1a) A operação $-$ não é associativa. De fato, $1,2,3 \in \mathbb{R}$, no entanto,

$$(1-2)-3 = -1-3 = -4$$
$$1-(2-3) = 1-(-1) = 2$$

A operação p é associativa. De fato, dados $x,y,z \in \mathbb{R}$, temos

$$p(p(x,y),z) = p(x,z) = x$$
$$p(x,p(y,z)) = p(x,y) = x$$

1b) A operação $-$ não é comutativa. De fato, $2,3 \in \mathbb{R}$, no entanto, $2-3 \neq 3-2$.

· A operação p não é comutativa. De fato, $2,3 \in \mathbb{R}$, no entanto, $p(2,3) = 2 \neq 3 = p(3,2)$.

1c) Se e é um elemento neutro de $-$, devemos ter, em particular,

$$e - x = x \quad \forall\, x \in \mathbb{R},$$

donde $e = 2x \ \forall\, x \in \mathbb{R}$. Portanto, a operação $-$ não possui elemento neutro.

Se e é um elemento neutro de p, devemos ter, em particular,

$$p(e,y) = y \quad \forall\, y \in \mathbb{R},$$

donde $e = y \ \forall\, y \in \mathbb{R}$. Um absurdo. Portanto, a operação p não possui elemento neutro.

1d) Se não existem elementos neutros, então em particular, não existem elementos simetrizáveis

1e) Note que para todo $a,b,c \in \mathbb{R}$, temos

$$a - c = b - c \Rightarrow a = b$$
$$c - a = c - b \Rightarrow a = b$$

Logo, todo elemento $c \in \mathbb{R}$ é regular em relação a operação $-$.

Dado $c \in \mathbb{R}$, temos que

$$p(c,1) = p(c,2),$$

no entanto, $1 \neq 2$. Logo c não é regular, isto é, nenhum elemento $c \in \mathbb{R}$ é regular em relação a operação p.

2- $(M_{2\times 3}(\mathbb{R}), +)$ é um grupo. De fato.

i) $A+(B+C) = (A+B)+C \quad \forall\, A,B,C \in M_{2\times3}(\mathbb{R})$

ii) $e = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ é um elemento neutro de $+$ em $M_{2\times3}(\mathbb{R})$

iii) Dado $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \in M_{2\times3}(\mathbb{R})$, temos que $B = \begin{bmatrix} -a_{11} & -a_{12} & -a_{13} \\ -a_{21} & -a_{22} & -a_{23} \end{bmatrix} \in M_{2\times3}(\mathbb{R})$ e

$$A+B = B+A = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

3a) • Para todas as funções $f, g, h \in F(\mathbb{R})$, temos
$$f\circ(g\circ h) = (f\circ g)\circ h$$
Logo, $\circ$ é associativa

• A operação $\circ$ não é comutativa. De fato, considere $f(x) = x^2$ e $g(x) = 5$ (g constante). Temos
$$f\circ g(x) = f(g(x)) = f(5) = 25 \quad \forall\, x \in \mathbb{R}$$
$$g\circ f(x) = g(f(x)) = g(x^2) = 5 \quad \forall\, x \in \mathbb{R}$$
Em particular, $f\circ g \neq g\circ f$

• A função $Id \begin{array}{l} \mathbb{R}\to\mathbb{R} \\ x \mapsto x \end{array}$ satisfaz $f\circ Id = Id\circ f = f \ \forall\, f \in F(\mathbb{R})$, logo Id é um elemento neutro de $F(\mathbb{R})$ com relação a operação $\circ$.

• As funções simetrizáveis são aquelas que possuem inversa, isto é, as funções bijetoras.

3b) $(F(\mathbb{R}), \circ)$ não é um grupo, pois nem todo elemento de $F(\mathbb{R})$ é inversível. No entanto, se considerarmos $F_B(\mathbb{R}) = \{ f \in F(\mathbb{R}) : f \text{ é bijetora} \}$, temos que a composição de funções é uma operação em $F_B(\mathbb{R})$ pois composição de funções bijetoras também é uma função bijetora. Além disso, $Id \in F_B(\mathbb{R})$ e todo elemento de $F_B(\mathbb{R})$ é inversível. Portanto, $(F_B(\mathbb{R}), \circ)$ é um grupo (não comutativo).

4a) As operações $+$ e $\cdot$ são associativas. De fato, dados $\bar{x}, \bar{y}$ e $\bar{z} \in \mathbb{Z}_m$, temos
$$(\bar{x}+\bar{y})+\bar{z} = \overline{x+y}+\bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x}+\overline{y+z} = \bar{x}+(\bar{y}+\bar{z})$$
$$(\bar{x}\cdot\bar{y})\cdot\bar{z} = \overline{x\cdot y}\cdot\bar{z} = \overline{(x\cdot y)\cdot z} = \overline{x\cdot(y\cdot z)} = \bar{x}\cdot\overline{y z} = \bar{x}\cdot(\bar{y}\cdot\bar{z})$$

4b) As operações $+$ e $\cdot$ são comutativas. De fato, dados $\bar{x}, \bar{y} \in \mathbb{Z}_m$, temos
$$\bar{x}+\bar{y} = \overline{x+y} = \overline{y+x} = \bar{y}+\bar{x}$$
$$\bar{x}\cdot\bar{y} = \overline{x\cdot y} = \overline{y\cdot x} = \bar{y}\cdot\bar{x}$$

4c) $\bar{0}$ é um elemento neutro de $+$. De fato,
$$\bar{0}+\bar{x} = \bar{x}+\bar{0} = \bar{x} \quad \forall\, \bar{x} \in \mathbb{Z}_m$$
$\bar{1}$ é um elemento neutro de $\cdot$. De fato,
$$\bar{1}\cdot\bar{x} = \bar{x}\cdot\bar{1} = \bar{x} \quad \forall\, \bar{x} \in \mathbb{Z}_m$$

4d) Todo elemento de $\mathbb{Z}_m$ é simetrizável em relação a soma. De fato, dado $\bar{x} \in \mathbb{Z}_m$, temos que $\overline{-x} \in \mathbb{Z}_m$ e
$$\bar{x}+\overline{-x} = \overline{-x}+\bar{x} = \bar{0}$$

4e) Dado $\bar{a} \in \mathbb{Z}_m$, temos que

$$
\begin{aligned}
\bar{a} \text{ é simetrizável} &\iff \exists\, \bar{x} \in \mathbb{Z}_m \text{ tal que } \bar{a}\cdot\bar{x} = \bar{1} \text{ em } \mathbb{Z}_m \\
&\iff \exists\, x \in \mathbb{Z} \text{ tal que } \overline{ax} = \bar{1} \text{ em } \mathbb{Z}_m \\
&\iff \exists\, x \in \mathbb{Z} \text{ tal que } (1 - ax) \mid m \\
&\iff \exists\, x, y \in \mathbb{Z} \text{ tal que } 1 - ax = my \\
&\iff ax + my = 1 \text{ possui solução inteira} \\
&\iff MDC(a, m) = 1
\end{aligned}
$$

Portanto $\bar{a}$ é simetrizável em $\mathbb{Z}_m$ apenas quando $MDC(a, m) = 1$.

4f) $(\mathbb{Z}_m, +)$ é um grupo, pois a operação $+$ é associativa, possui elemento neutro e todo elemento de $\mathbb{Z}_m$ possui inversa (ver (4a), (4c) e (4d)).

4g) $(\mathbb{Z}_m, \cdot)$ não é um grupo, pois $\bar{0}$ não é inversível em relação a operação de multiplicação.

4h) Como $(\mathbb{Z}_m, +)$ é um grupo, então todo elemento de $\mathbb{Z}_m$ é regular em relação a soma.

4i) Considere $\bar{a} \in \mathbb{Z}_m$ com $0 \leq a < m$.

- Se $MDC(a, m) = 1$, então vimos em (4e) que $\bar{a}$ é simetrizável e, em particular, $\bar{a}$ é regular pois a operação é associativa.
- Se $MDC(a, m) \neq 1$, seja $b = \dfrac{MMC(a, m)}{a}$, temos que $\bar{b} \neq \bar{0}$. Além disso,
$$\bar{a}\cdot\bar{b} = \bar{0} = \bar{a}\cdot\bar{0}$$

Logo $\bar{a}$ não é regular com relação a operação de multiplicação.

5a) A multiplicação de classes de congruência não é uma operação em $\mathbb{Z}_m^*$ quando m é composto. De fato, sejam $a, b \in \mathbb{Z}$ tais que $a \cdot b = m$ com $0 < a, b < m$. Temos que $\bar{a}, \bar{b} \in \mathbb{Z}_m^*$, no entanto, $\bar{a}\cdot\bar{b} = \bar{0} \notin \mathbb{Z}_m^*$.

5b) Considere m primo e tome $\bar{a} \in \mathbb{Z}_m^*$. Em particular, $MDC(a, m) = 1$, pois m é primo e "a" não é múltiplo de m. Assim, $\bar{a}$ é inversível.

Dados $\bar{a}, \bar{b} \in \mathbb{Z}_m^*$, suponha por absurdo que $\bar{a}\cdot\bar{b} \notin \mathbb{Z}_m^*$. Então $\bar{a}\cdot\bar{b} = \bar{0}$,

$\Rightarrow \bar{a}^{-1}(\bar{a}\cdot\bar{b}) = \bar{a}^{-1}\,\bar{0} \Rightarrow (\bar{a}^{-1}\cdot\bar{a})\,\bar{b} = \bar{0} \Rightarrow I\,\bar{b} = \bar{0} \Rightarrow \bar{b} = \bar{0}$. Absurdo, portanto $\bar{a}\,\bar{b} \in \mathbb{Z}_m^*$ e consequentemente, a multiplicação é uma operação em $\mathbb{Z}_m^*$

5c) Se m é primo, então a multiplicação é uma operação em $\mathbb{Z}_m^*$. (ver 5b) (4)
Além disso, a multiplicação é associativa (ver 4a) e possui elemento neutro (ver 4c).
Dado $\bar{a} \in \mathbb{Z}_m^*$, então como "$a$" não é múltiplo de m e m é primo, temos que $MDC(a,m)=1$. Logo, segue $\bar{a}$ é inversível em $\mathbb{Z}_m$ (ver 4e).

6i) Dados $(a,b),(c,d),(e,f) \in \mathbb{R}^2 \setminus \{0,0\}$, temos $(a,b)*(c,d)=(ac-bd,ad+bc)=(c,d)*(a,b)$
Logo $*$ é comutativa. Além disso,

$$\begin{aligned}((a,b)*(c,d))*(e,f) &= (ac-bd,ad+bc)*(e,f)\\ &= ((ac-bd)e-(ad+bc)f,\ (ac-bd)f+(ad+bc)e)\\ &= (ace-bde-adf-bcf,\ acf-bdf+ade+bce)\end{aligned}$$

$$\begin{aligned}(a,b)*((c,d)*(e,f)) &= (a,b)*(ce-df,cf+de)\\ &= (a(ce-df)-b(cf+de),\ a(cf+de)+b(ce-df))\\ &= (ace-adf-bcf-bde,\ acf+ade+bce-bdf)\end{aligned}$$

Logo

$$((a,b)*(c,d))*(e,f) = (a,b)*((c,d)*(e,f))$$

e, portanto, $*$ é associativa.

ii) Dado $(a,b) \in \mathbb{R}^2 \setminus \{(0,0)\}$, temos

$$(a,b)*(1,0) = (a\cdot 1 - b\cdot 0,\ a\cdot 0 + b\cdot 1) = (a,b)$$
$$(1,0)*(a,b) = (1\cdot a - 0\cdot b,\ 1\cdot b + 0\cdot a) = (a,b)$$

Logo $(1,0)$ é um elemento neutro de $\mathbb{R}^2 \setminus \{(0,0)\}$.

iii) Dado $(a,b) \in \mathbb{R}^2 \setminus \{(0,0)\}$, então temos $a^2+b^2 \neq 0$. Considere $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) \in \mathbb{R}^2 \setminus \{0,0\}$
Note que

$$(a,b)*\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = \left(a\cdot\frac{a}{a^2+b^2} - b\cdot\frac{-b}{a^2+b^2},\ a\frac{-b}{a^2+b^2} + b\frac{a}{a^2+b^2}\right) = (1,0)$$

Do mesmo modo,

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

pois $*$ é comutativo. Portanto, segue de (i), (ii) e (iii) que $(\mathbb{R}^2 \setminus \{0,0\}, *)$ é um grupo comutativo.

7) Dados $h_1 = a_1 + b_1\sqrt{3}$ e $h_2 = a_2 + b_2\sqrt{3}$ elementos de H, temos que

$$(a_2 + b_2\sqrt{3})(X + Y\sqrt{3}) = 1 \iff$$

$$a_2X + 3b_2Y + (b_2X + a_2Y)\sqrt{3} = 1 \iff$$

$$\begin{cases} a_2X + 3b_2Y = 1 \\ b_2X + a_2Y = 0 \end{cases} \iff$$

$$\begin{cases} Y = \dfrac{b_2}{-a_2^2 + 3b_2^2} \\ \\ X = \dfrac{-a_2}{-a_2^2 + 3b_2^2} \end{cases} \qquad (*)$$

Note que $-a_2^2 + 3b_2^2 = 0 \iff 3b_2^2 = a_2^2$

$\iff \sqrt{3} = a/b$

$\iff \sqrt{3}$ é racional.

Como $\sqrt{3}$ é irracional, segue que $-a_2^2 + 3b_2^2 \neq 0$. Logo, X e Y definidos em $(*)$ estão bem definidos e são racionais. Logo $(h_2)^{-1} = X + Y\sqrt{3} \in H$. Observe ainda que

$$h_1 \cdot (h_2)^{-1} = (a_1 + b_1\sqrt{3})(X + Y\sqrt{3})$$

$$= \underbrace{(a_1X + 3b_1Y)}_{\in \mathbb{Q}} + \underbrace{(b_1X + a_1Y)}_{\in \mathbb{Q}}\sqrt{3} \in H.$$

Portanto, H é um subgrupo de $(\mathbb{R}^*, \cdot)$.

8a) Dados $a, b \in H_1$, temos que a e b são da forma $a = (X_1, 0)$ e $b = (X_2, 0)$ com $X_1, X_2 \in \mathbb{R}$. Note que

$$a + b^{-1} = (X_1, 0) + (-X_2, 0) = (X_1 - X_2, 0) \in H_1$$

Portanto, H_1 é um subgrupo de $(\mathbb{R}^2, +)$

8b) H_2 não é um subgrupo de $(\mathbb{R}^2, \cdot)$, pois $(1,5)$ e $(1,8) \in H_2$, mas $(1,5)+(1,8) = (2,13) \notin H_2$

8c) Dados $a, b \in H_3$, temos que a e b são da forma $a = (X_1, Y_1)$ com $X_1 + Y_1 = 0$ e $b = (X_2, Y_2)$ com $X_2 + Y_2 = 0$. Note que

$$a + b^{-1} = (X_1, Y_1) + (-X_2, -Y_2) = (X_1 - X_2, Y_1 - Y_2)$$

Observe ainda que $(X_1 - X_2) + (Y_1 - Y_2) = (X_1 + Y_1) - (X_2 + Y_2) = 0 - 0 = 0$, Logo $a + b^{-1} \in H_3$ e, portanto, H_3 é um subgrupo de $(\mathbb{R}^2, +)$