MATH 100A: Homework #2

Due on October 12, 2023 at 12:00pm

Professor McKernan

Section A02 5:00PM - 5:50PM
Section Leader: Castellano

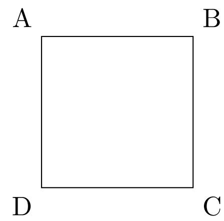
Source Consulted: Textbook, Lecture, Discussion, Office Hour, ChatGPT

Ray Tsai
A16848188

Problem 1

Give a description of D_4, the group of symmetries of the square, similar to the one given in class, and find all of its subgroups.

Proof. Let there be a square S with vertices A, B, C, D labeled clockwise, as shown below.



D_4 contains all the symmetries of S, including rotations, flips, and the identity I. There are three types of rotations, R, R^2, R^3, which rotates S counter-clockwise by $90°, 180°, 270°$, respectively. Note that the $360°$ rotation $R^4 = I$. Additionally, there are four types of flips, F_1, F_2, F_3, F_4. F_1 flips S vertically through its center. F_2 flips S horizontally through its center. F_3 flips S diagonally through vertices A, C. F_4 flips S diagonally through vertices B, D. Note that each flip is its own inverse.

We now show that there can be at most 8 configurations of the positions of vertices. Since A, C must be at the opposite position, A's position determines C's. We pick A's position first, then pick B and D's, so there are at most $\binom{4}{1}\binom{2}{1} = 8$ symmetries. Since the identity, rotations, and flips we mentioned are all distinct, they account for all 8 symmetries. Thus, we conclude that $D_4 = \{I, R, R^2, R^3, F_1, F_2, F_3, F_4\}$.

We now find all the subgroups of D_4. We first note $\{I\}$ and D_4 itself are subgroups of D_4. There are also the cyclic subgroups $\langle R\rangle = \langle R^3\rangle, \langle R^2\rangle, \langle F_1\rangle, \langle F_2\rangle, \langle F_3\rangle, \langle F_4\rangle$. Note that $\langle R\rangle = \langle R^3\rangle = \{I, R, R^2, R^3\}$ is the subgroup that contains all rotations. Suppose that we include some flip, say F_1 to $\langle R\rangle$. Then, we would also have $F_2 = R^2F_1, F_3 = RF_1, F_4 = R^3F_1$ in the group, which becomes D_4.

We also observe that $F_1F_3 = F_2F_4 = R$, and $F_2F_3 = F_1F_4 = R^3$. This implies that if we include any of those pairs of flips in the same group, the group untimately becomes D_4, by the result we obtained above.

Note that $F_1F_2 = F_2F_1 = F_3F_4 = F_4F_3 = R^2$, so we attempt to construct subgroups with $\langle R^2\rangle$. Suppose we include F_1 to $\langle R^2\rangle$, then we get $F_2 = F_1R^2$. Since each of $\{I, R^2, F_1, F_2\}$ is its own inverse and any two elements' product is still in the group, it is a subgroup. Suppose we include F_3 to $\langle R^2\rangle$, then we get $F_4 = F_3R^2$. Since each of $\{I, R^2, F_3, F_4\}$ is its own inverse and any two elements' product is still in the group, it is a subgroup.

Since no more combination of elements in D_4 can be use to generate a new group, we have exausted all subgroups of D_4, namely

$$\langle I\rangle, \langle R\rangle, \langle R^2\rangle, \langle F_1\rangle, \langle F_2\rangle, \langle F_3\rangle, \langle F_4\rangle, \{I, R^2, F_1, F_2\}, \{I, R^2, F_3, F_4\}, D_4.$$

$\square$

Problem 2

Suppose that G is a set closed under an associative operation such that

1. given $a, y \in G$, there is an $x \in G$ such that $ax = y$, and
2. given $a, w \in G$, there is a $u \in G$ such that $ua = w$.

Show that G is a group.

Proof. Let $b, c \in G$. We know that there exists $a, d \in G$ such that $ab = b$ and $bd = c$. Then, we get $abd = bd = ac = c$, and so a is a left identity element. Similarly, we can also find a right identity element f using the above approach. This follows that sicne $af = a = f$, the left and right inverse are the same element, and so G contains an identity element $e = a = f$.

Let $\alpha \in G$. We know that there exists $\beta, \gamma \in G$ such that $\alpha\beta = e$ and $\beta\gamma = e$. This follows that since $\alpha\beta\gamma = \alpha = \gamma$, $\alpha\beta = e$ and $\beta\alpha = e$, and thus all elements in G has an inverse. Therefore, G is a group. $\square$

Problem 3

If G is a finite set closed under an associative operation such that $ax = ay$ forces $x = y$ and $ua = wa$ forces $u = w$, for every $a, x, y, u, w \in G$, prove that G is a group.

Proof. Let $a \in G$. Define $f : G \to G$ to be $f(g) = ag$. Since $ax = ay$ implies $x = y$, we know f is injective. This follows that f is also surjective since G is a finite set, and so for each $c \in G$, there exists $b \in G$ such that $ab = c$. Similarly, we can define $h : G \to G$ to be $h(g) = ga$ and show that there exists $x \in G$ such that $xa = c$, and thus the rest of the proof follows the previous problem. $\square$

Problem 4

Verify that $Z(G)$, the center of G, is a subgroup of G.

Proof. We first verify that $Z(G)$ is closed under the operation of G. Let $a, b \in Z(G)$, and let $x \in G$. Since $abg = agb = gab$, $ab \in Z(G)$, and thus $Z(G)$ fulfills the closed property.

We now check the inverse property. Let $e \in G$ be the identity element, and let $c \in Z(G)$. Then, for all $x \in G$,

$$\begin{aligned} cx &= xc \\ x &= c^{-1}xc \\ xc^{-1} &= c^{-1}x, \end{aligned}$$

and thus $c^{-1} \in Z(G)$. Therefore, $Z(G)$ is a subgroup of G. □

Problem 5

If $C(a)$ is the centralizer of a in G, prove that $Z(G) = \bigcap_{a \in G} C(a)$.

Proof. Let $z \in Z(G)$, and let $a \in G$. Since $za = az$, $z \in C(a)$, and so $z \in \bigcap_{a \in G} C(a)$. Therefore, $Z(G) \subseteq \bigcap_{a \in G} C(a)$.

Let $c \in \bigcap_{a \in G} C(a)$. Since for all $a \in G$, $c \in C(a)$, and so $ca = ac$. Therefore, $c \in Z(G)$, which means that $\bigcap_{a \in G} C(a) \subseteq Z(G)$. Combining two results, we conclude that $Z(G) = \bigcap_{a \in G} C(a)$. $\square$

Problem 6

If G is an abelian group and if $H = \{a \in G \,|\, a^2 = e\}$, show that H is a subgroup of G.

Proof. Let $a, b \in H$. Since $(ab)^2 = abab = a^2b^2 = e$, we get $ab \in H$, and thus H is closed under the operation of G. Since $a^2a^{-2} = e = (a^{-1})^2$, $a^{-1} \in H$ for all $a \in H$. Therefore, H is a subgroup of G. $\square$

Problem 7

Prove that a cyclic group is abelian.

Proof. Let $G = \langle a \rangle$ be a cyclic group. Let $b = a^k, c = a^j \in G$. Since $bc = a^{k+j} = cb$, G is abelian. $\square$

Problem 8

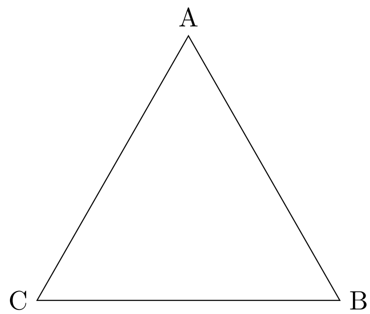
If A, B are subgroups of an abelian group G, let $AB = \{ab \,|\, a \in A, b \in B\}$. Prove that AB is a subgroup of G.

Proof. Let $c = a_1b_1, d = a_2b_2 \in AB$, for $a_1, a_2, b_1, b_2 \in G$. Since $a_1a_2 \in A$ and $b_1b_2 \in B$, we get $cd = a_1b_1a_2b_2 = (a_1a_2)(b_1b_2) \in AB$, and so AB is closed under the operation of G. Note that since A, B are subgroups of G, we know $a^{-1} \in A$ and $b^{-1} \in B$. Since $c^{-1} = (a_1b_1)^{-1} = b_1^{-1}a_1^{-1} = a^{-1}b^{-1}$, we get $c^{-1} \in AB$. Therefore, AB is a subgroup of G. $\square$

Problem 9

Give an example of a group G and two subgroups A, B of G such that AB is not a subgroup of G.

Proof. Consider D_3, the group of symmetries of a triangle. Let F_1, F_2, F_3 be the flips through vertex A, B, C respectively.



We take subgroups $A = \langle F_1 \rangle$ and $B = \langle R \rangle$. Consider F_3 and R. Since $F_3 = F_1 R$ and $R = IR$, we know $F_3, R \in AB$. However, $F_2 = F_3 R \neq ab$ for all $a \in A, b \in B$. This implies that AB does not have the closed property, and thus it is not a subgroup of G. $\square$