ADVANCED MATHEMATICS

Groups

1. Show that the following sets have a group structure:
(a) $G = \{x \in \mathbb{R} \mid x \neq 0\}$ with usual multiplication.
(b) $G = \{1, -1, i, -i\} \subset \mathbb{C}$ with multiplication.
(c) $G = \{x \in \mathbb{C} \mid x^n = 1\}$ with multiplication, for $n \in \mathbb{N}$ fixed.
(d) $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ with multiplication.
(e) $\mathrm{GL}(2, \mathbb{Z}_3) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_3, ad - bc \neq_3 0 \right\}$, with matrix multiplication.
(f) $\mathrm{O}(2, \mathbb{Z}_3) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_3, ad - bc \neq_3 0, A^t = A^{-1} \right\}$, with matrix multiplication.
(g) $\mathbb{Z}_m^* = \{[n] \in \mathbb{Z}_m : \exists [n]^{-1}\}$ with multiplication in $\mathbb{Z}_m$.

2. Show why the following sets are not groups under the corresponding operations:
(a) $G = \{x \in \mathbb{R} \mid x < 0\}$ with multiplication.
(b) $G = \{a \in \mathbb{Z} \mid a \text{ is a perfect square}\}$ with the usual sum.[1]
(c) $G = \{a \in \mathbb{Z} \mid a \text{ is a perfect square}\}$ with usual multiplication.
(d) $G = \{[0], [2], [3], [6]\} \subset \mathbb{Z}_8$ with sum in $\mathbb{Z}_8$.

3. Let $G = (-1, 1) \subset \mathbb{R}$. We define a product operation $x * y := \frac{x+y}{1+xy}$ for $x, y \in G$. Prove that $(G, *)$ is a group.

4. **(*)** Find a product operation over $G = \mathbb{R}$, such that the inverse of $x \in G$ is $1 - x$.

5. A non-empty subset H of a group $(G, *)$ is a *subgroup* of G if we can verify that:

$$a, b \in H \Rightarrow a * b \in H \text{ and also } a \in H \Rightarrow a^{-1} \in H$$

Prove that H is a subgroup if and only if $a, b \in H \Rightarrow a * b^{-1} \in H$.

6. Prove that if H is a **finite** subset of a group $(G, *)$ such that $a, b \in H \Rightarrow a * b \in H$ then H is a subgroup.

7. Show the elements of the linear group

$$\mathrm{GL}(2, \mathbb{Z}_2) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_2, ad - bc \neq_2 0 \right\}$$

and compute the table of the group. Compute the order of each of its elements and determine if the group is abelian or cyclic.

8. Show the eight elements of the orthogonal group $O(2, \mathbb{Z}_3)$ and compute the table of the group. Show the orders of its elements and determine if the group is cyclic or abelian.

9. Find out the order of the elements of $\mathbb{Z}_n^*$ for $n = 6, 7, 8, 9, 10, 12$. Show generators for each of these groups.

10. Find an explicit group isomorphism from $\mathbb{Z}_{12} \times \mathbb{Z}_{11}$ to $\mathbb{Z}_{132}$.

11. Let G be a group and $a, b \in G$. Prove that:
(a) If $\mathrm{ord}(a) = n \in \mathbb{N}$ and $n = pq$, then $\mathrm{ord}(a^p) = q$.
(b) $\mathrm{ord}(a^{-1}) = \mathrm{ord}(a)$ and $\mathrm{ord}(ab) = \mathrm{ord}(ba)$.
(c) If a and b have coprime finite orders, then $\langle a \rangle \cap \langle b \rangle = \{e\}$.

[1] A perfect square is a number that can be expressed as the product of two equal integers.

12. Consider the following complex matrices

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Show that the set $G = \{\mathbf{1}, \mathbf{-1}, \mathbf{i}, \mathbf{-i}, \mathbf{j}, \mathbf{-j}, \mathbf{k}, \mathbf{-k}\}$ is a group under matrix product (this is the so-called *quaternion group*). Compute the multiplication table of G and its order, as well as the orders of each of its elements. Study if G is isomorphic to the *dihedric group* D_4 or to the group of four elements permutations S_4.

13. **(*)** Let $f : \mathbb{R} \to \mathbb{C}^*$ be the application defined by $f(t) = \cos(2\pi t) + i \sin(2\pi t)$. Take $\mathbb{R}$ as a group with respect to sum and $\mathbb{C}^*$ as a group with the product operation.
(a) Prove that f is a group homomorphism.
(b) Find the Kernel and the Image of f.
(c) Show that the quotient group $\mathbb{R}/\mathbb{Z}$ is isomorphic to the group S^1 of exercise 1(d).

14. Show that the order of a finite group G is a prime number if and only if G has no proper subgroups (that is, its only subgroups are $\{e\}$ and G).

15. Let G be a group with order $|G|$ prime. Prove that G is cyclic.

16. **(*)** Use Lagrange theorem to show the *Fermat's Little Theorem* and *Euler's Theorem*.

17. Prove the following statements:
a) If p and $n > 0$ are coprime, there exists an $m \geq 1$ such that n divides $p^m - 1$.
b) If n and p are different primes, then n divides $p^{n-1} - 1$.

18. **(*)** It is said that a subgroup H of a group G is **normal** if $gH = Hg \ \forall g \in G$.
(a) Prove that if $[G : H] = 2$, then H is a normal subgroup of G
(b) Prove that $\mathrm{SL}(2, \mathbb{Z}_p) = \{A \in \mathcal{M}_2(\mathbb{Z}_p) \mid \det A = 1\}$ is a normal subgroup of $\mathrm{GL}(2, \mathbb{Z}_p) = \{A \in \mathcal{M}_2(\mathbb{Z}_p) \mid \det A \neq_p 0\}$ provided that p is a prime number. Prove that the quotient $\mathrm{GL}(2, \mathbb{Z}_p)/\mathrm{SL}(2, \mathbb{Z}_p)$ has a group structure that is isomorphic to $\mathbb{Z}_p^*$.

19. Let $G_1 = \mathbb{Z}_{24} \times \mathbb{Z}_{60}$ and $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_{20}$.
(a) Show that G_1 and G_2 are not isomorphic.
(b) Study if there exists surjective (onto) homomorphisms (of additive groups) of G_1 or G_2 over $\mathbb{Z}_{120}$
(c) Find four abelian groups of order 1440 not isomorphic between each other and neither isomorphic to G_1 nor G_2.