

# Algebra: Hungerford Page 120

David Joseph Stith

A ring  $R$  such that  $a^2 = a$  for all  $a \in R$  is called a **Boolean ring**.

**3. Theorem.** *Every Boolean ring  $R$  is commutative and  $a + a = 0$  for all  $a \in R$ .*

Suppose  $a, b \in R$ . To show that  $a + a = 0$ , we show that  $a = -a$ . We have,

$$\begin{aligned} -a &= (-a)^2 \quad \text{since } -a \in R \\ &= (-a)(-a) \\ &= aa \quad \text{by Theorem III.1.2(iii)} \\ &= a^2 \\ &= a \end{aligned}$$

Therefore since  $a$  is arbitrary in  $R$ ,  $a = -a$  and hence  $a + a = 0$  for all  $a \in R$ .

It remains to show that  $ab = ba$  and hence  $R$  is commutative. Consider,

$$\begin{aligned} (a + b)^2 &= (a + b) \quad \text{since } a + b \in R \\ \implies (a + b)(a + b) &= (a + b) \\ \implies (a + b)a + (a + b)b &= (a + b) \\ \implies a^2 + ba + ab + b^2 &= a + b \\ \implies a + ba + ab + b &= a + b \quad \text{since } a, b \in R \\ \implies ba + ab &= 0 \quad \text{by left and right cancellation} \\ \implies ba &= -ab \\ \implies ba &= ab \quad \text{since } x = -x \text{ for all } x \in R \text{ as shown above} \end{aligned}$$

Therefore since  $a$  and  $b$  are arbitrary in  $R$ ,  $R$  is commutative.

**Q.E.D.**

**6. Theorem.** *A finite ring with more than one element and no zero divisors is a division ring.*

Let  $R$  be a finite ring with more than one element and no zero divisors. Let  $a, b \in R$  such that  $a \neq 0$  and  $a \neq b$ . Then  $ac = 0 \implies c = 0$ . We need to show

- (i) There exists a  $1_R \in R$  such that  $b1_R = 1_Rb = b$ .
- (ii) There exists  $y, z \in R$  such that  $ya = az = 1_R$ .
- (i) Since  $R$  is finite, let  $x_1, x_2, \dots, x_n$  be the elements of  $R$ . Then  $ax_1, ax_2, \dots, ax_n$  are all distinct since

$$\begin{aligned} ax_i = ax_j &\implies ax_i - ax_j = 0 \\ &\implies a(x_i - x_j) = 0 \\ &\implies x_i - x_j = 0 \quad \text{since } ac = 0 \implies c = 0 \\ &\implies x_i = x_j \end{aligned}$$

Likewise we can show that the elements  $x_1a, x_2a, \dots, x_na$  are all distinct. Therefore it must be that  $ax_{i_0} = a$  for some  $i_0$ . Then since  $b = x_i a$  for some  $i$ ,

$$bx_{i_0} = (x_i a)x_{i_0} = x_i(ax_{i_0}) = x_i a = b$$

Likewise it must be that  $x_{j_0} a = a$  for some  $j_0$ . Then since  $b = ax_j$  for some  $j$ ,

$$x_{j_0} b = x_{j_0}(ax_j) = (x_{j_0} a)x_j = ax_j = b$$

Therefore since  $b$  is arbitrary in  $R$ ,  $x_{i_0}$  is a right identity and  $x_{j_0}$  is a left identity for all elements in  $R$ . But then  $x_{i_0}x_{j_0} = x_{i_0}$  and  $x_{i_0}x_{j_0} = x_{j_0}$  so  $1_R = x_{i_0} = x_{j_0}$  exists in  $R$  such that  $b1_R = 1_R b = b$ .

(ii)  $1_R$  itself can be represented by  $ax_i$  for some  $i$  and by  $x_j a$  for some  $j$  so that there exists  $y, z \in R$ ,  $y = x_j$ ,  $z = x_i$  such that  $ya = 1_R$  and  $az = 1_R$ .

Therefore  $R$  is a division ring.

Therefore a finite ring with more than one element and no zero divisors is a division ring. **Q.E.D.**

**7. Theorem.** *Let  $R$  be a ring with more than one element such that for each nonzero  $a \in R$  there is a unique  $b \in R$  such that  $aba = a$ . Then,*

- (i)  $R$  has no zero divisors.
- (ii)  $bab = b$
- (iii)  $R$  has an identity.
- (iv)  $R$  is a division ring.

Suppose  $a \in R$  such that  $a \neq 0$ . Let  $b \in R$  be the unique element such that  $aba = a$ .

(i) We need to show that  $ac = 0$  or  $ca = 0$  implies that  $c = 0$ .

Suppose to the contrary that there existed a  $c \neq 0$  such that  $ac = 0$  or  $ca = 0$  so that by Theorem III.1.2(i),

$$\begin{aligned} ac = 0 &\implies aca = 0 \cdot a = 0 \\ ca = 0 &\implies aca = a \cdot 0 = 0 \end{aligned}$$

Then,

$$\begin{aligned} aca = 0 &\implies aba + aca = a + 0 \text{ since } aba = a \\ &\implies a(ba + ca) = a \\ &\implies a(b + c)a = a \\ &\implies b + c = b \text{ since } axa = a \text{ for unique } x \\ &\implies c = 0 \end{aligned}$$

This contradicts  $c \neq 0$ , hence it cannot be that  $R$  has a left or right zero divisor.

(ii) We need to show  $bab = b$ .

Consider,

$$a(bab)a = (aba)ba = aba = a$$

Therefore  $bab = b$  since  $axa = a$  for **unique**  $x$ .

(iii) We need to show  $R$  has an identity.

Since  $aba = a$ , we have  $ba$  as a candidate for  $1_R$ . Note that  $b \neq 0$  since  $a0a = 0 \neq a$  by Theorem III.1.2(i). Let  $x \in R$  and let  $y = x(ba)$ . We will show that  $x = y$  and hence  $ba$  is a right identity for all elements of  $R$ . We have,

$$\begin{aligned} x(ba) = y &\implies xbab = yb \\ &\implies xbab - yb = 0 \\ &\implies xb - yb = 0 \text{ since } bab = b \text{ by part (ii) above} \\ &\implies (x - y)b = 0 \\ &\implies x - y = 0 \text{ since } R \text{ has no zero divisors and } b \neq 0 \\ &\implies x = y \end{aligned}$$

Likewise, if we let  $y = (ba)x$  we can show that  $x = y$  and hence  $ba$  is also a left identity for all elements of  $R$ .

$$\begin{aligned} (ba)x = y &\implies abax = ay \\ &\implies abax - ay = 0 \\ &\implies ax - ay = 0 \\ &\implies a(x - y) = 0 \\ &\implies x - y = 0 \text{ since } R \text{ has no zero divisors and } a \neq 0 \\ &\implies x = y \end{aligned}$$

Hence there exists an identity element  $1_R = ba$  such that  $1_Rx = x1_R = x$  for all  $x \in R$ .

(iv) We need to show  $R$  is a division ring.

To show that  $R$  is a division ring we will show that  $a$  is both left and right invertible and hence is a unit. Then since  $a$  is an arbitrary nonzero element of  $R$ , it will follow that every nonzero element of  $R$  is a unit and hence  $R$  is a division ring.

By part (iii) above,  $ba = 1_R$ , so  $a$  is left invertible. Now,

$$\begin{aligned} ba = 1_R &\implies aba = a1_R = a \\ &\implies aba - a = 0 \\ &\implies (ab - 1_R)a = 0 \\ &\implies ab - 1_R = 0 \text{ since } R \text{ has no zero divisors and } a \neq 0 \\ &\implies ab = 1_R \end{aligned}$$

Therefore  $a$  is right invertible as well and hence is a unit.

Therefore since  $a$  is an arbitrary nonzero element of  $R$ , every nonzero element of  $R$  is a unit. Therefore  $R$  is a division ring. **Q.E.D.**

**15(a) Problem.** Give an example of a nonzero homomorphism  $f : R \rightarrow S$  of rings with identity such that  $f(1_R) \neq 1_S$ .

Let  $R = (\mathbf{Z}, +, \cdot)$  and let  $S = (\mathbf{Z} \oplus \mathbf{Z}, +, \cdot)$  where multiplication in  $S$  is defined by  $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$ . Then  $1_R = 1$  and  $1_S = (1, 1)$ . Let  $f$  be defined by  $f(x) = (x, 0)$ . Then  $f(1_R) = f(1) = (1, 0) \neq 1_S$ .

**15(b) Theorem.** If  $f : R \rightarrow S$  is an epimorphism of rings with identity, then  $f(1_R) = 1_S$ .

Since  $f$  is onto, there exists an  $x \in R$  such that  $f(x) = 1_S$ . We need to show that  $f(1_R) = 1_S$ . We have

$$\begin{aligned} 1_S &= f(x) \\ &= f(x \cdot 1_R) \text{ since } f \text{ is a homomorphism} \\ &= 1_S \cdot f(1_R) \\ &= f(1_R) \end{aligned}$$

Therefore if  $f : R \rightarrow S$  is an epimorphism of rings with identity, then  $f(1_R) = 1_S$ . **Q.E.D.**

**15(c) Theorem.** If  $f : R \rightarrow S$  is a homomorphism of rings with identity and  $u$  is a unit in  $R$  such that  $f(u)$  is a unit in  $S$ , then  $f(1_R) = 1_S$  and  $f(u^{-1}) = f(u)^{-1}$ .

Since  $u$  is a unit in  $R$  and  $f(u)$  is a unit in  $S$ , there exists a  $u^{-1} \in R$  such that  $u^{-1}u = uu^{-1} = 1_R$  and there exists an  $f(u)^{-1} \in S$  such that  $f(u)^{-1}f(u) = f(u)f(u)^{-1} = 1_S$ .

Then,

$$\begin{aligned} f(u) &= f(u \cdot 1_R) \implies f(u) = f(u)f(1_R) \text{ since } f \text{ is a homomorphism} \\ &\implies f(u)^{-1}f(u) = f(u)^{-1}f(u)f(1_R) \text{ by left multiplication} \\ &\implies 1_S = 1_S f(1_R) \\ &\implies 1_S = f(1_R) \end{aligned}$$

Therefore  $f(1_R) = 1_S$ .

And,

$$\begin{aligned} 1_S &= f(1_R) \\ &= f(uu^{-1})[\text{resp. } f(u^{-1}u)] \\ &= f(u)f(u^{-1})[\text{resp. } f(u^{-1})f(u)] \end{aligned}$$

implies that  $f(u^{-1})$  is both a left and right inverse for  $f(u)$ , hence  $f(u)^{-1} = f(u^{-1})$ . **Q.E.D.**