Definition 1. A ring B is *boolean* if for all $b \in B$, $b^2 = b$.

Remark 1. For each b in a boolean ring B, $b + b = 0$. Furthermore, $b(1 + b) = 0$ and B is commutative.

Proof. Let $b \in B$. Then $4b = 4b^2 = (2b)^2 = 2b$. Thus $b + b + b + b = b + b$ and so $b + b = 0$. Therefore, $b(1 + b) = b + b^2 = b + b = 0$.

Finally, let $a, b \in B$. Then $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$. Thus $ab + ba = 0$ and so $ab = ba$. □

Definition 2. An element $s \in B$ is *singular* if $(s) = \{0, s\}$.

Proposition 1. Let B be a boolean ring. Then there exists a singular element of B.

Proof. Let us create a partial order on B by $a \leq b$ if $a = ab$. First we will show this is in fact a partial ordering:

1. Reflexivity: For all $b \in B$, $b = bb$, and so $b \leq b$.
2. Antisymmetry: Let $a, b \in B$ such that $a \leq b$ and $b \leq b$. Then $a = ab$ and $b = ba$. Since B is commutative, this means $a = b$.
3. Transitivity: Let $a, b, c \in B$ be such that $a \leq b$ and $b \leq c$. Then $a = ab$ and $b = bc$. Then $a = ab = a(bc) = (ab)c = ac$ and so $a \leq c$.

Thus this truly is a partial ordering. Note 0 is the least element under this ordering and 1 is the greatest element. Note that for all $a, b \in B$, $ab \leq a$. This is because $ab = aba$.

Since 0 is the least element of B, 0 is also a minimal element. Therefore by Zorn's Lemma there must also be a minimal element of $B \setminus \{0\}$. Call such an element s. Then for all $b \in B \setminus \{0\}$, $s \leq b$ or s and b are not comparable. In the former case, $s = sb$. In the latter case, $s \neq sb$ and so $sb < s$, which can only happen when $sb = 0$ since s is a minimal element of $B \setminus \{0\}$. Thus for all $b \in B$, sb is either s or 0 and so $(s) = \{0, s\}$ and thus s is singular. □

Remark 2. Let $a, b \in B$ be such that $ab = 0$. Then $a \leq a + b$. Furthermore, for all $s \in B$ singular, $1 + s$ is a maximal element of $B \setminus \{1\}$.

Proof. Let a, b be as above. Then $a = a + 0 = a^2 + ab = a(a + b)$. Thus $a \leq a + b$. Now let s be singular and let $b \in B$ be such that $1 + s \leq b$. then $1 + s = (1 + s)b = b + sb$. Since s is singular, sb is either 0 or s. In the case $sb = 0$, then $1 + s = b$. In the case $sb = s$, then $1 + s = b + s$ and so $b = 1$. Thus $1 + s$ is a maximal element of $B \setminus \{1\}$. □

Proposition 2. Let B be a boolean ring. Then B is a Bézout domain: every finitely-generated ideal of B is principal.

Proof. Let (a, b) be the ideal of B generated by a and b. Then we claim $(a, b) = (a+b+ab)$. First note that clearly $a + b + ab \in (a, b)$, so we have one inclusion. Also, $(a + b + ab)a = a^2 + ab + ab^2 = a + ab + ab = a$, so $a \in (a + b + ab)$. Similarly $b \in (a + b + ab)$. Thus we have equality $(a, b) = (a + b + ab)$.

Now let $(b_1, \ldots, b_n)$ be a finitely-generated ideal. Then $(b_1, \ldots, b_{n-1}) \subseteq (b_1, \ldots, b_n)$ is a principally generated ideal, generated by b. Then $(b_1, \ldots, b_n) = (b, b_n) = (b + b_n + bb_n)$ and so every finitely generated ideal is principal. □

Proposition 3. Let $A \subseteq B$. Then A has an infimum in B.

Proof. Let $L(A)$ be the set of lower bounds of A. That is,

$$L(A) = \{\ell \in B : \ell \leq a \text{ for all } a \in A\}.$$

Note $L(A) \neq \varnothing$ because $0 \in L(A)$. We will show that $L(A)$ has a greatest element.

Note we can also define $L(A)$ as

$$L(A) = \{\ell \in B : \ell = \ell a \text{ for all } a \in A\}.$$

So $\ell \in L(A)$ if and only if $\ell(1+a) = 0$, so $\ell \in \text{Ann}(1+A)$. Note this makes $L(A)$ a subgroup of B. Furthermore, for $\ell \in L(A)$, $b \in B$ and $a \in A$, $\ell b = \ell ba$ and so $\ell b \in L(A)$. Thus $L(A)$ is an ideal of B. □

Note that $ab = \inf\{a, b\}$ and $a + b + ab = \sup\{a, b\}$. To see this, let $\ell \leq a$ and $\ell \leq b$. Then $\ell = \ell a = \ell b$. So $\ell = \ell ab$ and so $\ell \leq ab$. Now note $a = a(a + b + ab)$ and so $a \leq a + b + ab$ and similarly $b \leq a + b + ab$. Let $a \leq g$ and $b \leq g$. Then $a = ag$ and $b = bg$. Then $ab = abg$, so $a + b + ab = ag + bg + abg = (a + b + ab)g$ and so $a + b + ab \leq g$.

We can also define $a \Rightarrow b = \sup\{b, 1 + a\} = 1 + a + ab$. Note then that

$$a \leq (b \Rightarrow c) \text{ iff } ab \leq c.$$

To see this, first let $a \leq (b \Rightarrow c)$. Then $a = a(1 + b + bc) = a + ab + abc$. Then $0 = ab + abc$ and so $ab = abc$, so $ab \leq c$. Now suppose $ab \leq c$. Then $ab = abc$ and so $0 = ab + abc$ and so $a = a + ab + abc = a(1 + b + bc) = a(b \Rightarrow c)$. Thus $a \leq (b \Rightarrow c)$.

Lemma 1. Let $b \neq 0 \in B$. Then there exists a ring homomorhpism $f : B \to \mathbb{Z}/2\mathbb{Z}$ such that $f(b) \neq 0$.

Proof. Let $\{(b_\gamma)\}_{\gamma\in\Gamma}$ be a chain of proper ideals containing $1+b$. We know that such a chain exists because $L(\{1+b\})$ is an ideal. Let $I = \bigcup_{\gamma\in\Gamma}(b_\gamma)$. Since $1 \notin (b_\gamma)$ for all $\gamma \in \Gamma$, it follows $1 \notin I$ and so I is a proper ideal of B and is a maximal element of the chain. Therefore, by Zorn's lemma there is a maximal ideal $\mathfrak{m}$ containing $1 + b$. We also have $b \notin \mathfrak{m}$ because then $b + 1 + b = 1 \in \mathfrak{m}$, and $\mathfrak{m}$ would not be proper. Therefore for every $b \neq 0$ there exists a maximal ideal not containing b. Hence there exits a homomorphism $f : B \to \mathbb{Z}/2\mathbb{Z}$ defined by

$$f(a) = \begin{cases} 0 & a \in \mathfrak{m} \\ 1 & a \notin \mathfrak{m} \end{cases}.$$

□

In his 1966 master's thesis *Boolean algebras and their topological duals*, Edward Walsh defines a topology on $\mathcal{P}(X) = \{0,1\}^X$ for a set X by giving $\{0,1\}$ the discrete topology and giving $\mathcal{P}(X)$ the product topology. We will explore this topology in detail.

Note that when X is finite, $\mathcal{P}(X)$ has the discrete topology. We will show that each singleton $\{U\} \subseteq \mathcal{P}(X)$ is open. Let $U = (\alpha_x)_{x\in X} \in \{0,1\}^X = \mathcal{P}(X)$ where $\alpha_x \in \{0,1\}$. For $x \in X$, let $\pi_x : \mathcal{P}(X) \to \{0,1\}$ be the projection from the x coordinate of X. That is, $\pi_x(S) = \pi(S)(x)$ under the natural correspondence $\pi : \mathcal{P}(X) \to \mathrm{Hom}_{\mathrm{Set}}(X, \{0,1\})$ where

$$\pi(S)(x) = \begin{cases} 0 & x \notin S \\ 1 & x \in S \end{cases}.$$

Then $\pi_x^{-1}(\alpha_x) = \{\alpha_x\} \times \{0,1\}^{X\setminus\{x\}}$, which is open since projections are continuous and $\{\alpha_x\} \subseteq \{0,1\}$ is open. Thus

$$\{(\alpha_x)_{x\in X}\} = \bigcap_{x\in X} \pi_x^{-1}(\alpha_x)$$

is a finite intersection of open sets and is thus open. Therefore $\mathcal{P}(X)$ has the discrete topology.

Even in the case X is not finite, we can still describe the topology on $\mathcal{P}(X)$ more generally. We can choose finitely many coordinates $x_1, \ldots, x_n \in X$ and values $\alpha_1, \ldots, \alpha_n \in \{0,1\}$ to ascribe to these coordinates. Then we get an open neighborhood consisting of all elements of $\mathcal{P}(X)$ having the assigned values at the assigned coordinates. For example, if $X = \mathbb{N}$ and our finite coordinates are $x_i = i$ for $i \leq 3$ and our assigned values are $\alpha_0 = 0$, $\alpha_1 = 1$, $\alpha_2 = 0$, and $\alpha_3 = 1$, then the set of all elements of $\{0,1\}^{\mathbb{N}}$ beginning with $(0,1,0,1,\ldots)$ is open. Translating this into the language of $\mathcal{P}(\mathbb{N})$, the set of all subsets of $\mathbb{N}$ that **don't** contain 0 or 2 and **do** contain 1 and 3 is open. We can denote this subset $U(\{1,3\},\{0,2\})$.

For general X and $F, G \subseteq X$, we can construct the basic open sets of $\mathcal{P}(X)$ as $U(F,G)$ defined as

$$U(F,G) = \{S \in \mathcal{P}(X) : F \subseteq S, S \cap G = \varnothing\}.$$

Note that when $F \cap G \neq \varnothing$, then $U(F,G) = \varnothing$. Also, when $F \cap G = \varnothing$, $F \in U(F,G)$. Furthermore, $U(\varnothing,\varnothing) = \mathcal{P}(X)$. Open sets of this form constitute a basis: they cover $\mathcal{P}(X)$ (for example $U(\{x\},\varnothing) \cup U(\varnothing,\{x\}) = \mathcal{P}(X)$ for $x \in X$) and for $S \in U(F,G) \cap U(H,J)$, $S \in U(F \cup H, G \cup J) \subseteq U(F,G) \cap U(H,J)$.

For $F, G \neq \varnothing$, $U(G,F) \subseteq \mathcal{P}(X) \setminus U(F,G)$, but the reverse is not necessarily true.

For $x \in X$ and $\alpha \in \{0,1\}$, sets of the form $U_{x,\alpha} = \{S \in \mathcal{P}(X) : S(x) = \alpha\}$ are simultaneously open and closed. When $\alpha = 0$, $U_{x,\alpha} = U(\varnothing,\{x\})$ and when $\alpha = 1$, $U_{x,\alpha} = U(\{x\},\varnothing)$. These are each other's complements (subsets and **do** contain x versus subsets that **don't** contain x) so both are open and closed. In fact, these clopen sets form a basis for the topology on $\mathcal{P}(X)$. For $F \cap G = \varnothing$,

$$U(F,G) = \bigcup_{f\in F} U_{f,1} \cup \bigcup_{g\in G} U_{g,0}.$$

Also $\mathcal{P}(X)$ is Hausdorff. Let $A, B \in \mathcal{P}(X)$ where $A \neq B$. Without loss of generality, let $a \in A \cap (X \setminus B)$. Then $A \in U_{a,1}$ and $B \in U_{a,0}$, separating A and B. When clopen sets

form a basis for a topology like this, the space is called totally disconnected. Furthermore, Tychonoff's theorem shows that $\mathcal{P}(X)$ is compact. (The product of any collection of compact topological spaces is compact with respect to the product topology.) A Hausdorff, compact, totally disconnected space is called a **boolean space**.

Finally, we will move on to the definition of an F-algebra of a set X. (Walsh calls this a "field" or "field of sets" but that name is no good.)

Definition 3. Let X be a set. A class of subsets V of X is an F-algebra of X if V is closed under finite union, intersection, and complements. Furthermore, V is separating if for any distinct points $x, y \in X$, there exists an $A \in V$ such that $x \in A$ and $y \in X \setminus A$.

The clopen subsets C of $\mathcal{P}(X)$ form an F-algebra. To see this, take $U_1, U_2 \in C$. Then $U_1 \cup U_2$ is open, and it is closed because its complement is the intersection of two open sets. Similarly, $U_1 \cap U_2$ is closed, and it is open because its complement is the union of two closed sets. Also remember $X \setminus U_1$ is clopen, so it is in C as well. In fact, C is a separating F-algebra. Let $x, y \in X$ be distinct. Then $A = U_{x,1} \cap U_{y,0} \in C$ because it is the intersection of two clopen sets.

Lemma 2. If P is a compact Hausdorff space and if V is a separating F-algebra of clopen sets of P then P is totally disconnected (thus boolean) and V is the F-algebra of all clopen subsets of P

Proof. We will follow the argument from Walsh's thesis. The proof is dependent upon the fact that since V separates points, it also separates points and closed sets. To verify this assertion, let F be closed in P, $F \neq P$ and suppose $p_0 \notin F$. V separates points in P, so that for each point $q \in F$, there exist disjoint clopen sets C_q, $q \in C_q$ and D_q, $p_0 \in D_q$. The collection $\{C_q\}_{q \in F}$ covers F so that by compactness there exists a finite subcover made up of members of $\{C_q\}_{q \in F}$. The union C of this subcollection contains F and, being a finite union, is clopen. Each member C_q of this subcollection corresponds to some D_q and $C_q \cap D_q = \varnothing$. Therefore, if the intersection D of the finite collection of D_q's corresponding to the C_q's of the finite subcover of F is considered, D is clopen and disjoint from C. Thus V separates points and closed sets.

Now since every open set is the complement of a closed one, the preceding paragraph implies that V is a basis for P, and thus P is boolean. Let G be an arbitrary clopen set in X. Since G is both compact and open it is a finite union of members of V. But V is closed under finite unions. Hence G is in V. □

Proposition 4. Let B be a boolean ring. Then $B \cong (\mathcal{P}(\mathrm{Hom}(B, \mathbb{Z}/2\mathbb{Z})), + = \triangle, \cdot = \cap)$, where $\triangle$ represents the symmetric difference. Note $\mathrm{Hom}(B, \mathbb{Z}/2\mathbb{Z})$ does not include the trivial map $f(1) = 0$.

Proof. We will denote $P = (\mathcal{P}(\mathrm{Hom}(B, \mathbb{Z}/2\mathbb{Z})), + = \triangle, \cdot = \cap)$. First let us construct a ring homomorphism $\varphi : B \to P$ by

$$\varphi(b) = \{f : B \to \mathbb{Z}/2\mathbb{Z} : f(b) = 1\}.$$

Note that $\varphi(0) = \varnothing$ and $\varphi(1) = \text{Hom}(B, \mathbb{Z}/2\mathbb{Z})$. We will show that φ is a ring homomorphism. Let $a, b \in B$. Then

$$\varphi(a+b) = \{f : B \to \mathbb{Z}/2\mathbb{Z} : f(a+b) = 1\} = \{f : B \to \mathbb{Z}/2\mathbb{Z} : f(a) + f(b) = 1\}$$
$$= \{f : B \to \mathbb{Z}/2\mathbb{Z} : f(a) = 1\} \triangle \{f : B \to \mathbb{Z}/2\mathbb{Z} : f(b) = 1\} = \varphi(a) + \varphi(b).$$

Furthermore,

$$\varphi(ab) = \{f : B \to \mathbb{Z}/2\mathbb{Z} : f(ab) = 1\} = \{f : B \to \mathbb{Z}/2\mathbb{Z} : f(a)f(b) = 1\}$$
$$= \{f : B \to \mathbb{Z}/2\mathbb{Z} : f(a) = 1\} \cap \{f : B \to \mathbb{Z}/2\mathbb{Z} : f(b) = 1\} = \varphi(a)\varphi(b).$$

Thus φ is a ring homomorphism.

Now we will define $\psi : P \to B$. First, we must show that for all ring homomorphisms $f : B \to \mathbb{Z}/2\mathbb{Z}$, the set $U(f) = \{b \in B : f(b) = 1\}$ has a least element under the partial ordering. Let $a, b \in U(f)$, then $ab \in U(f)$ and $ab \leq a, b$. We also know that $0 \notin U(f)$.

Note that if $b \in B$ is such that $f(b) = 0$, then $f(a) = 0$ for all $a \leq b$. This is because $a = ab$ and so $f(a) = f(ab) = f(a)f(b) = f(a) \cdot 0 = 0$.

Since $U(f) \subseteq B$, $U(f)$ must have at least one minimal element. Suppose there was more than one minimal element of $U(f)$, with a and b being two distinct minimal elements. Then $ab \in U(f)$ but $ab \leq a, b$ and so a and b cannot be minimal elements of $U(f)$. Therefore $U(f)$ has a *unique* minimal element m. In fact, m is the *least* element of $U(f)$. Let $b \in U(f)$. We will show $m \leq b$. If $m \not\leq b$, then $m \neq mb$, but $mb \leq m$ and $mb \in U(f)$, and so m cannot be minimal. Thus m is least. For $f : B \to \mathbb{Z}/2\mathbb{Z}$, define $\ell(f)$ to be the least element of $U(f)$.

We need to show that φ is injective and surjective. First we will show $\ker \varphi = 0$. Suppose $\{f : B \to \mathbb{Z}/2\mathbb{Z} : f(b) = 1\} = \varnothing$. Then from Lemma 1 we know that $b = 0$ and so $\ker \varphi = 0$.

Now we will show surjectivity. Note that since the image of a boolean homomorphism is always a boolean ring, the clopen sets of the form $\{f : f(b) = 1\}$ constitute an F-algebra. Since two distinct homomorphisms must disagree on some element of B (injectivity), the F-algebra is separating and thus by Lemma 2, this F-algebra is all of P. Hence φ is surjective. □

Proposition 5. The ring isomorphism φ respects the partial ordering. That is, for all $a, b \in B$, $a \leq b$ if and only if $\varphi(a) \subseteq \varphi(b)$.

Proof. First let $a \leq b$. Then $a = ab$. Now let $f \in \varphi(a)$, so $f(a) = 1$. Then $f(a) = f(ab) = f(a)f(b) = 1$ and so $f(b) = 1$. Thus $f \in \varphi(b)$ and so $\varphi(a) \subseteq \varphi(b)$.

Now suppose $a \not\leq b$. We will show that $\varphi(a) \not\subseteq \varphi(b)$ by demonstrating that there exists an $f : B \to \mathbb{Z}/2\mathbb{Z}$ such that $f(a) = 1$ and $f(b) = 0$. We will start by considering $\sup\{1 + a, b\} = 1 + a + b + (1 + a)b = 1 + a + b + b + ab = 1 + a + ab \neq 1$ since $ab \neq a$. Then there exists a maximal ideal $\mathfrak{m}$ such that $\sup\{1 + a, b\} \in \mathfrak{m}$ and therefore $1 + a, b \in \mathfrak{m}$ and $a \notin \mathfrak{m}$. Since $\mathfrak{m}$ is the kernel of some map $f : B \to \mathbb{Z}/2\mathbb{Z}$ we know that $f(b) = 0$ since $b \in \mathfrak{m} = \ker f$ and $f(a) \neq 0$ since $a \notin \mathfrak{m} \ker f$. Specifically, we can define f as

$$f(p) = \begin{cases} 0 & p \in \mathfrak{m} \\ 1 & p \notin \mathfrak{m} \end{cases}.$$

Thus $f \in \varphi(a)$ and $f \notin \varphi(b)$. Therefore $\varphi(a) \not\subseteq \varphi(b)$. □

The subset of $\mathcal{P}(\mathbb{N})$ comprising only finite and cofinite (complement is finite) subsets of $\mathbb{N}$ is a countably infinite boolean ring!