Math 127
Suggested solutions to Homework Set 1

Problem 1. (i) We first prove that $(-1) \cdot a = -a$. To do so, we will use the Proposition we discussed in class, which states that, for every $x \in \mathbb{F}$, we have that $0 \cdot x = 0$.

We have that

$$\begin{aligned} a + (-1) \cdot a &= 1 \cdot a + (-1) \cdot a && \text{(1 is the multiplicative identity)} \\ &= (1 + (-1)) \cdot a && \text{(by the right distributive law)} \\ &= 0 \cdot a && \text{(-1 is the additive inverse of 1)} \\ &= 0\,. && \text{(by the above fact)} \end{aligned}$$

We conclude that we have

$$a + (-1) \cdot a = a + (-a)$$

(given that the additive inverse $-a$ of a satisfies $a + (-a) = 0$).

Now, based on the uniqueness of the additive inverse, which we discussed in class, or based on the Cancellation Law for Addition (which we verify in Problem 2 below), we obtain that

$$(-1) \cdot a = -a,$$

as we wanted.

We now prove the second claim of part (i), that $-(b \cdot c) = (-b) \cdot c = b \cdot (-c)$. If we apply what we just showed with $a = b \cdot c$, we can write

$$\begin{aligned} -(b \cdot c) &= (-1) \cdot (b \cdot c) \\ &= \big((-1) \cdot b\big) \cdot c && \text{(multiplication is associative)} \\ &= (-b) \cdot c\,. && \text{(by the first claim again, applied for } a = b \text{ now)} \end{aligned}$$

Similarly,

$$\begin{aligned} -(b \cdot c) &= \big((-1) \cdot b\big) \cdot c && \text{(as before)} \\ &= \big(b \cdot (-1)\big) \cdot c && \text{(-1 commutes with b)} \\ &= b \cdot \big((-1) \cdot c\big) && \text{(multiplication is associative)} \\ &= b \cdot (-c)\,. && \text{(by the first claim again, applied for } a = c \text{ now)} \end{aligned}$$

(ii) We will use the second claim of part (i). By the assumption that $x \neq 0$, we know that x has a multiplicative inverse, denoted by x^{-1}. We can therefore use part (i) as well to write

$$x \cdot \big(-(x^{-1})\big) = -\big(x \cdot x^{-1}\big) = -1.$$

This implies that

$$\begin{aligned} 1 &= -(-1) && \text{(1 is the additive inverse of } -1) \\ &= -\big(x \cdot \big(-(x^{-1})\big)\big) && \text{(by the equality we just checked)} \\ &= (-x) \cdot \big(-(x^{-1})\big) && \text{(by the second claim of part (i) again)} \end{aligned}$$

and moreover

$$= \big(-(x^{-1})\big) \cdot (-x) \qquad \text{(multiplication is commutative in } \mathbb{F}).$$

It follows that $-x$ has a multiplicative inverse and that this is equal to $-(x^{-1})$.

(iii) We have that

$$\begin{aligned} \big([k] \cdot [l]\big) \cdot \big([k]^{-1} \cdot [l]^{-1}\big) &= \big([k] \cdot [l]\big) \cdot \big([l]^{-1} \cdot [k]^{-1}\big) && \text{(multiplication is commutative in } \mathbb{Z}_m) \\ &= \big[\big([k] \cdot [l]\big) \cdot [l]^{-1}\big] \cdot [k]^{-1} && \text{(multiplication is associative)} \\ &= \big[[k] \cdot \big([l] \cdot [l]^{-1}\big)\big] \cdot [k]^{-1} && \text{(multiplication is associative)} \\ &= \big([k] \cdot 1\big) \cdot [k]^{-1} && ([l]^{-1} \text{ stands for the multiplicative inverse of } [l]) \\ &= [k] \cdot [k]^{-1} && \text{(1 stands for the multiplicative identity)} \\ &= 1\,. && ([k]^{-1} \text{ stands for the multiplicative inverse of } [k]) \end{aligned}$$

Therefore, $[k] \cdot [l]$ has a multiplicative inverse, which is equal to $[k]^{-1} \cdot [l]^{-1}$.

Problem 2. (i) Our assumptions are that $a, b, c \in \mathbb{F}$ and that

$$a + b = a + c\,.$$

We recall that there is an element $-a \in \mathbb{F}$ such that $a + (-a) = (-a) + a = 0$. We add to both sides of the above equality the element $-a$: using the associativity of addition as well, we obtain that

$$\begin{aligned} (-a) + (a + b) = (-a) + (a + c) \quad &\Rightarrow \quad ((-a) + a) + b = ((-a) + a) + c \\ &\Rightarrow \quad 0 + b = 0 + c. \end{aligned}$$

Given that 0 is the neutral element of addition, the last equality implies $b = c$, as we wanted.

(ii) Our assumptions are that $a, b, c \in \mathbb{F},\ a \neq 0$ and

$$ab = ac\,.$$

Since $a \neq 0$, we recall that there is an element $a^{-1} \in \mathbb{F}$ such that $aa^{-1} = a^{-1}a = 1$. We multiply both sides of the above equality by the element a^{-1}: using the associativity of multiplication as well, we obtain that

$$a^{-1}(ab) = a^{-1}(ac) \quad \Rightarrow \quad (a^{-1}a)\, b = (a^{-1}a)\, c \quad \Rightarrow \quad 1\, b = 1\, c.$$

Given that 1 is the neutral element of multiplication, the last equality implies $b = c$, as we wanted.

Problem 3. (i) Part (i) of the Proposition continues to hold in commutative rings. In other words, given a commutative ring $\mathcal{R}$, we can prove that, for all $x \in \mathcal{R}$,

$$0 \cdot x,$$

where 0 is the additive identity in $\mathcal{R}$.

Indeed, we have that

$$\begin{aligned} 0 \cdot x + x &= 0 \cdot x + 1 \cdot x && \text{(1 is the multiplicative identity)} \\ &= (0+1) \cdot x && \text{(by the right distributive law in } \mathcal{R}) \\ &= 1 \cdot x && \text{(0 is the additive identity)} \\ &= x\,. && \text{(1 is the multiplicative identity)} \end{aligned}$$

We conclude that we have $0 \cdot x + x = x$, and add now $-x$, the additive inverse of x, to both sides:

$$\begin{aligned} 0 \cdot x &= 0 \cdot x + 0 && \text{(0 is the additive identity)} \\ &= 0 \cdot x + (x + (-x)) && \text{($-x$ is exactly the element for which we have } x + (-x) = 0) \\ &= (0 \cdot x + x) + (-x) && \text{(addition is associative)} \\ &= x + (-x) && \text{(by the above identity)} \\ &= 0. \end{aligned}$$

We have thus verified Part (i) of the Proposition for commutative rings too.

(ii) Part (ii) is not always true for commutative rings.

Consider the commutative ring $\mathbb{Z}_6$ (with modular addition and multiplication). We have seen that $[0]_6$ is the additive identity in $\mathbb{Z}_6$, and thus that the classes $[2]_6$ and $[3]_6$ are both non-zero elements of $\mathbb{Z}_6$. However, $[2]_6 \cdot [3]_6 = [2 \cdot 3]_6 = [0]_6$.

Therefore, in $\mathbb{Z}_6$ the implication

$$x \cdot y = 0 \qquad \Rightarrow \qquad x = 0 \text{ or } y = 0$$

does not hold true.

(iii) Assume towards a contradiction that w is invertible, or in other words

that we can find an element $u \in \mathcal{R}$ such that $wu = 1$. We can then write

$$\begin{aligned}
z &= z \cdot 1 && \text{(1 is the multiplicative identity)} \\
&= z \cdot (wu) && \text{(by our assumption)} \\
&= (zw) \cdot u && \text{(multiplication is associative)} \\
&= 0 \cdot u && \text{(by one of the given assumptions)} \\
&= 0\,. && \text{(by what we showed in part (i) of this problem)}
\end{aligned}$$

In other words, we get that $z = 0$, which contradicts the assumption that $z \neq 0$.

Thus assuming that w is invertible was incorrect.

Problem 4. (i) We confirm that $\mathbb{Q}\big(\sqrt{17}\big)$ is closed under the standard addition and multiplication in $\mathbb{R}$, namely that we have, for any two elements $x, y \in \mathbb{Q}\big(\sqrt{17}\big)$, that $x + y \in \mathbb{Q}\big(\sqrt{17}\big)$ and $xy \in \mathbb{Q}\big(\sqrt{17}\big)$ too.

Indeed, given $x, y \in \mathbb{Q}\big(\sqrt{17}\big)$, then by definition of the set we can find some $a, b, c, d \in \mathbb{Q}$ such that $x = a + \sqrt{17}\, b$ and $y = c + \sqrt{17}\, d$. But then

$$x + y = (a + \sqrt{17}\, b) + (c + \sqrt{17}\, d) = (a + c) + \sqrt{17}\, (b + d) \in \mathbb{Q}\big(\sqrt{17}\big)$$

given that $a + c, b + d \in \mathbb{Q}$. Similarly,

$$\begin{aligned} xy = (a + \sqrt{17}\, b)(c + \sqrt{17}\, d) &= ac + \sqrt{17}\, bc + \sqrt{17}\, ad + 17\, bd \\ &= (ac + 17\, bd) + \sqrt{17}\, (ad + bc) \in \mathbb{Q}\big(\sqrt{17}\big) \end{aligned}$$

given that $ac + 17\, bd$, $ad + bc \in \mathbb{Q}$.

(ii) Observe first of all that, since $\mathbb{Q}\big(\sqrt{17}\big)$ is a subset of $\mathbb{R}$, we immediately get that both addition and multiplication in $\mathbb{Q}\big(\sqrt{17}\big)$ are commutative and associative, and also that they satisfy the distributive law. This is due to the fact that if, for instance, we know that

$$\textit{for all } x, y, z \in \mathbb{R},\ (x + y)z = xz + yz,$$

then we also have that

$$\textit{for all } x, y, z \in \mathbb{Q}\big(\sqrt{17}\big),\ (x + y)z = xz + yz$$

(given that any element of $\mathbb{Q}\big(\sqrt{17}\big)$ is also an element of $\mathbb{R}$).

Moreover, $0 \in \mathbb{Q}\big(\sqrt{17}\big)$ (since $0 \in \mathbb{Q}$ and we can write $0 = 0 + \sqrt{17} \cdot 0$), therefore there is a neutral element of addition in $\mathbb{Q}\big(\sqrt{17}\big)$. Similarly, $1 \in \mathbb{Q}\big(\sqrt{17}\big)$ (since $0, 1 \in \mathbb{Q}$ and we can write $1 = 1 + \sqrt{17} \cdot 0$), therefore there is an identity element in $\mathbb{Q}\big(\sqrt{17}\big)$.

Finally, for every $x = a + \sqrt{17}\, b \in \mathbb{Q}\big(\sqrt{17}\big)$ the element $-x$ (the additive inverse of x in $\mathbb{R}$) is also in $\mathbb{Q}(\sqrt{17})$, given that

$$-x = -(a + \sqrt{17}\, b) = -a - \sqrt{17}\, b = (-a) + \sqrt{17}\, (-b)$$

and $-a, -b \in \mathbb{Q}$ when a, b are rationals.

Similarly, for every non-zero $x = a + \sqrt{17}\, b \in \mathbb{Q}\big(\sqrt{17}\big)$ the element $1/x$ (the multiplicative inverse of x in $\mathbb{R}$) is also in $\mathbb{Q}\big(\sqrt{17}\big)$, given that

$$1/x = 1/(a + \sqrt{17}\, b) = \frac{a - \sqrt{17}\, b}{(a + \sqrt{17}\, b)(a - \sqrt{17}\, b)} = \frac{a - \sqrt{17}\, b}{a^2 - 17\, b^2}$$
$$= \frac{a}{a^2 - 17\, b^2} + \sqrt{17}\, \frac{-b}{a^2 - 17\, b^2}$$

and both $a/(a^2 - 17\, b^2)$ and $(-b)/(a^2 - 17\, b^2)$ are in $\mathbb{Q}$ when a, b are rationals.

Note that here we could multiply and divide by $a - \sqrt{17}\, b$ because this number is non-zero. Indeed, if it were equal to zero, then we would have

$$a = \sqrt{17}\, b \Rightarrow$$
$$\text{either } b = 0, \text{ and hence } a = 0 \text{ too,} \qquad \text{or } b \neq 0 \text{ and } \sqrt{17} = a/b,$$

with both conclusions leading to contradictions:

- we have assumed that $(a, b) \neq (0, 0)$ since $a + \sqrt{17}\, b \neq 0$,
- and on the other hand, when $b \neq 0$, $\sqrt{17}$ cannot be equal to a/b because $a/b \in \mathbb{Q}$ while $\sqrt{17}$ is an irrational number.

Observe finally that, since both $(a + \sqrt{17}\, b)$ and $(a - \sqrt{17}\, b)$ here are non-zero, $a^2 - 17b^2 = (a + \sqrt{17}\, b)(a - \sqrt{17}\, b)$ is also non-zero, and thus the expression that we found above for $1/x$ is valid.

We conclude that $\mathbb{Q}\big(\sqrt{17}\big)$ is a field.

Problem 5. We will show that, out of the given structures, $\mathbb{Z}_3^2$ is the field, while $\mathbb{Z}_5^2$ is a commutative ring, but not a field.

(i) We begin by showing that $\mathbb{Z}_3^2$ together with the given operations is a field.

We have that

Addition is commutative: For any two elements $(a,b),(c,d) \in \mathbb{Z}_3^2$, we have that

$$(a,b)+(c,d) = (a+c, b+d) \quad \text{and} \quad (c,d)+(a,b) = (c+a, d+b).$$

But since addition in $\mathbb{Z}_3$ is commutative, it holds that $a+c = c+a$ and $b+d = d+b$. Hence $(a,b)+(c,d) = (c,d)+(a,b)$.

Addition is associative: For any three elements $(a,b),(c,d),(f,g) \in \mathbb{Z}_3^2$, we have that

$$\big((a,b)+(c,d)\big)+(f,g) = (a+c, b+d)+(f,g) = \big((a+c)+f, (b+d)+g\big)$$
$$\text{and} \quad (a,b)+\big((c,d)+(f,g)\big) = (a,b)+(c+f, d+g) = \big(a+(c+f), b+(d+g)\big).$$

Since addition in $\mathbb{Z}_3$ is associative, it holds that $(a+c)+f = a+(c+f)$ and $(b+d)+g = b+(d+g)$. Therefore, $\big((a,b)+(c,d)\big)+(f,g) = (a,b)+\big((c,d)+(f,g)\big)$.

Neutral element: We first need to determine which element could be the neutral element of addition: we are looking for an element $(c,d) \in \mathbb{Z}_3^2$ such that, for every $(a,b) \in \mathbb{Z}_3^2$, we will have $(c,d)+(a,b) = (a,b)$. But $(c,d)+(a,b) = (c+a, d+b)$, so we need to have $c+a = a$ and $d+b = b$. This is satisfied if $c = 0$ and $d = 0$. We can now verify directly that $(0,0)+(a,b) = (a,b)$ for every $(a,b) \in \mathbb{Z}_3^2$ by noting that $(0,0)+(a,b) = (0+a, 0+b)$.

Additive inverses: For every $(a,b) \in \mathbb{Z}_3^2$ we need to find an element (c,d) such that $(a,b)+(c,d) = (0,0)$. We fix an element (a,b) and note that $(a,b)+(c,d) = (a+c, b+d)$, so in order to have $a+c = 0$ and $b+d = 0$ it must hold that $c = -a$ (the additive inverse of a in $\mathbb{Z}_3$) and $d = -b$. We check that indeed $(a,b)+(-a,-b) = (0,0)$.

Multiplication is commutative: For any two elements $(a,b),(c,d) \in \mathbb{Z}_3^2$, we have that

$$(a,b)(c,d) = (ac-bd, ad+bc) \quad \text{and} \quad (c,d)(a,b) = (ca-db, cb+da).$$

Since both addition and multiplication in $\mathbb{Z}_3$ are commutative, it holds that $ac-bd = ca-db$ and $ad+bc = bc+ad = cb+da$. Hence $(a,b)(c,d) = (c,d)(a,b)$.

Multiplication is associative: For any three elements $(a,b),(c,d),(f,g) \in \mathbb{Z}_3^2$, we have that

$$\big((a,b)(c,d)\big)(f,g) = (ac-bd, ad+bc)(f,g)$$
$$= \big((ac-bd)f - (ad+bc)g, (ac-bd)g + (ad+bc)f\big)$$

$$\text{and } (a,b)\big((c,d)(f,g)\big) = (a,b)(cf-dg, cg+df)$$
$$= \big(a(cf-dg) - b(cg+df), a(cg+df) + b(cf-dg)\big).$$

Using the facts that addition in $\mathbb{Z}_3$ is commutative and associative, and that multiplication in $\mathbb{Z}_3$ is associative and also distributes over addition, we can write

$$(ac-bd)f - (ad+bc)g = (ac)f - (bd)f - (ad)g - (bc)g$$
$$= a(cf) - a(dg) - b(cg) - b(df) = a(cf-dg) - b(cg+df),$$

$$\text{and similarly } (ac-bd)g + (ad+bc)f = (ac)g - (bd)g + (ad)f + (bc)f$$
$$= a(cg) + a(df) + b(cf) + b(-dg) = a(cg+df) + b(cf-dg).$$

Therefore, $\big((a,b)(c,d)\big)(f,g) = (a,b)\big((c,d)(f,g)\big)$.

Identity element: We first need to determine which element could be the identity element: we are looking for an element $(c,d) \in \mathbb{Z}_3^2$ such that, for every $(a,b) \in \mathbb{Z}_3^2$, we will have $(c,d)(a,b) = (a,b)$. But $(c,d)(a,b) = (a,b)(c,d) = (ac-bd, ad+bc)$, so we need to have

$$\left\{ \begin{array}{l} ac-bd = a \\ ad+bc = b \end{array} \right\}.$$

To determine values for c and d it is easier to fix some specific non-zero element (a,b) initially, e.g. $(a,b) = (2,0)$. Then we need to have $2c = 2$ and $2d = 0$ for some $c,d \in \mathbb{Z}_3$, which implies a unique solution for c and d: $(c,d) = (1,0)$.

We can now verify directly that $(1,0)(a,b) = (a,b)$ for every $(a,b) \in \mathbb{Z}_3^2$ by noting that $(1,0)(a,b) = (1a-0b, 1b+0a) = (1a, 1b)$.

Distributive law: For any three elements $(a,b),(c,d),(f,g) \in \mathbb{Z}_3^2$, we have that

$$\big((a,b)+(c,d)\big)(f,g) = (a+c, b+d)(f,g) = \big((a+c)f - (b+d)g, (a+c)g + (b+d)f\big)$$

$$\text{while } (a,b)(f,g) + (c,d)(f,g) = (af-bg, ag+bf) + (cf-dg, cg+df)$$
$$= \big((af-bg) + (cf-dg), (ag+bf) + (cg+df)\big).$$

Using the facts that addition in $\mathbb{Z}_3$ is commutative and associative, and that multiplication in $\mathbb{Z}_3$ is associative and also distributes over addition, we can write

$$(a+c)f-(b+d)g=(af+cf)-(bg+dg)=(af-bg)+(cf-dg),$$
$$\text{and}\quad (a+c)g+(b+d)f=(ag+cg)+(bf+df)=(ag+bf)+(cg+df).$$

Therefore, $\big((a,b)+(c,d)\big)(f,g)=(a,b)(f,g)+(c,d)(f,g)$.

We can conclude that $\mathbb{Z}_3^2$ with the given operations is a commutative ring. It remains to check the existence of a multiplicative inverse for any non-zero element of this structure.

Multiplicative inverses: For every non-zero element $(a,b)\in\mathbb{Z}_3^2$ we need to find an element (c,d) such that $(a,b)(c,d)=(1,0)$. We fix an element (a,b) and note that $(a,b)(c,d)=(ac-bd,ad+bc)$, so we need to have

$$\left\{\begin{array}{c} ac-bd=1 \\ ad+bc=0 \end{array}\right\}.$$

To solve this system, we consider three cases, with the first one being the most difficult:

Case 1: $a\neq 0$, $b\neq 0$. In this case, we can multiply both sides of the second linear equation by ba^{-1} to get an equivalent linear system:

$$\left\{\begin{array}{c} ac-bd=1 \\ ad+bc=0 \end{array}\right\} \Leftrightarrow \left\{\begin{array}{c} ac-bd=1 \\ bd+a^{-1}b^2c=0 \end{array}\right\} \Leftrightarrow \left\{\begin{array}{c} (a+a^{-1}b^2)c=1 \\ bd+a^{-1}b^2c=0 \end{array}\right\}.$$

We could now solve for c in the first equation if we knew that $a+a^{-1}b^2$ is not zero: we can write

$$a+a^{-1}b^2=a^{-1}a^2+a^{-1}b^2=a^{-1}(a^2+b^2),$$

so it suffices (why?) to check that $a^2+b^2\neq 0$. But in the case we are analysing here, a is a non-zero element of $\mathbb{Z}_3$, so it is either 1 or 2, and hence $a^2=1$ (since $1^1=1=2^2$ in $\mathbb{Z}^3$); for the same reason $b^2=1$, therefore $a^2+b^2=2\neq 0$. We can thus continue solving the linear system above:

$$\left\{\begin{array}{c} c=(a+a^{-1}b^2)^{-1} \\ bd+a^{-1}b^2c=0 \end{array}\right\} \Leftrightarrow \left\{\begin{array}{c} c=(a+a^{-1}b^2)^{-1} \\ bd=-a^{-1}b^2c \end{array}\right\} \Leftrightarrow \left\{\begin{array}{c} c=(a+a^{-1}b^2)^{-1} \\ d=-a^{-1}b(a+a^{-1}b^2)^{-1} \end{array}\right\}.$$

We conclude that in the case that $a\neq 0$ and $b\neq 0$, the element (a,b) of $\mathbb{Z}_3^2$ has a multiplicative inverse.

Case 2: $a = 0$. In this case necessarily $b \neq 0$ (given that $(a, b) \neq (0, 0)$). Again, we need to find a solution to the system of linear equations $ac - bd = 1$ and $ad + bc = 0$, which now simplify to

$$\left\{ \begin{array}{c} -bd = 1 \\ bc = 0 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} d = -b^{-1} \\ c = 0 \end{array} \right\}.$$

Therefore in this case as well the element (a, b) has a multiplicative inverse.

Case 3: $b = 0$. This case is completely analogous to the previous one: in this case necessarily $a \neq 0$. The linear system we need to solve this time is

$$\left\{ \begin{array}{c} ac = 1 \\ ad = 0 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} c = a^{-1} \\ d = 0 \end{array} \right\}.$$

Therefore, in this final case too the system has a solution and thus the element (a, b) has a multiplicative inverse.

We finally observe that these three cases cover all possibilities for what values a and b can take, therefore we have checked that every non-zero (a, b) in $\mathbb{Z}_3^2$ has a multiplicative inverse.

Problem 5 (cont.) (ii) We now show that $\mathbb{Z}_5^2$ together with the given operations is a commutative ring but not a field.

First of all, we have that

Addition is commutative: We can repeat the argument above for the corresponding property, except that now we will use the fact that addition in $\mathbb{Z}_5$ is commutative.

Addition is associative: We can repeat the argument above for the corresponding property, except that now we will use the fact that addition in $\mathbb{Z}_5$ is associative.

Neutral element: We can check that $(0,0)+(a,b) = (a,b)$ for every $(a,b) \in \mathbb{Z}_5^2$ by noting that $(0,0) + (a,b) = (0+a, 0+b) = (a,b)$.

Additive inverses: We can check that, for every $(a,b) \in \mathbb{Z}_5^2$, $(a,b)+(-a,-b) = (0,0)$ (where $-a$ is the additive inverse of a in $\mathbb{Z}_5$ and $-b$ the additive inverse of b) by noting that $(a,b)+(-a,-b) = (a+(-a), b+(-b)) = (0,0)$.

Multiplication is commutative: We can repeat the argument above for the corresponding property, except that now we will use the fact that addition and multiplication in $\mathbb{Z}_5$ are commutative.

Multiplication is associative: We can repeat the argument above for the corresponding property, except that now we will use the fact that addition in $\mathbb{Z}_5$ is commutative and associative, while multiplication in $\mathbb{Z}_5$ is associative and also distributes over addition.

Identity element: We can check that $(1,0)(a,b) = (a,b)$ for every $(a,b) \in \mathbb{Z}_5^2$ by noting that $(1,0)(a,b) = (1a - 0b, 1b + 0a) = (1a, 1b) = (a,b)$.

Distributive law: We can repeat the argument above for the corresponding property, except that now we will use the fact that addition in $\mathbb{Z}_5$ is commutative and associative, while multiplication in $\mathbb{Z}_5$ is associative and also distributes over addition.

Based on these, we conclude that $\mathbb{Z}_5^2$ with the given operations is a commutative ring.

It remains to check that it is not a field. We could try to adapt the argument for showing the existence of multiplicative inverses which we have above and try to see what needs to be different. It is not hard to confirm

that Cases 2 and 3 would work in the same way. However in Case 1, where $a \neq 0$ and $b \neq 0$, in order to solve the system

$$\left\{ \begin{array}{l} ac - bd = 1 \\ ad + bc = 0 \end{array} \right\},$$

we need at some step to ensure that the element $a^2 + b^2 \neq 0$. This is not always true in $\mathbb{Z}_5$ as we can see for instance if $a = 2$ and $b = 1$: $a^2 + b^2 = 2^2 + 1^2 = 4 + 1 = 0$. This should make us suspect that the element $(2, 1)$ is not invertible.

We can verify this by observing that $(2, 1)(1, 2) = (0, 0)$ (given that $(2, 1)(1, 2) = (2 \cdot 1 - 1 \cdot 2,\ 2^2 + 1^2)$). But $(1, 2) \neq 0$ and according to Problem 3, part (iii) of this homework set, if $wz = 0$ and $z \neq 0$ then w is not invertible (here we choose $w = (2, 1)$ and $z = (1, 2)$). (*Alternatively, we could recall the related proposition that we discussed in class, which states that in every field* $\mathbb{F}$*, if* $x, y \in \mathbb{F}$ *satisfy* $xy = 0$ *then* $x = 0$ *or* $y = 0$*; given that in* $\mathbb{Z}_5^2$ *with the given operations* $(2, 1)(1, 2) = (0, 0)$ *with both* $(2, 1)$ *and* $(1, 2)$ *being non-zero, we see that this structure cannot be a field.*)

Problem 6. (i) We need to look at the multiplication table of $\mathbb{Z}_{13}$:

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
[0]													
[1]													
[2]													
[3]													
[4]													
[5]													
[6]													
[7]													
[8]													
[9]													
[10]													
[11]													
[12]													

We already know what its first row looks like, but we ignore this as we only care about non-zero elements. We also don't need to fill out the second row, as we already know that $[1]^{-1} = [1]$.

We move on to the third row (the row corresponding to [2]):

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[12]	[14]	[16]	[18]	[20]	[22]	[24]

which is the same as

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[12]	[1]	[3]	[5]	[7]	[9]	[11]

We thus see that $[2]^{-1} = [7]$, which also gives us that $[7]^{-1} = [2]$.

Similarly, we complete the rows corresponding to [3], [4], [5] and [6]:

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[12]	[1]	[3]	[5]	[7]	[9]	[11]
[3]	[0]	[3]	[6]	[9]	[12]	[2]	[5]	[8]	[11]	[1]	[4]	[7]	[10]
[4]	[0]	[4]	[8]	[12]	[3]	[7]	[11]	[2]	[6]	[10]	[1]	[5]	[9]
[5]	[0]	[5]	[10]	[2]	[7]	[12]	[4]	[9]	[1]	[6]	[11]	[3]	[8]
[6]	[0]	[6]	[12]	[5]	[11]	[4]	[10]	[3]	[9]	[2]	[8]	[1]	[7]

which gives that $[3]^{-1} = [9]$, that $[4]^{-1} = [10]$, that $[5]^{-1} = [8]$ and that $[6]^{-1} = [11]$. This also shows that $[9]^{-1} = [3]$ (which is why we don't have to

fill out the row corresponding to [9] after all), and analogously that $[10]^{-1} = [4]$, that $[8]^{-1} = [5]$ and that $[11]^{-1} = [6]$.

The only remaining non-zero element is [12], which necessarily will be its own multiplicative inverse too; we can verify this by computing $12 \cdot 12 = 144 = 13 \cdot 11 + 1$, which shows that $[12] \cdot [12] = [12 \cdot 12] = [1]$.

What we found is summarised in the following table:

x	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
x^{-1}	[1]	[7]	[9]	[10]	[8]	[11]	[2]	[5]	[3]	[4]	[6]	[12]

.

Alternative solution to (i) using Bézout's identity: Just as an example, we will confirm that $[5]^{-1} = [8]$ using an alternative method that we discussed in class, which relies on Bézout's identity. This method may be more helpful to use if we are asked the same question in a different $\mathbb{Z}_p$ with p really large: e.g. if we are asked to find the multiplicative inverse of 5 in $\mathbb{Z}_{1031}$ (note that 1031 is the 173-th prime number, as we can find with a simple internet search).

We begin by observing that $\gcd(5, 13) = 1$ and we recall that Bézout's identity tells us that we can find $t, s \in \mathbb{Z}$ such that

$$5t + 13s = 1 \tag{1}$$

(observe that this is an identity involving integers). This would imply that, in $\mathbb{Z}_{13}$, we have

$$\begin{aligned} [5t + 13s] = [1] \;&\Rightarrow\; [5t] = [5t] + [0] = [5t] + [13s] = [1] \\ &\Rightarrow\; [5] \cdot [t] = [1] \;\Rightarrow\; [5]^{-1} = [t]. \end{aligned}$$

Therefore, to find the multiplicative inverse of [10] in $\mathbb{Z}_{13}$, it suffices to find t and s such that (1) will hold. We can do so by consecutive applications of Euclidean division:

$$\begin{aligned} 13 &= 5 \cdot 2 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1. \end{aligned}$$

Once we end up with a line where the remainder is equal to $1 = \gcd(5, 13)$, we start reversing the process, and writing each remainder as a linear com-

bination of the dividend and the divisor:

$$\begin{aligned} 1 = 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) \cdot 1 &= 3 \cdot 2 - 5 \cdot 1 \\ &= (13 - 5 \cdot 2) \cdot 2 - 5 \cdot 1 = 13 \cdot 2 - 5 \cdot 4 - 5 \cdot 1 \\ &= 13 \cdot 2 + 5 \cdot (-5). \end{aligned}$$

Therefore (1) holds with $t = -5$ and $s = 2$. By the discussion above, this implies that $[5]^{-1} = [-5] = [8]$.

(ii) We will show that $\mathbb{Z}_{39}$ is not a field.

As we have seen, $[0]_{39}$ is the additive identity in $\mathbb{Z}_{39}$. Therefore, the classes $[3]_{39}$ and $[13]_{39}$ are non-zero elements of $\mathbb{Z}_{39}$. However, we have

$$[3]_{39} \cdot [13]_{39} = [3 \cdot 13]_{39} = [0]_{39}\,.$$

We now apply Problem 3, part (iii) of this homework set with, say, $z = [3]_{39}$ and $w = [13]_{39}$: this gives us that $[13]_{39}$ cannot have a multiplicative inverse in $\mathbb{Z}_{39}$, and thus that the axiom about the existence of multiplicative inverses for all non-zero elements is not satisfied.

Problem 7. (a) We have that

$$z + w = (3 + 4\mathbf{i}) + (2 - 3\mathbf{i}) = (3 + 2) + (4 - 3)\mathbf{i} = 5 + \mathbf{i}\,,$$
$$zw = (3 + 4\mathbf{i}) \cdot (2 - 3\mathbf{i}) = (3 \cdot 2 - 4 \cdot (-3)) + (3 \cdot (-3) + 4 \cdot 2)\mathbf{i} = 18 - \mathbf{i}\,,$$
$$z/w = z \cdot w^{-1} = z \cdot \frac{\overline{w}}{|w|^2} = (3 + 4\mathbf{i}) \cdot \frac{2 + 3\mathbf{i}}{13} = -\frac{6}{13} + \frac{17}{13}\mathbf{i}\,.$$
$$z \cdot \overline{w} = (3 + 4\mathbf{i}) \cdot (2 + 3\mathbf{i}) = -6 + 17\mathbf{i}\,.$$

Moreover,

$$\operatorname{Re} z = \operatorname{Re}(3 + 4\mathbf{i}) = 3, \qquad \operatorname{Im} z = \operatorname{Im}(3 + 4\mathbf{i}) = 4$$
$$\text{and} \quad |z| = \sqrt{3^2 + 4^2} = 5\,.$$

Finally, by the formula we have given for the argument, we have that

$$\arg(z) = \arg(3 + 4\mathbf{i}) = \arctan(4/3)\,.$$

(b) We want to find a complex number y satisfying

$$y^2 = \text{conjugate of } -3 - 4\mathbf{i} = -3 + 4\mathbf{i}\,.$$

We first find the exponential form of $-3 + 4\mathbf{i}$: we have that $|-3 + 4\mathbf{i}| = 5$, while $\arg(-3 + 4\mathbf{i}) = \arctan(-4/3) + \pi$. Thus

$$-3+4\mathbf{i} = |-3+4\mathbf{i}| \cdot \exp\big(\mathbf{i}\,(\arctan(-4/3)+\pi)\big) = 5 \cdot \exp\big(\mathbf{i}\,(\arctan(-4/3)+\pi)\big)\,.$$

We now recall that one square root of $-3 + 4\mathbf{i}$ is the number

$$\sqrt{5} \cdot \exp\Big(\mathbf{i}\,\frac{\arctan(-4/3) + \pi}{2}\Big)\,.$$

(c) We first observe that the multiplicative inverse of 4 in $\mathbb{Z}_{11}$ is equal to 3, since $4 \cdot 3 = 12 = 1$ (note also that here we are omitting brackets, and we are identifying the representatives with the classes they belong to as far as notation is concerned).

We can now write

$$\begin{aligned}\frac{(2 + 22 - 5)(3^2 + 6)}{4} &= (2 + 22 - 5)(9 + 6) \cdot 3 \\ &= (2 - 5) \cdot 15 \cdot 3 \\ &= -3 \cdot (4 \cdot 3) \\ &= -3 \cdot 1 \\ &= -3\,.\end{aligned}$$

(d) (i) In Problem 6, part (i) of this homework set, we found that $3^{-1} = 9$ in $\mathbb{Z}_{13}$.

Therefore, we can note that the linear equation $3x = 5$ implies that

$$x = (9 \cdot 3)x = 9(3x) = 9 \cdot 5 = 45 = 6\,.$$

In other words, $x = 6$ is the unique solution to the equation.

(ii) Again, in Problem 6, part (i) of this homework set, we found that $1^1 = 1 = 12^2$, hence $x = 1$ and $x = 12 = -1$ are solutions to the equation $x^2 = 1$ (alternatively, we could simply note that clearly $1 \cdot 1 = 1$, and also, as we've already established in Problem 1, $(-1) \cdot (-1) = 1$, with -1 being equal to 12 here).

We note that these are the only solutions, because we can write

$$x^2 = 1 \quad \Leftrightarrow \quad x^2 - 1^2 = 0 \quad \Leftrightarrow \quad (x-1)(x+1) = 0\,,$$

and, given that x takes values in the field $\mathbb{Z}_{13}$, we see that the last equation is true if and only if $x - 1 = 0$ or $x + 1 = 0$, which implies that only the values 1 and -1 for x will satisfy the equation.

(iii) By inspection, we see that $5^2 = 25 = 25 - 26 = -1$ in $\mathbb{Z}_{13}$.

To find the remaining solution of the equation $x^2 = -1$ in $\mathbb{Z}_{13}$, we write

$$x^2 = -1 = 5^2 \quad \Leftrightarrow \quad x^2 - 5^2 = 0 \quad \Leftrightarrow \quad (x-5)(x+5) = 0\,.$$

But since we are working in a field, $(x - 5)(x + 5) = 0$ can only be true if $x - 5 = 0$ or $x + 5 = 0$. In other words, if $x = 5$ or $x = -5$.

(e) (i) We can immediately see that $x = 0$ satisfies the equation $x^2 = 0$.

At the same time, by inspection we find that $x = 4$, $x = 8$ and $x = 12$ also solve the equation $x^2 = 0$ in $\mathbb{Z}_{16}$.

Also, by inspection we can check that these are the only solutions to the equation $x^2 = 0$ in $\mathbb{Z}_{16}$.

(ii) Analogously to part (d) (ii) above, we can directly see that $x = 1$ and $x = -1 = 16 - 1 = 15$ solve the equation $x^2 = 1$ in $\mathbb{Z}_{16}$.

By inspection, we also see that $7^2 = 49 = 49 - 48 = 1$, and thus $x = 7$ also solves the equation. But then, we can also conclude that $-7 = 16 - 7 = 9$ solves the equation.

Finally, we can double check that these are the only solutions to the equation in $\mathbb{Z}_{16}$ (given that for none of the classes corresponding to an even remainder k we can have $k^2 \equiv 1 \pmod{16}$, while for $k = 3$ and $k = 5$ we have $k^2 = 9 \not\equiv 1 \pmod{16}$ and $k^2 = 25 \equiv 25 - 16 = 9 \not\equiv 1 \pmod{16}$ respectively;

finally since the classes $k = 3$ and $k = 5$ do not solve the equation $x^2 = 1$, the classes $k = 13 = -3$ and $k = 11 = -5$ cannot solve it either).

(iii) We saw in parts (e) (i) and (ii) that 7 is invertible in $\mathbb{Z}_{16}$, while 12 satisfies $12^2 = 0$.

Assume now towards a contradiction that we could find $x_0 \in \mathbb{Z}_{16}$ such that $12x_0 = 7$.

Then we could write

$$1 = 7^2 = (12x_0) \cdot 7 = 12 \cdot (x_0 \cdot 7),$$

which would show that 12 is invertible too. But this contradicts what we showed in Problem 3, part (iii) of this homework set.

We conclude that there is no $x_0 \in \mathbb{Z}_{16}$ such that $12x_0 = 7$, or in other words that the equation $12x = 7$ has no solution.

(iv) We note that $12 = 4 \cdot 3$, and thus, if we can find x such that $3x = 1$, we will be able to write

$$4 = 4 \cdot 1 = 4 \cdot (3 \cdot x) = (4 \cdot 3) \cdot x = 12x.$$

It is not hard to check that 3 is invertible in $\mathbb{Z}_{16}$ (this is because $\gcd(3, 16) = 1$), and that $3^{-1} = 11$. Thus $x = 11$ solves the equation $12x = 4$.

Note however that this is not the only solution. Indeed, we want to have

$$4 = 12x = 4 \cdot 3x \quad \Leftrightarrow \quad 4 \cdot 3x - 4 = 0 \quad \Leftrightarrow \quad 4 \cdot (3x - 1) = 0,$$

where the last equivalence follows from the left distributive property and the fact that $4 = 4 \cdot 1$. But this shows that x is a solution to the equation $12x = 4$ if and only if $3x - 1$ multiplied by 4 will give us 0.

By inspection we find that $4y = 0$ if and only if $y = 0$ or $y = 4$ or $y = 8$ or $y = 12$. Therefore, to find all the solutions to the equation $12x = 4$, we need to solve the equations

$$3x - 1 = 0, \qquad 3x - 1 = 4, \qquad 3x - 1 = 8, \quad \text{and} \quad 3x - 1 = 12$$

or equivalently the equations

$$3x = 1, \qquad 3x = 5 \qquad 3x = 9, \quad \text{and} \quad 3x = 13\,.$$

We finally note that since 3 is invertible in $\mathbb{Z}_{16}$, each of these equations has a unique solution:

$$\begin{aligned} 3x = 1 \quad &\Leftrightarrow \quad x = 11, \\ 3x = 5 \quad &\Leftrightarrow \quad x = 11 \cdot 5 = 55 = 55 - 48 = 7, \\ 3x = 9 \quad &\Leftrightarrow \quad x = 11 \cdot 9 = 99 = 99 - 96 = 3, \\ \text{and} \quad 3x = 13 \quad &\Leftrightarrow \quad x = 11 \cdot 13 = 143 = 143 - 144 = -1 = 15. \end{aligned}$$

We conclude that the solutions to the equation $12x = 4$ are the elements 3, 7, 11 and 15.