

Section 18 Solutions

6.  $(-3, 5)(2, -4) = (-6, -20) = (2 - (2 \cdot 4), 2 - (2 \cdot 11)) = (2, 2)$  in  $\mathbb{Z}_2 \times \mathbb{Z}_{11}$ .

12. Consider the set  $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ . Is  $R$  a ring? Is  $R$  a field?

Notice that  $R \subset \mathbb{R}$ , so we are asking if  $R$  is a subgroup of  $\mathbb{R}$ .

First, note that  $R$  is an additive subgroup of  $\mathbb{R}$ :

- (a) If  $x, y \in R$  then  $x = a + b\sqrt{2}$  and  $y = a' + b'\sqrt{2}$  for appropriate rational numbers  $a, b, a', b'$ . Then  $x + y = (a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2} \in R$ , so  $R$  is closed under addition.
- (b) Observe  $0 = 0 + 0\sqrt{2} \in R$ .
- (c) If  $x \in R$  then  $x = a + b\sqrt{2}$ , so  $-x = -a - b\sqrt{2}$  is also in  $R$ .

Next note that  $R$  is closed under multiplication, for if  $x, y \in R$  then  $x = a + b\sqrt{2}$  and  $y = a' + b'\sqrt{2}$  for appropriate rational numbers  $a, b, a', b'$ . So  $xy = (a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2} \in R$ .

It follows that  $R$  is a subring of  $\mathbb{R}$ , so  $R$  is a ring.

Is  $R$  a field? Well,  $R$  is commutative because it's a subring of  $\mathbb{R}$ , and  $R$  contains the multiplicative identity  $1 = 1 + 0\sqrt{2}$ . We just need to show that any nonzero element  $a + b\sqrt{2}$  of  $R$  has a multiplicative inverse in  $R$ . Of course, in  $\mathbb{R}$ ,  $(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}}$ , but the obvious question is if  $\frac{1}{a + b\sqrt{2}}$  is in  $R$ . Observe:

$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$

Since  $a, b \in \mathbb{Q}$ , it follows  $\frac{a}{a^2 - 2b^2}$  and  $-\frac{b}{a^2 - 2b^2}$  are in  $\mathbb{Q}$  too, hence  $\frac{1}{a + b\sqrt{2}} \in R$ . Thus  $R$  is a field.

18. Find all units in  $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ .

Suppose  $(a, b, c)$  is a unit in  $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ .

This means there is an element  $(a', b', c') \in \mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$  with  $(a, b, c)(a', b', c') = (aa', bb', cc') = (1, 1, 1)$ .

Since  $a, a' \in \mathbb{Z}$  and  $aa' = 1$  it follows that  $a = \pm 1$ .

Since  $b, b' \in \mathbb{Q}$  and  $bb' = 1$  it follows that  $b = \pm 1$ .

Since  $c, c' \in \mathbb{Z}$  and  $cc' = 1$  it follows that  $c \neq 0$  (and  $c' = 1/c$ ).

Thus the units in  $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$  are all the elements of form  $(\pm 1, c, \pm 1)$  with  $c \neq 0$

That is, the units are  $\{1, -1\} \times \mathbb{Q}^* \times \{1, -1\}$ .

50. Suppose  $a$  is an element of a ring  $R$  and  $I_a = \{x \in R \mid ax = 0\}$ . Show  $I_a$  is a subring of  $R$ .

Proof. First note that  $I_a$  is an additive subgroup of  $R$ :

- (a)  $I_a$  is closed under addition: If  $x, y \in I_a$  then  $ax = 0$  and  $ay = 0$ . Then  $0 = ax + ay = a(x + y)$ . But  $a(x + y) = 0$  means  $x + y \in I_a$ .
- (b) The additive identity  $0$  is in  $I_a$  because  $a0 = 0$ .
- (c) If  $x \in I_a$ , then  $ax = 0$ , hence  $a(-x) = -(ax) = -0 = 0$ , meaning  $-x \in I_a$ .

Now we just need to check  $I_a$  is closed under multiplication.

Suppose  $x, y \in I_a$  so  $ax = 0$  and  $ay = 0$ .

Then  $a(xy) = (ax)y = 0y = 0$ .

But  $a(xy) = 0$  means  $xy \in I_a$ , so  $I_a$  is closed under multiplication.

Therefore  $I_a$  is a subring of  $R$ .