Homework 10

Jaden Wang

Problem (19.2)**.** For both cases, we wish to find the multiplicative inverse of 3 to solve for x. It exists because both cases are fields.

Case. $\mathbb{Z}_7$: to find $a \in \mathbb{Z}_7$, the inverse of 3, we know that $3 \times_7 a = 3a \mod 7 = 1$. So $3a = 7n + 1$ for some $n \in \mathbb{Z}$. $n = 1$ doesn't work but $n = 2$ does, and we have $3a = 2 \times 7 + 1 = 15 \Rightarrow a = 5 \in \mathbb{Z}_7$. Thus,

$$\begin{aligned} 3x &= 2 \\ 5 \times_7 3x &= 5 \times_7 2 \\ 1 \cdot x &= 10 \mod 7 \\ x &= 3 \end{aligned}$$

Case. $\mathbb{Z}_{23}$: Similarly, we wish to find the inverse of 3, a, such that $3a = 23n + 1$. $n = 1$ works and gives us $a = 8$. Thus,

$$\begin{aligned} 3x &= 2 \\ 8 \times_7 3x &= 8 \times_{23} 2 \\ 1 \cdot x &= 16 \mod 23 \\ x &= 16 \end{aligned}$$

Problem (19.3)**.** In $\mathbb{Z}_6$:

$$\begin{aligned} x^2 + 2x + 2 &= 0 \\ x^2 + 2x + 1 &= -1 \\ (x+1)^2 &= 5 \end{aligned}$$

Let's find the solution(s) by exhaustion:

$$\begin{aligned}(0+1)^2 &= 1\\ (1+1)^2 &= 4\\ (2+1)^2 &= 3\\ (3+1)^2 &= 4\\ (4+1)^2 &= 1\\ (5+1)^2 &= 0\end{aligned}$$

None of them equals to 5. Hence there is no solution.

Problem (19.11)**.** Since R is commutative, has multiplicative identity, and has characteristic 4, we have $4a = 0$, and

$$\begin{aligned}(a+b)^4 &= (a+b)^2(a+b)^2\\ &= (a^2+2ab+b^2)(a^2+2ab+b^2)\\ &= a^4+2a^3b+a^2b^2+2a^3b+4a^2b^2+2ab^3+a^2b^2+2ab^3+b^4 \text{ by distributivity}\\ &= a^4+4a^3b+4a^2b^2+2a^2b^2+4ab^3+b^4\\ &= a^4+2a^2b^2+b^4 \text{ by } 4a=0\end{aligned}$$

Problem (19.14)**.** Note $\begin{pmatrix}-2 & -2\\ 1 & 1\end{pmatrix} \in M_2(\mathbb{Z})$, we have

$$\begin{pmatrix}1 & 2\\ 2 & 4\end{pmatrix}\begin{pmatrix}-2 & -2\\ 1 & 1\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}.$$

which is the additive identity of $M_2(\mathbb{Z})$. Thus, it is a zero divisor.

Problem (19.15)**.** If a, b are the non-zero elements of the ring R such that $ab = 0$, then a, b are zero divisors of R.

Problem (19.16)**.** If $n \cdot a = 0$ for all elements a in a ring R, then such smallest integer $n > 0$ is the characteristic of R. If no such positive integer exists, then the characteristic of R is 0.

Problem (19.17)**.**

a) False. Let $a, b \in n\mathbb{Z}$, if $ab = 0$ under real multiplication, we have $a = 0$ or $b = 0$. Thus, a, b cannot be zero divisors.

b) True. By theorem.

c) False. It is 0. Suppose there exists a n such that $n \cdot a = 0 \; \forall \; a \in n\mathbb{Z}$, which is true iff $n = 0$ which isn't positive, so such n doesn't exist. Then by definition it's 0.

d) False. If $n = 2$, then $2\mathbb{Z}$ doesn't have multiplicative identity, and this is a structural difference to $\mathbb{Z}$.

e) True. If R is isomorphic to an integral domain, R must have no zero divisors. Thus Theorem 19.5 applies.

f) True. Suppose that the integral domain is finite. Given $a \neq 0 \in R$, it follows that $|a| < \infty$ under addition. Therefore, there exists an $n \in \mathbb{N}$ such that $na = 0$, and by Theorem 19.15, R cannot have characteristic 0. By the contrapositive, if R has characteristic 0, it has to be infinite.

g) False. Consider $(1, 0) \in D_1, (0, 1) \in D_2$. Notice the additivity identity in $D_1 \times D_2$ is $(0, 0)$ which neither equals to. But $(1, 0) * (0, 1) = (0, 0)$, so both are zero divisors. Then the direct product cannot be an integral domain.

h) False. Let's show the contrapositive: An element a in a commutative ring with unity that has a multiplicative inverse $a^{-1} \in R$ cannot be a divisor of zero. Suppose $a \neq 0$ is a zero divisor, by commutativity there exists $b \neq 0$ such that $ab = 0$. We know that $aa^{-1} = 1$ and $ab = 0$, so

$$\begin{aligned}
aa^{-1} - 1 &= ab = 0 \\
a(a^{-1} - b) &= 1 \\
a^{-1}a(a^{-1} - b) &= a^{-1} \cdot 1 \\
a^{-1} - b &= a^{-1} \\
-b &= 0 \\
b &= 0
\end{aligned}$$

which is a contradiction!

i) False. Let $n = 2$, $2\mathbb{Z}$ doesn't have identity and thus cannot be an integral domain.

j) False. The inverse of 2 is $\frac{1}{2} \notin \mathbb{Z}$, so $\mathbb{Z}$ is not a field.

Problem (19.18)**.**

1) $\mathbb{R}$ is a field.

2) $\mathbb{Z}$ is an integral domain.

3) $\mathbb{Z}_{12}$ is a commutative ring with 1, but has zero divisors $3 \times_{12} 4 = 0$.

4) $2\mathbb{Z}$ doesn't have 1 but is commutative.

5) $M_2(\mathbb{R})$ isn't commutative but has the identity matrix.

6) $2\mathbb{Z} \times M_2(\mathbb{R})$ is just a ring because direct product of rings is still a ring, but since $2\mathbb{Z}$ doesn't have identity and $M_2(\mathbb{R})$ isn't commutative, their direct product can't either.

Problem (19.23)**.** Let R be a divisor ring and $a \in R$.

Case. $a \neq 0$, then by definition of division ring, $a^{-1} \in R$, and

$$\begin{aligned} a^2 &= a \\ a^{-1}a^2 &= a^{-1}a \\ a &= 1 \in R \end{aligned}$$

Case. $a = 0$, then $a^2 = 0^2 = 0 \in R$.

Thus, we have considered all cases of a, and only found exactly two elements, 0 and 1, that are idempotent.