UNIVERSIDAD YACHAY TECH

School of Mathematical and Computational Sciences
Abstract Algebra

Prof. Pablo Rosero
& Christian Chávez
Problem Set 2

Groups, Subgroups and Homomorphisms

(Lessons 3, 4 and 5)

1. Determine which of the following binary operations are associative.

(a) the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$

(b) the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$

(c) the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \dfrac{a+b}{5}$

(d) the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a,b) \star (c,d) = (ad + bc, bd)$

(e) the operation $\star$ on $\mathbb{Q} \setminus \{0\}$ defined by $a \star b = \dfrac{a}{b}$

2. Determine which of the following sets are groups under addition:

(a) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd

(b) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even

(c) the set of rational numbers of absolute value < 1

(d) the set of rational numbers of absolute value ≥ 1 together with 0

(e) the set of rational numbers with denominators equal to 1 or 2

(f) the set of rational numbers with denominators equal to 1, 2 or 3

3. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

(a) Prove that G is a group under multiplication (called the group of *roots of unity* in $\mathbb{C}$).

(b) Prove that G is not a group under addition.

4. Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.

(a) Prove that G is a group under addition.

(b) Prove that the nonzero elements of G are a group under multiplication. ("Rationalize the denominators" to find multiplicative inverses.)

5. (i) Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

(ii) Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times$:

$$\overline{1}, \overline{-1}, \overline{5}, \overline{7}, \overline{-7}, \overline{13}.$$

(iii) Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$:

$$\overline{1}, \overline{2}, \overline{6}, \overline{9}, \overline{10}, \overline{12}, \overline{-1}, \overline{-10}, \overline{-18}.$$

6. Let x be an element of G. Prove that

(i) $x^2 = 1$ if and only if $|x|$ is either 1 or 2.

(ii) if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.

(iii) x and x^{-1} have the same order.

7. Let x and y be elements of G. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.

8. Let $x \in G$ and let $a, b \in \mathbb{Z}^+$.

(a) Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.

(b) Prove that $(x^a)^{-1} = x^{-a}$.

(c) Establish part (a) for arbitrary integers a and b (positive, negative or zero).

9. If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

10. Prove that if $x^2 = 1$ for all $x \in G$, then G is abelian.

11. Assume H is a nonempty subset of $(G, \star)$ which is closed under the binary operation on G and is closed under inverses, i.e., for all h and k elements of H it holds $hk, h^{-1} \in H$. Prove that H is a group under the operation $\star$ restricted to H (such a subset H is called a subgroup of G).

12. Prove that if x is an element of the group G then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup (cf. the preceding exercise) of G (called the cyclic subgroup of G generated by x).

13. Compute the order of each of the elements in (a) D_6, (b) D_8, and (c) D_{10}.

14. Let σ be the permutation

$$1 \mapsto 3 \quad 2 \mapsto 4 \quad 3 \mapsto 5 \quad 4 \mapsto 2 \quad 5 \mapsto 1$$

and let τ be the permutation

$$1 \mapsto 5 \quad 2 \mapsto 3 \quad 3 \mapsto 2 \quad 4 \mapsto 4 \quad 5 \mapsto 1.$$

Find the cycle decompositions of each of the following permutations: $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma$, and $\tau^2\sigma$.

15. Find the order of (1 12 8 10 4)(2 13)(5 11 7)(6 9).

16. Prove that if σ is the m-cycle $(a_1 a_2 \ldots a_m)$, then for all $i \in \{1, 2, \ldots, m\}$, it holds $\sigma^i(a_k) = a_{k+i}$, where $k+i$ is replaced by its least residue mod m when $k+i > m$. Deduce that $|\sigma| = m$.

17. Let σ be the m-cycle $(1\ 2\ 3\ \cdots\ m)$. Show that σ^i is also an m-cycle if and only if i is relatively prime to m.

18. Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.

19. Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition. (Hint: use problem 16.)

20. Write out all the elements of $GL_2(F_2)$ and compute the order of each element.

21. Show that $GL_2(F_2)$ is non-abelian.

22. Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.

23. Let F be a field.

    (i) Show that $GL_n(F)$ is a finite group if and only if F has a finite number of elements.

    (ii) If $|F| = q$ is finite prove that $|GL_n(F)| < q^{n^2}$.

24. Show that $GL_n(F)$ is non-abelian for any $n \geq 2$ and any F.

25. Let G and H be groups. Let $\varphi : G \to H$ be a homomorphism.

    (a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.

    (b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

26. Let G and H be groups. If $\varphi : G \to H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assumed to be a homomorphism?

27. Let G and H be groups. If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \to H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H?

28. Prove that D_{24} and S_4 are not isomorphic.

29. Let A and B be groups. Prove that $A \times B \cong B \times A$.

30. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Prove that the image of φ is a subgroup of H. Prove that, if φ is injective, then $G \cong \varphi(G)$.

31. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Define the kernel of φ to be $\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\}$ (so the kernel is is the *fiber* over the identity of H). Prove that the kernel of φ is a subgroup of G. Prove that φ is injective if and only if the kernel of φ is the identity subgroup of G.

32. Define a map $\pi_1 : \mathbb{R}^2 \to \mathbb{R}$ by $\pi_1((x, y)) = x$. Prove that π_1 is a homomorphism and find the kernel of π_1.

33. Let G be any group. Prove that

(i) the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian, and

(ii) the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

34. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but is not an isomorphism.

35. Let G be a group and let $\mathrm{Aut}(G)$ be the set of all isomorphisms from G onto G. Prove that $\mathrm{Aut}(G)$ is a group under function composition (called the *automorphism group* of G and the elements of $\mathrm{Aut}(G)$ are called automorphisms of G).

36. In each of (a) – (e) below prove that the specified subset is *not* a subgroup of the given group:

(a) the set of 2-cycles in S_n for $n \geq 3$,

(b) the set of reflections in D_{2n} for $n \geq 3$,

(c) for n a composite integer > 1 and G a group containing an element of order n, the set $\{x \in G : |x| = n\} \cup \{1\}$,

(d) the set of (positive and negative) odd integers in $\mathbb{Z}$ together with 0, and

(e) the set of real numbers whose square is a rational number (under addition).

37. Show that the following subsets of the dihedral group D_8 are actually subgroups: (a) $\{1, r^2, s, sr^2\}$, (b) $\{1, r^2, sr, sr^3\}$.

38. Give an explicit example of a group G and an infinite subset H of G that is closed under the group operation but is not a subgroup of G.

39. Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

40. Let G be an abelian group. Prove that $\{g \in G : |g| < \infty\}$ is a subgroup of G (called the *torsion subgroup* of G). Give an explicit example where this set is not a subgroup when G is non-abelian.

41. Fix some $n \in \mathbb{Z}$ with $n > 1$. Find the torsion subgroup (cf. the previous exercise) of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. Show that the set of elements of infinite order together with the identity is *not* a subgroup of this direct product.

42. Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

43. Let $G = GL_n(F)$, where F is any field. Define

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\}$$

(called the *special linear group* over F). Prove that $SL_n(F) \leq GL_n(F)$.

44. (a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.

(b) Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable).

45. Let A and B be groups. Prove that the following sets are subgroups of the direct product $A \times B$:

(a) $\{(a, 1) \mid a \in A\}$,

(b) $\{(1, b) \mid b \in B\}$, and

(c) $\{(a, a) \mid a \in A\}$, where we asume $A = B$.

46. Let $H_1 \leq H_2 \leq \cdots$ be an ascending chain of subgroups of G. Prove that $\cup_{i=1}^{\infty} H_i$ is a subgroup of G.

47. Let $n \in \mathbb{Z}^+$and let F be a field. Prove that the set $\left\{ \left(a_{ij}\right) \in GL_n(F) \mid a_{ij} = 0 \text{ for all } i > j \right\}$ is a subgroup of $GL_n(F)$ (called the *group of upper triangular marices*).

48. Let G be a group.

(i) Prove that $C_G(A) = \left\{ g \in G \mid g^{-1}ag = a \text{ for all } a \in A \right\}$.

(ii) Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

(iii) Prove that $Z(G) \leq N_G(A)$ for any subset A of G.

49. In each of parts (a) to (c) show that for the specified group G and subgroup A of G, $C_G(A) = A$ and $N_G(A) = G$.

(a) $G = S_3$ and $A = \{1, (123), (132)\}$

(b) $G = D_8$ and $A = \left\{1, s, r^2, sr^2\right\}$

(c) $G = D_{10}$ and $A = \left\{1, r, r^2, r^3, r^4\right\}$

50. Let H be a subgroup of the group G.

(a) Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.

(b) Show that $H \leq C_G(H)$ if and only if H is abelian.