HW 5
Due: Tuesday, March 4

Do exercises 2/33, 34, 36, 38, 40, and the following:

A. Show that if G is an abelian group, $g, h \in G$, g has order m and h has order n, then gh has order $\operatorname{lcm}(m, n)$.

B. Let $n \geq 2$ be an integer. Let $U(n) = \{[a] \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$. List all elements of $U(5)$, $U(12)$, and $U(15)$.

C. Prove that $U(n)$ is a group.

D. Construct the multiplication table for $U(8)$.

Chapter 2 Solutions

Proposition 1 (Exercise 2.33)**.** *The number of elements of order 2 in S_n is given by the sum:*

$$\sum_{i=1}^{m} \frac{(2i)!}{i!2^i}\binom{n}{2i}$$

where m is the largest integer such that $1 \leq 2m \leq n$.

Proof. We observe that determining the number of elements of order 2 for any permutation group S_n, also determines how many elements of order 2 there are in S_5 and S_6. So, we begin with the general case.

It follows from previous results that if a permutation has order two the cycles in its complete factorization have at most order two. Thus, each factor is of order two or order 1. Thus, to find the number of all permutations of order two, it suffices to count the number of possible products of disjoint 2 cycles, where order doesn't matter.

First, we want the number of ways to choose k disjoint transpositions from S_n. We observe that in k transpositions there are $2k$ many symbols. We need to choose this collection of $2k$ to be distinct (so they don't repeat) and if they occur in different orders we will still consider it the same collection. Thus, there are $\binom{n}{2k}$ many ways to choose $2k$ symbols from a bank of n symbols in this way. Moreover, we must now choose the number distinct strings we can make with these symbols that correspond to k disjoint cycles. Thus, we must choose a string of symbols without repetition, which yields $2k!$. However, we care about arrangements, just in a very specific way. We do not want transposition and there inverse to be counted as distinct in different strings. Because disjoint cycles commute we have to divide by $k!$. Then secondly, we remove the strings with inverses by dividing by two for each possible transposition. Thus, we have $\frac{(2k)!}{k!2^k}$ many ways to choose a string of $2k$ symbols that corresponds to a product of k disjoint cycles. Then altogether this gives us the following formula:

$$\begin{aligned}\frac{(2k)!}{k!2^k}\binom{n}{2k} &= \frac{(2k)!}{k!2^k}\frac{n!}{(2k)!(n-2k)!} \\ &= \frac{1}{k!}\frac{1}{2^k}\Big[n\cdots(n-2k+1)\Big]\end{aligned}$$

Given that we are looking for the number of elements of order 2 in S_n, it follows that this number is given by the sum

$$\sum_{i=1}^{m} \frac{(2i)!}{i!2^i}\binom{n}{2i} \tag{1}$$

where m is the largest integer such that $2m \leq n$. We see that for each i, $\frac{(2i)!}{i!2^i}\binom{n}{2i}$ gives the number of permutations of order 2 that can be completely factored into i transpositions, so the sum the finds the total number of permutations with complete

factorizations made of transpositions that are possible in S_n. Thus, the sum (1) is the number we were searching for. For S_5 this sum is

$$\frac{(2)!}{1!2^1}\binom{5}{2} + \frac{(4)!}{2!2^2}\binom{5}{4} = 10 + 15 = 25.$$

For S_6 this sum is

$$\frac{(2)!}{1!2^1}\binom{6}{2} + \frac{(4)!}{2!2^2}\binom{6}{4} + \frac{(6)!}{3!2^3}\binom{6}{6} = 15 + 3 \cdot 15 + 15 \cdot 1 = 75.$$

■

Proposition 2 (Exercise 2.34)**.** *Let y be a group element of order m; if $m = pt$ for some prime p, prove that y^t has order p.*

Proof. Since y has order m, it follows that $y^{tp} = y^m = e$, where e is the identity element of the group. By Proposition 2.51, $(y^t)^p = e$.

Now we must show that p is the smallest positive integer n such that $(y^t)^n = e$. Suppose there exists some positive integer n such that $(y^t)^n = e$. It follows that $y^{nt} = e$. Thus, by Lemma 2.53, $pt|nt$, so $p|n$. Thus, $p \leq n$. Since n was chosen to be arbitrary, this shows that p divides all periods of y^t. Thus, p is the order of y^t, by Lemma 2.53. ■

Proposition 3 (Exercise 2.36)**.** *Let $G = GL(2, \mathbb{Q})$, and let*

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$$

Then $A^4 = I = B^6$ where I is the identity matrix, but $(AB)^n \neq I$ for all $n > 0$.

Proof. We find the order of A and B through direct calculation below.

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$A^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
$$A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

$$B^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$
$$B^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$B^4 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$
$$B^5 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$
$$B^6 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

Observe that

$$AB = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Then we proceed with a proof by induction on n. We claim that

$$(AB)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}.$$

Observe that

$$(AB)^2 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}.$$

Then we assume that

$$(AB)^{k-1} = \begin{pmatrix} 1 & -(k-1) \\ 0 & 1 \end{pmatrix}$$

for some $k \in \mathbb{N}$ with $k > 3$. Using the exponent laws, we see that

$$(AB)^k = (AB)(AB)^{k-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -(k-1) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}.$$

Thus, $(AB)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ for all $n > 0$. It follows there does not exist any $n \in \mathbb{N}$ such that $(AB)^n = 1$. Hence, AB has no finite order. ■

Proposition 4 (Exercise 2.38)**.** *Let G be a group. Suppose that $x^2 = e$ for all $x \in G$ where e is the group identity. Then G is abelian.*

Proof. Let $x, y \in G$. We note that $yx \in G$, because G is a group. By the hypothesis, we see that, $x^2 = y^2 = (yx)^2 = e$. Thus,

$$xy = y^2xyx^2 = y(yx)^2x = yx$$

by the associativity of the group operation. Since x and y were chosen to be arbitrary, it follows that G is abelian. ■

Lemma 5 (Page 133.)**.** *An element $g \in G$ has order 2 if and only if $g \neq e$ and $g = g^{-1}$.*

Proof. Suppose that $g \in G$ has order 2. Then $g^2 = e$. Multiplying both sides by g^{-1} we see that, $g = g^{-1}$. Moreover, if $g = e$ then g has order 1 which contradicts the hypothesis. Now suppose that g is not the identity and $g = g^{-1}$. Multiplying both sides by g yields, $g^2 = e$. So, the claim is proven. ■

Proposition 6 (Exercise 2.40)**.** *If G is a group with an even number of elements then the number of elements in G of order 2 is odd. In particular, G must contain an element of order 2.*

Proof. If G has an even number of elements then $G - \{e\}$ has an odd number of elements. Let $g \in G - \{e\}$. Then g has a unique inverse by Proposition 2.45. We observe that if $g^{-1} \notin G - \{e\}$ then $g^{-1} = e$, but then $g = e$ by Proposition 2.45. This contradicts our choice of g. Thus, $g^{-1} \in G - \{e\}$. Since G is arbitrary, it follows that every element in $G - \{e\}$ has an inverse in $G - \{e\}$.

Say that N is the set of all elements in $G - \{e\}$ that do not have order 2. Thus, N has an even number of elements, since each element comes in a pair with it's unique inverse. This implies that $(G - \{e\}) - N$ has an odd number of elements. Moreover, we observe that $(G - \{e\}) - N$ is the set of all elements that are not e and are not an element that does not have order 2. This implies that $(G - \{e\}) - N$ is the set of elements of order 2 in G. The claim has been proven. ■

Non-Text Solutions

Proposition 7 (Exercise A)**.** *Let G be an abelian group. Suppose that $g, h \in G$ such that g has order m and h has order n. Then gh has order $lcm(m, n)$.*

Proof. Let $L = lcm(m, n)$. By Lemma 2.53, $g^L = e$ and $h^L = e$. By the commutativity of G,

$$(gh)^L = g^L h^L = e.$$

Choose some other number $N \leq L$ such that $(gh)^N = e$. Then $g^N h^N = e$. Thus, $g^N = (h^N)^{-1}$. This implies that $g = h^{-1}$. Since h^{-1} has the same order as h, it follows that $m|N$ and $n|N$. Then N is a common multiple of m and n by Lemma 2.53. Thus, $L \leq N$. It follows that $N = L$. ■

Proposition 8 (Exercise B)**.** *Let $n \geq 2$ be an integer. Let $U(n) = \{[a] : \mathbb{Z}/n\mathbb{Z} : gcd(a, n) = 1\}$. Then list all of the elements of $U(5)$, $U(12)$, and $U(15)$.*

Proof.

$$U(5) = \{[1], [2], [3], [4]\}$$

$$U(12) = \{[1], [5], [7], [11]\}$$

$$U(15) = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$$

■

Proposition 9 (Exercise C)**.** *Prove that $U(n)$ is a group under multiplication. Where we define*

$$[a][b] = [ab].$$

Proof. Since modding out forms an equivalence relation on the integers, we know that the group operation is well defined. Associativity is inherited from multiplication on the integers as well.

Observe that $gcd(1, n) = 1$ for any positive integer. Thus, $[1] \in U(n)$. Moreover, $[1][a] = [a]$ for all $[a] \in U(n)$ because $1 \cdot a = a$ for all $a \in \mathbb{Z}$. Thus, $U(n)$ has an identity. So, the only thing left to show is that every element has an inverse.

Suppose that $[a] \in U(n)$. We observe that $a \neq 0$, else $gcd(0, n) = n$. By Theorem 1.32, there exists integers x and y such that $ax + ny = 1$. Taking the whole equation modulo n, gives us that $ax \equiv 1 \bmod n$. Thus, $x = a^{-1}$. It's possible that x is negative but since every negative integer belongs to an equivalence class with a positive representative we can assume that $x > 0$.

Say that $gcd(x, n) = d$. Thus, $d|ax + ny$. Hence, $d|1$. But then $d = 1$. Thus, $a^{-1} \in U(n)$. It follows that $U(n)$ is a group. ■

Proposition 10 (Exercise D)**.** *Construct the multiplication table for $U(8)$.*

Proof. We observe that $U(8) = \{[1], [3], [5], [7]\}$.

"."	[1]	[3]	[5]	[7]
[1]	[1]	[3]	[5]	[7]
[3]	[3]	[1]	[7]	[5]
[5]	[5]	[7]	[1]	[3]
[7]	[7]	[5]	[3]	[1]

■