}$ is an ideal for Z , such that $\{\Lambda^{N^+}\} \leq \{\Lambda^N\}$. That is, we obtain Z by algebraic operations on elements of N and their inverses. Then the lattice \mathfrak{L}^z of the group Z of the ring Z is a Boolean algebra. Moreover, Z is cyclic. Now expand G in exactly the same way, and let L be the expansion of G . By Definition 3.7, L is equinumerous with Z , and it follows that the elements of L are exactly the elements of Z by Theorem 2.5 and Corollary 3.6.1. Then we obtain a lattice \mathfrak{L}^n defined by a structure $\langle L, *, \cdot \rangle$,

where, for every $\mathcal{L} \in \mathcal{L}$, $\mathcal{L} \leq \omega$ and L is a Boolean ring under exactly the same conditions as Z . Then L is cyclic if Z is cyclic. Since a group is cyclic if it contains some element a such that for all a^k , where $k \in \mathbb{Z}$, the group is the set of all a^k , L is cyclic if for every $\mathcal{L} \in \mathcal{L}$, $\mathcal{L} \leq \omega$, where ω obtains the filter $\{V^{N^+}\}$ and an ideal $\{\Lambda^{N^+}\}$. Then clearly L is cyclic. ■

Theorem 3.9. L is abelian.

Follows from L being cyclic.

It is most important to show that L is Boolean.

Theorem 3.10. L is a Boolean group.

Proof. We recall that, according to Principle 1.6, an algebra is Boolean if it is pseudo-Boolean and if, for all elements of the class for the algebra, the union of the element with its inverse obtain the greatest element. Then L is a Boolean group if \mathcal{Q}^n is a Boolean algebra. We have already claimed (in the proof of Theorem 3.8) that \mathcal{Q}^z is a Boolean algebra. It follows from Definition 3.7 and Theorem 3.8 that, if \mathcal{Q}^z is Boolean, so is \mathcal{Q}^n . We now show that \mathcal{Q}^z , and thus \mathcal{Q}^n , satisfy the conditions of Principle 1.6.

Let $\mathcal{Q}^z = (Z, \cup, \cap, \rightarrow, \dashv)$, where, by substitution, we obtain the structure $\langle L, *, \cdot \rangle$, where $*$ and \cdot are group addition and group multiplication, and L is the group defined on Z by Definition 3.7. We recall that Z was obtained as an extension of N . Thus, if G is Boolean, L is Boolean, and L is an elementary extension of G . Then if $N \subset Z$, $G \subset L$, and for Z Boolean, L is Boolean. Moreover, we proved that \mathcal{R} is Boolean (Theorem 2.5). If \mathcal{R} is Boolean, then so is \mathcal{Q}^n . We say, then, that \mathcal{Q}^n is Boolean if, for any $n_L \in L$, $-n_L = n_L \rightarrow \Lambda$. The zero element for \mathcal{Q}^n is the zero for Z , and is associated to the group element $e \in L$. It is also easy to show that, for all $n_L \in L$, $n_L \cup -n_L = V^{N^+}$. ■

One may also show that Z is Boolean for a ring $\langle Z, +, \cdot \rangle$, and that, therefore, L is Boolean for the ring $\langle L, *, \cdot \rangle$.

We next have to prove that \mathcal{Q}^n has a greatest element V^{N^+} for \mathcal{Q}^n Boolean.

Theorem 3.11. Let ω_L^+ be V^{N^+} for \mathcal{Q}^n if, for $\{x_L | x_L \in L \rightarrow x \leq \omega_L\}$. Then V^{N^+} is the greatest element for \mathcal{Q}^n if $\omega_L^+ = x \cdot x$.

Proof. We note that Z obtains the structure $\mathcal{Q}^z = \langle Z, *, \cdot \rangle$, and that G obtains the structure $\mathcal{Q}^n = \langle G, *, \cdot \rangle$. Then for all $n_z \in Z$, there is an element $n_L \in L$ corresponding to $n_z \in Z$ and $\text{Cl}(n_L \cdot n_L)$. If ω_z is sup for Z , there is some $\omega_L \in L$ such that ω_L is the sup for the lattice of the group L . Suppose ω_L is infinite (clearly ω_L is infinite if ω_z is infinite). Now define ω_L^+ as the element obtained by $\text{Cl}(\omega_L \cdot \omega_L)$. But if ω_L is infinite, then $\omega_L^+ = \omega_L \cdot \omega_L = \omega_L$. Then V^{N^+} exists for L . ■

Theorem 3.12. Let ω_L^- be Λ^{N^+} for \mathcal{Q}^n if for $\{-x_L | -x_L \in L \rightarrow -x \leq -\omega_L\}$. Then V^{N^+} is the least element for \mathcal{Q}^n if $-\omega = x \cdot -x$.

This theorem is the dual of the previous theorem, and its proof is thus the dual of the previous proof.

Theorem 3.13. For $\omega_Z \in Z$, if $\omega_Z = \sup(Z)$, Z has a greatest element and Z is infinite. Let ω_Z correspond to ω_L for $\omega_L \in L$. Then there is a $\omega_Z \in Z$ for Z closed under addition and multiplication, where $\omega_Z \cdot \omega_Z$ in $\langle Z, +, \cdot \rangle$ is ω_Z^+ . Then there is a ω_L^+ for L closed under group addition and multiplication, where $\omega_L \cdot \omega_L$ in $\langle L, *, \cdot \rangle$ is ω_L^+ . Then $\omega_L^+ = \omega_L \cdot \omega_L = \omega_L$. Then L is an infinite cyclic group closed under group addition and multiplication.

Proof. Follows directly from Theorems 3.11 and 3.12.

L is a Boolean group defined on the integers. It is standard that the integers closed under addition is an infinite cyclic group.

We next prove that L closed under multiplication is infinite cyclic. Recall that any group C is cyclic if, for any $n_L \in L$, n_L is the period of C and x is the generator of C such that $x^{n_L} = e$ and $e, x, x^2, \dots, x^{n-1} \in C$, with e the identity element. Let $n_L \leq \omega_L$. Let $x^{n_L} = e$ and $-x^{n_L} = e$. If $\omega_L^+ = \omega_L \cdot \omega_L$, we obtain $\omega_L^+ = e$ for $x^{n-1} \cdot x^{n-1}$. Then $\omega_L^+ = x^{n_L}$. Now recall that a cyclic group is infinite if, for any $x \in C$, x and $-x$ are generators for C . Also note that for a group $[x]$ generated by x , $[x] = C$, C is infinite when for all x^m , $x^n \neq x^v$ if $u \neq v$ and $u, v \in Z$. Recall too that L is a Boolean ring closed under addition and multiplication. If L^{-1} is the set of invertibles of the ring L with unity, then L^{-1} is a multiplicative group. Let $m_L^+, n_L^+ \in L^{-1}$. Then $(m_L^+ \cdot n_L^+)^{-1} = m_L^- \cdot n_L^- = (m_L \cdot n_L)^{-1}$ and $(m_L \cdot n_L)^{-1} \in L$. We also note that for all $m_L^+, n_L^+ \in L$, $m_L^-, n_L^- \in L$, and that multiplication of inverses of m_L^+ and n_L^+ obtain the same product in L as do multiplication of m_L^- and n_L^- . Now let $n_L \leq \omega_L^+$. Then $\omega_L^+ \cdot \omega_L^+ = \omega_L^- \cdot \omega_L^-$ where ω_L^- is the inverse of ω_L^+ , and in each case we obtain $x^{n-1} \cdot x^{n-1}$, where $x^{n-1} \cdot x^{n-1}$ gives us our zero element if $\omega_L^+ = e$ for $x^{n-1} \cdot x^{n-1}$, with $\omega_L^+ = x^{n_L}$. For both ω_L^+ and ω_L^- generators of L , we obtain the same product, and in each case identity is preserved. ■

Remark. Z under multiplication is a group iff there is a subset of Z under group multiplication which is a group. Then if H is a group I is a subgroup of H if, for any $i_\alpha, i_\beta \in I$, $i_\alpha i_\beta \in I$, and $i_\alpha i_\beta \equiv h$ where $h \in H$, and if the zero of H is a zero of I . Suppose $\alpha \cdot \beta = (n-1)_Z$ for the mod- n_Z group Z . Then we define the zero for Z under multiplication as n_Z for $\alpha\beta/n_Z$, such that $n_Z = 0$. Clearly, the same consideration obtains for subgroups of L .

Example. $\langle 0, 1, 2, \cdot \rangle$ is a group if $\langle 1, 2, \cdot \rangle$ is a subgroup for $\langle 0, 1, 2, \cdot \rangle$, as indicated by the following table:

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

We finally prove that the Boolean group L is a Boolean ring isomorphic with the ring of integers.

Theorem 3.14. $\mathfrak{Q}^m + \mathfrak{Q}^k = \|\mathbb{L}^m/\mathbb{L}^k\|$, where $\mathfrak{Q}^m, \mathfrak{Q}^k$ are Boolean lattices of m -many and k -many elements respectively.

Proof. Let $m+k=n$, $n \leq \omega_L^+$. Suppose both \mathcal{Q}^m and \mathcal{Q}^k are quotient algebras. Then for any $\alpha, \beta \in L/p$, $[\alpha] \cup [\beta] = [\alpha \cup \beta]$, $[\alpha] \cap [\beta] = [\alpha \cap \beta]$, $[\alpha] \rightarrow [\beta] = [\alpha \rightarrow \beta]$, $-[\alpha] = [-\alpha]$, and $\alpha \in [V]$ iff $\alpha \in \nabla$. We obtain a partition $n/m=k$, $n/k=m$. Let the additive property hold between elements of \mathcal{Q}^m , \mathcal{Q}^k , such that, for all $\alpha, \beta \in L/p$, $\alpha = m_\alpha + k_\alpha$, $\beta = m_\beta + k_\beta$. Then the power of the sum of lattices \mathcal{Q}^m and \mathcal{Q}^k has a value determined by the number of elements of groups of any modulus m , k , $m+k=n$, $n \leq \omega_L^+$. ■

Theorem 3.15. $\mathcal{Q}^n = \langle L, *, \cdot \rangle$.

Proof. Let $n=m+k$. Then $\mathcal{Q}^n = \mathcal{Q}^m + \mathcal{Q}^k$ by the previous theorem. For $n \leq \omega_L^+$ and $n_Z \leq \omega_Z^+$, we obtain a ring \mathcal{Q}^n of integers, such that $Cl(x_L * y_L)$, $Cl(x_L \cdot y_L)$ for all $x_L, y_L \in L$, L the expansion of the Boolean group G by the integers. Then \mathcal{Q}^n is the ring defined on the Boolean group L . ■

Corollary 3.15.1. \mathcal{Q}^n is a Boolean ring.

Proof. Follows directly from Theorem 3.15.

Theorem 3.16. $\mathcal{Q}^n \cong \mathfrak{R}$ for \mathfrak{R} the ring of integers and \mathcal{Q}^n the Boolean ring for the group L .

Proof. The lattice \mathcal{Q}^n is just the lattice \mathcal{Q}^Z where for all $n_L \in L$, n_L is associated to an $n_Z \in Z$. Recall that \mathcal{Q}^Z is given by the structure $\langle Z, +, \cdot \rangle$, \mathcal{Q}^n by $\langle L, *, \cdot \rangle$, and that L is the natural extension of G to the integers. We know that a Boolean ring with a unit element is equivalent to a Boolean algebra. For the Boolean algebra \mathcal{Q}^n , the ring of integers is a Boolean algebra if the ring is Boolean. Say \mathcal{Q}^Z is the natural extension of \mathcal{Q}^n for the group G and the elements of Z . If so, then \mathcal{Q}^Z is the ring \mathfrak{R} or \mathcal{Q}^Z is a subring of \mathfrak{R} .

Case I: If $\mathcal{Q}^Z = \mathfrak{R}$, then $\mathcal{Q}^n \cong \mathfrak{R}^Z$ such that $\mathcal{Q}^n \cong \mathfrak{R}$.

Case II: Suppose \mathcal{Q}^Z is a subring of \mathfrak{R} . We know that two groups are isomorphic which have the same order. Then if any two groups have the same residue, they are isomorphic. Moreover, we know that infinite groups, such as Z , may be isomorphic to other infinite groups, provided they satisfy the condition of having the same residue. We also know that, for a group H , I is a subgroup of H if, for any $i_\alpha, i_\beta \in I$, $i_\alpha i_\beta \in I$ is equivalent to a product $h \in H$, and if the zero of H is the zero of I . Then if \mathcal{Q}^Z is a subring of \mathfrak{R} , we suppose that L is a subgroup of Z . But we recall from Theorem 3.13 that for $\omega_Z \sup(\mathcal{Q}^Z)$, there corresponds a ω_L for L , and that $\omega_L^+ = \omega_L \cdot \omega_L = \omega_L$, whereby L is an infinite cyclic group. We also recall that Z is the infinite cyclic group, and that all infinite cyclic groups are isomorphic with Z . Consider now the rings \mathcal{Q}^n and \mathfrak{R} . We note that for some homomorphism θ of \mathcal{Q}^n into \mathfrak{R} , there exists a kernel $\ker \theta$ for \mathcal{Q}^n , \mathfrak{R} , such that $\ker \theta$ is the set of all $n_L \in \mathcal{Q}^n$, $\theta(n_L) = (0)$, where 0 is the zero of \mathfrak{R} . Now let \mathcal{Q}^n be an ideal of \mathcal{Q}^Z . Then for \mathcal{Q}^n the kernel of \mathcal{Q}^Z , by the homomorphism of $\mathcal{Q}^Z \cong \mathfrak{R}$, $\mathcal{Q}^Z/\mathcal{Q}^n \cong \mathfrak{R}$. But by Theorem 3.13, we obtain $\omega_L^+ = \omega_Z^+$. Then if $\mathcal{Q}^Z/\mathcal{Q}^n \cong \mathfrak{R}$, we obtain for $\mathcal{Q}^Z/\mathcal{Q}^n$ the zero, and $\mathcal{Q}^Z = \mathcal{Q}^n$, so that, if $\mathcal{Q}^Z \cong \mathfrak{R}$, $\mathcal{Q}^n \cong \mathfrak{R}$. ■

Remark. Halmos [2] has defined a Boolean group as an (additive) abelian group in which every element has order two, i.e. $\forall p(p+p=0)$. We note that the \mathcal{L} -group

defined by Birkhoff [1] is also an additive group, and very close to that defined by Halmos. Our own work has shown that we may remove the restriction from Halmos's definition and define a Boolean group as an abelian group which is infinite cyclic under addition and multiplication. Halmos asks in the same place whether every Boolean group is the additive group of some Boolean ring. Theorems 3.15, 3.16, and Corollary 3.15.1 answer this question.

References

- [1] Garrett David BIRKHOFF, **Lattice Theory**. Vol. 25, Colloquium Publications; Providence: American Mathematical Society, 3rd edition, 1967.
- [2] Paul R. HALMOS, **Lectures on Boolean Algebras**. New York, Heidelberg, Berlin: Springer-Verlag, 1974.
- [3] Pierre SAMUEL, „Modèles Booléens et Hypothèse du continu“, **Séminaire Bourbaki**, vol. 1966/1967, Exposé 317–03. New York & Amsterdam: W. A. Benjamin, Inc., 1968.