Problem §2
Fill in the tables for powers of 2 in $\mathbb{F}_{13}$.

Solution:

Table 1: Problem 2

n	0	1	2	3	4	5	6	7	8	9	10	11
2^n	1	2	4	8	3	6	12	11	9	5	10	7

Problem §2 Let

$$\begin{aligned} f : \mathbb{R}^2 &\longrightarrow \mathbb{R}^3 \\ (x, y) &\longmapsto f((x, y)) = (x, x + y, y). \end{aligned}$$

(a) Write down, using the definition of injectivity and preferably using universal quantifiers, the statement that f is injective, and the statement that f is not injective. Then prove the correct statement (that f is injective).

(b) Write down, using universal quantifiers, the statement that f is surjective, and the statement that f is not surjective. Then prove the correct statement (that f is not surjective).

Solution:

(a) f is injective: For any $a, b \in \mathbb{R}^2$, if $f(a) = f(b)$, then $a = b$.
f is not injective: There exists $a, b \in \mathbb{R}^2$ such that $f(a) = f(b)$ and $a \neq b$.
Now, we prove that f is injective.

Proof. Choose $(x_0, y_0), (x_1, y_1) \in \mathbb{R}^2$ such that $(x_0, x_0 + y_0, y_0) = (x_1, x_1 + y_1, y_1)$. From this, we see that $x_0 = x_1, y_0 = y_1$, so $(x_0, y_0) = (x_1, y_1)$ and thus f is injective. $\square$

(b) f is surjective: For any $v \in \mathbb{R}^3$, there exists an $u \in \mathbb{R}^2$ such that $f(u) = v$.
f is not surjective: There exists a $v \in \mathbb{R}^3$ such that for any $u \in \mathbb{R}^2$, $f(u) \neq v$.
Now, we prove that f is not surjective.

Proof. Choose $(0, 10, 0) \in \mathbb{R}^3$. Clearly, for any $(x_0, y_0) \in \mathbb{R}^2$, if $f((x_0, y_0)) = (0, 10, 0)$, then $x_0 = y_0 = 0$; but then $x_0 + y_0 = 0 \neq 10$. Thus f is not surjective. $\square$

Problem §3 Let X be any set, and let V be the set of all subsets of X. Define addition on V as

$$A + B = A \Delta B$$

for subsets $A, B \subseteq X$, and scalar multiplication on V with scalars $\mathbb{F}_2 = \{0, 1\}$ as

$$0 \cdot A = \varnothing, 1 \cdot A = A$$

for any subset $A \subseteq X$.
Check that $V_{\mathbb{F}_2}$ is a vector space.

Solution: In order to be a vector space, $V_{\mathbb{F}_2}$ must satisfy 6 properties:

- **Associativity**: We start with additive associativity. Let $A, B, C \subseteq X$. Then

$$\begin{aligned} A\Delta\,(B\Delta C) &= (A \cap ((B \cap C^c) \cup (C \cap B^c))^c) \cup (((B \cap C^c) \cup (C \cap B^c)) \cap A^c) \\ &= (A \cap ((B^c \cup C) \cap (C^c \cup B))) \cup ((A^c \cap (B \cap C^c)) \cup (A^c \cap (C \cap B^c))) \\ &= (A \cap ((B^c \cap C^c) \cup (B^c \cap B)) \cup ((C \cap C^c) \cup (C \cap B))) \cup ((A^c \cap (B \cap C^c)) \cup (A^c \cap (C \cap B^c))) \\ &= (A \cap ((B^c \cap C^c) \cup (B \cap C))) \cup ((A^c \cap B \cap C^c) \cup (A^c \cap C \cap B^c)) \\ &= ((A \cap B^c \cap C^c) \cup (A \cap B \cap C)) \cup ((B \cap A^c \cap C^c) \cup (C \cap A^c \cap B^c)). \end{aligned}$$

Conversely,

$$\begin{aligned}(A\Delta B)\,\Delta C &= (((A\cap B^c)\cup(B\cap A^c))\cap C^c)\cup(C\cap((A\cap B^c)\cup(B\cap A^c))^c)\\ &= ((A\cap B^c\cap C^c)\cup(B\cap A^c\cap C^c))\cup(C\cap((A^c\cup B)\cap(B^c\cup A)))\\ &= ((A\cap B^c\cap C^c)\cup(B\cap A^c\cap C^c))\cup(C\cap((A^c\cap B^c)\cup(B\cap B^c))\cup((A^c\cap A)\cup(A\cap B)))\\ &= ((A\cap B^c\cap C^c)\cup(B\cap A^c\cap C^c))\cup((C\cap A^c\cap B^c)\cup(C\cap A\cap B))\,.\end{aligned}$$

Due to commutativity of union and intersection of sets, we observe that $A\Delta\,(B\Delta C) = (A\Delta B)\Delta C$, and so it satisfies additive associativity.

Now, we show scalar multiplicative associativity. Let $\alpha, \beta \in \mathbb{F}_2$. Then we show associativity holds for the four possible cases:

- $1\cdot(1\cdot A) = 1\cdot A = A = 1\cdot A = (1\cdot 1)\cdot A$
- $1\cdot(0\cdot A) = 1\cdot\varnothing = 0\cdot A = (1\cdot 0)\cdot A$
- $0\cdot(1\cdot A) = 0\cdot A = \varnothing = 0\cdot A = (0\cdot 1)\cdot A$
- $0\cdot(0\cdot A) = 0\cdot\varnothing = \varnothing = 0\cdot\varnothing = (0\cdot 0)\cdot A$

Thus scalar multiplicative associativity holds as well, and so associativity holds.

- **Commutativity**: Let $A, B \subseteq X$. Then

$$\begin{aligned}A\Delta B &= (A\setminus B)\cup(B\setminus A)\\ &= (B\setminus A)\cup(A\setminus B)\\ &= B\Delta A,\end{aligned}$$

by commutativity of set union. Thus commutativity holds.

- **Additive Identity**: Observe that for any $A \subseteq X$,

$$A\Delta\varnothing = \varnothing\Delta A = A.$$

Thus additive identity holds.

- **Additive Inverse**: For any $A \in X$, choose $A' = A^c \subseteq X$ (the complement of A). Then

$$A\Delta A' = A'\Delta A = \varnothing.$$

Thus additive inverse holds.

- **Multiplicative Identity**: Observe that for any $A \subseteq X$,

$$1\cdot A = A$$

by definition. Thus scalar multiplicative identity holds.

- **Distributive Properties**: First we show that for any $\lambda \in \mathbb{F}_2, A, B \in X$, $\lambda\cdot(A+B) = \lambda\cdot A + \lambda\cdot B$:

$$\begin{aligned}\lambda\cdot(A+B) &= A+B\\ &= \lambda\cdot A + \lambda\cdot B.\end{aligned}$$

The last statement holds true for both $\lambda = 0$ and $\lambda = 1$, and so the first distributive property holds.

Now, we show that the second distributive property, $(\alpha+\beta)\,A = \alpha\cdot A + \beta\cdot A$, is true for all $\alpha, \beta \in \mathbb{F}_2, A \subseteq X$; we do this by evaluating the three cases $(0+1 = 1+0 = 1)$:

- If $\alpha = \beta = 1$:

$$\begin{aligned}(1+1)\cdot A &= 0 \cdot A \\ &= \varnothing \\ &= A \Delta A \\ &= 1 \cdot A + 1 \cdot A.\end{aligned}$$

- If $\alpha = 0, \beta = 1$:

$$\begin{aligned}(1+0)\cdot A &= 1 \cdot A \\ &= A \\ &= A \Delta \varnothing \\ &= 1 \cdot A + 0 \cdot A.\end{aligned}$$

- If $\alpha = \beta = 0$:

$$\begin{aligned}(0+0)\cdot A &= 0 \cdot A \\ &= \varnothing \\ &= A \Delta A \\ &= 0 \cdot A + 0 \cdot A \\ &.\end{aligned}$$

Thus the second distributive identity holds as well, and so distributive properties hold.