MATH 4107 (Prof. Heil) PRACTICE PROBLEMS WITH SOLUTIONS Spring 2018

Here are a few practice problems on rings. **You should first work through these WITHOUT LOOKING at the solutions!** After you write your own solution, you can compare to my solution. Your solution does not need to be identical to mine—there are often many ways to solve a problem—but it does need to be CORRECT.

1. Find the inverses of the nonzero elements of $\mathbb{Z}_{11}$.

Solution

Note the following facts:

$$\begin{aligned} 1 \cdot 1 &= 1, \\ 2 \cdot 6 &= 12 = 11 + 1, \\ 3 \cdot 4 &= 12 = 11 + 1, \\ 5 \cdot 9 &= 45 = 4 \cdot 11 + 1, \\ 7 \cdot 8 &= 56 = 5 \cdot 11 + 1, \\ 10 \cdot 10 &= 100 = 9 \cdot 11 + 1. \end{aligned}$$

Therefore, computing in $\mathbb{Z}_{11}$, we have

$$\begin{aligned} [1] \cdot [1] &= [1], \\ [2] \cdot [6] &= [12] = [1], \\ [3] \cdot [4] &= [12] = [1], \\ [5] \cdot [9] &= [45] = [1], \\ [7] \cdot [8] &= [56] = [1], \\ [10] \cdot [10] &= [100] = [1]. \end{aligned}$$

Hence,

$$\begin{aligned} [1]^{-1} &= [1], \\ [2]^{-1} &= [6], \\ [3]^{-1} &= [4], \\ [4]^{-1} &= [3], \\ [5]^{-1} &= [9], \\ [6]^{-1} &= [2], \\ [7]^{-1} &= [8], \\ [8]^{-1} &= [7], \\ [9]^{-1} &= [5], \\ [10]^{-1} &= [10]. \quad \square \end{aligned}$$

2. Let $\mathcal{F}(\mathbb{R})$ be the set of all functions $f\colon \mathbb{R} \to \mathbb{R}$, i.e., all functions which map real numbers to real numbers. Parts a and b of this problem are two of the steps required to prove that $\mathcal{F}(\mathbb{R})$ is a commutative ring with identity under the operations of addition and multiplication of functions. For the remaining parts of the problem, you may assume that $\mathcal{F}(\mathbb{R})$ is a commutative ring with 1.

a. Prove that multiplication distributes over addition in $\mathcal{F}(\mathbb{R})$, i.e., $f(g+h) = fg + fh$ for all $f$, $g$, $h \in \mathcal{F}(\mathbb{R})$. Remark: If $p$ and $q$ are functions, then to prove $p = q$ you must show that $p(t) = q(t)$ for every $t$.

Solution

If $f$, $g$, $h \in \mathcal{F}(\mathbb{R})$ then

$$(f(g+h))(t) \;=\; f(t)(g+h)(t) \;=\; f(t)(g(t)+h(t)) \;=\; f(t)g(t) + f(t)h(t).$$

The last step is valid because $f(t)$, $g(t)$, and $h(t)$ are all REAL NUMBERS, and we know that multiplication of real numbers distributes over addition. On the other hand, we have

$$(fg+fh)(t) \;=\; (fg)(t) + (fh)(t) \;=\; f(t)g(t) + f(t)h(t),$$

so $(f(g+h))(t) = (fg+fh)(t)$ for every $t$ and therefore $f(g+h) = fg + fh$. □

b. Prove that a multiplicative identity exists in $\mathcal{F}(\mathbb{R})$.

Solution

Define the function $\mathbf{1}\colon \mathbb{R} \to \mathbb{R}$ by $\mathbf{1}(t) = 1$ for every $t$. Then for any $f \in \mathcal{F}(\mathbb{R})$ we have

$$(f\mathbf{1})(t) \;=\; f(t)\mathbf{1}(t) \;=\; f(t)\cdot 1 \;=\; f(t) \;=\; 1\cdot f(t) \;=\; \mathbf{1}(t)\cdot f(t) \;=\; (\mathbf{1}f)(t),$$

which says that $f\mathbf{1} = f = \mathbf{1}f$. Thus $\mathbf{1}$ is the multiplicative identity. □

c. Find all the units in $\mathcal{F}(\mathbb{R})$. Is $\mathcal{F}(\mathbb{R})$ a field?

Solution

Let $f \in \mathcal{F}(\mathbb{R})$. For $f$ to be a unit in $\mathcal{F}(\mathbb{R})$, there must be a function $g \in \mathcal{F}(\mathbb{R})$ such that $fg = \mathbf{1}$, the multiplicative identity in $\mathcal{F}(\mathbb{R})$. The function $fg$ is defined by $(fg)(x) = f(x)g(x)$ for all $x \in \mathbb{R}$. Therefore we must have $f(x)g(x) = 1$ for all $x$. This is possible if and only if $f(x) \neq 0$ for each $x$, and in this case we have $g(x) = 1/f(x)$ (not to be confused with the *inverse function* $f^{-1}$!). Therefore the units in $\mathcal{F}(\mathbb{R})$ are exactly those functions $f$ that never vanish, i.e., $f(x) \neq 0$ for every $x \in \mathbb{R}$. Therefore $\mathcal{F}(\mathbb{R})$ is not a field, because there are functions that are not the zero function yet are not units. For example, $f(x) = \sin x$ is not a unit. □

d. Find the order of $\mathcal{F}(\mathbb{Z}_2)$, the ring of all functions mapping $\mathbb{Z}_2$ to $\mathbb{Z}_2$, and prove that $f + f = 0$ for every $f \in \mathcal{F}(\mathbb{Z}_2)$.

Solution

Recall that $\mathbb{Z}_2$ has only two elements: $\mathbb{Z}_2 = \{0, 1\}$. By definition, a function $f \in \mathcal{F}(\mathbb{Z}_2)$ must map $\mathbb{Z}_2$ to $\mathbb{Z}_2$. There are only four such functions possible, namely the functions $f_1$,

$f_2$, $f_3$, and $f_4$ defined by

$$\begin{array}{llll} f_1(0) = 0, & f_2(0) = 1, & f_3(0) = 0, & f_4(0) = 1, \\ f_1(1) = 0, & f_2(1) = 0, & f_3(1) = 1, & f_4(1) = 1. \end{array}$$

We compute:

$$\begin{aligned} (f_1 + f_1)(0) &= 0 + 0 = 0, \\ (f_1 + f_1)(1) &= 0 + 0 = 0, \\ (f_2 + f_2)(0) &= 1 + 1 = 0, \\ (f_2 + f_2)(1) &= 0 + 0 = 0, \\ (f_3 + f_3)(0) &= 0 + 0 = 0, \\ (f_3 + f_3)(1) &= 1 + 1 = 0, \\ (f_4 + f_4)(0) &= 1 + 1 = 0, \\ (f_4 + f_4)(1) &= 1 + 1 = 0. \end{aligned}$$

Thus $f + f$ is the zero function for each $f \in \mathcal{F}(\mathbb{Z}_2)$. □

3. (i) If $R$ is a domain and $S$ is a subring of $R$, show that $S$ is a domain.

Solution

We already know that $S$ is a subring of $R$, so it is itself a commutative ring. Therefore we just have to show that $S$ is a domain. So, suppose that $a$, $b \in S$ are any two nonzero elements of $S$. Then they are certainly two nonzero elements of $R$, so we must have $ab \neq 0$ since $R$ is a domain. Thus, the product of any two nonzero elements of $S$ is nonzero, so $S$ is a domain by Theorem 3.5. □

(ii) Prove that $\mathbb{C}$ is a domain, and conclude that $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are domains.

Solution

We already know that $\mathbb{C}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are commutative rings (see page 143). Suppose that $z = a + bi$ and $w = c + di$ are any two complex numbers in $\mathbb{C}$. This means that $a$, $b$, $c$, and $d$ are arbitrary real numbers. Suppose further that $z$ and $w$ are nonzero. This means that $a$ and $b$ can't both be zero, and $c$ and $d$ can't both be zero. Then $zw = (a + bi)(c + di) = (ac - bd) + (ad + bc)i$, since $i^2 = -1$. Suppose that $zw = 0$. Then $ac = bd$ and $ad = -bc$. Hence $bd^2 = acd = -bc^2$. If $b \neq 0$ then this implies $d^2 = -c^2$, which implies $c = d = 0$ since $c^2$ and $d^2$ are both positive real numbers. But this is impossible since $c$ and $d$ can't both be zero. On the other hand, if $b = 0$ then $ac = bd = 0$ and $ad = -bc = 0$. But either $c$ or $d$ is nonzero, so this implies $a = 0$. And that's impossible, since $a$ and $b$ can't both be zero. Thus, in any case, $zw = 0$ is impossible. Hence the product of any two nonzero elements of $\mathbb{C}$ is nonzero, and therefore $\mathbb{C}$ is a domain.

It follows immediately now from part (i) that $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are all domains, because they are subrings of the domain $\mathbb{C}$. □

(iii) Prove that the ring of Gaussian integers is a domain.

Solution

The ring of Gaussian integers is $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. This is a subset of $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$. Since we know $\mathbb{Z}[i]$ is a commutative ring, it is therefore a subring of $\mathbb{C}$. However, $\mathbb{C}$ is a domain, so any subring of $\mathbb{C}$ is also a domain by part (i). $\square$