

## MATH 113 HW 6: Orbits and cycles

Due in class on Thursday, October 12.

1. Prove that  $(a_1, a_2, \dots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \cdots (a_1, a_3)(a_1, a_2)$ .

SOLUTION:

Prove this by induction on  $n$ , where  $n \geq 2$ .

Base Case: Let  $n = 2$ . Then  $(a_1, \dots, a_n) = (a_1, a_2)$ .

Inductive Step: Assume that  $(a_1, a_2, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_3)(a_1, a_2)$ .

We want to show that  $(a_1, a_2, \dots, a_k, a_{k+1}) = (a_1, a_{k+1})(a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_3)(a_1, a_2)$ .

We see that  $(a_1, a_2, \dots, a_k, a_{k+1}) = (a_1, a_{k+1})(a_1, a_2, \dots, a_k)$ , by looking at the two-line notation for these permutation products. So

$$\begin{aligned}(a_1, a_2, \dots, a_k, a_{k+1}) &= (a_1, a_{k+1})(a_1, a_2, \dots, a_k) \\ &= (a_1, a_{k+1})(a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_3)(a_1, a_2)\end{aligned}$$

2. Section 8, exercise 40.

SOLUTION:

Let  $R$  denote the set  $\{\sigma \in S_A \mid \sigma(b) = b\}$ . Then  $R$  is a subgroup of  $S_A$ .

To see this check the three subgroup properties.

closure: Assume  $\sigma, \tau \in R$ . Then  $\sigma(\tau(b)) = \sigma(b) = b$ . So  $\sigma\tau \in R$ .

Identity: Since  $id(b) = b$  for all  $b \in A$ ,  $id \in R$ .

Inverse: Assume  $\sigma \in R$ . Then

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & b & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & b & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

Therefore

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & \dots & b & \dots & n-1 & n \\ \sigma^{-1}(1) & \sigma^{-1}(2) & \dots & b & \dots & \sigma^{-1}(n-1) & \sigma^{-1}(n) \end{pmatrix}$$

So  $\sigma^{-1} \in R$ .

3. Section 8, exercise 53.

SOLUTION:

(a) We saw in class that every permutation group is isomorphic to a subgroup of  $S_n$  for some  $n$ . We also saw that an injective map  $\psi : G \rightarrow H$  defines an isomorphism  $G \cong \psi(G)$ . Begin with an arbitrary finite group  $G$  and let  $\sigma$  be an element of the permutation subgroup isomorphic to  $G$ . Consider an orbit  $(a_1, a_2, \dots, a_k)$  of  $\sigma$ . This orbit corresponds to the matrix obtained from the identity matrix by shifting the  $a_1^{th}$  row and column to the  $a_2^{th}$  position and so on. Doing this for each orbit produces a permutation matrix corresponding to  $\sigma$ . Let this matrix be  $\psi(\sigma)$ .

$\psi$  is a homomorphism: Let  $\sigma$  and  $\tau$  be permutations in the permutation group isomorphic to  $G$ . Then  $\psi(\sigma\tau)$  is the permutation matrix you get by permuting the rows and columns of the identity matrix according to the orbits of  $\sigma\tau$ . But this is the same as first permuting the rows and columns according to the orbits of  $\tau$  and then according to the orbits of  $\sigma$ . Therefore  $\psi(\sigma\tau) = \psi(\sigma)\psi(\tau)$ .

$\psi$  is injective: Assume  $\psi(\sigma) = \psi(\tau)$ . Then the orbits of  $\sigma$  are the same as those of  $\tau$ . Therefore  $\sigma = \tau$ .

(b)

$$e = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$a = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$c = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

4. Section 9, exercise 2.

SOLUTION:

$$\sigma = (1, 5, 8, 7)(2, 6, 3)(4).$$

5. Section 9, exercise 10.

SOLUTION:

$$\sigma = (1, 8)(2)(3, 6, 4)(5, 7) = (1, 8)(3, 4)(3, 6)(5, 7)$$

6. Section 9, exercise 27.

(a) Write  $\sigma \in S_n$  as the product of  $k$  disjoint cycles, of lengths  $l_1, l_2, \dots, l_k$ . By exercise 1, the  $i^{\text{th}}$  cycle can be written as a product of  $l_i - 1$  transpositions. Then  $\sigma$  can be written as a product of

$$\sum_{i=1}^k (l_i - 1) = \left( \sum_{i=1}^k l_i \right) - k$$

transpositions. But

$$\left( \sum_{i=1}^k l_i \right) \leq n, \quad \text{so} \quad \left( \sum_{i=1}^k l_i \right) - k \leq n - k.$$

If  $k = 0$ , then  $\sigma$  is the identity and can be written as a product of 0 transpositions, which is certainly less than  $n - 1$ . Otherwise  $n - k \leq n - 1$ , and so  $\sigma$  can be written as a product of at most  $n - 1$  transpositions.

(b) If  $\sigma$  is not a cycle, then the number  $k$  in part (a) must be greater than or equal to 2. Hence  $\sigma$  can be written as a product of at most  $n - 2$  transpositions.

(c) If  $\sigma \in S_n$  is odd, it can be written as a product of  $j$  transpositions, where  $j = 2k + 1$  for some positive integer  $k$ , and  $j \leq n - 1$ . Then  $2n + 3 > j$ , and the difference between  $2n + 3$  and  $2k + 1$  is an even number since the difference between two odds is even. Therefore multiply by  $(1, 2)(1, 2)$  until there are  $2n + 3$  transpositions.

Similarly, if  $\sigma \in S_n$  is even, it can be written as a product of  $j$  transpositions, where  $j = 2k$  for some positive integer  $k$ , and  $j \leq n - 1$ . Then  $2n + 3 > j$ , and the difference between  $2n + 8$  and  $2k$  is an even number since the difference between two evens is even. Therefore multiply by  $(1, 2)(1, 2)$  until there are  $2n + 8$  transpositions.

7. Prove that the order of an element in  $S_n$  is equal to the least common multiple of the lengths of the cycles in its cycle notation.

SOLUTION:

Let  $\sigma \in S_n$  be the product of  $k$  disjoint cycles,  $c_1 c_2 \dots c_k$  of lengths  $l_1, l_2, \dots, l_k$  as in exercise 6. Then the order of  $\sigma$  is the smallest positive integer  $r$  such that  $\sigma^r = id$ . We saw in class that multiplication of disjoint cycles is commutative, so  $\sigma^m = (c_1 c_2 \dots c_k)^m = c_1^m c_2^m \dots c_k^m$  for all positive integers  $m$ . Therefore the smallest positive integer  $r$  such that  $\sigma^r = id$  is the smallest positive integer  $r$  such that  $c_i^r = id$  for all  $c_i$ . But  $c_i^r = id$  precisely when  $l_i$  divides  $r$ . So the smallest positive integer  $r$  such that  $\sigma^r = id$  is the smallest positive integer  $r$  such that  $l_i$  divides  $r$  for all  $i$  from 1 to  $k$ . This is precisely the least common multiple of lengths  $l_i$  as defined in class.

8. (a) Section 9, exercise 34.

SOLUTION:

Let  $\sigma = (a_1, a_2, \dots, a_{2k+1})$  be a cycle of odd length. Then  $\sigma^2 = (a_1, a_3, a_5, \dots, a_{2k-1}, a_{2k+1}, a_2, a_4, \dots, a_{2k})$ , which is a cycle.

- (b) Give an example of a cycle  $\sigma$  such that  $\sigma^2$  is not a cycle.

SOLUTION:

Let  $\sigma = (1, 2, 3, 4) \in S_4$ . Then  $\sigma^2 = (1, 3)(2, 4)$ , which is not a cycle.

9. The Fibonacci numbers  $f_i$  are defined by:

$$f_1 = 1, f_2 = 1, \text{ and } f_{n+2} = f_n + f_{n+1}, \text{ for } n \in \mathbb{Z}^+.$$

Prove that by induction that  $k|n$  implies  $f_k|f_n$ .

SOLUTION:

We'll rephrase the question as: "prove that  $f_k$  divides  $f_{kj}$  for all  $j \in \mathbb{Z}_+$  and prove by induction on  $j$ ."

Base case:

Let  $j = 1$ . Then  $f_k$  divides  $f_{k1} = f_k$ .

Inductive step:

Assume that  $f_k$  divides  $f_{kj}$ . Then  $f_{k(j+1)} = f_{kj+k} = f_{kj+(k-1)} + f_{kj+(k-2)}$  by the definition of the Fibonacci numbers.

$$\begin{aligned} f_{kj+k} &= f_{kj+(k-1)} + f_{kj+(k-2)} \\ &= 2f_{kj+(k-2)} + f_{kj+(k-3)} \\ &= 3f_{kj+(k-3)} + 2f_{kj+(k-4)} \\ &= 5f_{kj+(k-4)} + 3f_{kj+(k-5)} \\ &= 8f_{kj+(k-5)} + 5f_{kj+(k-6)} \\ &= \vdots \\ &= f_{r+1}f_{kj+(k-r)} + f_r f_{kj+(k-(r+1))} \end{aligned}$$

Let  $r = k$ . Then  $f_{k(j+1)} = f_{k+1}f_{kj+(k-k)} + f_k f_{kj+(k-(k+1))} = f_{k+1}f_{kj} + f_k f_{kj-1}$ . Since  $f_k$  divides  $f_{kj}$ , we see that  $f_k$  divides the first term. Since  $f_k$  appears in the second term,  $f_k$  divides the second term. Therefore,  $f_k$  divides their sum, and so  $f_k$  divides  $f_{k(j+1)}$ .

10. (from class) Prove that the least common multiple of two integers  $r$  and  $s$  is  $\frac{rs}{\gcd(r,s)}$ .

SOLUTION:

Write  $\frac{rs}{\gcd(r,s)} = r\left(\frac{s}{\gcd(r,s)}\right) = s\left(\frac{r}{\gcd(r,s)}\right)$ , since  $\gcd(r,s)$  divides both  $r$  and  $s$ . So  $\frac{rs}{\gcd(r,s)}$  is a common multiple of  $r$  and  $s$ , but possibly not the least.

Also, one has the following:

$$r = \left(\frac{rs}{lcm(r,s)}\right)\left(\frac{lcm(r,s)}{s}\right),$$

$$s = \left(\frac{rs}{lcm(r,s)}\right)\left(\frac{lcm(r,s)}{r}\right).$$

Therefore  $\frac{rs}{lcm(r,s)}$  divides both  $r$  and  $s$ . By the definition of the greatest common divisor,  $\frac{rs}{lcm(r,s)}$  divides  $gcd(r,s)$ . So there exists some integer  $a \in \mathbb{Z}$  such that  $a\left(\frac{rs}{lcm(r,s)}\right) = gcd(r,s)$ .

Then  $\frac{rs}{gcd(r,s)} = \frac{lcm(r,s)}{a}$ . But  $\frac{lcm(r,s)}{a}$  is a common multiple of  $r$  and  $s$ , since  $\frac{rs}{gcd(r,s)}$  is a common multiple of  $r$  and  $s$ . So  $a = 1$  and hence  $\frac{rs}{gcd(r,s)} = lcm(r,s)$ , as desired.

### Group Problem (Due in class on Thursday, October 10)

Prove that  $\{(1, 2), (1, 2, \dots, n)\}$  is a generating set for  $S_n$ .

SOLUTION:

Step 1: Any transposition  $(i, j)$  can be written as a product of adjacent transpositions  $(a, a + 1)$ .

**Proof:**

$$(i, j) = (i, i+1)(i+1, i+2), \dots, (j-1, j)(j-2, j-1)(j-3, j-2) \dots (i+1, i+2)(i, i+1),$$

since  $(i, i + 1)(i + 1, i + 2), \dots, (j - 1, j) = (i, j, j - 1, j - 2, \dots, i + 1)$ , the cycle which shifts the numbers between  $i + 1$  and  $j$  back by one while sending  $i$  to  $j$ . The second part leaves the element  $j$  fixed in the  $i^{th}$  position while shifting the numbers between  $i$  and  $j - 1$  forward by one. Hence  $i$  and  $j$  are permuted but all others are fixed.

Step 2: The transposition  $(a, a + 1)$  is given by products of  $\sigma = (1, 2)$  and  $\tau = (1, 2, \dots, n)$ .

**Proof:** We claim that  $(a, a + 1) = \tau^{1-a}\sigma\tau^{a-1}$ . To see this, notice that applying  $\tau^{1-a}$  subtracts  $a$  modulo  $n$  from each number. Applying  $\sigma$  after

this switches 1 and 2, which are in the  $a^{th}$  and  $(a+1)^{th}$  position respectively. Applying  $\tau^{a-1}$  to the result sends everything back to where it began except the entries in the  $a^{th}$  and  $(a+1)^{th}$  positions are shifted. This is precisely the transposition  $(a, a+1)$ .

Since any permutation can be written as the product of transpositions and any transposition can be written (by step 2) as the product of adjacent transpositions, any permutation may be written as the product of adjacent transpositions. Step 2 implies that any product of adjacent transpositions can be produced by  $\sigma$  and  $\tau$ , so any permutation can be produced by  $\sigma$  and  $\tau$ . Therefore  $\{\sigma, \tau\}$  is a generating set for  $S_n$ .