

1. Let  $R$  be a ring with unity and  $G$  a finite nontrivial group. For any  $g \in G$  with  $g \neq e$ , prove that  $g - 1$  is a zero divisor in  $RG$ .

Solution:

Since  $G$  is a finite group, therefore  $g^n = e$  for some integer  $n > 1$ . We have

$$(g - 1)(g^{n-1} + g^{n-2} + \dots + 1) = g^n - 1 = 0. \text{ Also}$$

$(g^{n-1} + g^{n-2} + \dots + 1)(g - 1) = g^n - 1 = 0$ . Note that both  $g - 1$  and  $g^{n-1} + g^{n-2} + \dots + 1$  are nonzero. This shows that  $g - 1$  is a zero divisor.

2. Let  $R$  be a ring with unity and  $G = \{g_1, g_2, \dots, g_n\}$  a finite group. Prove that the element  $x = g_1 + g_2 + \dots + g_n$  is in the center of  $RG$ .

Solution:

Claim: Let  $G$  be a group and  $g \in G$ . The map  $\phi : G \rightarrow G$  defined as  $\phi(a) = ga$  is a bijection.

We now prove this claim: Suppose that  $a, b \in G$  with  $\phi(a) = \phi(b)$ . Then  $ga = gb$ .

Multiplying both sides of this equality by  $g^{-1}$  on the left gives  $a = b$ . This shows that  $\phi$  is one-to-one. To show that  $\phi$  is onto, let  $a \in G$ . Then

$$\phi(g^{-1}a) = g(g^{-1}a) = (gg^{-1})a = ea = a. \text{ This shows that } \phi \text{ is onto. Thus } \phi \text{ is a bijection.}$$

If  $g \in G$  the above claim implies that  $gx = x$ . Similarly one can show that  $xg = x$ . We

now show that  $x$  is in the center of  $RG$ : Let  $\alpha \in RG$ . Then  $\alpha = r_1g_1 + r_2g_2 + \dots + r_ng_n$  for some  $r_i \in R$ . We have

$$\alpha x = (r_1g_1 + r_2g_2 + \dots + r_ng_n)x = r_1g_1x + r_2g_2x + \dots + r_ng_nx = r_1x + r_2x + \dots + r_nx = r_1xg_1 + r_2xg_2 + \dots + r_nxg_n = xr_1g_1 + xr_2g_2 + \dots + xr_ng_n = x(r_1g_1 + r_2g_2 + \dots + r_ng_n) = x\alpha.$$

This shows that  $x$  is in the center of  $RG$

3. Find all the units and zero divisors of  $\mathbb{Z}_6 \times \mathbb{Z}_4$ .

Solution:

Claim: Let  $R$  and  $S$  be rings with unity. Then the units of  $R \times S$  are

$$\{(a, b) \mid a \text{ is a unit of } R \text{ and } b \text{ is a unit of } S\}.$$

We now prove this claim. Assume that  $(a, b)$  is a unit of  $R \times S$ . Then there exists

$$(a', b') \in R \times S \text{ and } (a'', b'') \in R \times S \text{ such that } (a', b')(a, b) = (1, 1) \text{ and}$$

$$(a, b)(a'', b'') = (1, 1). \text{ This implies that } a'a = 1, b'b = 1, aa'' = 1 \text{ and } bb'' = 1. \text{ Therefore } a$$

is a unit of  $R$  and  $b$  is a unit of  $S$ . Conversely if  $a$  is a unit of  $R$  and  $b$  is a unit of  $S$  then

there exist  $a', a'' \in R$  and  $b', b'' \in S$  such that  $a'a = 1, aa'' = 1, b'b = 1$  and  $bb'' = 1$ . Then

$$\text{we have } (a', b')(a, b) = (1, 1) \text{ and } (a, b)(a'', b'') = (1, 1) \text{ so } (a, b) \text{ is a unit of } R \times S.$$

The units of  $\mathbb{Z}_6$  are 1 and 5 and the units of  $\mathbb{Z}_4$  are 1 and 3 so from the above claim the units of  $\mathbb{Z}_6 \times \mathbb{Z}_4$  are  $\{(1, 1), (1, 3), (5, 1), (5, 3)\}$ .

Claim: Let  $R \neq \{0\}$  and  $S \neq \{0\}$  be commutative rings. Define

$$A = \{(r, s) \mid (r, s) \in R \times S \setminus \{(0, 0)\} \text{ and } r = 0 \text{ or } s = 0\} \text{ and}$$

$$B = \{(r, s) \mid (r, s) \in R \times S, r \neq 0, s \neq 0 \text{ and } r \text{ is a zero divisor or } s \text{ is a zero divisor}\}.$$

The zero divisors of  $R \times S$  are  $A \cup B$ .

We now prove the claim. Assume that  $(r, s) \in A$ . Then  $(r, s) \neq (0, 0)$  and  $r = 0$  or  $s = 0$ .

If  $r \neq 0$  and  $s = 0$  then choose  $s' \in S \setminus \{0\}$ . We have  $(r, 0)(0, s') = (0, 0)$ . If  $s \neq 0$  and

$r = 0$  then choose  $r' \in R \setminus \{0\}$ . We have  $(0, s)(r', 0) = (0, 0)$ . This shows that all elements

of  $A$  are zero divisors. Now let  $(r, s) \in B$ . Then  $r \neq 0, s \neq 0$  and either  $r$  is a zero divisor

or  $s$  is a zero divisor. Assume that  $r$  is a zero divisor. Then there exists  $r' \in R \setminus \{0\}$  with

$$rr' = 0. \text{ Then we have } (r, s)(r', 0) = (0, 0). \text{ Since } R \times S \text{ is commutative this shows that}$$

$(r, s)$  is a zero divisor of  $R \times S$ . Similarly if  $s$  is a zero divisor then  $(r, s)$  is a zero divisor of

$R \times S$ . Thus we have shown that elements of  $B$  are zero divisors of  $R \times S$ . To complete

the proof of the claim we need to show that if  $(r, s)$  is a zero divisor of  $R \times S$ , then

$$(r, s) \in A \cup B. \text{ Assume that } (r, s) \text{ is a zero divisor. If } r = 0 \text{ or } s = 0 \text{ then } (r, s) \in A.$$

Otherwise  $r \neq 0$  and  $s \neq 0$ . Since  $(r, s)$  is a zero divisor there exists  $(r', s') \in R \times S \setminus \{(0, 0)\}$  with  $(r, s)(r', s') = (0, 0)$ . so  $rr' = 0$  and  $ss' = 0$ . Since  $(r', s') \neq (0, 0)$  therefore  $r' \neq 0$  or  $s' \neq 0$ . Since both  $R$  and  $S$  are commutative, this implies that  $r$  is a zero divisor or  $s$  is a zero divisor so  $(r, s) \in B$ . This completes the proof of the claim.

The only zero divisor of  $\mathbb{Z}_4$  is 2 and the zero divisors of  $\mathbb{Z}_6$  are 2, 3 and 4. From the above claim the zero divisors of  $\mathbb{Z}_6 \times \mathbb{Z}_4$  are  $\{(1, 0), (2, 0), (3, 0), (4, 0), (5, 0), (0, 1), (0, 2), (0, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (4, 1), (4, 2), (4, 3), (1, 2), (5, 2)\}$

4. Find the characteristics of the following rings:

- (a)  $\mathbb{Z}_4 \times \mathbb{Z}_6$       (b)  $\mathbb{Z}_4 \times 4\mathbb{Z}$       (c)  $M_{22}(\mathbb{Z}_5)$   
 (d) The group ring  $RG$  where  $R = \mathbb{Z}_4$  and  $G = \mathbb{Z}_8$

Solution:

- (a)  $\text{lcm}(4,6)=12$  (b) 0 (c) 5 (d) 4

5. An element  $a$  of a ring is an idempotent if  $a^2 = a$ . Prove that the only idempotents of an integral domain are 0 and 1.

Solution:

Note that 0 and 1 are certainly idempotents. For the other containment, assume that  $a$  is an idempotent of an integral domain. Then  $a^2 = a$  so  $a^2 - a = 0$ . This implies that  $a(a - 1) = 0$ . Since an integral domain has no zero divisors this implies that  $a = 0$  or  $a - 1 = 0$  i.e.  $a = 0$  or  $a = 1$ .

6. In a commutative ring of characteristic 2, prove that the idempotents forms a subring.

Solution:

Let  $R$  be the ring in question and let  $S$  be the set of its idempotents. Note that since  $\text{char}(R) = 2$  we have  $a = -a$  for any  $a$  in  $R$

(i)  $0^2 = 0$  so  $0 \in S$ . Therefore  $S \neq \emptyset$

(ii) Let  $a, b \in S$ . Then  $a^2 = a$  and  $b^2 = b$ . Since  $R$  is commutative and  $\text{char}(R) = 2$  we have  $(a - b)^2 = (a - b)(a - b) = a^2 - ab - ba + b^2 = a^2 - 2ab + b^2 = a^2 + b^2 = a + b = a - b$  so  $a - b \in S$ .

(iii) Let  $a, b \in S$ . Then  $a^2 = a$  and  $b^2 = b$ . Since  $R$  is commutative we have  $(ab)^2 = abab = a^2b^2 = ab$  so  $ab \in S$ .

From (i), (ii) and (iii)  $S$  is a subring of  $R$ .