2.5 Exercise Solutions

Solution 2.1.

- *Union of A and B:*
$$A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$$
- *Intersection of B and C:*
$$B \cap C = \{4, 6\}$$
- *Set difference $A - B$:*
$$A - B = \{1, 2\}$$
- *Symmetric difference of A and C:*
$$A \Delta C = \{1, 3, 5, 8, 10\}$$

Solution 2.2.

1. *$a \in E$: True. Since $E = \{a, b, c\}$, a is an element of E.*
2. *$a \subset E$: False. a is not a subset of E; $\{a\}$ is a subset of E.*
3. *$\{a\} \subset E$: True. $\{a\}$ is a subset of E because $a \in E$.*
4. *$\emptyset \in E$: False. $\emptyset$ (empty set) is not an element of E.*
5. *$\emptyset \subset E$: True. The empty set $\emptyset$ is a subset of every set, including E.*
6. *$\{\emptyset\} \subset E$: False. $\{\emptyset\}$ is not a subset of E because $\emptyset \notin E$.*

Solution 2.3.

1. $A \setminus B = A \cap B^c$ *By definition:*
$$A \setminus B = \{x \in A \mid x \notin B\},$$
and on the other hand:
$$A \cap B^c = \{x \in A \mid x \in B^c\} = \{x \in A \mid x \notin B\}.$$

Thus:

$$A \setminus B = A \cap B^c.$$

2. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Using the distributive property of intersection over union:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Using the distributive property of union over intersection:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

This can also be verified using element-based reasoning: If $x \in A \cup (B \cap C)$*, then* $x \in A$ *or* $x \in B \cap C$*. If* $x \in B \cap C$*, then* $x \in B$ *and* $x \in C$*, so* $x \in A \cup B$ *and* $x \in A \cup C$*.*
Conversely, if $x \in (A \cup B) \cap (A \cup C)$*, then* $x \in A \cup B$ *and* $x \in A \cup C$*. This implies* $x \in A$*, or* $x \in B$ *and* $x \in C$*, so* $x \in A \cup (B \cap C)$*.*

4. $A \triangle B = (A \cup B) \setminus (A \cap B)$

By the definition of symmetric difference:

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

Using part (1):

$$A \setminus B = A \cap B^c \quad \textit{and} \quad B \setminus A = B \cap A^c.$$

Thus:

$$A \triangle B = (A \cap B^c) \cup (B \cap A^c).$$

On the other hand:

$$(A \cup B) \setminus (A \cap B) = (A \cup B) \cap (A \cap B)^c.$$

Since $(A \cap B)^c = A^c \cup B^c$, *we have:*

$$(A \cup B) \setminus (A \cap B) = (A \cup B) \cap (A^c \cup B^c).$$

Using the distributive property:

$$(A \cup B) \cap (A^c \cup B^c) = [(A \cup B) \cap A^c] \cup [(A \cup B) \cap B^c].$$

Simplifying each term:

$$(A \cup B) \cap A^c = (A \cap A^c) \cup (B \cap A^c) = B \cap A^c,$$

$$(A \cup B) \cap B^c = (A \cap B^c) \cup (B \cap B^c) = A \cap B^c.$$

Thus:

$$(A \cup B) \setminus (A \cap B) = (A \cap B^c) \cup (B \cap A^c).$$

Therefore:

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

Solution 2.4.

The Power Set $\mathcal{P}(E)$

The power set $\mathcal{P}(E)$ *of a set* E *is the set of all subsets of* E*, including the empty set and* E *itself. For* $E = \{a, b, c, d\}$*, the power set* $\mathcal{P}(E)$ *is:*

$$\mathcal{P}(E) = \big\{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a,b\}, \{a,c\}, \{a,d\}, \{b,c\}, \{b,d\}, \{c,d\},$$
$$\{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}, E\big\}.$$

In total, $\mathcal{P}(E)$ *contains* 2^n *subsets, where* $n = 4$ *is the number of elements in* E*. Thus,* $|\mathcal{P}(E)| = 2^4 = 16$.

Example of a Partition of E

A partition of E *is a collection of non-empty, pairwise disjoint subsets of* E *whose union equals* E*. An example of a partition of* E *is:*

$$\mathcal{P}_1 = \{\{a, b\}, \{c\}, \{d\}\}.$$

Verify:

- *Each subset is non-empty.*
- *The subsets are pairwise disjoint:*

$$\{a, b\} \cap \{c\} = \emptyset, \quad \{a, b\} \cap \{d\} = \emptyset, \quad \{c\} \cap \{d\} = \emptyset,$$

- *The union of all subsets equals E:*

$$\{a, b\} \cup \{c\} \cup \{d\} = \{a, b, c, d\} = E.$$

Thus, $\mathcal{P}_1 = \{\{a, b\}, \{c\}, \{d\}\}$ is a valid partition of E.

Solution 2.5.

1. ***Images and Pre-images under** $f(x) = \sin(x)$**:***

   (a) *The image of $\mathbb{R}$ under $f(x) = \sin(x)$ is:*

   $$f(\mathbb{R}) = [-1, 1],$$

   because the sine function oscillates between -1 and 1 for all real x.

   (b) *The image of $[0, 2\pi]$ under $f(x) = \sin(x)$ is:*

   $$f([0, 2\pi]) = [-1, 1],$$

   because $\sin(x)$ completes one full cycle in the interval $[0, 2\pi]$.

   (c) *The image of $[0, \frac{\pi}{2}]$ under $f(x) = \sin(x)$ is:*

   $$f([0, \frac{\pi}{2}]) = [0, 1],$$

   because the sine function is strictly increasing from 0 to 1 in this interval.

   (d) *The inverse image of $[0, 1]$ under $f(x) = \sin(x)$ is:*

   $$f^{-1}([0, 1]) = \bigcup_{k \in \mathbb{Z}} [2k\pi, 2k\pi + \pi],$$

   as sine is periodic with period 2π.

(e) *The inverse image of* $[3,4]$ *under* $f(x) = \sin(x)$ *is:*

$$f^{-1}([3,4]) = \emptyset,$$

because $\sin(x) \notin [3,4]$ *for any* $x \in \mathbb{R}$.

(f) *The inverse image of* $[1,2]$ *under* $f(x) = \sin(x)$ *is:*

$$f^{-1}([1,2]) = f^{-1}(\{1\}) = \bigcup_{k\in\mathbb{Z}} \left\{\frac{\pi}{2} + 2k\pi\right\},$$

because $\sin(x) = 1$ *occurs only at* $x = \frac{\pi}{2} + 2k\pi$ *for* $k \in \mathbb{Z}$, *and* $\sin(x) \notin (1,2]$.

2. ***Comparison of*** $f(A \setminus B)$ ***and*** $f(A) \setminus f(B)$***:***

Let $f(x) = x^2 + 1$, $A = [-3,2]$, *and* $B = [0,4]$*:*

(a) *The set* $A \setminus B = [-3,0)$, *as* $B = [0,4]$ *removes* $[0,4]$ *from* A.

(b) *The image of* $A \setminus B$ *under* $f(x)$*:*

$$f(A \setminus B) = f([-3,0)) = (1,10],$$

because $f(x) = x^2 + 1$ *is increasing on* $[0,\infty)$ *and symmetric about* $x = 0$.

(c) *The image of* A *under* $f(x)$*:*

$$f(A) = f([-3,2]) = [1,10],$$

and the image of B *under* $f(x)$*:*

$$f(B) = f([0,4]) = [1,17].$$

(d) *The set* $f(A) \setminus f(B)$ *is:*

$$f(A) \setminus f(B) = [1,10] \setminus [1,17] = \emptyset.$$

Comparing:

$$f(A \setminus B) = [1,10), \quad f(A) \setminus f(B) = \emptyset.$$

Thus, $f(A \setminus B) \neq f(A) \setminus f(B)$.

3. ***Condition for*** $f(A \setminus B) = f(A) \setminus f(B)$***:***

*For $f(A \setminus B) = f(A) \setminus f(B)$ to hold, the function f must be **injective** (one-to-one). Injectivity ensures that elements in $A \setminus B$ map uniquely to $f(A \setminus B)$, without overlap from elements in B.*

Solution 2.6.

1. *$E = \mathbb{Z}$ and $x\mathcal{R}y \Leftrightarrow |x| = |y|$:*
   - ***Reflexive**: Yes, since $|x| = |x|$ for all $x \in \mathbb{Z}$.*
   - ***Symmetric**: Yes, since $|x| = |y| \implies |y| = |x|$.*
   - ***Antisymmetric**: No, because $|x| = |y|$ does not imply $x = y$ (e.g., $x = 3, y = -3$).*
   - ***Transitive**: Yes, since $|x| = |y|$ and $|y| = |z|$ imply $|x| = |z|$.*
   - ***Type**: This is an **equivalence relation**, not an order.*
2. *$E = \mathbb{R} \setminus \{0\}$ and $x\mathcal{R}y \Leftrightarrow xy > 0$:*
   - ***Reflexive**: Yes, since $x \cdot x > 0$ for all $x \neq 0$.*
   - ***Symmetric**: Yes, since $xy > 0 \implies yx > 0$.*
   - ***Antisymmetric**: No, because $xy > 0$ does not imply $x = y$ (e.g., $x = 1, y = 2$).*
   - ***Transitive**: Yes, since $xy > 0$ and $yz > 0$ imply $xz > 0$.*
   - ***Type**: This is an **equivalence relation**, not an order.*
3. *$E = \mathbb{Z}$ and $x\mathcal{R}y \Leftrightarrow x - y$ is even:*
   - ***Reflexive**: Yes, since $x - x = 0$, which is even.*
   - ***Symmetric**: Yes, since $x - y$ even implies $y - x$ is even.*
   - ***Antisymmetric**: No, because $x - y$ even does not imply $x = y$ (e.g., $x = 2, y = 4$).*
   - ***Transitive**: Yes, since $x - y$ even and $y - z$ even imply $x - z$ is even.*
   - ***Type**: This is an **equivalence relation**, not an order.*

Summary

- *$\mathcal{R}_1$, $\mathcal{R}_2$, and $\mathcal{R}_3$ are all **equivalence relations**.*
- *None of them is an **order** because they fail antisymmetry.*

Solution 2.7.

1. *$E = \mathbb{R}$ and $x\mathcal{R}y \Leftrightarrow x = -y$:*
   - ***Reflexive**: No, since $x = -x$ only holds for $x = 0$, so it is not reflexive.*
   - ***Symmetric**: Yes, since $x = -y \implies y = -x$.*
   - ***Antisymmetric**: No, because $x = -y$ and $y = -x$ do not imply $x = y$ (e.g., $x = 1, y = -1$).*
   - ***Transitive**: No, because $x = -y$ and $y = -z$ imply $x = -(-z) = z$, which contradicts the original definition unless $x = 0$ or $z = 0$.*
   - ***Type**: This is **not an equivalence relation** because it is not reflexive, and it is **not an order** because it is not antisymmetric.*

2. *$E = \mathbb{R}$ and $x\mathcal{R}y \Leftrightarrow \cos^2(x) + \sin^2(y) = 1$:*
   - ***Reflexive**: Yes, since $\cos^2(x) + \sin^2(x) = 1$ for all $x \in \mathbb{R}$.*
   - ***Symmetric**: Yes, since $\cos^2(x) + \sin^2(y) = 1 \implies \cos^2(y) + \sin^2(x) = 1$.*
   - ***Antisymmetric**: No, because $\cos^2(x) + \sin^2(y) = 1$ and $\cos^2(y) + \sin^2(x) = 1$ do not imply $x = y$.*
   - ***Transitive**: Yes, since $\cos^2(x) + \sin^2(y) = 1$ and $\cos^2(y) + \sin^2(z) = 1$ imply $\cos^2(x) + \sin^2(z) = 1$.*
   - ***Type**: This is **an equivalence relation** but **not an order**.*

3. *$E = \mathbb{N}$ and $x\mathcal{R}y \Leftrightarrow \exists p, q \geq 1$ such that $y = px^q$ (where $p, q \in \mathbb{Z}$):*
   - ***Reflexive**: Yes, since $x = px^q$ holds for $p = 1, q = 1$, implying $x\mathcal{R}x$.*
   - ***Symmetric**: No, since $y = px^q$ does not imply $x = py^q$.*
   - ***Antisymmetric**: Yes, because if $y = px^q$ and $x = p'y^{q'}$, then $x = y$.*
   - ***Transitive**: Yes, since if $y = px^q$ and $z = p'y^{q'}$, then $z = (pp')x^{qq'}$.*
   - ***Type**: This is a **partial order**, not an equivalence relation.*

Solution 2.8.

1. ***Relation*** $\sim_1$*:* $x \sim_1 y$ *if and only if* $x + y$ *is even.*

   Reflexive*:* *Yes, because* $x + x = 2x$ *is always even for any* $x \in \mathbb{Z}$*.*

   Symmetric*:* *Yes, because if* $x + y$ *is even, then* $y + x = x + y$*, which is also even.*

   Transitive*:* *Yes, because if* $x + y$ *is even and* $y + z$ *is even, then* $(x + y) + (y + z) = x + 2y + z$ *is even, implying that* $x + z$ *is even.*

   Equivalence Classes*:* *The equivalence classes are:*

$$\dot{0} = \{x \in \mathbb{Z} \mid x \text{ is even}\}, \quad \dot{1} = \{x \in \mathbb{Z} \mid x \text{ is odd}\}.$$

2. ***Relation*** $\sim_2$*:* $x \sim_2 y$ *if and only if* x *and* y *have the same remainder when divided by 5.*

   Reflexive*:* *Yes, because* $x \mod 5 = x \mod 5$ *for any* $x \in \mathbb{Z}$*.*

   Symmetric*:* *Yes, because if* $x \mod 5 = y \mod 5$*, then* $y \mod 5 = x \mod 5$.

   Transitive*:* *Yes, because if* $x \mod 5 = y \mod 5$ *and* $y \mod 5 = z \mod 5$*, then* $x \mod 5 = z \mod 5$*.*

   Equivalence Classes*:* *The equivalence classes are:*

$$\dot{0} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 5\}, \quad \dot{1} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 5\},$$

$$\dot{2} = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 5\}, \dot{3} = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod 5\},$$

$$\dot{4} = \{x \in \mathbb{Z} \mid x \equiv 4 \pmod 5\}.$$

3. ***Relation*** $\sim_3$*:* $x \sim_3 y$ *if and only if* $x - y$ *is a multiple of 7.*

   Reflexive*:* *Yes, because* $x - x = 0$ *is a multiple of 7 for any* $x \in \mathbb{Z}$*.*

   Symmetric*:* *Yes, because if* $x - y$ *is a multiple of 7, then* $y - x = -(x - y)$ *is also a multiple of 7.*

   Transitive*:* *Yes, because if* $x - y$ *and* $y - z$ *are multiples of 7, then* $(x - y) + (y - z) = x - z$ *is also a multiple of 7.*

***Equivalence Classes**: The equivalence classes are:*

$$\dot{0} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 7\}, \quad \dot{1} = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 7\},$$

$$\dot{2} = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 7\}, \dot{3} = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod 7\},$$

$$\dot{4} = \{x \in \mathbb{Z} \mid x \equiv 4 \pmod 7\}, \quad \dot{5} = \{x \in \mathbb{Z} \mid x \equiv 5 \pmod 7\},$$

$$\dot{6} = \{x \in \mathbb{Z} \mid x \equiv 6 \pmod 7\}.$$

Solution 2.9.

We will prove the equivalence in two directions.

(1) If** $x\mathcal{R}y$**, then** $\dot{x} = \dot{y}$**:

Since $\mathcal{R}$ is an equivalence relation, it satisfies three properties: reflexivity, symmetry, and transitivity. By the definition of an equivalence relation, if $x\mathcal{R}y$, then x and y belong to the same equivalence class, denoted $\dot{x} = \dot{y}$. This means that the equivalence classes of x and y are identical.

$$x\mathcal{R}y \quad \Rightarrow \quad \dot{x} = \dot{y}.$$

(2) If** $\dot{x} = \dot{y}$**, then** $x\mathcal{R}y$**:

If $\dot{x} = \dot{y}$, then by the definition of equivalence classes, x and y belong to the same equivalence class. Therefore, by the properties of an equivalence relation, $x\mathcal{R}y$.

$$\dot{x} = \dot{y} \quad \Rightarrow \quad x\mathcal{R}y.$$

Thus, we have shown both directions, completing the proof.

Solution 2.10.

Let $\mathbb{N}^*$ denote the set of positive integers. Define the relation $\mathcal{R}$ on $\mathbb{N}^*$ by $x\mathcal{R}y$ if and only if x divides y.

1. ***Show that** $\mathcal{R}$ **is a partial order relation on** $\mathbb{N}^*$**:***

   To show that $\mathcal{R}$ is a partial order, we need to verify that it is reflexive, antisymmetric, and transitive.

   - ***Reflexive:** For any $x \in \mathbb{N}^*$, x divides itself, i.e., $x\mathcal{R}x$.*

- ***Antisymmetric:*** *If* $x\mathcal{R}y$ *and* $y\mathcal{R}x$*, then* x *divides* y *and* y *divides* x*. This implies that* $x = y$*, because the only way two distinct positive integers can divide each other is if they are equal.*
- ***Transitive:*** *If* $x\mathcal{R}y$ *and* $y\mathcal{R}z$*, then* x *divides* y *and* y *divides* z*. This implies that* x *divides* z*, so* $x\mathcal{R}z$*.*

Since $\mathcal{R}$ *is reflexive, antisymmetric, and transitive, it is a partial order on* $\mathbb{N}^*$*.*

2. ***Is*** $\mathcal{R}$ ***a total order relation?***

   A relation is a total order if it is a partial order and, for any two elements x *and* y *in* $\mathbb{N}^*$*, either* $x\mathcal{R}y$ *or* $y\mathcal{R}x$ *holds. In this case,* $\mathcal{R}$ *is not a total order because, for example, 2 and 3 do not divide each other, so neither* $2\mathcal{R}3$ *nor* $3\mathcal{R}2$ *holds. Therefore,* $\mathcal{R}$ *is not a total order.*

3. ***Describe the sets*** $\{x \in \mathbb{N}^* \mid x\mathcal{R}5\}$ ***and*** $\{x \in \mathbb{N}^* \mid 5\mathcal{R}x\}$***:***

   - *The set* $\{x \in \mathbb{N}^* \mid x\mathcal{R}5\}$ *is the set of all positive integers that divide 5. The divisors of 5 are* 1 *and* 5*, so:*

   $$\{x \in \mathbb{N}^* \mid x\mathcal{R}5\} = \{1, 5\}.$$

   - *The set* $\{x \in \mathbb{N}^* \mid 5\mathcal{R}x\}$ *is the set of all positive integers divisible by 5. This set is:*

   $$\{x \in \mathbb{N}^* \mid 5\mathcal{R}x\} = \{5, 10, 15, 20, 25, \dots\}.$$

4. ***Does*** $\mathbb{N}^*$ ***have a least element? A greatest element?***

   - ***Least element:*** *The least element in* $\mathbb{N}^*$ *with respect to the relation* $\mathcal{R}$ *is 1, because* 1 *divides all positive integers. Therefore, 1 is the least element.*
   - ***Greatest element:*** *The greatest element in* $\mathbb{N}^*$ *with respect to the relation* $\mathcal{R}$ *does not exist because there is no single integer that is divisible by all positive integers. Thus, there is no greatest element.*

Solution 2.11.

Let f *be the function from* $\mathbb{R}$ *to* $\mathbb{R}$ *defined by* $f(x) = x^2 + x - 2$*.*

1. ***Definition of*** $f^{-1}(\{4\})$***:*** *The set* $f^{-1}(\{4\})$ *is the preimage of* $\{4\}$ *under* f*, i.e., it consists of all* $x \in \mathbb{R}$ *such that* $f(x) = 4$*.*

$$f(x) = 4 \quad \Rightarrow \quad x^2 + x - 2 = 4$$

Solving this equation:

$$x^2 + x - 6 = 0$$

Factorizing:

$$(x - 2)(x + 3) = 0$$

Thus, $x = 2$ *or* $x = -3$*. Therefore,* $f^{-1}(\{4\}) = \{2, -3\}$*.*

2. ***Is the function*** f ***bijective?***

Injectivity: f *is not bijective because* f *is not injective.*

Surjectivity: For surjectivity, we would need to show that for every $y \in \mathbb{R}$*, there exists* $x \in \mathbb{R}$ *such that* $f(x) = y$*. However, since the function is quadratic and opens upwards, it is not surjective over* $\mathbb{R}$*. Specifically,* $f(x) = x^2 + x - 2$ *has a minimum value, but no maximum, meaning it cannot take all real values. Therefore,* f *is not surjective.*

Since f *is neither injective nor surjective, it is not bijective.*

3. ***Definition of*** $f([-1, 1])$***:*** *The set* $f([-1, 1])$ *is the image of the interval* $[-1, 1]$ *under the function* f*, i.e., it is the set of all values* $f(x)$ *for* $x \in [-1, 1]$*.*

To calculate $f([-1, 1])$*, we need to find the minimum and maximum values of* $f(x) = x^2 + x - 2$ *on the interval* $[-1, 1]$*.*

First, evaluate $f(x)$ *at the endpoints of the interval:*

$$f(-1) = (-1)^2 + (-1) - 2 = 1 - 1 - 2 = -2$$

$$f(1) = 1^2 + 1 - 2 = 1 + 1 - 2 = 0$$

Next, compute the derivative of $f(x)$*:*

$$f'(x) = 2x + 1$$

Setting $f'(x) = 0$ *to find critical points:*

$$2x + 1 = 0 \quad \Rightarrow \quad x = -\frac{1}{2}$$

Since $-\frac{1}{2} \in [-1, 1]$*, we evaluate* f *at* $x = -\frac{1}{2}$*:*

$$f\left(-\frac{1}{2}\right) = \left(-\frac{1}{2}\right)^2 + \left(-\frac{1}{2}\right) - 2 = \frac{1}{4} - \frac{1}{2} - 2 = -\frac{9}{4}$$

Thus, the minimum value of $f(x)$ *on* $[-1, 1]$ *is* $-\frac{9}{4}$*, and the maximum value is 0.*

Therefore, $f([-1, 1]) = \left[-\frac{9}{4}, 0\right]$.

4. ***Definition of*** $f^{-1}([-2, 4])$***:*** *The set* $f^{-1}([-2, 4])$ *is the preimage of the interval* $[-2, 4]$*, i.e., it consists of all* $x \in \mathbb{R}$ *such that* $f(x) \in [-2, 4]$.

   We need to solve for x *such that* $-2 \leq f(x) = x^2 + x - 2 \leq 4$.

   First, solve $f(x) \geq -2$*:*

$$x^2 + x - 2 \geq -2 \quad \Rightarrow \quad x^2 + x \geq 0$$

   Factoring:

$$x(x + 1) \geq 0$$

   This inequality holds when $x \leq -1$ *or* $x \geq 0$.

   Next, solve $f(x) \leq 4$*:*

$$x^2 + x - 2 \leq 4 \quad \Rightarrow \quad x^2 + x - 6 \leq 0$$

   Factoring:

$$(x - 2)(x + 3) \leq 0$$

   This inequality holds when $-3 \leq x \leq 2$.

   Combining the two results, we have:

$$-3 \leq x \leq -1 \quad or \quad 0 \leq x \leq 2$$

   Therefore, the set $f^{-1}([-2, 4]) = [-3, -1] \cup [0, 2]$.

Solution 2.12.

1. ***Injectivity:***

   A function f *is injective if* $f(x_1) = f(x_2)$ *implies* $x_1 = x_2$*. Let's assume*

$f(x_1) = f(x_2)$, which gives:

$$\frac{2x_1}{1+x_1^2} = \frac{2x_2}{1+x_2^2}.$$

Simplifying this equation:

$$x_1(1+x_2^2) = x_2(1+x_1^2),$$

*which does not necessarily imply $x_1 = x_2$. Therefore, the function is **not injective**.*

***Counterexample:** Take $x_1 = 2$ and $x_2 = \frac{1}{2}$:*

$$f(2) = \frac{4}{5}, \quad f\left(\frac{1}{2}\right) = \frac{4}{5}.$$

Clearly, $f(2) = f\left(\frac{1}{2}\right)$, but $2 \neq \frac{1}{2}$, proving that the function is not injective.

2. ***Surjectivity:***
*A function f is surjective if for every $y \in \mathbb{R}$, there exists an $x \in \mathbb{R}$ such that $f(x) = y$. We know that the function $f(x) = \frac{2x}{1+x^2}$ has a maximum at $x = 1$ where $f(1) = 1$ and a minimum at $x = -1$ where $f(-1) = -1$, and as $x \to \pm\infty$, $f(x) \to 0$. Therefore, the range of $f(x)$ is $(-1, 1)$, and the function is **not surjective** because it cannot take values outside of this interval.*

3. ***Range of** $f(x)$**:***
We now show that the range of $f(x) = \frac{2x}{1+x^2}$ is $[-1, 1]$. To do this, we need to find the maximum and minimum values of $f(x)$.

First, we calculate the derivative of $f(x)$:

$$f'(x) = \frac{(1+x^2)(2) - 2x(2x)}{(1+x^2)^2} = \frac{2(1-x^2)}{(1+x^2)^2}.$$

Setting $f'(x) = 0$ gives:

$$1 - x^2 = 0 \quad \Rightarrow \quad x = \pm 1.$$

Evaluating $f(x)$ at $x = 1$ and $x = -1$:

$$f(1) = \frac{2 \times 1}{1+1^2} = 1, \quad f(-1) = \frac{2 \times (-1)}{1+(-1)^2} = -1.$$

As $x \to \pm\infty$, $f(x) \to 0$. Therefore, the range of $f(x)$ is $[-1,1]$, so we have shown that:

$$f(\mathbb{R}) = [-1,1].$$

4. ***Restriction** $g(x) = f(x)$ **on** $[-1,1]$**:***

   Now, we need to show that the restriction of f to $[-1,1]$, which we denote by $g(x) = f(x)$, is a bijection.

   ***Injectivity:** Since the derivative $f'(x)$ is positive over the entire interval $[-1,1]$, the function $f(x) = \frac{2x}{1+x^2}$ is strictly increasing on this interval.*

   *Therefore, the function $f(x)$ is **injective** on $[-1,1]$.*

   ***Surjectivity:** The range of $f(x)$ on $[-1,1]$ is $[-1,1]$, so the restriction $g(x)$ is surjective.*

   Since $g(x)$ is both injective and surjective, it is a bijection.

Solution 2.13.

Let $f : E \to F$, $g : F \to G$, and $h = g \circ f$.

1. ***Injectivity of** f**:** Show that if h is injective, then f is injective. Also, show that if h is surjective, then g is surjective.*

   Proof:

   1.1 Injectivity of f: Assume that $h = g \circ f$ is injective. To show that f is injective, we need to prove that for any $x_1, x_2 \in E$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

   Since $h(x_1) = g(f(x_1))$ and $h(x_2) = g(f(x_2))$, if $f(x_1) = f(x_2)$, then

$$h(x_1) = h(x_2).$$

   Since h is injective, it follows that

$$x_1 = x_2.$$

   Hence, f is injective.

   1.2 Surjectivity of g: Assume that $h = g \circ f$ is surjective. To show that g is surjective, we need to prove that for every $y \in G$, there exists some $x \in F$ such that $g(x) = y$.

   Since h is surjective, for each $y \in G$, there exists $x \in E$ such that $h(x) = g(f(x)) = y$. Therefore, for every $y \in G$, we can find an $x \in F$ such that $g(x) = y$, which proves that g is surjective.

2. ***Surjectivity of*** f***:*** *Show that if* h *is surjective and* g *is injective, then* f *is surjective.*

   Proof:

   Assume that h *is surjective and* g *is injective. To prove that* f *is surjective, we need to show that for every* $y \in F$*, there exists some* $x \in E$ *such that* $f(x) = y$*.*

   Since h *is surjective, for each* $y \in G$*, there exists* $z \in E$ *such that* $h(z) = g(f(z)) = y$*. Since* g *is injective, there exists a unique* $x \in F$ *such that* $f(x) = y$*, which implies that* f *is surjective.*

3. ***Injectivity of*** g***:*** *Show that if* h *is injective and* f *is surjective, then* g *is injective.*

   Proof:

   Assume that h *is injective and* f *is surjective. To show that* g *is injective, we need to prove that if* $g(x_1) = g(x_2)$*, then* $x_1 = x_2$*.*

   Since $h(x_1) = g(f(x_1))$ *and* $h(x_2) = g(f(x_2))$*, if* $g(x_1) = g(x_2)$*, we have*

   $$h(x_1) = h(x_2).$$

   Since h *is injective, it follows that*

   $$f(x_1) = f(x_2).$$

   Since f *is surjective, there exists some* $x \in F$ *such that* $f(x) = y$*, and therefore,* $g(x_1) = g(x_2)$*.*

   Hence, g *is injective.*

Solution 2.14.

1. *Let* $x \in E$*. By definition of the indicator function:*

   - *If* $x \in A$*, then* $\phi_A(x) = 1$ *and* $\phi_{A^c}(x) = 0$*.*
   - *If* $x \notin A$*, then* $\phi_A(x) = 0$ *and* $\phi_{A^c}(x) = 1$*.*

   In both cases:

   $$\phi_A(x) + \phi_{A^c}(x) = 1.$$

Since this holds for all $x \in E$, we conclude:

$$\phi_A + \phi_{A^c} = 1. \quad \square$$

2. *Let $x \in E$. We analyze two cases:*

   (a) ***If** $x \in A \cap B$:*

   - *Then $\phi_{A\cap B}(x) = 1$.*
   - *Since $x \in A$ and $x \in B$, $\phi_A(x) = 1$ and $\phi_B(x) = 1$.*
   - *Thus, $\phi_A(x) \cdot \phi_B(x) = 1 \cdot 1 = 1$.*

   (b) ***If** $x \notin A \cap B$:*

   - *Then $\phi_{A\cap B}(x) = 0$.*
   - *At least one of $\phi_A(x)$ or $\phi_B(x)$ is 0 (since $x \notin A$ or $x \notin B$).*
   - *Thus, $\phi_A(x) \cdot \phi_B(x) = 0$.*

3. *In both cases, $\phi_{A\cap B}(x) = \phi_A(x) \cdot \phi_B(x)$. Therefore:*

$$\phi_{A\cap B} = \phi_A \cdot \phi_B. \quad \square$$

4. *For any $x \in E$:*

   (a) ***If** $x \in A \setminus B$: $\phi_{A\setminus B}(x) = 1$, $\phi_A(x) = 1$, $\phi_B(x) = 0$.*

$$\phi_A(x)(1 - \phi_B(x)) = 1 \cdot (1 - 0) = 1.$$

   (b) ***If** $x \notin A \setminus B$: Either $x \notin A$ or $x \in B$:*

   - ***Subcase 1:** $x \notin A$ $\phi_A(x) = 0$:*

$$\phi_A(x)(1 - \phi_B(x)) = 0 \cdot (1 - \phi_B(x)) = 0.$$

   - ***Subcase 2:** $x \in B$ $\phi_B(x) = 1$:*

$$\phi_A(x)(1 - \phi_B(x)) = \phi_A(x) \cdot 0 = 0.$$

   In both subcases, $\phi_{A\setminus B}(x) = 0$.

Thus, $\forall x \in E$, $\phi_{A\setminus B}(x) = \phi_A(x)(1 - \phi_B(x))$.

$$\boxed{\phi_{A\setminus B} = \phi_A(1 - \phi_B).}$$

Chapter 3

Algebraic Structures

3.1 Law of internal composition

Definition 3.1.1.
Let E be a non-empty set.

1. *A* ***law of internal composition*** *on E is a function from $E \times E$ to E. If T denotes this function, then the image of the pair $(x, y) \in E \times E$ under T is denoted as xTy.*

2. ***A structured set*** *is any pair (E, T) where E is a non-empty set and T is a law of internal composition on E.*

Example 3.1.1.
The most common internal composition laws are:

1. $+$ *in* $\mathbb{N}, \mathbb{N}^*, \mathrm{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, *but not in* $\mathrm{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$

2. $-$ *in* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

3. $\times$ *in* $\mathbb{N}, \mathbb{N}^*, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

4. $/$ *in* $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$

5. $\circ$ *(composition of functions) defined on the set of functions from* E *to E.*

6. *The law $\oplus$ defined on $\mathbb{R}^2$ by* $(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$

7. *The law T defined on $\mathbb{R}$ by* $xTy = x + y - xy$

8. *The laws* $\cup$, $\cap$ *(union, intersection) defined on* $P(E)$ *(power set of a set* E*)*

Definition 3.1.2. *(Properties of laws)*
Let (E, T) *be a structured set.*

1. *The law* T *is called* ***associative*** *on* E *if* $(xTy)Tz = xT(yTz)$ *for all* x, y, z *in* E.

2. *The law* T *is called* ***commutative*** *on* E *if* $xTy = yTx$ *for all* x, y *in* E.

Example 3.1.2.
Addition and multiplication are associative and commutative on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Definition 3.1.3. *(Properties of laws)*
Let (E, T) *be a structured set.*

1. *An element* e *of* E *is called* ***neutral*** *for the law* T *if,*

$$\forall x \in E, \;\; xTe = eTx = x.$$

2. *If* (E, T) *has a neutral element* e*, then an element* x *of* E *is said to be invertible (or symmetrizable) for the law* T *if there exists an element* x' *in* E *such that:*

$$xTx' = x'Tx = e$$

The element x' *is then called the symmetric element of* x *for the law* T.

Proposition 3.1.1.
Let (E, T) *be a structured set. If the neutral element of* E *for the law* T *exists, then it is unique.*

Proof 3.1.1.
Suppose there exist two neutral elements e *and* e'*. Then,*

$$e' = eTe' = e$$

which implies $e = e'$.

Proposition 3.1.2.
Let (E, T) *be a structured set where the law* T *is associative and has a neutral element.*

1. *If $x \in E$ is symmetrizable, then its symmetric element is unique.*
2. *If $x \in E$ and $y \in E$ are symmetrizable, then xTy is symmetrizable and its symmetric element $(xTy)'$ is given by $(xTy)' = y'Tx'$ where x' denotes the symmetric element of x and y' denotes the symmetric element of y.*

Proof 3.1.2.

1. *Let's suppose an element x has two symmetric elements x' and x''. Then,*

$$xTx' = e \Rightarrow x''T(xTx') = x'' \Rightarrow (x''Tx)Tx' = x'' \Rightarrow x' = x''.$$

2. *We have*

$$(y'Tx')T(xTy) = y'T(x'Tx)Ty = y'Ty = e.$$

Also,

$$(xTy)T(y'Tx') = xT(yTy')Tx' = xTx' = e.$$

Thus, $(xTy)' = y'Tx'$.

3.2 Groups

3.2.1 Group Structure

Definition 3.2.1.
Let (G, T) be a structured set.

1. *We say that (G, T) is a **group** if*
   (a) the operation T is associative on G,
   (b) there exists a neutral element for the operation T in G,
   (c) every element of G is symmetrizable for the operation T.

   *We also say that the set G has a **group structure** for the operation T.*
2. *We say that the group (G, T) is **commutative (or abelian)** if the operation T is commutative on G.*

Example 3.2.1.
First, examples of groups are provided:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *equipped with addition.*

2. $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$ *equipped with multiplication.*

Example 3.2.2.
For various reasons (to be determined), the following pairs are not groups:

1. $(\mathbb{N}, +)$, $(\mathbb{R}, \times)$.

2. $(\mathcal{P}(E), \cup)$, $(\mathcal{P}(E), \cap)$.

3.2.2 Subgroups

Definition 3.2.2. *(Subgroups)*
A ***subgroup*** *of a group* $(G, *)$ *is a non-empty subset* H *of* G *such that:*

1. $*$ *induces an internal composition law on* H.

2. *With this law,* H *forms a group. We denote this as* $H < G$.

Proposition 3.2.1.
The subset $H \subset G$ *is a* ***subgroup*** *of a group* $(G, *)$ *if and only if*

1. $H \neq \varnothing$,

2. $\forall (x, y) \in H^2,\ x * y \in H$,

3. $\forall x \in H,\ x^{-1} \in H$.

Example 3.2.3.

1. *Let* $(G, *)$ *be a group. Then* G *and* $\{e_G\}$ *are subgroups of* G.

2. $(\mathbb{Z}, +)$ *is a subgroup of* $(\mathbb{R}, +)$.

Proposition 3.2.2.
The subset $H \subset G$ *is a subgroup of a group* $(G, *)$ *if and only if*

1. $H \neq \varnothing$,
2. $\forall (x, y) \in H^2,\ x * y^{-1} \in H$.

Proposition 3.2.3.
The intersection of any family of subgroups of a group $(G, *)$ is a subgroup of $(G, *)$.

Proof 3.2.1.
Let $(H_i)_{i \in I}$ be a family of subgroups of a group G. Define $K = \bigcap_{i \in I} H_i$, the intersection of all H_i. The set K is non-empty since it contains the identity element e, which belongs to each subgroup H_i. Let x and y be two elements of K. For every $i \in I$, we have $x * y^{-1} \in H_i$ because H_i is a subgroup. Therefore, $x * y^{-1} \in K$. This proves that K is a subgroup of G.

Remark 3.2.1.
The arbitrary union of subgroups of a group $(G, *)$ is not necessarily a subgroup of $(G, *)$.

Example 3.2.4.
Let T be the internal composition law defined on $\mathbb{R}^2$ by

$$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2, \quad (x_1, y_1) * (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

We have $(\mathbb{R}^2, T)$ is a group, $\mathbb{R} \times \{0\}$ and $\{0\} \times \mathbb{R}$ are two subgroups of $(\mathbb{R}^2, T)$ but $\mathbb{R} \times \{0\} \cup \{0\} \times \mathbb{R}$ does not form a subgroup of $(\mathbb{R}^2, T)$.

Proposition 3.2.4.
The union of two subgroups H and K of the same group $(G, *)$ is a subgroup ($H \cup K < G$) if and only if $H \subset K$ or $K \subset H$.

Proof 3.2.2.
Suppose $H \cup K$ is a subgroup of G and H is not included in K, meaning there exists $h \in H$ such that $h \notin K$. Let's show that $K \subset H$. Take any $k \in K$. We have $h * k \in H \cap K$. However, $h * k \notin K$ because otherwise $h = (h * k) * k' \in K$. Hence, $h * k \in H$, implying $k = h' * (h * k) \in H$.

3.2.3 Examples of Groups

3.2.3.1 The Group $\mathbb{Z}/n\mathbb{Z}$

It is initially clear that if n is a positive integer (which we can assume to be positive and non-zero), the set $n\mathbb{Z}$ consisting of integers of the form nk, where k ranges over $\mathbb{Z}$ (the set of multiples of n), is an additive subgroup of $(\mathbb{Z}, +)$.

Proposition 3.2.5.
Every subgroup of $(\mathbb{Z}, +)$ is of the form $n\mathbb{Z}$.

Proof 3.2.3.
Let S be a subgroup of $\mathbb{Z}$ other than $\{0\}$ and $\mathbb{Z}$. Hence, S does not contain 1. The set of positive integers in S, denoted by S^+, has a smallest element n which is at least 2 (since S is countable and bounded below). Every integer of the form kn, where k is a natural number, belongs to S (clear from induction since $kn = n + n + \ldots + n$). Therefore, S contains $n\mathbb{Z}$.

By Euclidean division, every positive integer in S^+ that is not of the form kn can be written as $a = kn + r$, where $0 < r < n$. It follows that $r = a - kn > 0$. Since both a and kn are in S^+, r must also be in S^+. This contradicts n being the smallest element of S^+, hence $r = 0$. This shows that $S = n\mathbb{Z}$.

We easily show that the congruence relation modulo n, where $n \in \mathbb{N}$, due to Gauss, denoted by $\equiv$, is defined as:

$$\forall x, y \in \mathbb{Z}, \quad x \equiv y[n] \Leftrightarrow (x - y) \in n\mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z}, \quad y = x - nk.$$

$x \equiv y[n]$ reads as "x is congruent to y modulo n," which is an equivalence relation defined in $(\mathbb{Z}, +)$. The quotient set is finite and can thus be written:

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, \ldots, \overset{\bullet}{\widehat{n-1}}\}.$$

For example: $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}$, $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$, $\mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$, and $\mathbb{Z}/6\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}\}$.

- Quotient addition on $\mathbb{Z}/n\mathbb{Z}$ induced by $\mathbb{Z}$ is:

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z}, \quad \dot{x} \dot{+} \dot{y} = \overset{\bullet}{\widehat{x+y}}.$$

- Quotient multiplication on $\mathbb{Z}/n\mathbb{Z}$ induced by $\mathbb{Z}$ is:

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z}, \quad \dot{x} \dot{\times} \dot{y} = \dot{\widehat{x \times y}}.$$

Proposition 3.2.6.
The set $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ is a commutative additive group (the quotient group of $\mathbb{Z}$ by the congruence relation).

Proof 3.2.4. *Leave it to the reader.*

3.2.3.2 Group of Permutations

Definition 3.2.3.
Let E be a set. A permutation of E is a bijection from E to itself. We denote by S_E the set of permutations of E. If $E = \{1, \dots, n\}$, we simply denote it by S_n. The set S_E, equipped with the composition of mappings, forms a group with identity $e = id$, called the symmetric group on the set E.

Example 3.2.5.
Let's assume $E = \{1, 2, 3, 4, 5\}$. A permutation $\sigma \in S_5$ is represented as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

which means $\sigma(1) = 3$, $\sigma(2) = 5$, and so on.

3.2.4 Group Homomorphisms

Definition 3.2.4.
Let $(G, *)$ and (H, T) be two groups. A function f from G to H is a ***group homomorphism*** *if:*

$$\forall x, y \in G, \quad f(x * y) = f(x) T f(y).$$

Moreover:

1. *If $G = H$ and $* = T$, it is called an* ***endomorphism***.
2. *If f is bijective, it is an* ***isomorphism***.

3. *If f is a bijective endomorphism, it is an* ***automorphism****.*

Example 3.2.6.

The map $x \mapsto 2x$ defines an automorphism of $(\mathbb{R}, +)$.

Example 3.2.7.

The function $f : \mathbb{R} \to \mathbb{R}_+^*$, where $\mathbb{R}_+^*$ is the set of positive real numbers under multiplication, defined by $f(x) = \exp(x)$, is a group homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_+^*, \times)$ because $\exp(x + y) = \exp(x) \times \exp(y)$ for all $x, y \in \mathbb{R}$.

Proposition 3.2.7. *(Properties of Group Homomorphisms)*

Let f be a homomorphism from $(G, *)$ to (H, T):

1. *$f(e_G) = e_H$.*
2. *$\forall x \in G, f(x^{-1}) = \big(f(x)\big)^{-1}$,*
3. *If f is an isomorphism, then its inverse f^{-1} is also an isomorphism from (H, T) to $(G, *)$.*
4. *If $G' < G$ (subgroup of G), then $f(G') < H$.*
5. *If $H' < H$ (subgroup of H), then $f^{-1}(H') < G$.*

Definition 3.2.5.

Let f be a homomorphism from G to H:

1. *The kernel of f, denoted $Ker(f)$, is the set of pre-images of e_H:*

$$Ker(f) = \{x \in G \mid f(x) = e_H\} = f^{-1}(\{e_H\}).$$

   (Note: f is not assumed to be bijective; hence there's no mention of the inverse bijection of f.)

2. *The image of f, denoted $Im(f)$, is $f(G)$ (set of images by f of elements of G).*

Remark 3.2.2.

According to the last two points of proposition (3.2.7), the kernel and image of f are respective subgroups of G and H.

Proposition 3.2.8.

Let f be a homomorphism from $(G, *)$ to (H, T):

1. *f is surjective if and only if $Im(f) = H$.*

2. *f is injective if and only if $Ker(f) = \{e_G\}$.*

Proof 3.2.5.
The point (1) follows directly from the definition of surjectivity. To prove (2), suppose first that f is injective. Let $x \in Ker(f)$. Then $f(x) = e_H$, and since $f(e_G) = e_H$ as stated, we conclude $f(x) = f(e_G)$, which implies $x = e_G$ by injectivity of f. Thus, $Ker(f) = \{e_G\}$. Conversely, suppose $Ker(f) = \{e_G\}$ and show that f is injective. Consider $x, y \in G$ such that $f(x) = f(y)$. Then $f(x)Tf(y)' = e_H$, so $f(x * y') = e_H$, meaning $x * y' \in Ker(f)$. The assumption $Ker(f) = \{e_G\}$ then implies $x * y' = e_G$, hence $x = y$. Injectivity of f is thus demonstrated, completing the Proof.

3.3 Ring Structure

Definition 3.3.1.
A ring *is a set equipped with two binary operations $(A, *, T)$ such that:*

1. *$(A, *)$ is a commutative group with identity element denoted by 0_A.*

2. *The operation T is associative and distributive on the left and right with respect to $*$:*

$$\forall x, y, z \in A, \quad xT(y * z) = xTy * xTz \quad \text{and} \quad (x * y)Tz = xTz * yTz.$$

3. *The operation T has a neutral element different from 0_A, denoted by 1_A.*

Example 3.3.1.
$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, *and* $(\mathbb{C}, +, \times)$ *are well-known rings.*

Remark 3.3.1.

1. *If the operation T is commutative, the ring is called commutative or abelian.*

2. *The set $A - \{0_A\}$ is denoted by A^*.*

3. *For simplicity, we temporarily use the additive $(+)$ and multiplicative $(\times)$ notations instead of the internal operations $*$ and T. Therefore, we refer to the ring $(A, +, \times)$ instead of $(A, *, T)$.*

Definition 3.3.2.

1. *A commutative ring* $(A, +, \times)$ *is called* ***integral*** *if it is*

   (a) *non-zero (i.e.,* $1_A \neq 0_A$*),*

   (b) $\forall (x, y) \in A^2, \quad x \times y = 0 \Rightarrow (x = 0 \text{ or } y = 0)$.

2. *When a product* $a \times b$ *is zero but neither* a *nor* b *is zero,* a *and* b *are called zero divisors.*

Example 3.3.2.

1. $(\mathbb{Z}, +, \times)$ *of integers is integral: it has no zero divisors.*

2. *The ring* $\mathbb{Z}/6\mathbb{Z}$ *of residue classes modulo* 6 *is not integral because* $\dot{2} \times \dot{3} = \dot{6}$*, hence* $\dot{2} \times \dot{3} = \dot{0}$*. Similarly,* $\mathbb{Z}/4\mathbb{Z}$*.*

Proposition 3.3.1.
Let $(A, +, \times)$ *be a ring. The following rules apply in rings:*

1. $x \times 0_A = 0_A \times x = 0_A$*. The element* 0_A *is absorbing for the operation* $\times$*.*

2. $\forall (x, y) \in A^2, \quad (-x) \times y = x \times (-y) = -(x \times y)$.

3. $\forall x \in A, \quad (-1_A) \times x = -x$.

4. $\forall (x, y) \in A^2, \quad (-x) \times (-y) = x \times y$.

5. $\forall (x, y, z) \in A^3, \quad x \times (y - z) = x \times y - x \times z$ *and* $(y - z) \times x = y \times x - z \times x$.

Proof 3.3.1.

1. $x \times 0_A = x \times (0_A + 0_A) = x \times 0_A + x \times 0_A$*. Therefore, by the regularity of elements in the group* $(A, +)$*,* $x \times 0_A = 0_A$*. Similarly for the other side.*

2. $x \times y + (-x) \times y = (x + (-x)) \times y = 0_A \times y = 0_A$*. Thus,* $(-x) \times y = -(x \times y)$*. Similarly for the other equality.*

3. $(-1_A) \times x + x = (-1_A) \times x + 1_A \times x = (-1_A + 1_A) \times x = 0_A \times x = 0_A$*. Hence,* $(-1_A) \times x = -x$*.*