

- (1) Let  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  be given by  $f(a) = 2a + 1$  for  $a \in \mathbb{Z}$ . Show that  $f$  is injective but not surjective.

Since  $2a + 1$  is odd for every integer  $a$ , 0 is not in the range so  $f$  is not surjective. We now show that  $f$  is injective. Let  $a, b \in \mathbb{Z}$  such that  $f(a) = f(b)$ . Then we have

$$\begin{array}{ll} 2a + 1 = 2b + 1 & \text{by definition of } f \\ 2a = 2b & \text{by adding } -1 \text{ to both sides} \\ a = b & \text{by cancellation.} \end{array}$$

Hence,  $f$  is injective as required. ◆

- (2) Let  $\varphi : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  be defined by  $\varphi((a, b)) = a$  for all  $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ . Show that  $\varphi$  is a homomorphism.

We must show that  $\varphi$  preserves both addition and multiplication. Let  $x_1, x_2 \in \mathbb{Z} \times \mathbb{Z}$ ; then  $x_1 = (a_1, b_1)$  and  $x_2 = (a_2, b_2)$  where  $a_i, b_i \in \mathbb{Z}$  for  $i = 1, 2$ . We have

$$\begin{aligned} \varphi(x_1 + x_2) &= \varphi((a_1, b_1) + (a_2, b_2)) = \varphi((a_1 + a_2, b_1 + b_2)) = a_1 + a_2 \\ &= \varphi(x_1) + \varphi(x_2); \end{aligned}$$

so  $\varphi$  preserves addition. Moreover,

$$\begin{aligned} \varphi(x_1 x_2) &= \varphi((a_1, b_1)(a_2, b_2)) = \varphi((a_1 a_2, b_1 b_2)) = a_1 a_2 \\ &= \varphi(x_1) \varphi(x_2); \end{aligned}$$

so  $\varphi$  also preserves multiplication. Therefore,  $\varphi$  is a homomorphism as required. ◆

- (3) Show that for every  $y \in \mathbb{Z}$  there exists  $x \in \mathbb{Z}$  such that  $3x \equiv y \pmod{11}$ . Find all solutions to the congruence:

$$3x \equiv 7 \pmod{11}.$$

Since  $(3, 11) = 1$ , the congruence  $3x \equiv y \pmod{11}$  has a unique solution modulo 11 for every  $y \in \mathbb{Z}$ ; this may also be shown directly. Note that  $3 \cdot 4 \equiv 1 \pmod{11}$ . Let  $y \in \mathbb{Z}$  be given and set  $x = 4y$ . Then we have

$$3x \equiv 3(4y) \equiv (3 \cdot 4)y \equiv 1 \cdot y \equiv y \pmod{11}.$$

Hence, for every  $y \in \mathbb{Z}$  there exists  $x \in \mathbb{Z}$  such that  $3x \equiv y \pmod{11}$ . Note that if  $x \equiv 4 \cdot 7 \equiv 6 \pmod{11}$ , we have  $3x \equiv 7 \pmod{11}$ ; so  $x$  is a solution to this congruence if  $x \equiv 6 \pmod{11}$ . Moreover, if  $3x \equiv 7 \pmod{11}$ , then

$$x \equiv 4(3x) \equiv 4 \cdot 7 \equiv 6 \pmod{11}.$$

Hence,  $x \in \mathbb{Z}$  is a solution to the congruence if and only if  $x \equiv 6 \pmod{11}$ . ◆

- (4) Show that  $R = \{0, 3, 6, 9\}$  is a subring of  $\mathbb{Z}_{12}$  (*Hint*: use tables). Is  $R$  isomorphic to  $\mathbb{Z}_4$ ? Find if possible a nonzero homomorphism  $f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_{12}$ .

Clearly  $0 \in R$ . The addition and multiplication tables below show that  $R$  is closed under both operations. Moreover, since there is a 0 in every row of the addition table, additive inverses exist for every element. Hence,  $R$  is a subring of  $\mathbb{Z}_{12}$ .

+	0	9	6	3		·	0	9	6	3
0	0	9	6	3		0	0	0	0	0
9	9	6	3	0		9	0	9	6	3
6	6	3	0	9		6	0	6	0	6
3	3	0	9	6		3	0	3	6	9

We compare these tables to those of  $\mathbb{Z}_4$ :

+	0	1	2	3		·	0	1	2	3
0	0	1	2	3		0	0	0	0	0
1	1	2	3	0		1	0	1	2	3
2	2	3	0	1		2	0	2	0	2
3	3	0	1	2		3	0	3	2	1

and observe that the two rings must be isomorphic under the bijection  $\mathbb{Z}_4 \rightarrow R$  given by:

$$0 \mapsto 0, \quad 1 \mapsto 9, \quad 2 \mapsto 6, \quad 3 \mapsto 3.$$

We may define a nonzero homomorphism  $f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_{12}$  by the same assignment (which is now injective but not surjective) or by the formula  $f([a]_4) = [9a]_{12}$  for  $a \in \mathbb{Z}$ . ◆

(5) Let  $\mathbb{Q}[\sqrt{5}]$  denote the set  $\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ . Show that  $\mathbb{Q}[\sqrt{5}]$  is a subring of  $\mathbb{R}$ . Is  $\mathbb{Q}[\sqrt{5}]$  a field?

To show that  $\mathbb{Q}[\sqrt{5}]$  is a subring of  $\mathbb{R}$  observe first that it is a nonempty subset of  $\mathbb{R}$  (note,  $0 = 0 + 0\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$ ). We must now verify that  $\mathbb{Q}[\sqrt{5}]$  is closed under subtraction and multiplication. So let  $x_1, x_2 \in \mathbb{Q}[\sqrt{5}]$  be given. Then  $x_i = a_i + b_i\sqrt{5}$  for some  $a_i, b_i \in \mathbb{Q}$  for  $i = 1, 2$ . We have

$$\begin{aligned}x_1 - x_2 &= (a_1 + b_1\sqrt{5}) - (a_2 + b_2\sqrt{5}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{5} \in \mathbb{Q}[\sqrt{5}] \\x_1x_2 &= (a_1 + b_1\sqrt{5})(a_2 + b_2\sqrt{5}) = (a_1a_2 + 5b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{5} \in \mathbb{Q}[\sqrt{5}]\end{aligned}$$

since  $a_1 - a_2, b_1 - b_2, a_1a_2 + 5b_1b_2, a_1b_2 + a_2b_1$  are all rational. Hence,  $\mathbb{Q}[\sqrt{5}]$  is a subring of  $\mathbb{R}$ .

Moreover,  $\mathbb{Q}[\sqrt{5}]$  is a field. To see this note first that  $\mathbb{Q}[\sqrt{5}]$  is a commutative ring with identity (observe that  $1 = 1 + 0\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$  since  $0, 1 \in \mathbb{Q}$ ). It remains to show that every nonzero element is a unit. Let  $x \in \mathbb{Q}[\sqrt{5}]$  be given so that  $x \neq 0$ . Then  $x = a + b\sqrt{5}$  with  $a, b \in \mathbb{Q}$  not both 0. Set

$$y = \frac{a}{a^2 - 5b^2} + \frac{-b}{a^2 - 5b^2}\sqrt{5};$$

then  $y \in \mathbb{Q}[\sqrt{5}]$  since  $\frac{a}{a^2 - 5b^2}, \frac{-b}{a^2 - 5b^2} \in \mathbb{Q}$  (note  $a^2 - 5b^2 \neq 0$  because  $\sqrt{5}$  is irrational). A straightforward calculation reveals that  $xy = 1$ . Thus,  $\mathbb{Q}[\sqrt{5}]$  is a field.  $\blacklozenge$

(6) Let  $a, b$  be integers such that  $a$  and  $b$  are not both 0 and set  $d = (a, b)$ . Show that

$$\{dk \mid k \in \mathbb{Z}\} = \{am + bn \mid m, n \in \mathbb{Z}\}.$$

Denote the set on the left by  $A$  and the set on the right by  $B$ . We must show that for an integer  $c$ , that  $c \in A$  if and only if  $c \in B$ . So let  $c \in \mathbb{Z}$  be given. Suppose first that  $c \in A$ . Then  $c = dk$  for some  $k$ . Since  $d = (a, b)$ , we have  $d = au + bv$  for some  $u, v \in \mathbb{Z}$ . Hence, we have

$$c = dk = (au + bv)k = a(uk) + b(vk) = am + bn$$

where  $m = uk$  and  $n = vk$ ; since,  $m$  and  $n$  are both integers  $c \in B$ .

Conversely, suppose  $c \in B$ . Then,  $c = am + bn$  for some  $m, n \in \mathbb{Z}$ . Since  $d$  is a common divisor of  $a$  and  $b$ , there are integers  $a', b'$  such that  $a = da'$  and  $b = db'$ . Hence,

$$c = am + bn = da'm + db'n = d(a'm + b'n) = dk$$

where  $k = a'm + b'n$ . Since  $k$  is an integer, we have  $c \in A$ . Hence,  $A = B$  as required.  $\blacklozenge$