

MAT240 Problem Set 1 Solutions

September 30, 2008

Note: There is often more than one solution to a given problem, and so do not interpret these solutions as the only possible set. Also, only partial solutions are given for some problems when appropriate. Finally, if you see any errors, you should let your TA know.

1. Express the following complex numbers in the form $a + bi$, $a, b \in \mathbb{R}$.

(a)

$$\begin{aligned}\frac{(2-i)^3}{(4i+1)^2} &= \frac{2-11i}{(4i+1)^2} \\ &= \frac{(2-11i)(-4i+1)^2}{(4i+1)^2(-4i+1)^2} \\ &= \frac{(2-11i)(-15-8i)}{|4i+1|^4} && \text{(complex conjugates!)} \\ &= \frac{(-118)}{289} + \frac{149}{289}i\end{aligned}$$

(b)

$$\begin{aligned}\frac{1}{\sqrt{5}+i} - \frac{2}{3-i} &= \frac{\sqrt{5}-i}{(\sqrt{5}+i)(\sqrt{5}-i)} - \frac{2(3+i)}{(3-i)(3+i)} \\ &= \frac{\sqrt{5}-i}{6} - \frac{6+2i}{10} \\ &= \frac{-18+5\sqrt{5}}{30} + \frac{-11i}{30}\end{aligned}$$

2. In each case below, find all complex numbers that belong to the indicated set S . (Sketches not included.)

(a) $S = \{z \in \mathbb{C} \mid z^4 \in \mathbb{R}\}$.

Solution. Let $z = r(\cos(\theta) + i \sin(\theta))$ be in S . Then,

$$\begin{aligned}z^4 &= r^4(\cos(\theta) + i \sin(\theta))^4 \\ &= r^4(\cos(4\theta) + i \sin(4\theta)) && \text{(de Moivre's formula!)} \\ &= r^4 \cos(4\theta) + ir^4 \sin(4\theta).\end{aligned}$$

Since we want z^4 to be a real number, we must have an imaginary part of 0. That is, we must have

$$r^4 \sin(4\theta) = 0.$$

If $r = 0$, then $z = 0 \in \mathbb{R}$ and we are done. However, if $r \neq 0$, then divide both sides above by r^4 , and we are left with

$$\sin(4\theta) = 0.$$

Recalling your trigonometry, this means that $4\theta = \pi k$ where $k \in \mathbb{Z}$, or that $\theta = \frac{\pi}{4}k$, $k \in \mathbb{Z}$. The result is the set of complex numbers of the form $z = c(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})$ and $z = c(\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})$ where c is any real number.

- (b) $S = \{z \in \mathbb{C} \mid z^3 \in i\mathbb{R}\}$.

Solution. Let $z = r(\cos(\theta) + i\sin(\theta))$ be in S . Then,

$$\begin{aligned} z^3 &= r^3(\cos(\theta) + i\sin(\theta))^3 \\ &= r^3(\cos(3\theta) + i\sin(3\theta)) && \text{(de Moivre's formula!)} \\ &= r^3 \cos(3\theta) + ir^3 \sin(3\theta). \end{aligned}$$

We want z to be pure imaginary, and so we want $r^3 \cos(3\theta)$ to be 0. Similar to above, if $r = 0$, then $z = 0 = 0i$, and we are done. However, if $r \neq 0$, then $\cos(3\theta) = 0$, and so $3\theta = \frac{(2k+1)\pi}{2}$ or $\theta = \frac{(2k+1)\pi}{6}$, $k \in \mathbb{Z}$. The result is the set of complex numbers of the form $z = r(\cos(\frac{(2k+1)\pi}{6}) + i\sin(\frac{(2k+1)\pi}{6}))$, with $k \in \mathbb{Z}$ and $r \geq 0$.

3. Let $F = \{(a_1, a_2) \mid a_1, a_2 \in \mathbb{R}\}$. If $(a_1, a_2), (b_1, b_2) \in F$, define

$$\begin{aligned} (a_1, a_2) + (b_1, b_2) &= (a_1 + b_1, a_2 + b_2) && \text{(addition in } F) \\ (a_1, a_2)(b_1, b_2) &= (a_1b_1 + 3a_2b_2, a_1b_2 + a_2b_1) && \text{(multiplication in } F) \end{aligned}$$

- (a) Find a multiplicative inverse of the element $(\sqrt{5}, 1)$ in F .

Solution. The element $(\frac{\sqrt{5}}{2}, \frac{-1}{2})$ is a multiplicative inverse for $(\sqrt{5}, 1)$. Recall that the definition of the multiplicative inverse requires knowing what the multiplicative identity is, and so we must first find this. We claim it is $(1, 0)$. Fix any $(a_1, a_2) \in F$. Then,

$$(a_1, a_2)(1, 0) = (a_1 + 0, 0 + a_2) = (a_1, a_2).$$

So, $(1, 0)$ is indeed the inverse. Now, proceeding with the problem,

$$(\sqrt{5}, 1)(\frac{\sqrt{5}}{2}, \frac{-1}{2}) = (\frac{5}{2} - \frac{3}{2}, \frac{-\sqrt{5}}{2} + \frac{\sqrt{5}}{2}) = (1, 0).$$

And so we are done. (Technically, we should show that $(\frac{\sqrt{5}}{2}, \frac{-1}{2})(\sqrt{5}, 1) = (1, 0)$ as well, but the commutativity of multiplication is clear from the definition and the fact that multiplication in \mathbb{R} is commutative.)

- (b) Prove that F is not a field relative to the above addition and multiplication by finding an example of a nonzero element of F which does not have a multiplicative inverse.

Proof. Consider the element $(\sqrt{3}, 1)$, and assume that it has an inverse (b_1, b_2) . Then, by definition of multiplicative inverses,

$$(\sqrt{3}, 1)(b_1, b_2) = (1, 0)$$

which gets us

$$(\sqrt{3}b_1 + 3b_2, \sqrt{3}b_2 + b_1) = (1, 0).$$

Solving for b_1 and b_2 (similar to what we did in part (a)), we get $b_1 = -\sqrt{3}b_2$, which gets us $1 = -3b_2 + 3b_2 = 0$, which is absurd, a contradiction. Hence, our assumption that (b_1, b_2) actually exists is false, and hence F is not a field. \square

4. Let \mathbb{F}_5 be the finite field containing 5 elements. Let $F = \{(a_1, a_2) \mid a_1, a_2 \in \mathbb{F}_5\}$. If $(a_1, a_2), (b_1, b_2) \in F$, then define

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1 \pmod{5}, a_2 + b_2 \pmod{5}) \quad (\text{addition in } F)$$

$$(a_1, a_2)(b_1, b_2) = (a_1b_1 + 2a_2b_2 \pmod{5}, a_1b_2 + a_2b_1 \pmod{5}) \quad (\text{multiplication in } F).$$

- (a) Find an additive identity and a multiplicative identity in F .

Solution. Consider $(0, 0) \in F$. For any $(a_1, a_2) \in F$,

$$(a_1, a_2) + (0, 0) = (a_1 + 0, a_2 + 0) = (a_1, a_2),$$

and so $(0, 0)$ is the additive identity of F . Similarly, consider $(1, 0) \in F$.

$$(a_1, a_2)(1, 0) = (a_1 + 0, 0 + a_2) = (a_1, a_2),$$

and so $(1, 0)$ is the multiplicative identity of F .

- (b) Find an additive inverse of $(2, 1)$ in F .

Solution. Consider $(3, 4) \in F$.

$$(2, 1) + (3, 4) = (2 + 3 \pmod{5}, 1 + 4 \pmod{5}) = (0, 0).$$

Commutativity of addition is clear, and so $(3, 4)$ is indeed the additive inverse of $(2, 1)$.

- (c) Find a multiplicative inverse of $(1, 2)$ in F .

Solution. Consider $(2, 1) \in F$.

$$(1, 2)(2, 1) = (2 + 4 \pmod{5}, 1 + 4 \pmod{5}) = (1, 0).$$

Again, commutativity of multiplication is clear, and so $(2, 1)$ is indeed the multiplicative inverse of $(1, 2)$.

- (d) Find all elements (a_1, a_2) in F that satisfy $(a_1, a_2)^2 = (1, 1)$.

Solution. We must find *all* such elements to the formula above; that is, we must solve for a_1 and a_2 (and make note of possible multiple answers).

$$\begin{aligned} (a_1, a_2)^2 = (1, 1) &\Rightarrow (a_1^2 + 2a_2^2 \pmod{5}, 2a_1a_2 \pmod{5}) = (1, 1) \\ &\Rightarrow \begin{cases} a_1^2 + 2a_2^2 = 1 \pmod{5} \\ 2a_1a_2 = 1 \pmod{5} \end{cases} \end{aligned}$$

In \mathbb{F}_5 , 3 is the multiplicative inverse of 2, and so $2a_1a_2 = 1 \pmod{5}$ is the same as saying $a_1a_2 = 3 \pmod{5}$. We want to multiply by a_2^{-1} , so let us assume for the moment that $a_2 \neq 0$. So, in this case, $a_1 = 3a_2^{-1} \pmod{5}$. Plugging this into $a_1^2 + 2a_2^2 = 1 \pmod{5}$, we get $9a_2^{-2} + 2a_2^2 = 4a_2^{-2} + 2a_2^2 = 1 \pmod{5}$. Multiplying both sides by a_2^2 , we get a quadratic equation in a_2^2 :

$$\begin{aligned} 2a_2^4 - a_2^2 + 4 &= 2a_2^4 + 4a_2^2 + 4 = 0 \pmod{5} \\ \Rightarrow a_2^4 + 2a_2^2 + 2 &= 0 \pmod{5} && (\text{multiply both sides by } 3 = 2^{-1}) \\ \Rightarrow (a_2^2 + 3)(a_2^2 + 4) &= 0 \pmod{5} \end{aligned}$$

Since \mathbb{F}_5 is a field, either $(a_2^2 + 3)$ or $(a_2^2 + 4)$ has to be $0 \pmod{5}$, or equivalently, $a_2^2 = -3 = 2 \pmod{5}$ or $a_2^2 = -4 = 1 \pmod{5}$. Now, note the squares in \mathbb{F}_5 : $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$

and $4^2 = 1$, all modulo 5, of course. Thus, $a_2^2 = 2$ has no solution, whereas $a_2^2 = 1$ has two: namely $a_2 = 1$ or $a_2 = 4$, in which case $a_1 = 3(1^{-1}) = 3$ or $a_1 = 3(4^{-1}) = 2 \pmod{5}$, respectively. Thus, we have two solutions to the problem: $(3, 1)$ and $(2, 4)$: you can check by squaring them that their squares are indeed $(1, 1)$ yourselves. Remember we skipped the case where $a_2 = 0$. If this was the case, then,

$$(a_1, 0)^2 = (a_1^2 + 0, 0) \neq (1, 1),$$

and so no solutions arise from this case.

Note that we could also have squared all possible pairs $(a_1, a_2) \in F$ to see which ones get us $(1, 1)$ in order to obtain the solution.

5. If $a \in \mathbb{F}$ such that $a = a^{-1}$, then $a = 1$ or $a = -1$.

Proof. Note that $a \neq 0$ since a^{-1} exists (by the definition of the multiplicative inverse).

$$\begin{aligned}
 a = a^{-1} &\Rightarrow a^2 = aa^{-1} && \text{(multiplication on the left by } a) \\
 &\Rightarrow a^2 = 1 && \text{(multiplicative inverse)} \\
 &\Rightarrow a^2 - 1 = 1 - 1 && \text{(addition on the right by } -1) \\
 &\Rightarrow a^2 - 1 = 0 && \text{(additive inverse)} \\
 &\Rightarrow (a^2 - 1) + 0 = 0 && \text{(additive identity)} \\
 &\Rightarrow (a^2 - 1) + (-a + a) = 0 && \text{(additive inverse)} \\
 &\Rightarrow ((a^2 - 1) + (-a)) + a = 0 && \text{(associativity of addition)} \\
 &\Rightarrow (a^2 + (-1 + (-a))) + a = 0 && \text{(associativity of addition)} \\
 &\Rightarrow (a^2 + ((-a) - 1)) + a = 0 && \text{(commutativity of addition)} \\
 &\Rightarrow ((a^2 + (-a)) - 1) + a = 0 && \text{(associativity of addition)} \\
 &\Rightarrow (a^2 + (-a)) + (-1 + a) = 0 && \text{(associativity of addition)} \\
 &\Rightarrow (a^2 + (-1)a) + (-1 + a) = 0 && -c = (-1)c \text{ for all } c \in \mathbb{F} \\
 &\Rightarrow (a - 1)a + (-1 + a) = 0 && \text{(distributivity)} \\
 &\Rightarrow (a - 1)a + (a - 1) = 0 && \text{(commutativity of addition)} \\
 &\Rightarrow (a - 1)(a + 1) = 0 \quad (*) && \text{(distributivity)}
 \end{aligned}$$

If $a - 1 = 0$, then $(a - 1) + 1 = 0 + 1$, and so by associativity of addition, $a + (-1 + 1) = 0 + 1$. Then $a + 0 = 0 + 1$ by definition of an additive inverse, $a = 0 + 1$ by definition of the additive identity, and again by definition of the additive identity $a = 1$, and we are done. If, however, $a - 1 \neq 0$, then there

exists a multiplicative inverse $(a - 1)^{-1}$. So starting from (*) above:

$$\begin{aligned}
(a - 1)(a + 1) = 0 &\Rightarrow (a - 1)^{-1}((a - 1)(a + 1)) = (a - 1)^{-1}0 && \text{(multiplication on the left by } (a - 1)^{-1}\text{)} \\
&\Rightarrow ((a - 1)^{-1}(a - 1))(a + 1) = (a - 1)^{-1}0 && \text{(associativity of multiplication)} \\
&\Rightarrow 1(a + 1) = (a - 1)^{-1}0 && \text{(multiplicative inverse)} \\
&\Rightarrow a + 1 = (a - 1)^{-1}0 && \text{(multiplicative identity)} \\
&\Rightarrow a + 1 = (a - 1)^{-1}(a - a) && \text{(additive inverse)} \\
&\Rightarrow a + 1 = (a - 1)^{-1}a + (a - 1)^{-1}(-a) && \text{(distributivity)} \\
&\Rightarrow a + 1 = (a - 1)^{-1}a + (a - 1)^{-1}((-1)a) && -c = (-1)c \text{ for all } c \in \mathbb{F} \\
&\Rightarrow a + 1 = (a - 1)^{-1}a + ((a - 1)^{-1}(-1))a && \text{(associativity of multiplication)} \\
&\Rightarrow a + 1 = (a - 1)^{-1}a + ((-1)(a - 1)^{-1})a && \text{(commutativity of multiplication)} \\
&\Rightarrow a + 1 = (a - 1)^{-1}a + (-1)((a - 1)^{-1}a) && \text{(associativity of multiplication)} \\
&\Rightarrow a + 1 = (a - 1)^{-1}a - ((a - 1)^{-1}a) && -c = (-1)c \text{ for all } c \in \mathbb{F} \\
&\Rightarrow a + 1 = 0 && \text{(additive inverse)} \\
&\Rightarrow (a + 1) - 1 = 0 - 1 && \text{(addition on the right by } -1\text{)} \\
&\Rightarrow a + (1 - 1) = 0 - 1 && \text{(associativity of addition)} \\
&\Rightarrow a + 0 = 0 - 1 && \text{(additive inverse)} \\
&\Rightarrow a = 0 - 1 && \text{(additive identity)} \\
&\Rightarrow a = -1 && \text{(additive identity)}
\end{aligned}$$

So, either $a = 1$ or $a = -1$. □

6. Find the zeroes of each polynomial f below in the indicated field \mathbb{F} .

(a) $\mathbb{F} = \mathbb{F}_7$, $f(x) = x^2 + 6x + 1$.

Solution.

$$\begin{aligned}
x^2 + 6x + 1 = 0 \pmod{7} &\Rightarrow x^2 + 6x + 8 = 0 \pmod{7} \\
&\Rightarrow (x + 4)(x + 2) = 0 \pmod{7},
\end{aligned}$$

and so $x = -4 = 3 \pmod{7}$ or $x = -2 = 5 \pmod{7}$.

(b) $\mathbb{F} = \mathbb{F}_5$, $f(x) = x^3 + 1$.

Solution.

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

Hence, 4 is the only zero of f .

(c) $\mathbb{F} = \mathbb{C}$, $f(x) = x^4 - i$.

Solution. This is equivalent to finding the fourth roots of $i = \cos(\frac{\pi}{2}) + i \sin(\frac{\pi}{2})$. That is, some numbers $\cos(\theta + \frac{2k\pi}{4}) + i \sin(\theta + \frac{2k\pi}{4})$ for $k = 0, 1, 2, 3$ such that (by de Moivre) $4\theta = \frac{\pi}{2}$. That is to say, $\theta = \frac{\pi}{8}$. Hence the solution is $x = \cos(\frac{\pi}{8} + \frac{2k\pi}{4}) + i \sin(\frac{\pi}{8} + \frac{2k\pi}{4})$, $k = 0, 1, 2, 3$.

7. Let $\mathbb{F}_4 = \{0, 1, a, b\}$ be the field containing 4 elements. Assume that $1 + 1 = 0$. Prove that $b = a^{-1} = a^2 = a + 1$.

Proof. Consider $ab \in \mathbb{F}_4$. There are four possibilities for what ab is equal to. (Note that a and b are fixed elements of the field; they are not arbitrary elements of it.) If $ab = 0$, then $a = 0$ or $b = 0$, a contradiction (i.e. fields do not have “zero divisors” – if you have not proved this already, then it is worth doing). If $ab = a$, then $b = 1$, a contradiction; likewise, $ab \neq b$. Hence, ab must be equal to 1. In other words, $b = a^{-1}$.

Now, clearly $a^2 \neq 0$. If $a^2 = 1$, then $a = a^{-1} = b$, which is not allowed. If $a^2 = a$, then $a = 1$; again, not allowed. So, $a^2 = b$. Finally, if $a + 1 = 0$, then $a = -1 = 1$ (since $1 + 1 = 0$). If $a + 1 = 1$, then $a = 0$. If $a + 1 = a$, then $1 = 0$. So, $a + 1 = b$. \square

8. Let p be an odd prime number, and let \mathbb{F}_p be the field of order p .

- (a) Prove that if n is an integer that is not divisible by p , then $r_p(n) \neq r_p(-n)$.

Proof. We will prove the “contrapositive”, which is logically equivalent: if $r_p(n) = r_p(-n)$, then p divides n . Let $q_1, q_2 \in \mathbb{Z}$ such that $n = q_1p + r_p(n)$ and $-n = q_2p + r_p(-n)$. Then,

$$\begin{aligned} 2n &= n - (-n) \\ &= q_1p + r_p(n) - q_2p - r_p(-n) \\ &= (q_1 - q_2)p + (r_p(n) - r_p(-n)) \\ &= (q_1 - q_2)p + 0 && \text{(by assumption)} \\ &= (q_1 - q_2)p \end{aligned}$$

and so $2n$ is divisible by p . Since p is an *odd* prime, we conclude that n is divisible by p . \square

- (b) If a is a nonzero element of \mathbb{F}_p , then $a \neq -a$.

Proof. This follows almost directly from part (a): if n is not divisible by p , then $r_p(n) \neq 0 \pmod{p}$. Let $a = r_p(n)$. But then, as we just proved, $a = r_p(n) \neq r_p(-n)$. We need only show that $r_p(-n) = -r_p(n)$ (since $-r_p(n) = -a$). However, since for some $q \in \mathbb{Z}$, $n = qp + r_p(n)$,

$$\begin{aligned} n = qp + r_p(n) &\Rightarrow -n = -qp - r_p(n) \\ &\Rightarrow -n = -qp + p - p - r_p(n) \\ &\Rightarrow -n = (-q - 1)p + (p - r_p(n)). \end{aligned}$$

But, remember that $r_p(n) \in \{0, \dots, p-1\}$, and so $p - r_p(n) \in \{0, \dots, p-1\}$. Thus, $r_p(-n) = p - r_p(n) = -r_p(n) \pmod{p}$. So we have in conclusion that $a \neq -a$. \square

- (c) Suppose $a, b \in \mathbb{F}_p$ such that $a \neq 0 \neq b$ and $a \neq \pm b$. Then $a^2 \neq b^2$.

Proof. Well, $a^2 - b^2 = (a-b)(a+b) \pmod{p}$. Now, $a \neq \pm b$ translates to $(a-b) \neq 0 \neq (a+b)$, and so their product is nonzero. Hence $a^2 - b^2 \neq 0 \pmod{p}$, or $a^2 \neq b^2 \pmod{p}$, and we are done. \square

- (d) There are exactly $\frac{p+1}{2}$ squares in \mathbb{F}_p .

Proof. $0 = 0^2$ is a square, and so we need to show that there are $\frac{p-1}{2}$ nonzero squares in \mathbb{F}_p . Let $f : \mathbb{F}_p \rightarrow \mathbb{F}_p$ be the function taking $x \in \mathbb{F}_p$ to $x^2 \in \mathbb{F}_p$. Now, note that the converse of part (c) is also true: if $a = b$ or $a = -b$, then $a^2 = b^2$. Combined with part (c), what this tells us is that for every pair of nonzero elements $\{a, -a\}$ in \mathbb{F}_p , we get a unique (nonzero) square in \mathbb{F}_p , and vice versa. Of course, we are assuming that we always get a pair: for any nonzero $a \in \mathbb{F}_p$, $-a \neq a$.

But we proved this assumption in part (b). So, let's count: there are p elements in \mathbb{F}_p , and 0 is a square, which comes from squaring 0. The remaining $p - 1$ nonzero elements can be grouped into pairs $\{a, -a\}$, and each pair gives a different square. That's another $\frac{p-1}{2}$ squares. So, in total, we have $1 + \frac{p-1}{2} = \frac{p+1}{2}$ squares in \mathbb{F}_p . \square

9. For each of the following sets, determine whether or not the set is a field.

(a) $F = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ with addition and multiplication as in \mathbb{R} .

Solution. This is a field. The details for associativity, commutativity and distributivity are left to you, however, note that this is a subset of \mathbb{R} , and so all of these properties will in fact be inherited from \mathbb{R} . That leaves checking F to see if it is closed under addition and multiplication, as well as making sure the additive and multiplicative identities and inverses are in there.

Let $a + b\sqrt{3}, c + d\sqrt{3} \in F$. Then,

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + \sqrt{3}(b + d)$$

and

$$(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + \sqrt{3}(ad + bc).$$

As we can see, F is closed under the two operations since \mathbb{Q} is (recall that \mathbb{Q} is a field). Now, what about identities? We know that the additive identity in \mathbb{R} is $0 = 0 + 0\sqrt{3} \in F$, and the multiplicative identity is $1 = 1 + 0\sqrt{3} \in F$. (Feel free to confirm that these are indeed the identities in F .) As for the inverses, if $a + b\sqrt{3} \in F$, then

$$(a + b\sqrt{3}) + (-a + (-b)\sqrt{3}) = 0$$

and

$$(a + b\sqrt{3})\left(\frac{a - b\sqrt{3}}{a^2 - 3b^2}\right) = 1,$$

assuming that $a \neq 0 \neq b$ when checking the multiplicative inverse. Note that the denominator in $\frac{a - b\sqrt{3}}{a^2 - 3b^2}$ is never 0. For if it were, then $a^2 = 3b^2$, and so $a = \pm\sqrt{3}b$. But $a, b \in \mathbb{Q}$, which is a contradiction. So we're safe from dividing by 0. So we're done.

(b) $F = \{a + b\sqrt{7} \mid a, b \in \mathbb{Z}\}$ with addition and multiplication as in \mathbb{R} .

Solution. This is in fact not a field. Note that it is a subset of \mathbb{R} . Consider $2 = 2 + 0\sqrt{7} \in F$. The multiplicative inverse of 2 is $\frac{1}{2}$, which is in \mathbb{R} , but not in F . The corresponding axiom thus fails.

(c) $F = \{(a, b) \mid a, b \in \mathbb{F}_5\}$ with

$$\begin{aligned} (a_1, b_1) + (a_2, b_2) &= (a_1 + a_2, b_1 + b_2) \\ (a_1, b_1)(a_2, b_2) &= (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1). \end{aligned}$$

Solution. This is not a field. Consider the element $(2, 1) \in F$. Assume that it has a multiplicative inverse $(a_1, a_2) \in F$. Then, (after checking that $(1, 0)$ is the multiplicative identity of F),

$$\begin{aligned} (1, 0) &= (2, 1)(a_1, a_2) \\ &= (2a_1 - a_2, 2a_2 + a_1). \end{aligned}$$

So,

$$\begin{cases} 2a_1 - a_2 = 1 \\ 2a_2 + a_1 = 0 \end{cases}$$

and from the second equation, we see that $a_1 = -2a_2 = 3a_2 \pmod{5}$, and inserting this into the first equation, we get $1 = 6a_2 - a_2 = 5a_2 = 0 \pmod{5}$. This is a contradiction. Hence, $(2, 1)$ has no multiplicative inverse.

(d) $F = \{(a, b) \mid a, b \in \mathbb{F}_5\}$ with

$$\begin{aligned}(a_1, b_1) + (a_2, b_2) &= (a_1 + a_2, b_1 + b_2) \\ (a_1, b_1)(a_2, b_2) &= (a_1a_2 + 3b_1b_2, a_1b_2 + a_2b_1).\end{aligned}$$

Solution. This is a field. The associativity, commutativity, distributivity and closure of the operations is for you to check. The additive identity is $(0, 0)$: for any $(a, b) \in F$,

$$(a, b) + (0, 0) = (a + 0, b + 0) = (a, b).$$

The multiplicative identity is $(1, 0)$: for any $(a, b) \in F$,

$$(a, b)(1, 0) = (a + 0, 0 + b) = (a, b).$$

Let $(a, b) \in F$. Then its additive inverse is $(5 - a, 5 - b)$:

$$(a, b) + (5 - a, 5 - b) = (5, 5) = (0, 0) \pmod{5}.$$

Now, let (a, b) be a nonzero element of F . Then its multiplicative inverse is $(\frac{-a}{3b^2 - a^2}, \frac{b}{3b^2 - a^2})$:

$$(a, b)\left(\frac{-a}{3b^2 - a^2}, \frac{b}{3b^2 - a^2}\right) = (1, 0).$$

Note that since $3 \in \mathbb{F}_5$ is not a square (which you are invited to check), $3b^2 - a^2$ can never be 0.

10. (a) Find an odd prime p for which every element in \mathbb{F}_p is a cube in \mathbb{F}_p .

Solution. Consider \mathbb{F}_3 . $0^3 = 0$, $1^3 = 1$ and $2^3 = 8 = 2 \pmod{3}$. So $p = 3$ is an example.

- (b) Find an odd prime p having the property that the set of cubes in \mathbb{F}_p is $\{0, 1, p - 1\}$.

Solution. $p = 3$ satisfies this as well, as demonstrated in part (a). Another example is $p = 7$.

- (c) Suppose that p is an odd prime having the property that if a and b belong to \mathbb{F}_p and $a \neq b$, then $a^2 + ab + b^2 \neq 0$. Then, every element of \mathbb{F}_p is a cube in \mathbb{F}_p .

Proof. Let C be the set of all cubes in \mathbb{F}_p . Then, $C \subseteq \mathbb{F}_p$. We need to show that $\mathbb{F}_p \subseteq C$. We can accomplish this by constructing a one-to-one function from \mathbb{F}_p to C ; that is, a function f so that if $a \neq b$, then $f(a) \neq f(b)$, and so for each element a in the domain, there is a unique element $f(a)$ in the range (or image). So, let f be defined by $f(a) = a^3$. This clearly takes elements from \mathbb{F}_p to C . Let's check to see if it is one-to-one: recall $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$. So if $a \neq b$, which in turn implies that $a^2 + ab + b^2 \neq 0$, then the product $(a - b)(a^2 + ab + b^2)$ is nonzero. Hence, $a^3 \neq b^3$. So, for every element of \mathbb{F}_p , we have a distinct cube. Since \mathbb{F}_p has exactly p elements, then C must have exactly p elements. Since $C \subseteq \mathbb{F}_p$, we can only conclude that $C = \mathbb{F}_p$, and so we are done. \square