# Title - Thomas Boyko - 30191728

1. Let X be any set and let P (X ) denotes its power set, i.e. $P(X) = \{A : A \subset X\}$, all subsets of $X$ . Define the operation on $P(X) : A\Delta B = (A \cup B) \setminus (A \cap B)$.

   (a) Show that $(P(X), \Delta)$ forms a group. Is it Abelian ?

      (i) We begin with closure. Take two sets $A, B$ in $P(X)$. Suppose we have an element $x \in A\Delta B$. We must show that $x$ is also in $X$, hence that $A\Delta B \in P(X)$.
      Since $x \in A\Delta B$, $x$ must be in $A \cup B$ but not $A \cap B$. In other words, $x$ is in $A$ or $B$ but not both. Since $A$ and $B$ are both subsets of $X$, $x \in X$. So our group is closed.

      (ii) Next is identity. We must show that there exists some $E \subseteq X$ so that for any $A \in P(X)$, $E\Delta A = A = A\Delta E$.
      We can choose the null set $\varnothing$. Of course $\varnothing \subseteq X$ since the null set is a subset of any set. Now we examine $\varnothing\Delta A = (A\cup\varnothing)\setminus(A\cap\varnothing)$ for any $A \in P(X)$. Notice that $\varnothing \cup A = A$ and $\varnothing \cap A = \varnothing$, as well as $\varnothing \cup A = A \cup \varnothing$ and $\varnothing \cap A = A \cap \varnothing$. So we now have $\varnothing\Delta A = A \setminus \varnothing$, in both the cases ($A\Delta\varnothing$ and $\varnothing\Delta A$).
      So for an element to be in $A\Delta\varnothing$ or $\varnothing\Delta A$, it must be in $A$ but not in $\varnothing$. This is true for every element of $A$ so $\varnothing$ is our identity

      (iii) Next we find inverses for any $A \subseteq X$. The inverse in this context $A$. So we must show that $A\Delta A = \varnothing$.
      $A\Delta A = (A \cap A) \setminus (A \cup A)$. Notice that $A \cap A = A$ and $A \cup A = A$. So this becomes $A\Delta A = A \setminus A$. And since $A \setminus A$ represents all the elements of $A$ that are not in $A$, this is simply the empty set.

      (iv) Now we check associativity. We must show that for all $A, B \subseteq X$, $A\Delta(B\Delta C) = (A\Delta B)\Delta C$.
      For the following, let $A, B, C \in P(X)$.
      Consider $(A \cup B) \cup C$. This is the set of all elements that are in $A$ or $B$, or those that are in $C$. Clearly this is the same as the set $A \cup (B \cup C)$.
      Now consider $(A \cap B) \cap C$. This is the set of all elements in $A$ and $B$, as well as those in $C$. Again this is the same as $A \cap (B \cap C)$.
      This part is incomplete, I was not able to keep track of the expressions this created for more than a couple of lines.

      (v) Finally we check if the group is abelian.

      $$A\Delta B = (A \cup B) \setminus (A \cap B) = (B \cup A) \setminus (B \cap A) = B\Delta A$$

      Which comes from the fact that set union and intersection are both commutative.

   (b) Take $X = \{1, 2\}$ and write the Cayley table for this group. Compare it to the tables we did in lectures, try to determine "upto isomorphism" which group it is.

| $\Delta$ | $\varnothing$ | $\{1\}$ | $\{2\}$ | $\{1,2\}$ |
|---|---|---|---|---|
| $\varnothing$ | $\varnothing$ | $\{1\}$ | $\{2\}$ | $\{1,2\}$ |
| $\{1\}$ | $\{1\}$ | $\varnothing$ | $\{1,2\}$ | $\{2\}$ |
| $\{2\}$ | $\{2\}$ | $\{1,2\}$ | $\varnothing$ | $\{1\}$ |
| $\{1,2\}$ | $\{1,2\}$ | $\{2\}$ | $\{1\}$ | $\varnothing$ |

   This set maintains the same structure as the group we saw in class with $|G| = 4$ and with every element as its own inverse. We called it the Kliens four group $K_4$.

2. Consider the set

$$GL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} a, b, c, d \in \mathbb{Z}_2, ad - bc \neq 0 \right\}$$

   (a) Show that $GL_2(\mathbb{Z}_2)$ forms a group under matrix multiplication.

      (i) First we show closure. Let $A, B \in GL_2(\mathbb{Z}_2)$. Then by the laws of matrix multiplication, $AB$ is a $2 \times 2$ matrix, by properties of the determinant, $\det(AB) = \det(A)\det(B)$. Since $\det(A), \det(B)$ are both nonzero, $\det(AB) \neq 0$, and since $\mathbb{Z}_2$ is closed under multiplication and addition. So $AB$ is a $2 \times 2$ matrix with entries in $\mathbb{Z}_2$ and nonzero determinant, $AB \in GL_2(\mathbb{Z}_2)$. So $GL_2(\mathbb{Z}_2)$ is closed.

(ii) Next we show identity. We choose $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. For any $A \in GL_2(\mathbb{Z}_2)$, $AI = IA = A$.

(iii) Now we show inverses. For some $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, let $A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Then multiplying:

$$AA^{-1} = \begin{bmatrix} ad - bc & -ba + ba \\ cd - cd & ad - bc \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$$

(iv) Finally we show associativity.
Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, $C = \begin{bmatrix} i & j \\ k & l \end{bmatrix}$.
Then:

$$\begin{aligned} (AB)C &= \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) C \\ &= \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix} C \\ &= \begin{bmatrix} i(ae + bg) + k(af + hb) & j(ae + bg) + l(af + hb) \\ i(ce + dg) + l(fe + dh) & j(ce + dg) + l(fe + dh) \end{bmatrix} \\ &= \begin{bmatrix} aei + bgi + afk + bhk & aej + bgj + afl + hbl \\ cei + dgi + efl + dhl & cdj + dgj + fel + dhl \end{bmatrix} \\ A(BC) &= A \begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} i & j \\ k & l \end{bmatrix} \\ &= A \begin{bmatrix} ie + kf & je + lf \\ ig = kh & jg + lh \end{bmatrix} \\ &= \begin{bmatrix} a(ie + kf) + b(ig + kh) & a(je + lf) + b(jg + lh) \\ c(ie + kf) + d(ig + kh) & c(je + lf) + d(jg + lh) \end{bmatrix} \\ &= \begin{bmatrix} aei + afk + bgi + bhk & aej + afl + bgj + bhl \\ cei + cfk + dgi + dhk & cej + cfl + dgj + dhl \end{bmatrix} \end{aligned}$$

And from this disgusting expansion of matricies we see $A(BC) = (AB)C$ and $GL_2(\mathbb{Z}_2)$ is associative.

(b) Compute the order of this group with justification.
Looking for matricies where $ad \neq cb$, and since each entry must be 0 or 1, we are interested in all matricies where one diagonal has a product of 1 and the other has a product of 0.
So we create some arbitrary $A \in GL_2(\mathbb{Z}_2)$. First we must choose which diagonal will have a product of 0 and which will be 1. We have 2 ways to do this. Both of the entries on this diagonal must be 1. Then we choose the elements on the other diagonal. These can both be 0 or 1, so long as they are not both 1. So there are 3 ways to choose this diagonal.
Therefore, there are 6 ways to make a matrix in $GL_2(\mathbb{Z}_2)$, and the order of $GL_2(\mathbb{Z}_2)$ is 6.

(c) Show that the group is not Abelian.
Choose $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. Notice that $AB = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = BA$ so $B$ is not abelian.

3. Let $G$ be a group with identity $e$.

(a) Show that if $(ab)^2 = a^2b^2$ for all $a, b \in G$, then $G$ must be Abelian.
Suppse $(ab)^2 = a^2b^2$ for any $a, b \in G$. This means:

$$\begin{aligned} (ab)^2 &= a^2b^2 && \\ (ab)(ab) &= a^2b^2 && \\ a(ba)b &= a(ab)b && \text{By Associativity} \\ (a^{-1}a)(ba)(bb^{-1}) &= (a^{-1}a)(ab)(bb^{-1}) && \text{By inverses and Asoociativity} \\ e(ba)e &= e(ab)e && \\ be &= ab && \text{By Identity} \end{aligned}$$

And since $ab = ba$ for any $a, b$ in $G$, $G$ is abelian.

(b) Show that if $g^2 = e$ for all $g \in G$, then $G$ must be Abelian.

Suppose $a, b \in G$ so that $a^2 = e = b^2$.

$$\begin{aligned}
ab &= ab \\
(ab)(ab) &= (ab)^2 \\
a(ba)b &= e && \text{By Associativity} \\
(aa)(ba)(bb) &= ab && \text{Multiplying left by } a\text{, right by } b. \\
e(ba)e &= ab \\
ba &= ab
\end{aligned}$$

And since $ab = ba$ for any $a, b$ in $G$, $G$ is abelian.

(c) Show that if $|G|$ is even, then there exists an element $h \in G$ such that $h^2 = e$.

Suppose that $|G| = n$ is even. Argue by pairing. Trivially, $e$ satisfies this property. But we have $n - 1$ other elements in $G$, and each element has an inverse in $G$.

So for every element in $G$, we can pair it with its inverse. However there are two elements we cannot pair. One is trivial, the identity, which is its own inverse. Then we have another element in $G$ that has an inverse in $G$, which cannot be paired with any other element than itself (since inverses are unique). So there exists some $h \in G$ so that $h^2 = e$.

4. Let $S_n$ be the symmetric group of degree $n$.

(a) Take $n = 4$. In $S_4$, list the elements as cycles and determine the order of each element.

The list of elements in $S_4$ with order 1 is simply the element $e$, or the map $\sigma$ given by $\sigma(x) = x$ for any $x \in X_4$

The list of elements in $S_4$ with order 2: $(1\,2), (1\,3), (1\,4), (2\,3), (2\,4), (3\,4), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)$

The list of elements in $S_4$ with order 3: $(1\,2\,3), (3\,2\,1), (2\,3\,4), (4\,3\,2), (1\,3\,4), (4\,3\,1), (1\,2\,4), (4\,2\,1)$

The list of elements in $S_4$ with order 4: $(1\,2\,3\,4), (1\,2\,4\,3), (1\,3\,2\,4), (1\,3\,4\,2), (1\,4\,2\,3), (1\,4\,3\,2)$

(b) What is the highest possible order of an element in $S_6$? Give an example. What about $S_7$? Give an example.

The highest possible order of an element in $S_6$ is 6. An example of this is the cycle $(1\,2\,3\,4\,5\,6)$. We can make a cycle of order 6 with any cycle of length 6 or two disjoint cycles of length 3 and 2.

The highest possible order of an element in $S_7$ is 12. An example of this would be the cycle $(1\,2\,3\,4)(5\,6\,7)$. Any permutation created by two disjoint cycles of length 3 and 4 will satisfy this.