Ilana Sivan
205634272
Honors Course
Homework 7

Question 1

Show that ($\mathbb{Z}$,$-$) is not a group.

($\mathbb{Z}$,$-$) denotes an algebraic structure formed by the set of integers under subtraction. We will show that ($\mathbb{Z}$,$-$) is not a group by checking which axioms it fulfills. We know that the set of integers is closed under subtraction, as all $a, b \in \mathbb{Z} : a - b \in \mathbb{Z}$. We can prove this formally by the definition of subtraction as $a - b := a + (-b)$ where $-b$ is the inverse of integer addition. The group of integers under addition form an abelian group and the structure ($\mathbb{Z}$,+) is a group, so all $a, b \in \mathbb{Z} : a + (-b) \in \mathbb{Z}$ so integer subtraction is closed. So the group fulfills the closure axiom and we can continue to associativity. Subtraction on numbers is not associative as in general for $a - (b - c) \neq (a - b) - c$. We can show this formally as $a - (b - c) = a + (-(b + (-c))) = a + (-b) + c$ and $(a - b) - c = (a + (-b) + (-c) = a + (-b) + (-c)$, so we have $a - (b - c) = (a - b) - c$ **iff** $c = 0$, so in general we have $a - (b - c) \neq (a - b) - c$. Therefore, since subtraction on numbers is not associative we get that ($\mathbb{Z}$,$-$) does not satisfy the associative axiom and therefore it is not a group.

Question 2

Complete the following Cayley Diagram:

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

- Describe the group corresponding to this diagram.

  The group corresponding to the diagram is addition modulo 5.

- Is it finite? Abelian? Cyclic?

  The integers under addition are closed because the sum of two integers is always an integer. Therefore, the integers with the operation of addition, $(\mathbb{Z}, +)$, form a group. And, this group is **abelian** because $a + b = b + a$ for all $a, b \in \mathbb{Z}$. Any two numbers added together and reduced mod 5 will always equal 0, $1, 2, 3$ or 4 so the group is closed. The identity is 0 just like any group under addition, and every element has a unique inverse. A cyclic group is defined as a group which can be generated by a single element, so it is **cyclic**. And it is indeed **finite** as it contains a limited set.

- What is the order of the group?

  The number of elements of a group is called the order. For the group, G, we denote $|G|$ to denote the order of G. Since $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, we can see that $\mathbb{Z}_5$ has order 5.

Question 3

Show that there is a unique group of order 5.

It suffices to show that the group is cyclic up to isomorphism. First we show that any group of prime order is cyclic. Let p be a prime and G be a group such that $|G| = p$. Therefore, G contains more than one element. Now, let $g \in G$ such that $g \neq e_G$. Then $\langle g \rangle$ contains more than one element. We know that $\langle g \rangle \leq G$, and also by Lagrange's theorem, $|\langle g \rangle|$ divides p . Since $|\langle g \rangle| > 1$ and$|\langle g \rangle|$ divides the prime p, we have that $|\langle g \rangle| = p = |G|$. Hence, $\langle g \rangle = G$. So G is cyclic. We recall that $(\mathbb{Z}, +)$ is cyclic, since $\mathbb{Z} =< 1 >=< -1 >$ and its order is $|\mathbb{Z}| = \infty$. Let $(G, \circ)$ be a cyclic group of order n. $G = \{a^0, a^1, a^2, \ldots, a^n\}$, and $a^0 = e, a^1 = a$. Let

$\varphi = G \to \mathbb{Z}$ be the mapping defined as $\forall k \in \{0, 1, ..., n-1\} : \varphi(a^k) = k_n$, we can see that this is a bijection because $\mathbb{Z}_n = \{0_n, 1_n, ...(n-1)_n\}$. Since $\varphi$is a bijection then can see that it is also a group isomorphism. Now, let G a group of order 5. We will show that $G \cong \mathbb{Z}_5$. We will show that G is a cyclic group as any cyclic group of order 5 is isomorphic to $\mathbb{Z}_5$ (according to the proof above). Let $a \neq e \in G$ (as $|G| > 1$ this exists), therefore we have $O(a)|5$ and $O(a) \neq 1$. 5 is a prime so we can see that $O(a) = 5$, therefore $|a| = 5$ and as $a \subseteq G$ we have $a = G$. So any group of order 5 is cyclic and therefore isomorphic to $\mathbb{Z}_5$. As 5 is prime and our claim holds, we can see that up to isomorphism there is a unique group of order 5.

Question 4

For a finite group G, show that O(element)|O(group).
Let G be a finite group and let $a \in G$. We will prove that $O(a)|O(g)$, where $O(a)$ is the order of element a, and $O(G)$ is the order of the group G and | means divides. By definition, the order of a is the order of the subgroup generated by a. Therefore, by Lagrange's Theorem, $|a|$ is a divisor of $|G|$. In other words, if we let m be the order of the element $a$then the smallest positive integer m such that a^m is the identity element e, then m divides the order of G, so we have for any $a \in G$, we have that $a^{|G|} = e$.

Question 5

1. Let $\mathbb{R}$ be the set of real numbers. Show that the 4-dimensional Euclidean space $\mathbb{R} = \mathbb{R}\mathrm{x}\mathbb{R}\mathrm{x}\mathbb{R}\mathrm{x}\mathbb{R} = \{(\mathrm{r}_1, \mathrm{r}_2, \mathrm{r}_3, \mathrm{r}_4) : \mathrm{r}_\mathrm{i} \in \mathbb{R}\}$ is a group under component wise addition.

   $\mathbb{R}$ is closed under addition because $\forall a, b \in R : a + b \in R$. So for the Eucledian space $\mathbb{R}\mathrm{x}\mathbb{R}\mathrm{x}\mathbb{R}\mathrm{x}\mathbb{R}$ we have $(a_1, ..., a_4) + (b_1, ..., b_4) = (a_1 + b_1, ..., a_4 + b_4) \in \mathbb{R}$ because $a_i + b_i \in \mathbb{R}$. $(\mathbb{R}, +)$ is associative, because $\forall a, b, c \in \mathbb{R} : a + (b + c) = (a + b) + c$ so for $\mathbb{R}\mathrm{x}\mathbb{R}\mathrm{x}\mathbb{R}\mathrm{x}\mathbb{R}$ we have $(a_1, \ldots, a_4) + ((b_1, \ldots, b_4) + (c_1, \ldots, c_4)) = (a_1, \ldots, a_4) + (b_1 + c_1, \ldots, b_4 + c_4) = (a_1 + b_1 + c_1, \ldots, a_4 + b_4 + c_4) = (a_1 + b_1, \ldots, a_4 + b_4) + (c_1, \ldots, c_4) = ((a_1, \ldots, a_4) + (b_1, \ldots, b_4)) + (c_1, \ldots, c_4)$. The identity of $(\mathbb{R}, +)$ is 0, since $\exists 0 \in \mathbb{R} : \forall a \in \mathbb{R} : a + 0 = a = 0 + a$, so for $\mathbb{R}\mathrm{x}\mathbb{R}\mathrm{x}\mathbb{R}\mathrm{x}\mathbb{R}$ we have $(a_1, ..., a_4) + (0, 0, 0, 0) = (a_1, ..., a_4)$. Finally, each element a of the set of real numbers$\mathbb{R}$ has an inverse element $-a$ under the operation of real number addition: $\forall a \in \mathbb{R} : \exists -a \in \mathbb{R} : a + (-a) = 0 = (-a) + a$. So for $\mathbb{R}\mathrm{x}\mathbb{R}\mathrm{x}\mathbb{R}\mathrm{x}\mathbb{R}$, $(a_1, ..., a_4) + (-a_1, ..., -a_4) = (0, 0, 0, 0)$. And finally, it is commutative, as is $\mathbb{R}$ under addition, as $\forall a, b \in \mathbb{R} : a + b = b + a$.

2. Let $\mathbb{C}$ be the set of complex numbers. Show that the space $\mathbb{R}\mathrm{x}(\mathbb{C}\backslash\{0\}) \coloneqq \{(\mathrm{r}, \mathrm{c}) : \mathrm{r} \in \mathbb{R}, \mathrm{c} \in \mathbb{C}, \mathrm{c} \neq 0\}$ is a group under the following operation: $(r_1, c_1) * (r_2, c_2) \coloneqq (r_1 + r_2, c_1 * c_2)$ where $c_1 * c_2$ is complex multiplication.

   $\mathbb{R}$ under addition is a group and $\mathbb{C}\backslash\{0\}$ is also a group under complex multiplication so

   $\mathbb{R}\mathrm{x}(\mathbb{C}\backslash\{0\}) \coloneqq \{(\mathrm{r}, \mathrm{c}) : \mathrm{r} \in \mathbb{R}, \mathrm{c} \in \mathbb{C}, \mathrm{c} \neq 0)$ is a valid group with this operator :)

Question 6

Let $\varphi : G \to H$ be a group homomorphism. Show that $Ker\varphi$ is a subgroup of G and that image$\varphi$is a subgroup of H.

We define: let G and H be groups and let $\varphi : G \to H$ be a mapping from G to H. φ is called a homomorphism if for all $x, y \in G$ we have $\varphi(xy) = \varphi(x)\varphi(y)$. We will first prove that a group is preserved under homomorphism. If $\varphi : G \to H$ is a homomorphism, then $\varphi(e_G) = e_H$ where e is an identity or unit, and for all $x \in G, \varphi(x-1) = \varphi(x) - 1$. As φ is a homomorphism, we have that for all $x, y \in G$ we have $\varphi(xy) = \varphi(x)\varphi(y)$. And $\varphi(y) = \varphi(e_G y) = \varphi(e_G)\varphi(y)$, which implies that $\varphi(e_G) = e_H$. Furthermore, $\varphi(e_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) = e_H$, which implies $\varphi(x^{-1}) = \varphi(x)^{-1}$. Therefore, if $\varphi : G \to H$ is a homomorphism, the image of φ is a subgroup of H. Now,we let a and b be in the image of φ. We will show that ab^{-1} is also in the image of φ. If a and b are in the image of φ, then there are $x, y \in G$ such that $\varphi(x) = a$ and $\varphi(y) = b$. As we showed before, this means that $ab^{-1} = \varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1})$, and it is a subgroup of H. As we know that G, H are groups and $\varphi : G \to H$ is a group homomorphism, we know that $ker\varphi \subset G$ so it is associative. As we have shown that $\varphi(e_G) = e_H$, we have $e_G \in ker\varphi$. Since $e_G * a = a * e_G = a$ for all $a \in G$ this property holds for all $a \in ker\varphi \subset G$. Finally, let $a \in ker\varphi$, then we have $\varphi(a) = e_H$. Since $a^{-1} * a = e_G$, we know that $e_H = \varphi(a^{-1}a) = \varphi(a)\varphi(a^{-1}) = e_H\varphi(a^{-1}) = \varphi(a^{-1})$ and therefore $a^{-1} \in ker\varphi$. Therefore we can conclude that $ker\varphi$ is a subgroup of G.

Question 7

Check if the following are group homomorphisms. If they are, describe the $ker\varphi$ and $im\varphi$.

- $\varphi : \mathbb{R}^x \to \mathbb{R}^x = (\{\mathbb{R}\backslash\{0\}\}, *)$, $x \to |x|$

  $x \to |x|$ is a homomorphism since $|a|\,|b| = |ab|$. Its image is $\{x : x > 0\}$ and its kernel is $\{1, -1\}$. Let $a, b \in \mathbb{R}^x$, $\varphi(a) = |a| \in \mathbb{R}^x$ is well defined, so $\varphi(ab) = |ab| = |a||b| = \varphi(a)\varphi(b)$, and therefore $\varphi(a^{-1}) = |a^{-1}| = |a|^{-1} = (\varphi(a))^{-1}$.

- $\varphi : \mathbb{R} \to \mathbb{R} = (\mathbb{R}, +)$, $x \to x^2$

  $x \to x^2$ is a homomorphism since $a^2b^2 = (ab)^2$. Its image is $\{x : x > 0\}$ and its kernel is $\{1, -1\}$.

- $\varphi : \frac{\mathbb{Z}}{6} \to \frac{\mathbb{Z}}{2}$, $x\text{mod}6 \to x\text{mod}2$
  - If $x \mod 6$ is even (odd) then x is even (odd), therefore $\varphi(\{1, 3, 5\}) = 1$ and $\varphi(\{0, 2, 4\}) = 0$.
  - If x and y are odd then xy is odd and therefore $x \mod 6 \in \{1, 3, 5\} \Rightarrow x \mod 2 = 1$, and $y \mod 6 \in \{1, 3, 5\} \Rightarrow y \mod 2 = 1$ and

  $$(xy) \mod 2 = 0 \Rightarrow \begin{cases} \varphi(x \mod 6)\,\phi(y \mod 6) = 0 \\ \varphi((xy) \mod 6) = 0 \end{cases} \Rightarrow \varphi((xy) \mod 6) = \varphi(x \mod 6)\,\varphi(y \mod 6).$$

  - If x and y are even then xy is even and therefore $x \mod 6 \in \{0, 2, 4\} \Rightarrow x \mod 2 = 0$, and $y \mod 6 \in \{0, 2, 4\} \Rightarrow y \mod 2 = 0$, and

  $$(xy) \mod 2 = 0 \Rightarrow \begin{cases} \varphi(x \mod 6)\,\varphi(y \mod 6) = 0 \\ \varphi((xy) \mod 6) = 0 \end{cases} \Rightarrow \varphi((xy) \mod 6) = \varphi(x \mod 6)\,\varphi(y \mod 6)$$

  - If x is odd and y is even then xy is even and therefore $x \mod 6 \in \{1, 3, 5\} \Rightarrow x \mod 2 = 1$, and $y \mod 6 \in \{0, 2, 4\} \Rightarrow y \mod 2 = 0$ and

  $$(xy) \mod 2 = 0 \Rightarrow \begin{cases} \varphi(x \mod 6)\,\varphi(y \mod 6) = 0 \\ \varphi((xy) \mod 6) = 0 \end{cases} \Rightarrow \varphi((xy) \mod 6) = \varphi(x \mod 6)\,\varphi(y \mod 6).$$

  So φ is a homomorphism. Its image is $\{0, 1\}$ and its kernel is $\{0, 2, 4\}$.

Question 8

Show that the following is a group homomorphism that outputs the 2nd least significant bit of its input:

$\varphi : \frac{\mathbb{Z}}{8} \to \frac{\mathbb{Z}}{2}$
$x \to (\frac{x - \varphi_0(x)}{2})$
Where φ_0 is the map $\varphi_0(x) = x\text{mod}2$

A homomorphism from a group G to a group G is a mapping $G \to G$ that preserves the group operation: $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. This is not a group homomorphism and fails already from

Let $a, b \in \frac{\mathbb{Z}}{8}$. $\varphi(a) = (\frac{a - \varphi_0(a)}{2})\text{mod}2 \in \frac{\mathbb{Z}}{2}$ is well defined, so $\varphi(ab) = (\frac{a+b-\varphi_0(a+b)}{2})\text{mod}2 = (\frac{a+b-\varphi_0(a)-\varphi_0(b)}{2})\text{mod}2 = (\frac{a-\varphi_0(a)+b-\varphi_0(b)}{2})mod2 = (\frac{a-\varphi_0(a)}{2}) + (\frac{b-\varphi_0(b)}{2})\text{mod}2 = \varphi(\text{a}) + \varphi(\text{b})$

$\varphi(a^{-1}) = (\frac{a^{-1}\text{mod}8 - \varphi_0(a^{-1}\text{mod}8}{2})\text{mod}2 = (\frac{\text{a}^{-1} - \varphi_0(\text{a}^{-1})}{2})^{-1}\text{mod}2 = (\varphi(a))^{-1}$

This is not a group homomorphism and fails as $\varphi(a + b) \neq \varphi(a) + \varphi(b)$ in this question.

Question 9

The following question gives an example of the Cayley's theorem . Recall that Cayley 's theorem says that every finite group is isomorphic to a subgroup of the permutation group S_n for some integer $n > 1$.

Permutation of a set A is a function from A to A that is both 1 -1 and onto.

Let $A(n) \coloneqq \{1, 2, ..., n\}$. Then ({permuations}, $\circ$) where $\circ$is function composition, forms a group. This group is called the symmetric group on n elements denoted by S_n.

- What is the order of S_3?

  $O(S_3) = |S_3| = 3!$

- What is the order of σ_3?

  $\sigma_3\sigma_3 = (123) \rightarrow O(\sigma_3) = 2$

  $\sigma_5\sigma_5\sigma_5 = (123) \rightarrow O(\sigma_3) = 3$

- Check that it is an isomorphism

  We can draw the Cayley diagrams:

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_6	σ_5	σ_4	σ_3
σ_3	σ_3	σ_5	σ_1	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_5	σ_1	σ_3	σ_2
σ_5	σ_5	σ_3	σ_4	σ_2	σ_6	σ_1
σ_6	σ_6	σ_4	σ_2	σ_3	σ_1	σ_5

	R_0	$Flip_2$	$Flip_3$	$Flip_1$	R_{60}	R_{120}
R_0	R_0	$Flip_2$	$Flip_3$	$Flip_1$	R_{60}	R_{120}
$Flip_2$	$Flip_2$	R_0	R_{120}	R_{60}	$Flip_1$	$Flip_3$
$Flip_3$	$Flip_3$	R_{60}	R_0	R_{120}	$Flip_2$	$Flip_1$
$Flip_1$	$Flip_1$	R_{120}	R_{60}	R_0	$Flip_3$	$Flip_2$
R_{60}	R_{60}	$Flip_3$	$Flip_1$	$Flip_2$	R_{120}	R_0
R_{120}	R_{120}	$Flip_1$	$Flip_2$	$Flip_3$	R_0	R_{60}

As we can see, the diagrams of the two groups are the same, so they are isomorphic.