Boolean rings

In this talk, we are going to define Boolean rings and study their structure.

1 preliminaries

Definition 1. A ring $R$ is said to be a subdirect product (or sum) of the family of rings $\{ R_i \mid i \in I \}$ if $R$ is a subring of the direct product $\prod_{i \in I} R_i$ such that $\pi_k(R) = R_k$ for all $k \in I$, where $\pi_k : \prod_{i \in I} R_i \to R_k$ is the canonical epimorphism.

Example 1. The direct product $\prod_{i \in I} R_i$ is itself a subdirect product of the rings $R_i$. There could be other subdirect products of the rings $R_i$. If a ring $R$ is isomorphic to a subdirect product $T$ of rings $R_i, i \in I$, $T$ may be called a representation of $R$ as a subdirect product of the rings $R_i$.

Theorem 1. A ring $R$ has a representation as a subdirect product of rings $R_i, i \in I$ iff for each $i \in I$, there exists an epimorphism $\phi_i : R \to R_i$ such that if $r \neq 0$ in $R$, then $\phi_i(r) \neq 0$ for at least one $i \in I$.

Example 2. The ring $\mathbb{Z}$ is a subdirect product of the fields $\mathbb{Z}_p$ for all prime numbers $p$. To prove this, let $\phi_p : \mathbb{Z} \to \mathbb{Z}_p$ be the canonical epimorphism $\phi_p(n) = n(mod p) = [n]_p$. If $r \neq 0$ in $\mathbb{Z}$, then $r$ can not be a multiple of all primes $p \in \mathbb{Z}$, and hence there is at least one prime number $p$ such that $\phi_p(r) \neq 0$. Then, by Theorem 1, $\mathbb{Z}$ is a subdirect product of the fields $\mathbb{Z}_p$.

Definition 2. A ring $R$ is subdirectly irreducible if the intersection of all nonzero ideals of $R$ is not $\{0\}$.

Example 3. A nonzero simple ring $R$ has no proper nonzero ideals, and hence the intersection of all nonzero ideals is $R \neq \{0\}$. Thus, a nonzero simple ring is subdirectly irreducible. Consequently, any division ring is subdirectly irreducible.
Proposition 1. Let $R$ be a subdirectly irreducible ring with identity and let $e$ be a central idempotent in $R$. Then $e = 0$ or $e = 1$.

Proof. Suppose $e$ is a central idempotent element with $e \neq 0$ and $e \neq 1$. Let $A = eR$. $A$ is two-sided ideal since $e$ is central. Since $e^2 = e \neq 0$ and $e^2 \in A$, then $A \neq \{0\}$.

Since $e \neq 1$ and $e$ is central, then there exists $r \in R$ such that $r - er \neq 0$. Let $B = \{r - er | r \in R\}$. Then $B \neq \{0\}$. Since $e$ is central, then $B$ is two-sided ideal.

Now, we will show that $A \cap B = \{0\}$:

Let $x \in A \cap B$, then $x = er = r' - er'$ and $e^2r = er' - e^2r'$ which implies that $er = er' - er' = 0$. Thus $x = 0$.

Since $A \neq \{0\}$ and $B \neq \{0\}$, then $\bigcap(\text{all non zero ideals}) \subseteq A \cap B$, and hence $\bigcap(\text{all non zero ideals}) = \{0\}$ which contradicts the hypothesis that $R$ is subdirectly irreducible. Therefore,

$$e = 0 \quad \text{or} \quad e = 1.$$ 

\[\square\]

Theorem 2 (Birkhoff’s Theorem). Every ring is isomorphic to a subdirect product of subdirectly irreducible rings.

2 Structure of Boolean rings

Definition 3. A Boolean ring is a ring in which every element is idempotent; that is, $x^2 = x$ for all $x \in R$.

Remark 1. A subring of a Boolean ring is Boolean. Furthermore, a homomorphic image of a Boolean ring is also Boolean.

Proof. Let $S$ be a subring of the Boolean ring $R$. Then, for every $x \in S$, $x$ is an element of $R$ and hence $x$ is idempotent. Therefore $S$ is Boolean.

Let $T$ be a homomorphic image of $R$ where $\pi : T \to R$ is a ring epimorphism.

Let $t \in T$, then $t = \pi(r)$ for some $r \in R$. Hence,

$$t^2 = \pi(r)\pi(r) = \pi(r^2) = \pi(r) = t.$$ 

Thus every element of $T$ is idempotent. Therefore, $T$ is Boolean. \[\square\]
Lemma 1. Let $R$ be a Boolean ring. Then $\text{char}(R) = 2$.

Proof. Let $x \in R$. Then $x^2 = x$ and $(x+x)^2 = x+x$ which implies that $x^2+2x+x^2 = x+x$ and hence $2x = 0$. Thus, $\text{char}(R) = 2$. It follows then that $x = -x$ for all $x \in R$. \qed

Lemma 2. If a ring $R$ is Boolean, then $R$ is commutative.

Proof. Let $x, y \in R$; we want to show that $xy = yx$. Since $R$ is Boolean, then $x^2 = x$ and $y^2 = y$. Now,

$$x + y = (x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y.$$

Therefore, $xy = -yx$. Using the previous lemma, we have $x = -x$ for every $x$ in $R$. Hence, $xy = yx$. \qed

Proposition 2. Let $R$ be a field. If $R$ is Boolean, then $R \cong \mathbb{Z}_2$.

Proof. Let $x \in R$ and $x \neq 0$. Then $x^2 = x$ which implies that $x(x-1) = 0$. But $x^{-1}$ exists, thus $x = 1$. Therefore, $R = \{0, 1\} \cong \mathbb{Z}_2$. \qed

Proposition 3. Let $R$ be a Boolean ring with identity. Then every prime ideal is maximal in $R$.

Proof. Let $P$ be a prime ideal of $R$. To show that $P$ is maximal, we will show that $R/P$ is a field.

Let $x + P \in R/P$ where $x + P \neq P$; that is, $x \notin P$. We have

$$(x + P)^2 = x^2 + P = x + P,$$

and hence $x^2 - x \in P$ which gives that $x(x-1) \in P$. Since $x \notin P$ and $P$ is prime ideal, then $x-1 \in P$. Thus $x + P = 1 + P$. Therefore, $R/P = \{P, 1 + P\}$ and hence $R/P$ is a field. This completes the proof. \qed

Corollary 1. Let $R$ be a subdirectly irreducible ring with identity $1 \neq 0$. If $R$ is Boolean, then $R \cong \mathbb{Z}_2$.

Proof. Let $x \in R$. Since $R$ is Boolean, then $x$ is a central idempotent ($R$ is commutative). But $R$ is subdirectly irreducible with identity, then by Proposition 1, $x = 0$ or $x = 1$. Thus $R \cong \mathbb{Z}_2$. \qed

Now, we will introduce the main result in this talk which was motivated by the above theorem:
Theorem 3. Let $R$ be a ring with identity $1 \neq 0$. Then $R$ is Boolean iff $R$ is isomorphic to a subdirect product of copies of the field $\mathbb{Z}_2$.

Proof. Let $R$ be a Boolean ring. By Birkhoff’s Theorem (Theorem 2), $R$ is isomorphic to a subdirect product of nonzero subdirectly irreducible rings $R_i$, $i \in I$. For each $i \in I$, $R_i$ is the homomorphic image of $R$, and hence each $R_i$ is a Boolean ring with a nonzero identity. But, $R_i$ is a subdirectly irreducible ring, and then, by Corollary 1, $R_i \cong \mathbb{Z}_2$ for each $i \in I$. Therefore,

$$R \cong \text{subdirect product of copies of } \mathbb{Z}_2.$$  

Conversely, let $R$ be isomorphic to a subdirect product of copies of $\mathbb{Z}_2$. Note that for $x \in \mathbb{Z}_2$, $x^2 = x$. Then every element $x \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots$, $x = (x_i)_{i \in I}$, satisfies the identity $x^2 = x$ since $x^2 = (x_i^2)_{i \in I} = (x_i)_{i \in I} = x$. Thus, every element of the direct product $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots$ is idempotent. Since $R$ is isomorphic to a subdirect product of copies of $\mathbb{Z}_2$, then $R$ is isomorphic to a subring of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots$ which is Boolean. Therefore, $R$ is Boolean.

Theorem 4. If $R$ is a finite Boolean ring, then $R$ has $2^k$ elements for some positive integer $k$.

Proof. Suppose $|R| = m$. We will show that $m = 2^k$ for some positive integer $k$. Suppose not, then $m$ has a prime factor $p$ other than 2. Since $R$ is an additive group, then by Cauchy’s Theorem, $R$ has an element $x \neq 0$ of order $p$; that is, $px = 0$. Since $p$ is odd, then $p = 2n + 1$. Thus $(2n + 1).x = 0$, but $\text{char}(R) = 2$ by Lemma 1, and hence $x = 0$, a contradiction. This ends the proof.

References: