MISCELLANEOUS EXAMPLES AND EXERCISES

"*A miscellany is a collection with a natural ordering relation*."
J. E. Littlewood
British mathematician

The few examples and exercises, given below cover the concepts and processes you have studied in this block. Studying the examples, and solving the exercises, will give you a better understanding of the concepts concerned. This will also give you more practice in solving such problems.

Example 1: Which of the following statements are true? Give reasons for your answers.

i) The domain of a binary operation on a set S is S.

ii) If $(G, \cdot)$ is an abelian group, then $x^2 = e \ \forall \ x \in G$.

iii) If $n, m \in \mathbb{N}$, then $[n, m](n, m) = nm$.

Solution: i) False. The domain is $S \times S$.

ii) False. For instance, $\mathbb{Z}$ is abelian, but $2n \neq 0 \ \forall \ n \neq 0$.

iii) True. Here we use the unique factorisation theorem.
Let $n = p_1^{n_1} \ldots p_r^{n_r}$ and $m = p_1^{m_1} \ldots p_r^{m_r}$, where $n_i \geq 0, m_i \geq 0$ for $i = 1, \ldots, r$.
Let $s_i = \min(n_i, m_i)$ and $t_i = \max(n_i, m_i)$ for $i = 1, \ldots, r$. Then
$(n, m) = p_1^{s_1} p_2^{s_2} \ldots p_r^{s_r}$ and $[n, m] = p_1^{t_1} p_2^{t_2} \ldots p_r^{t_r}$.
(For example, consider 15 and 100. Here $15 = 2^0 \cdot 3^1 \cdot 5^1$ and $100 = 2^2 \cdot 3^0 \cdot 5^2$. So $(15, 100) = 2^0 \cdot 3^0 \cdot 5^1$ and $[15, 100] = 2^2 \cdot 3^1 \cdot 5^2$.)
Also $s_i + t_i = n_i + m_i \ \forall \ i = 1, \ldots r$.
Then
$$\begin{aligned}(n, m)[n, m] &= p_1^{s_1+t_1} \cdot p_2^{s_2+t_2} \ldots p_r^{s_r+t_r} \\ &= p_1^{n_1+m_1} \ldots p_r^{n_r+m_r} \\ &= (p_1^{n_1} \ldots p_r^{n_r})(p_1^{m_1} \ldots p_r^{m_r}) \\ &= nm.\end{aligned}$$

***

Example 2: Let $G = GL_2(\mathbb{Q})$. Let $X \in G$. Prove that the operation $*$, defined on $G \times G$ by $A * B = X^{-1}ABX$, is a binary operation on G.
Further, is $(G, *)$ a group? Why, or why not?

Solution: First, for $A, B \in G$, $\det(A) \neq 0, \det(B) \neq 0$.
$\therefore \det(X^{-1}ABX) = [\det(X)]^{-1} \det(A) \det(B) \det(X) \neq 0$.
Also, all the entries of $X^{-1}ABX$ are from $\mathbb{Q}$.
Thus, $X^{-1}ABX \in G$.
Thus, $*$ is closed on G.

Next, note that there is no $Y \in G$ s.t. $A * Y = A \ \forall \ A \in G$.
This is because $A * Y = A$ iff $Y = A^{-1}XAX^{-1}$.
So, for example, if A does not commute with X, then
$$\begin{aligned}I * Y &= X^{-1}YX = X^{-1}A^{-1}XAX^{-1}X \\ &= X^{-1}A^{-1}XA \neq I.\end{aligned}$$
Hence, $(G, *)$ is not a group.

***

Example 3: Prove that if $a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0$ is a positive integer, then $a \equiv a_n + a_{n-1} + \cdots + a_0 \pmod 9$.
Hence prove that a is a multiple of 9 iff $9 \mid (a_0 + a_1 + \cdots + a_n)$.

Solution: For $m \in \mathbb{N}$, $10^m = (10^m - 1) + 1 = (10-1)(10^{m-1} + 10^{m-2} + \cdots + 10 + 1) + 1$
$= 9(10^{m-1} + \cdots + 1) + 1$
Hence, $a = 9[a_n(10^{n-1} + \cdots + 1) + a_{n-1}(10^{n-2} + \cdots + 1) + \cdots + a_2(10+1) + a_1]$
$+ (a_n + a_{n-1} + \cdots + a_1 + a_0)$.
$\therefore a \equiv a_n + a_{n-1} + \cdots + a_0 \pmod 9$.

Now, $9 \mid a \Leftrightarrow a \equiv 0 \pmod 9 \Leftrightarrow a_n + a_{n-1} + \cdots + a_0 \equiv 0 \pmod 9$
$\Leftrightarrow 9 \mid (a_n + \cdots + a_0)$.

***

Example 4: Show that $(\mathbb{Z}, *)$ is a group, where
$* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : *(m, n) = m + n + a$ for a fixed $a \in \mathbb{Z}$.

Solution: First check that $*$ is a well-defined binary operation on $\mathbb{Z}$.
Next, check that $(m * n) * p = m * (n * p)\ \forall\ m, n, p \in \mathbb{Z}$, using the properties that $+$ is associative and commutative in $\mathbb{Z}$.
Thirdly, check that $m * (-a) = m = (-a) * m\ \forall\ m \in \mathbb{Z}$.
Finally, check that $m * (-2a - m) = (-2a - m) * m = (-a)\ \forall\ m \in \mathbb{Z}$.
Hence, $(\mathbb{Z}, *)$ is a group.

***

Example 5: Define a relation ~ on $\mathbb{R}$ by '$x \sim y$ iff $x - y \in \mathbb{Z}$.' Check whether or not ~ is an equivalence relation on $\mathbb{R}$. If it is, find $[\pi]$. If ~ is not an equivalence relation on $\mathbb{R}$, find a subset of $\mathbb{R}$ on which it is an equivalence relation.

Solution: Since $x - x = 0 \in \mathbb{Z}\ \forall\ x \in \mathbb{R}$, ~ is reflexive.
Also show why ~ is symmetric and transitive.
Hence, ~ is an equivalence relation on $\mathbb{R}$.
Next, $[\pi] = \{x \in \mathbb{R} \mid x \sim \pi\} = \{x \in \mathbb{R} \mid x - \pi \in \mathbb{Z}\}$
$= \{\pi + n \mid n \in \mathbb{Z}\}$.

***

Miscellaneous Exercises

E1) Check whether or not $A = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}$ and $B = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \middle| a \in \mathbb{R} \right\}$ are subgroups of $(\mathbb{M}_2(\mathbb{R}), +)$.
Is $A \cap GL_2(\mathbb{R}) \leq (GL_2(\mathbb{R}), \cdot)$? Why, or why not?

E2) Give an example of a proper non-trivial cyclic subgroup of $(\wp(X), \Delta)$, where $X = \{x_1, x_2\}$.

E3) If G is a group s.t. $(xy)^2 = x^2y^2 \ \forall\ x, y \in G,$ then G is abelian. Is this statement true? Give reasons for your answer.

E4) Show that $(\mathbb{Z}[\sqrt{n}], +)$ is a group, where n is a square-free integer.

E5) Find $o(A)$, where $A = \begin{bmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{bmatrix}$, treating A as an element of $\mathbb{M}_2(\mathbb{Z}_7)$, and as an element of $GL_2(\mathbb{Z}_7)$.

E6) Is D_6 a subgroup of D_8? Why, or why not?

E7) i) Let G be an abelian group and $T = \{g \in G \mid o(g) < \infty\}$. Show that $T \leq G$. (T is called the **torsion subgroup of** G.)

ii) Find the torsion subgroup of $\mathbb{Z} \times K_4$.

E8) Which of the following statements are true? Justify your answers.

i) If G is a group and $n \in \mathbb{N}$, $\{g^n \mid g \in G\}$ is a subgroup of G.

ii) If G is a non-abelian group and $n \in \mathbb{N}$, $\{g \in G \mid o(g) = n\}$ is a subgroup of G.

iii) $\mathbb{Z}_{45}$ has exactly 6 distinct subgroups.

iv) If G is a group and $x, y \in G,$ of orders n and m, respectively, then $o(xy) = [n, m]$, the ℓ.c.m of n and m.

v) If G is an infinite group s.t. $x \in G,$ with $o(x)$ being infinite, then $G = \langle x \rangle$.

E9) Prove that if X is an infinite set, then the set of permutations, $S(X)$, is infinite.

E10) i) If $\sigma = (1\ 2\ 3\ 4\ 5\ 6) \in S_{10}$, then for which $n \in \mathbb{N}$ is σ^n also a 6-cycle?

ii) Prove that if $\sigma = (1\ 2 \ldots m)$, then σ^n is a cycle of length m iff $(n, m) = 1$. Here $m, n \in \mathbb{N}$.

E11) Show that if G is a non-cyclic group of order n, then G has no element of order n.

E12) Write the permutation $(3\ 5\ 7)(1\ 3\ 5)(5\ 7)$ as a product of disjoint cycles. Is this permutation even? Give reasons for your answer.

E13) Find the orders of the following elements in the group $(\mathbb{Z}_{36}, +)$: $\overline{1}, -\overline{1}, \overline{5}, \overline{6}, \overline{13}, -\overline{13}$.

E14) Under what conditions on c will $(\mathbb{Z}, *)$ be a group, where $*$ is defined by $a * b = ab + a + b + c,$ for a fixed $c \in \mathbb{Z}$?

E15) Check whether or not $GL_2(\mathbb{Z}_4)$ and $GL_2(\mathbb{Z}_5)$ are groups w.r.t. matrix multiplication.

SOLUTIONS / ANSWERS

E1) A and B are subgroups of $(\mathbb{M}_2(\mathbb{R}), +)$, applying the subgroup test.

$A \cap GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| \, a^2 \neq b^2, \, a, b \in \mathbb{R} \right\}$. This is a subgroup of $(GL_2(\mathbb{R}), \cdot)$, by the subgroup test.

E2) For any $A \in \wp(X)$, $A \Delta A = \phi$, $(A \Delta A) \Delta A = A, \ldots$.

So, $A^n = \phi$ if n is even, and $A^n = A$ if n is odd.

Thus, $< A > = \{\phi, A\}$.

Hence, if $A = \{x_1\}$, then $< A >$ is a proper non-trivial cyclic subgroup of $\wp(X)$.

E3) True. Since $xyxy = xxyy \; \forall \; x, y \in G$, by cancellation on the left and on the right, we get $yx = xy \; \forall \; x, y \in G$, i.e., G is abelian.

E4) $\mathbb{Z}[\sqrt{n}] \subseteq \mathbb{C}$ and $\mathbb{Z}[\sqrt{n}] \neq \phi$.

Now, if $a + b\sqrt{n}, \, c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, then

$(a + b\sqrt{n}) - (c + d\sqrt{n}) = (a - c) + (b - d)\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$.

Hence, $\mathbb{Z}[\sqrt{n}] \leq \mathbb{C}$. Thus, $(\mathbb{Z}[\sqrt{n}], +)$ is a group.

E5) For $n \in \mathbb{N}$, $n \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{bmatrix} = \begin{bmatrix} \bar{n} & \bar{0} \\ \bar{n} & \bar{n} \end{bmatrix}$.

Thus, the least n for which $nA = \mathbf{0}$ is $n = 7$.

$\therefore o(A) = 7$ in $\mathbb{M}_2(\mathbb{Z}_7)$.

$A \in GL_2(\mathbb{Z}_7)$ also, since $\det(A) = \bar{1} \neq \bar{0}$.

Now, $A = I + \begin{bmatrix} \bar{0} & \bar{0} \\ \bar{1} & \bar{0} \end{bmatrix}$.

So, $A^n = I + \begin{bmatrix} \bar{0} & \bar{0} \\ \bar{n} & \bar{0} \end{bmatrix}$, $n \in \mathbb{N}$.

$\therefore o(A) = 7$ in $GL_2(\mathbb{Z}_7)$, since $7 \cdot \bar{1} = \bar{0}$.

E6) Since $R_{120} \in D_6$ and $R_{120} \notin D_8$, $D_6 \not\subset D_8$. Hence, $D_6 \not\leq D_8$.

E7) i) Firstly, $e \in T$. So $T \neq \phi$.

Next, for $g \in T$, $o(g^{-1}) = o(g) < \infty$. So $g^{-1} \in T$.

Finally, if $g_1, g_2 \in T$, then $o(g_1 g_2) \leq o(g_1) o(g_2) < \infty$.

So, $g_1 g_2 \in T$.

Thus, $T \leq G$.

ii) Note that $o((a, b)) = \max(o(a), o(b)) \; \forall \; a \in \mathbb{Z}, \, b \in K_4$.

Also, the only element in $\mathbb{Z}$ with finite order is 0; and $o(x) < \infty \; \forall \; x \in K_4$. Thus, $T = \{(0, x) \,|\, x \in K_4\} = \{0\} \times K_4$.

E8) i) This is true if G is abelian, not otherwise. Look at S_3 and $n = 3$, to get a counter-example for when G is non-abelian.

ii) False. Again, take $G = S_3$ and $n = 2$, for a counter-example.

iii) True. For each positive divisor of 45, there is a unique subgroup of $\mathbb{Z}_{45}$. These divisors are $1, 3, 5, 9, 15, 45$.

iv) False. For example, consider $\mathbb{Z}_8 = <\bar{1}>$.
Then $o(\bar{2}) = 4$ and $o(\bar{4}) = 2$, i.e., $o(\bar{2} \cdot \bar{2}) = 2 \neq [4, 4]$.

v) False. For example, $\mathbb{Z} = <1> \neq <2>$, but $o(2)$ is infinite.

E9) Let $X = \{x_1, x_2, \ldots\}$.
Then $(x_i \; x_{i+1}) \in S(X) \; \forall \; i \in \mathbb{N}$.
Also, $(x_i \; x_{i+1}) \neq (x_j \; x_{j+1})$ unless $i = j$, since $(x_i \; x_{i+1})$ fixes x_j, or x_{j+1}, or both, if $i \neq j$; but $(x_j \; x_{j+1})$ moves both x_j and x_{j+1}.
Hence, $S(X)$ contains the infinitely many transpositions $(x_i \; x_{i+1})$, $i \in \mathbb{N}$.
Hence, $S(X)$ is infinite.

E10) i) $\sigma^2 = (1\ 3\ 5)(2\ 4\ 6)$, $\sigma^3 = (1\ 4)(2\ 5)(3\ 6)$,
$\sigma^4 = (1\ 5\ 3)(2\ 6\ 4)$, $\sigma^5 = (1\ 6\ 5\ 4\ 3\ 2)$,
$\sigma^6 = I$, $\sigma^7 = \sigma$, and so on.
Thus, σ^n is a 6-cycle only for $n = 1, 5, 1+6, 5+6, \ldots$, i.e.,
$n \in \{1+6k, 5+6k \mid k \in \mathbb{N}\}$.
Note that σ^n will be a 6-cycle iff $o(\sigma^n) = 6 = o(\sigma)$.
But $o(\sigma^2) = \dfrac{o(\sigma)}{2} \neq o(\sigma)$. Similarly, $o(\sigma^3) = \dfrac{o(\sigma)}{3}$.
In general, $o(\sigma^n) = \dfrac{6}{(6, n)}$.

ii) In this case, σ^n is an m-cycle iff $o(\sigma^n) = m$.
Also, $o(\sigma^n) = \dfrac{m}{(n, m)}$.
$\therefore \sigma^n$ is an m-cycle iff $\dfrac{m}{(n, m)} = m$, i.e., iff $(n, m) = 1$.

E11) You can show the contrapositive of the statement, i.e., prove that if G has an element x of order n, then $G = <x>$.
Here, note that $<x> \leq G$ and both have the same order.

E12) $(3\ 5\ 7)(1\ 3\ 5)(5\ 7) = (5\ 3\ 7\ 1)$, a 4-cycle.
Since $(5\ 3\ 7\ 1) = (5\ 1)(5\ 7)(5\ 3)$, a product of 3 transpositions, it is an odd permutation.

E13) $o(\bar{1}) = 36$, as $35 \cdot \bar{1} \neq \bar{0}$ and $36 \cdot \bar{1} = \bar{0}$; $o(-\bar{1}) = 36$;

$o(\overline{5}) = 36$, as $(5, 36) = 1$; $o(\overline{6}) = 6$; $o(\overline{13}) = 36$, $o(\overline{-13}) = o(\overline{23}) = 36$.

E14) Check that $*$ is a well-defined binary operation on $\mathbb{Z}$.
Since $(\mathbb{Z}, *)$ is a group, $*$ is associative on $\mathbb{Z}$.
Hence, show that c must be 0.
Then the additive identity must be 0.
However, then no element in $\mathbb{Z}^*$ has an inverse w.r.t. $*$. (Why?)
Thus, for no c is $(\mathbb{Z}, *)$ a group.

E15) $GL_2(\mathbb{Z}_4) = \left\{ \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} \in \mathbb{M}_2(\mathbb{Z}_4) \;\middle|\; \overline{a}\,\overline{d} - \overline{b}\,\overline{c} \neq \overline{0} \right\}$.

Now $\begin{bmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{2} \end{bmatrix} \in GL_2(\mathbb{Z}_4)$. Suppose $\begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix}$ is its inverse. Then

$$\begin{bmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{2} \end{bmatrix} \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} = \begin{bmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{bmatrix}.$$

So $\overline{2d} = \overline{1}$ in $\mathbb{Z}_4$. Hence, $4 \mid (1 - 2d)$, i.e., $4x = 1 - 2d$ for some $x \in \mathbb{Z}$. So $2d + 4x = 1$ in $\mathbb{Z}$, i.e., $2(d + 2x) = 1$ in $\mathbb{Z}$, which is not possible.
Thus, not every element has an inverse in $GL_2(\mathbb{Z}_4)$. Hence, it is not a group w.r.t. matrix multiplication.

However, $(GL_2(\mathbb{Z}_5), \cdot)$ is a group, which you should check.