Tutorial #3.1: Group

1 Exercise 1:

Prove that: $G = (\mathbb{R}^*, *)$ is a group.

i) Let $a, b, c \in \mathbb{R}^*$, $(a * b) * c = abc = a * (b * c)$. Thus, G is associative.

ii) There exists $e = 1$ such that $a*e = a = e*a$. Thus, G has indentity element.

iii) There exists $1/a$ $\forall a \in \mathbb{R}^*$ such that $a * 1/a = 1 = e$. Thus, G has inverse element.

iv) Since $a * b = ab = ba = b * a$, G is commutative.

Conclusion: G is not only a group, but also an abelian group.

2 Exercise 2:

Prove that: $G = (\mathbb{R}^* \times \mathbb{Z}, \circ)$ is a group with $(a, m) \circ (b, n) = (ab, m+n)$.

i) Let arbitrary $(a, m), (b, n), (c, q) \in \mathbb{R}^* \times \mathbb{Z}$

$$((a, m) \circ (b, n)) \circ (c, q) = (ab, m + n) \circ (c, q) = (abc, m + n + q)$$

$$(a, m) \circ ((b, n) \circ (c, q)) = (a, m) \circ (bc, n + q) = (abc, m + n + q)$$

Thus, G is associative.

ii) There exists $e = (1, 0)$ such that $(a, m) * e = (a, m)$. Thus, G has identity element.

iii) There exists $(1/a, -m)$ such that $(1/a, -m) \circ (a, m) = (1, 0) = e$. Thus, G has inverse element for all element in $(\mathbb{R}^* \times \mathbb{Z})$

iv) Since $(a, m) \circ (b, n) = (ab, m + n) = (ba, n + m) = (b, n) \circ (a, m)$. G is also commutative.

Conclusion: G is an abelian group.

3 Exercise 3:

Let a, b, c be arbitrary in $\mathbb{Z}$.

a) Since $(a+b)+c \equiv a+b+c \equiv a+(b+c) \pmod{n}$, addition mod n is associative operation in $\mathbb{Z}$.

b) Since $(ab)c \equiv abc \equiv a(bc) \pmod{n}$, multiplication mod n is associative operation in $\mathbb{Z}$.

Conclusion: Addition and multiplication mod n are associative operations in $\mathbb{Z}$.

4 Exercise 4:

Prove that: (G, *) such that $(ab)^2 = a^2b^2$ is an abelian group.
Indeed:

$$\begin{aligned} (ab)^2 &= a^2b^2 \\ abab &= aabb \\ (a^{-1} * a)ba(b * b^{-1}) &= (a^{-1} * a)ab(b * b^{-1}) \\ ba &= ab \qquad (1) \end{aligned}$$

Conclusion: Since $(G, *)$ is group, with (1) satisfied, $(G, *)$ is also commutative. Hence, $(G, *)$ is an abelian group.

5 Exercise 5:

Prove that: $G = (\mathbb{R}\backslash\{-1\}, *)$ is an abelian group with $a*b = a+b+ab$.

i) Let a, b, c be arbitrary in $\mathbb{R} \setminus \{-1\}$, we have:

$$\begin{aligned} (a*b)*c = (a+b+ab)*c &= (a+b+ab)+c+(a+b+ab)c \\ &= a+b+c+ab+bc+ac+abc \qquad (1) \end{aligned}$$

$$
\begin{aligned}
a * (b * c) = a * (b + c + bc) &= a + (b + c + bc) + a(b + c + bc) \\
&= a + b + c + ab + bc + ac + abc \quad (2)
\end{aligned}
$$

With $(1) = (2)$, we conclude that G is associative.

ii) There exists $e = 0$ such that $a * e = (a + 0 + a * 0) = a$. Thus, G has identity element.

iii) With arbitrary element $a \in \mathbb{R} \setminus \{-1\}$, there exists a^{-1} is an inverse element of a. Indeed:

$$
\begin{aligned}
a * a^{-1} = e &\iff a + a^{-1} + aa^{-1} = 0 \\
&\iff a^{-1} = \frac{-a}{a+1}
\end{aligned}
$$

iv) Since $a * b = a + b + ab = b + a + ba = b * a$, G is commutative.

Conclusion: Hence, G is an abelian group.

6 Exercise 6:

Prove that: $ab = ba$ with $a^4 b = ba$ and $a^3 = e \; \forall a, b \in G$.
Proof: It's trivial (write EASY! in exam will get you score ;)).

$$
\begin{aligned}
a^4 b &= ba \\
a^3 * ab &= ba \\
e * ab &= ba \\
(e * a)b &= ba \\
ab &= ba \qquad \text{(Q.E.D)}
\end{aligned}
$$

7 Exercise 7:

Skip

8 Exercise 8:

Prove that: $(a^n)^{-1} = (a^{-1})^n$ with a is an element in group G.
Proof: We can easily deduce that

$$(a^n)^{-1} * (a^n) = e \tag{1}$$

$$(a^{-1})^n * (a^n) = a^{-1}...a^{-1}(a^{-1}a)a...a = a^{-1}...(a^{-1}a)...a = ... = e \tag{2}$$

Proposition #2 saying that the inverse element of an element in group G is unique, while both $(a^n)^{-1}$ and $(a^{-1})^n$ is inverse element of a^n. Thus, $(a^n)^{-1}$ and $(a^{-1})^n$ must be equal.

9 Exercise 9:

Prove that: $ax = xa \iff a^{-1}x = xa^{-1}$
Proof:

$$\begin{aligned} ax &= xa \\ a^{-1}ax &= a^{-1}xa \\ x &= a^{-1}xa \\ xa^{-1} &= a^{-1}xaa^{-1} \\ xa^{-1} &= a^{-1}x \end{aligned} \tag{Q.E.D}$$

10 Exercise 10:

Prove that: $ab = ba$. Given $a^3b = ba^3$, $a, b \in G$ order 5.
Proof:

$$\begin{aligned} a^3b &= ba^3 \\ (a^3 * a^3)b &= (a^3 * b)aa^3 \\ a^5 * ab &= ba^3a^3 \\ e * ab &= b(a^3a^3) \\ ab &= ba \end{aligned} \tag{Q.E.D}$$

11 Exercise 11:

Prove that: $G = (a\mathbb{Z} + b\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$. Given that a, b are integers.

Proof:

Let $\mathbb{M} = a\mathbb{Z}+b\mathbb{Z}$. Thus, the elements of $\mathbb{M}$ satisfies that it is an integer.

i) It's trivial that $e = 0$ is the identity element of $(\mathbb{Z}, +)$. Let $x \in \mathbb{M}$, we have $x + e = x + 0 = X$. Thus, G also has identity element $e = 0$.

ii) Let $y \in \mathbb{M}$, x, y must satisfies that $x = ak + bl$; $y = ai + bj$ with $l, k, i, j \in \mathbb{Z}$. Hence, $x + y = a(k + i) + b(l + j)$. This satisfies that $x + y \in \mathbb{M}$

iii) Let x^{-1} be the inverse element of x. By definition, $x * x^{-1} = e$ $\iff x+x^{-1} = 0 \iff x^{-1} = -x \iff x^{-1} = a(-k)+b(-l)$. Since there exist such $(-k), (-l) \in \mathbb{R}$, there also exists such $x^{-1} \in \mathbb{M}$.

Conclusion: G is subgroup of $(Z, +)$