Math113Hw1

Trustin Nguyen

April 28, 2023

Homework 1

Exercise 1: For any $k \in \mathbb{Z}$, let $f_k : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ be defined by $n \mapsto kn$. Show that f_k is a group homomorphism. Are there any other homomorphisms $(\mathbb{Z}, +) \to (\mathbb{Z}, +)$? Carefully justify your answer.

Proof. We first observe what happens with two elements z_1, z_2 in the domain Z:

$$\begin{aligned} f_k(z_1 z_2) = f_k(z_1 + z_2) &= kz_1 + kz_2 \\ &= f_k(z_1) + f_k(z_2) = f(z_1) f_k(z_2) \end{aligned}$$

so f_k is indeed a homomorphism. □

Proof. If we were to find a group homomorphism $g : (\mathbb{Z}, +) \mapsto (\mathbb{Z}, +)$, then there would be the property:

$$g(z_1 + z_2) = g(z_1) + g(z_2)$$

We can look at what happens with the identity element when $z_2 = 0$:

$$g(z_1) = g(z_1) + g(0)$$

therefore, $g(0) = 0$. Suppose $g(1) = k$. observe that now,

$$g(z_1 + 1) = g(z_1) + k$$

By induction, the function of g is restricted to the positive integers must be $g(x) = kx$. But for the negative numbers:

$$\begin{aligned} g(-1 + 1) &= g(-1) + g(1) \\ g(0) &= g(-1) + k \\ -k &= g(-1) \end{aligned}$$

Therefore,

$$g(z_1 - 1) = g(z_1) - k$$

By backwards induction, the same formula $g(x) = kx$ applies to the negative domain. So there are no other homomorphisms. □

Better proof:

Proof. Notice that the image necessarily a subgroup of $\mathbb{Z}$, the homomorphism is subsequently determined by what the generator of $\mathbb{Z}$, 1, is mapped to, and this is the smallest positive nonzero element in the image. Therefore, there are no other homomorphisms other than the ones represented by $n \mapsto kn$. □

Exercise 2: Let H_1 and H_2 be two subgorups of G.

1. Show that $H_1 \cap H_2$ is a subgroup of G.

Proof. Since H_1, H_2 are subgroups of G, they contain the same identity element as G. Suppose that $a \in H_1 \cap H_2$. Then $a^{-1} \in H_2$, $a^{-1} \in H_2$. Therefore, every element has an inverse in $H_1 \cap h_2$. Suppose that $a \in H_1 \cap H_2$. Then $a_1, a_2 \in H_1$ and $a_1, a_2 \in H_2$. By closure under the operations, $a_1 a_2 \in H_1 \cap h_2$ and the new set is closed under the operation defined in the previous two. □

2. Show that $H_1 \cup H_2$ is a subgroup of G iff one of the H_i contains the other.

Proof. ($\leftarrow$) Suppose that $H_1 \subseteq H_2$ wlog. then that implies that $H_1 \cup H_2 = H_2$. Therefore, the resulting set is a subgroup since H_2 is a group.
($\rightarrow$) Proof by contrapositive. Suppose that neither H_1 and H_2 are subsets of the other. Then there is an element $h_1 \in H_1$ that is not in H_2 and an element $h_2 \in H_2$ that is not in H_1. We must check if $h_1 h_2$ is in $H_1 \cup H_2$. Suppose for contradiction that it is in $H_1 \cup H_2$. Then wlog assume that it is in H_1:

$$\begin{aligned} h_1 h_2 &\in H_1 \\ h_1^{-1} h_1 h_2 &\in H_1 \\ h_2 &\in H_1 \end{aligned}$$

which gives us a contradiction. □

Exercise 3: Let G be a finite group.

1. Let $g \in G$. Show that there is a positive integer n such that $g^n = e$. The least such integer is called the order of g.

Proof. Let $G' = \{g^0, g^1, \dots, g^k\}$. Suppose that $g \neq e$, for if it is, then $n = 1$. And suppose that $g^a \neq g^b$ whenever $a \neq b$. But we must have k be finite since G' is in G and otherwise, the order of G would be infinite. Therefore, we have $g^{k+1} = g^a$ for some $a \neq k+1$. We take inverses and we should get an exponent that gives us the identity. □

2. Show that there exists a positive integer n such that $g^n = e$ for all $g \in G$. The least such integer is called the exponent of G.

Proof. Since G has finitely many elements, we take the order of each element and subsequently the lcm of these elements. Since the order divides the exponent, then the exponent makes all elements the identity. □

Exericise 4:

1. Let G be a finite group of even order, i.e. $|G|$ is finite and even. Show that G contains an element of order 2.

Proof. Consider the set $G \backslash \{0\}$. This set has odd order but since every element has an inverse, there must be at least one element that maps back to itself in the mapping $g \mapsto g^{-1}$. Therfore, there is an element of order 2. □

2. Let G be a group and suppose now that every element of G, other than the identity, has order 2. Show that G is abelian.

Proof. We follow from the definition:

$$g_1^2 = e$$
$$g_2^2 = e$$

We multiply these elements together:

$$g_1^2 g_2^2 = e$$

Now take inverses:

$$g_1 g_2 = g_1^{-1} g_2^{-1} = (g_2 g_1)^{-1}$$

But notice that when an element has order 2, then $g^{-1} = g$. Therefore, we have that

$$g_1 g_2 = g_2 g_1$$

as desired. □

Little note: When elements have order 2, it is usually crucial to use the observation that $g^{-1} = g$ or that an element is its inverse.

Exercise 5: Let X be a set. Recall that $\mathcal{P}(X)$ is the power set of X, i.e. the set of all subsets of X:

$$\mathcal{P}(X) = \{A : A \subseteq X\}$$

1. Does $\mathcal{P}(X)$ form a group under intersection?

Proof. Notice that the identity element is unique for every element in $\mathcal{P}(X)$:

$$\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$
$$\{1\} \cap \{1\}^{-1} = \{1\}^{-1} \cap \{1\} = \{1, 2\}$$

Since for two sets $A, B, A \cap B \subseteq A$ and $A \cap B \subseteq B$. So

$$\{1\} \cap \{1\}^{-1} \subseteq \{1\} \subseteq \{1, 2\}$$

which shows that $\mathcal{P}(X)$ does not form a gorup under intersection. □

2. Does $\mathcal{P}(X)$ form a group under union?

Proof. The same problem as the first group but with a different identity element:

$$A \cup \emptyset = \emptyset \cup A = A$$

But observe that there is no inverse of A that yields $\emptyset$, for example, $X = \{1, 2\}$:

$$A \cup A^{-1} = \emptyset$$
$$\{1\} \cup \{1\}^{-1} = \emptyset$$

But the union must be nonempty since $1 \in \{1\} \cup \{1\}^{-1}$. Therefore, the union cannot be the identity element. □

3. The symmetric difference of $A, B \in \mathcal{P}(X)$ is defined by $A \Delta B = (A \cup B)\ (A \cap B)$. Show that $(\mathcal{P}(X), \Delta)$ is a group.

Proof. (Closure) First to show under the closure of the operation where $A, B \in \mathcal{P}(X)$, there is the statement:

$$
\begin{aligned}
A\Delta B &= (A \cup B)\backslash(A \cap B) \\
A \subseteq X &\text{ and } B \subseteq X \to X
\end{aligned}
$$

Suppose that $s \in A\Delta B$. Then

$$
\begin{aligned}
(s \in A \cup B) \wedge (s \notin A \cap B) \\
(s \in A \vee s \in B) \wedge \neg(s \in A \cap B)
\end{aligned}
$$

(a) Case 1: $s \in A \wedge s \notin B$. Then since $A \subseteq S, s \in X$
(b) Case 2: $s \in B \wedge s \notin A$. Then since $B \subseteq S, s \in X$

Therefore, we conclude that $A\Delta B \subseteq X$.
(Existence of Inverses) To show the existence of an inverse, we have to find a A^{-1} such that

$$A\Delta A^{-1} = \emptyset$$

Observe that

$$
\begin{aligned}
A\Delta A &= (A \cup A)\backslash(A \cap A) \\
&= A\backslash A \\
&= \emptyset
\end{aligned}
$$

(Associative Property) We have the verify:

$$(A\Delta B)\Delta C = A\Delta(B\Delta C)$$

We can do this through a membership table. □

<-i(1) <-i(2) matrix 1<-i(1) <-i(2)