ABSTRACT ALGEBRA

1. Let $(G, \cdot)$ be a group and X any set. Let F be the set of functions with domain X and range G. Define a binary operation $*$ on F by $(f * g)(x) := f(x) \cdot g(x)$. Is

$(F, *)$ a group? If so, prove that it is. If not, give an axiom which is violated and prove that this is so.

Yes, $(F, *)$ is a group.

Proof:

identity The identity element is the function $I : X \to G$ which is identically equal to the identity element, e, of G. Indeed, for any $f \in F$ and any $x \in X$ we have $(I * f)(x) = I(x) \cdot f(x) = e \cdot f(x) = f(x)$. Hence, $I * f = f$.

inverse Let $f \in F$ be any element of F. Let $g : X \to G$ be defined by $g(x) := (f(x))^{-1}$. Then for any $x \in X$ we have $(g * f)(x) = g(x) \cdot f(x) = (f(x))^{-1} \cdot f(x) = e = I(x)$. Hence, $g * f = I$ so that g is a left-inverse of f.

associativity Let f, g, and h be elements of F. For any $x \in X$ we have $f * (g * h)(x) = f(x) \cdot (g * h)(x) = f(x) \cdot (g(x) \cdot h(x)) = (f(x) \cdot g(x)) \cdot h(x) = (f * g)(x) \cdot h(x) = (f * g) * h(x)$. Hence, $f * (g * h) = (f * g) * h$.

2. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 4 & 3 & 2 & 7 & 6 & 1 & 5 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 2 & 7 & 8 & 1 & 6 & 4 \end{pmatrix}$

a. Write τ as a product of cycles.

Solution: $\tau = (1, 3, 2, 5, 8, 4, 7, 6)$ is already a cycle.

b. Write σ as a product of transpostions.

Solution: $\sigma = (1, 7)(1, 5)(1, 8)(2, 4)$

c. Compute $\sigma\tau$ and $\tau\sigma$.

Solution: $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 4 & 1 & 5 & 8 & 6 & 2 \end{pmatrix}$ and $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 2 & 5 & 6 & 1 & 3 & 8 \end{pmatrix}$

d. What is the order of σ? of $\sigma\tau$?

Solution: The order of $\sigma = (1, 8, 5, 7)(2, 4)$ is four while the order of $\sigma\tau = (1, 3, 4)(2, 7, 6, 8)$ is twelve.

3. How many generators does the group $\mathbb{Z}_{225}$ have?

Solution: There are one hundred twenty generators of $\mathbb{Z}_{225}$: a positive integer $a < 225$ is a generator of $\mathbb{Z}_{225}$ just in case it is divisible by neither 3 nor 5.

4. Let $G := [0, 1)$ be the set of real numbers x with $0 \leq x < 1$. Define an operation $*$ on G by

$$x * y := \begin{cases} x + y \text{ if } x + y < 1 \text{ and} \\ x + y - 1 \text{ if } x + y \geq 1 \end{cases}$$

Is $(G, *)$ a group? If so, prove that it is. If not, demonstrate how some axiom is violated.

Yes, $(G, *)$ is a group.

Proof:

identity 0 is the identity as for any $y \in [0, 1)$, the sum $0+y = y < 1$ so that $0*y = y$.

inverse Let $x \in [0, 1)$. If $x = 0$, then 0 is a left inverse of x. Otherwise, set $y := 1 - x$ which lies in $(0, 1)$ as $0 < x < 1$. Then $y + x = 1 \geq 1$ so that $y * x = y + x - 1 = 0$ so that y is a left inverse of x.

associativity Let x, y, and z be elements of $[0, 1)$. In each way of computing $x * (y * z)$ (respectively, $(x*y)*z$) we obtain $x+(y+z)-n$ (respectively, $(x+y)+z-n$ where n is 0, 1 or 2 depending on which value yields an element of $[0, 1)$. As ordinary addition is associative, these values are equal.

5. Prove or disprove: Every associative binary operation on a set with two elements is commutative.

Solution: False. On any set X we may define a binary operation $*$ by $x * y := x$.

Then, $*$ is associative as for any x, y, and z from X we have $x*(y*z) = x = (x*y) = (x * y) * z$. However, if X has at least two elements, then $*$ is not commutative. Indeed, if $x \neq y$, then $x * y = x \neq y = y * x$.

6. Complete the following table to form a multiplication table for a group (if possible) and explain why the resulting multiplication gives a group, or demonstrate that no such completion is possible.

If the table extends to the multiplication table of a group, the e must be a two-sided identity. Moreover, successively ensuring that the equations $\alpha X = \beta$ and $X\alpha = \beta$ always have unique solutions, we see that up to a permutation of $\{a, b, c, d, f\}$, the only possible table is given below

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	**a**	e	**c**	**d**	**f**	**b**
b	**b**	**f**	e	**a**	**c**	**d**
c	**c**	**d**	**f**	e	**b**	**a**
d	**d**	**b**	**a**	**f**	e	**c**
f	**f**	**c**	**d**	**b**	**a**	e

However, this binary operation is *not* associative, as, for instance, $(a * c) * f = d * f = c \neq e = a * a = a * (c * f)$. Thus, the table does not extend to the multiplication table of a group.

7. Let $G := \mathbb{R}_+$ be the set of positive real numbers and let $\cdot$ be the usual multiplication operation. Is the function $x \mapsto x^2$ an isomorphism of G with itself? If so, prove so. If not, demonstrate that it is not.

Yes, this function is an isomorphism from G to G. It is one-to-one and onto as the function $x \mapsto \sqrt{x}$ is a two-sided inverse function. Moreover, $(x \cdot y)^2 = x^2 \cdot y^2$.

8. Prove or disprove: the set $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ is a subgroup of $(\mathbb{C}, +)$. Yes, this is a subgroup. The set $\mathbb{Q}(i)$ contains $0 = 0 + 0i$, is closed under addition as for a, b, c, and d ratinonal numbers, $(a + bi) + (c + di) = (a + c) + (b + d)i$ and each of $a + c$ and $b + d$ is a rational number, and is closed under taking inverses as for a and b rational numbers, $-(a + bi) = (-a) + (-b)i$ and each of $-a$ and $-b$ is rational.

9. Prove or disprove: If $(G, *)$ is a group and for every pair of elements $(a * b)^6 = a^6 * b^6$, then G is commutative.

Solution: This is false. Consider $G = S_3$. Then for any $\sigma \in G$ we have $\sigma^6 = \iota$. Hence, for any two a and b in G we have $(ab)^6 = \iota = \iota \cdot \iota = a^6 b^6$, but G is not commutative.

10. Prove or disprove: If G is a group and $H \leq G$ and $K \leq G$ are two subgroups, then $(H \cap K) \leq G$. **Proof:**

identity $e \in H$ and $e \in K$ as each is a subgroup of G. Hence, $e \in (H \cap K)$. inverse For any $x \in (H \cap K)$, we have $x^{-1} \in H$ as $x \in H \leq G$ and $x \in K \leq G$. Thus, $x^{-1} \in (H \cap K)$. closure under multiplication For x and y in $(H \cap K)$ we have $xy \in H$ as $H \leq G$ and likewise, $xy \in K$. Thus, $xy \in (H \cap K)$.

11. Prove or disprove: If G is a finite group and some element of G has order equal to the size of G, then G is cyclic.

Proof: Let $g \in G$ have order $n = \#(G)$. Then for each i with $1 \leq i < n$ we have $g^i \neq e$, the identity of G. I claim that $G = \langle g \rangle$. For this, it suffices to see that there are exactly n elements of $\{g^i : 0 \leq i < n\}$. If $g^i = g^j$ for some $j > i$, then multiplying both sides of the equation by $g^{-i} = (g^i)^{-1}$ we have $e = g^{j-i}$ even though $1 \leq j - i < n$ contrary to the above observation. Hence, $G = \langle g \rangle$ is cyclic.

12. Consider the function $\sigma : \{0, \ldots, 15\} \to \{0, \ldots, 15\}$ defined by

$$x \mapsto \begin{cases} x + 4 \text{ if } x < 12 \\ x - 12 \text{ if } x \geq 12 \end{cases}$$

Show that σ is a permutation and describe its orbits.

Solution: To see that σ is a permutation it suffices to check that it is onto. Let $\in \{0, \ldots, 15\}$. If $a < 4$, then $a = \sigma(12 + a)$. If $a \geq 4$, then $a = \sigma(a - 4)$.

The orbits are

$$\{0, 4, 8, 12\}, \{1, 5, 9, 13\}, \{2, 6, 10, 14\} \text{ and } \{3, 7, 11, 15\}.$$

18. Let G be the set of all permutations of $\mathbb{R}$ which move at most finitely many points. That is, $\sigma : \mathbb{R} \to \mathbb{R}$ belongs to G just in case $\sigma \in S_{\mathbb{R}}$ and $\{r \in \mathbb{R} : \sigma(r) \neq r\}$ is finite.