Homework 9

Jaden Wang

Problem (18.4)**.**

$$20 \times_{26} (-8) = -160 \mod 26 = -4.$$

Problem (18.5)**.**

$$(2,3)(3,5) = (2 \times_5 3, 3 \times_9 5) = (1,6).$$

Problem (18.11)**.** First let's show that $R = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a ring. Take $a + b\sqrt{2}$ and $c+d\sqrt{2}$ where $a, b, c, d \in \mathbb{Z}$.

Since the addition operation is the addition of complex numbers which is commutative and associative, we have

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}.$$

Since $a+c, b+d \in \mathbb{Z}$, $(a+c)+(b+d)\sqrt{2} \in R$. So R is closed under addition.

Since the identity of addition of complex numbers is 0, and $0 = 0+0\sqrt{2} \in R$, R contains the additive identity.

Notice

$$(-a)+(-b)\sqrt{2}+a+b\sqrt{2} = a+b\sqrt{2}+(-a)+(-b)\sqrt{2} = (a-a)+(b-b)\sqrt{2} = 0+0\sqrt{2} = 0$$

so $(-a)+(-b)\sqrt{2}$ is its inverse. Since $(-a), (-b) \in \mathbb{Z} \Rightarrow (-a)+(-b)\sqrt{2} \in R$. R is closed under inverses.

Hence, we just showed that R is an abelian group under addition.

Since the multiplication is the multiplication of complex numbers which is commutative, associative, and left and right distributive with addition, we have

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+bc\sqrt{2})+(ad\sqrt{2}+2bd) = (ac+2bd)+(bc+ad)\sqrt{2}.$$

Since $ad + 2bd, bc + ad \in \mathbb{Z}$, $(ac + 2bd) + (bc + ad)\sqrt{2} \in R$. So R is closed under associative multiplication.

Therefore, by satisfying an abelian group under addition, closed under associative multiplication, and left and right distributive laws, R is a ring.

Since multiplication is commutative, R is a commutative ring.

Since the multiplicative identity is 1, and $1 = 1 + 0\sqrt{2} \in R$, R contains the multiplicative identity.

However, R is not a field. Consider $(0 + 1\sqrt{2})$. Since

$$(0 + 1\sqrt{2})(0 + \frac{1}{2}\sqrt{2}) = (0 + \frac{1}{2}\sqrt{2})(0 + 1\sqrt{2}) = 1,$$

$0 + \frac{1}{2}\sqrt{2}$ is its multiplicative inverse. Yet $0 + \frac{1}{2}\sqrt{2} \notin R$. Thus $0 + 1\sqrt{2} \in R$ is not a unit and R is not a field.

Problem (18.12)**.** First let's show that $R = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a ring. Take $a + b\sqrt{2}$ and $c + d\sqrt{2}$ where $a, b, c, d \in \mathbb{Q}$.

Since the addition operation is the addition of complex numbers which is commutative and associative, we have

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}.$$

Since $a + c, b + d \in \mathbb{Q}$, $(a + c) + (b + d)\sqrt{2} \in R$. So R is closed under addition.

Since the identity of addition of complex numbers is 0, and $0 = 0 + 0\sqrt{2} \in R$, R contains the additive identity.

Notice

$$(-a)+(-b)\sqrt{2}+a+b\sqrt{2} = a+b\sqrt{2}+(-a)+(-b)\sqrt{2} = (a-a)+(b-b)\sqrt{2} = 0+0\sqrt{2} = 0$$

so $(-a)+(-b)\sqrt{2}$ is its inverse. Since $(-a), (-b) \in \mathbb{Q} \Rightarrow (-a)+(-b)\sqrt{2} \in R$. R is closed under inverses.

Hence, we just showed that R is an abelian group under addition.

Since the multiplication is the multiplication of complex numbers which is commutative, associative, and left and right distributive with addition, we have

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+bc\sqrt{2})+(ad\sqrt{2}+2bd) = (ac+2bd)+(bc+ad)\sqrt{2}.$$

Since $ad + 2bd, bc + ad \in \mathbb{Q}$, $(ac + 2bd) + (bc + ad)\sqrt{2} \in R$. So R is closed under associative multiplication.

Therefore, by satisfying an abelian group under addition, closed under associative multiplication, and left and right distributive laws, R is a ring.

Since multiplication is commutative, R is a commutative ring.

Since the multiplicative identity is 1, and $1 = 1 + 0\sqrt{2} \in R$, R contains the multiplicative identity.

To show R is a field, consider $a + b\sqrt{2} \in R$, so $a, b \in \mathbb{Q}$.

Case. $a \neq 0, b = 0$, then clearly its inverse is $\frac{1}{a} + 0\sqrt{2} \in R$.

Case. $a = 0, b \neq 0$, then clearly its inverse is $\frac{1}{2b}\sqrt{2} \in R$.

Case. $a \neq 0, b \neq 0$, then its inverse is $-\frac{a}{2b^2-a^2} + \frac{b}{2b^2-a^2}\sqrt{2}$, because $a \neq b\sqrt{2}\ \forall\ a, b \in \mathbb{Q} \Rightarrow 2b^2 - a^2 \neq 0$ and

$$\begin{aligned}
&(a + b\sqrt{2})\left(-\frac{a}{2b^2 - a^2} + \frac{b}{2b^2 - a^2}\sqrt{2}\right) \\
&= \left(-\frac{a^2}{2b^2 - a^2} + \frac{2b^2}{2b^2 - a^2}\right) + \left(\frac{ab}{2b^2 - a^2} - \frac{ab}{2b^2 - a^2}\right)\sqrt{2} \\
&= \left(\frac{2b^2 - a^2}{2b^2 - a^2}\right) + 0\sqrt{2} \\
&= 1
\end{aligned}$$

The other direction follows from commutativity. Moreover, since rational numbers are closed under addition and multiplication, the two coefficients of the inverse are in $\mathbb{Q}$ and thus the inverse is in R.

Case. $a = 0, b = 0$, then we get the zero element which we disregard.

Therefore, for all possible cases of $a, b \in \mathbb{Q}$, we show that nonzero $a + b\sqrt{2}$ is a unit, proving R is a field.

Problem (18.13)**.** Given purely imaginary numbers ri, si where $r, s \in \mathbb{R}$. It is closed under addition:

$$ri + si = (r + s)i$$

where $r + s \in \mathbb{R}$. However, it is not closed under multiplication:

$$1i \cdot 2i = 2i^2 = -2$$

which is not purely imaginary. Since it's not closed under multiplication, it is not a ring.

Problem (18.15)**.** Let $a, b \in \mathbb{Z}$, so $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Since the identity of $\mathbb{Z} \times \mathbb{Z}$ is $(1, 1)$, for (a, b) to be a unit, we need $(c, d) \in \mathbb{Z} \times \mathbb{Z}$ such that

$$\begin{aligned}(a, b)(c, d) &= (1, 1)\\ (ac, bd) &= (1, 1)\\ ac &= 1, bd = 1\\ c = \frac{1}{a} &\in \mathbb{Z}, d = \frac{1}{b} \in \mathbb{Z}, a, b \neq 0\end{aligned}$$

This means that a, b are divisors of 1, implying that $a, b = \pm 1$. Therefore, the units are $(1, 1), (-1, 1), (-1, -1), (1, -1)$.

Problem (18.17)**.** Taken $a \in \mathbb{Q} \setminus \{0\}$, then $\frac{1}{a} = a^{-1} = \in \mathbb{Q}$, thus the units of $\mathbb{Q}$ are $\mathbb{Q} \setminus \{0\}$.

Problem (18.18)**.** Since direct product has elementwise operations, the units of $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ are simply the direct product of units of each set. By 18.15 and 18.17, the units are

$$\{(a, b, c) : a, c = \pm 1, b \in \mathbb{Q} \setminus \{0\}\}.$$

Problem (18.23)**.** Recall that the only functions that satisfy injective group homomorphism from $\mathbb{Z} \to \mathbb{Z}$ are $\phi(x) = x$ and $\phi(x) = -x$. Since ring homomorphism must satisfy group homomorphism, these two are our only candidates. For the identity map, it clearly still works, since

$$\phi(a + b) = a + b = \phi(a) + \phi(b) \text{ and } \phi(ab) = ab = \phi(a)\phi(b).$$

But $\phi(x) = -x$ no longer works:

$$\phi(1 \times 2) = -(2) = -2 \neq 2 = (-1)(-2) = \phi(1) \times \phi(2).$$

So the only injective ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}$ is $\phi(x) = x$.

Problem (18.33).

a) True. By definition.

b) False. $2\mathbb{Z}$ under usual $+, \times$ has no multiplicative identity, yet is a ring.

c) False. $\mathbb{Z}_2$ is a ring, but the multiplicative identity 1 is the only unit.

d) False. $\mathbb{R}$ has infinite units and is a ring.

e) True. Consider $\mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{Z}$ is clearly a ring but not a field, and $\mathbb{Q}$ is a field.

f) False. They govern how $+, \times$ interact!

g) True. By definition.

h) True. We get closure and associativity of the definition of ring, and identity and inverses from the definition of field.

i) True. By definition.

j) True. By definition.