

# Math 504 HW4

Rohan Mukherjee

December 4, 2023

1. We claim that  $S_n = \langle (12), (12 \cdots n) \rangle$ . Notice first that  $(12 \cdots n)^i$  sends  $a$  to  $a + i$ . Thus,  $(12 \cdots n)^{-i}$  sends  $a$  to  $a - i$ . We see then that  $(12 \cdots n)^{-i}(12)(12 \cdots n)^i = (i + 1 \ i + 2)$ , since it sends  $i + 1$  first to 1, then to 2 by the transposition, then to  $i + 2$  by the last. Next,  $i + 2$  gets sent to 2 which gets sent to 1 which gets sent to  $i + 1$ . Everything mapping to neither 1 or 2 is fixed, since we can ignore the middle transposition, which completes this step. Now we claim every permutation can be generated by those of the form  $(i + 1 \ i + 2)$ . We shall prove this algorithmically. Suppose that  $\sigma(j) = 1$ . If  $j = 1$  we move on. We claim that multiplying a permutation  $\sigma$  by  $(ij)$  will result in the same  $\sigma$  with the  $i$ th and  $j$ th column swapped, that is, it is the same permutation but with  $\sigma(i) = \sigma(j)$  and  $\sigma(j) = \sigma(i)$ . Indeed,  $\nu = (ij) \cdot \sigma$  is so that  $\nu(i) = \sigma(j)$  and  $\nu(j) = \sigma(i)$ , and everything else fixed since  $(ij)$  will fix everything else. Now, with 1 at the  $i$ th column for  $i \neq 1$ , we can multiply by  $(i - 1 \ i)$  on the right to move the 1 left one column. Continue this until we have 1 in the first column. Do the same thing until 2 is in the second column, and eventually we will have every element fixed. Thus the permutation can be written as the product of transpositions of the form  $(i \ i + 1)$  (since  $(i \ i + 1)^{-1} = (i \ i + 1)$ ), which we can generate with  $(12)$  and  $(12 \cdots n)$ , so we are done.
2. We shall give an algorithm for finding the disjoint cycles. Let  $\sigma$  be the permutation. Starting with 1,  $1 \mapsto \sigma(1)$ , so first we should have  $(1\sigma(1))$ . Then  $\sigma(1) \mapsto \sigma(\sigma(1))$ , so we should get  $(1\sigma(1)\sigma(\sigma(1)))$ . Continue this process until  $(\sigma \circ \cdots \circ \sigma)(1) = 1$ . If not all of  $\{1, \dots, n\}$  show up in this cycle, open a new cycle and start with the lowest element not occurring in the first one. Continue this process, and in the end one will have a product of disjoint cycles. For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (14)(23)$$

3. We shall first prove that conjugating a cycle preserves the length. Let  $\tau = (a_1 \cdots a_k)$  be a cycle of length  $k$ . Consider  $\eta = \sigma^{-1}\tau\sigma$ . Notice that  $\eta(\sigma(a_i)) = (\sigma \circ \tau \circ \sigma^{-1})\sigma(a_i) = \sigma(a_{i+1})$ , and that if  $k$  is not of the form  $\sigma(a_j)$  for any  $j$ , then  $\eta(k)$  will just be  $k$  since  $\sigma^{-1}(k)$  will be fixed by the middle permutation and hence will be canceled out by  $\sigma$ . So, we have proven that  $\sigma^{-1}\tau\sigma = (\sigma(a_1) \sigma(a_2) \cdots \sigma(a_k))$ . We now prove the claim by induction on the number of cycles. By the above, if  $\sigma, \tau$  are both cycles of the same length, write  $\sigma = (a_1 \cdots a_k)$  and  $\tau = (b_1 \cdots b_k)$ , we just need to find a permutation which satisfies  $\sigma(a_i) = b_i$  for each  $a_i$ . This exists (one could fix every other element to “extend” the permutation), so we have shown they are conjugate. Similarly, the above shows that if they are conjugate they are of the same length, so we are done with the base case. Let  $\sigma = \prod a_i, \tau = \prod b_i$  be a product of disjoint cycles where  $a_i$  and  $b_i$  have the same length (since they are cycles, we can actually say  $|a_i| = |b_i|$ ). Then  $\omega^{-1}\sigma\omega = \prod \omega^{-1}a_i\omega$ , by cancellation. Now we just have to find an  $\omega$  such that  $\omega^{-1}a_i\omega = b_i$  for each  $a_i$ , which we can do by the above (instead of fixing everything else at the start, keep doing the above process and only fix at the end), which shows they are conjugate. If two permutations are conjugate, that is if  $\tau = \omega^{-1} \prod a_i \omega = \prod \omega^{-1}a_i\omega$ , then  $\tau$ 's composition into disjoint cycles have the same lengths as  $\sigma$  since  $\omega^{-1}a_i\omega$  has the same length as  $a_i$  for each  $a_i$ .
4. This follows immediately from  $\sigma = (a_1 a_2 \cdots a_k) = (a_{k-1} a_k)(a_{k-2} a_{k-1}) \cdots (a_1 a_2)$ . Note  $a_{2j-1}$  only shows up in the  $j$ th from the right transposition, gets sent to  $a_{2j}$  which is fixed in the remaining permutations to the right. Then  $a_{2j}$  is sent to  $a_{2j+1}$  in the  $j+1$ th transposition which is fixed by all the right transpositions. Since  $j$  was arbitrary, this holds for every  $j \in \{1, \dots, \lfloor k/2 \rfloor\}$ , which shows the above identity. Finally,  $a_k$  gets sent to  $a_1$  since  $a_k \mapsto a_{k-1} \mapsto a_{k-2} \mapsto \cdots \mapsto a_1$ . Since any permutation is a product of disjoint cycles, and since we can generate every cycle, we are done.
5. I shall instead define  $g(x_1, \dots, x_n) = \prod_{i < j} (x_j - x_i)$ . Notice that  $g(x_1, \dots, x_n) = (-1)^{\binom{n}{2}} f(x_1, \dots, x_n)$ , and in particular,  $\sigma g = -g$  iff  $\sigma f = -f$  and  $\sigma g = g$  iff  $\sigma f = f$  (we can ignore the constant  $(-1)^{\binom{n}{2}}$ .)  $g(x_1, \dots, x_n)$  is now the determinant of the Vandermonde matrix,

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{pmatrix}$$

This is well-known, thus its proof is omitted. Notice that  $(i \ j)g(x_1, \dots, x_n) = -g(x_1, \dots, x_n)$ , since  $(i \ j)g(x_1, \dots, x_n)$  is just  $g(x_1, \dots, x_n)$  with  $x_i$  swapped with  $x_j$ . Since  $g$  is the determinant of the Vandermonde matrix, and swapping entries will swap columns of the above matrix,

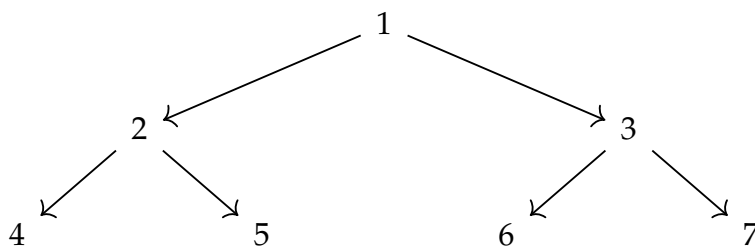
and since swapping columns multiplies the determinant by  $-1$ , we have proven the above claim. Thus for any permutation  $p$ , if we decompose  $p$  into  $a$  transpositions as in question

4, repeatedly using the above claim would give us that  $\text{Sgn}(p) = \begin{cases} 1, a \equiv_2 0 \\ -1, a \equiv_2 1 \end{cases}$ . Now,

given  $\sigma$  and  $\tau$  be the product of  $a, b$  transpositions respectively, we would have  $\text{Sgn}(\sigma + \tau)$  be 1 if  $a + b$  is even and  $-1$  if  $a + b$  is odd. Now we can just run a case by case analysis. If  $a$  is even and  $b$  is even, then the product of their signs is 1, if  $a, b$  are both odd we have the same, and if only 1 is even then we get  $-1$ , which gives the same result as above. Next, we can clearly see that the subset of all even permutations is just the kernel of  $\text{Sgn}$ , which shows it is a normal subgroup.

6. We proved (1) and also showed the reverse direction of (2) in the last question. Suppose that  $\sigma$  is even, and that it is the product of an odd number of transpositions. By the previous question we would have  $\text{Sgn}(\sigma) = -1$  a contradiction. Since every permutation is the product of a number of transpositions, and that number can't be odd, it must be even, and we are done.
7. We claim we can get every  $(ijk) \in A_n$  from those generators. Notice that  $(12i)^{-1}(12j)(12i) = (2ij)$ . Now,  $(2ij)^{-1}(12k)(2ij) = (1ik)$  for  $k \neq j$  and  $(1i2)$  otherwise. Next,  $(1k2)^{-1}(1ij)(1k2) = (kij)$ , so we can get all 3-cycles not containing either a 1 or a 2. By hypothesis we have each  $(12i)$ , and we showed we could also find  $(1i2)$ , which covers all 3-cycles involving both a 1 and a 2. We also got those with only a 2 or 1, so we have all 3-cycles. Now we just need to show that every even permutation is a product of 3-cycles. Actually, we just have to show that these can generate the product of all distinct 2-cycles, since the product of two nondistinct 2-cycles is either a 3 cycle or the identity. Notice that  $(ij)(kl) = (ilj)(ljk)$ . Now write  $\sigma = \prod (a_1^i a_2^i)$  be a product of transpositions. Commute this product so that overlapping transpositions are next to each other (if they are not overlapping they may commute). Any overlapping transposition is either the identity or a 3-cycle, which we can generate by the above. Remove all of those from this, and we must generate the remaining transpositions which are in  $A_n$  and are all disjoint. Since this is in  $A_n$  we cannot have an odd number of them, so we have an even number of them, and by the above we can generate the product of any two disjoint transpositions, so we are done. For example, suppose we had the permutation  $(34)(56)(23)(12)$ , first we move the disjoint factors away to the right side as  $(34)(23)(12)(56)$ . We now collapse from the left to right by  $(234)(12)(56)$  until we have just 3-cycles and disjoint transpositions. We can make  $(234)$ , and we can make  $(12)(56)$ , so we are done.

8. (a) We claim that the largest power of 2 dividing  $(2^n)!$  is  $2^{2^n-1}$ . We prove this by induction, and the base case is clear as the largest power of 2 dividing  $2! = 2$  is just 1. Let  $x \in \{2^n + 1, \dots, 2^{n+1} - 1\}$ , and let  $2^b$  be the highest power of 2 dividing  $x$ . Notice that since  $x \neq 2^{n+1}$ , the highest  $b$  can be is  $n$ , so  $2^b \mid x - 2^n$  since  $2^b \mid 2^n$  by the above. Since  $b$  was maximal, we cannot have a larger  $c$  so that  $2^c \mid x - 2^n$ , or else we could run this procedure backwards to get  $2^c \mid x$ , a contradiction. So the largest power of 2 dividing  $x$  is precisely the largest power of 2 dividing  $x + 2^n$  for  $x \in \{1, \dots, 2^n - 1\}$ . Thus the sum of the powers of 2 dividing  $x$  for  $x \in \{1, \dots, 2^n - 1\}$  is the same as the sum in  $\{2^n + 1, \dots, 2^{n+1} - 1\}$ , which by the inductive hypothesis is just  $2^n - 1 - n$  (we must remove the  $n$  from the  $2^n$  we excluded). So our total sum is just  $2 \cdot (2^n - 1 - n) + n + n + 1 = 2^{n+1} - 1$ , completing this subclaim. Since the size of the Sylow subgroup is the highest power of 2 dividing  $(2^n)!$ , we get that it's size is just  $2^{2^n-1}$ .
- (b) Let  $G_n$  be the complete binary tree of height  $n$  (one vertex is considered height 0). We claim that the automorphism group of  $G_n$  is a Sylow 2-group of  $S_{2^n}$ . First, we count the number of automorphisms. Now we just have to count the number of tree automorphisms. We of course claim there are  $2^{2^n-1}$  graph automorphisms of  $G_n$ . The base is clear: the complete binary tree with 1 vertex has  $1 = 2^{2^0-1}$  automorphisms. Now, to get an automorphism of  $G_{n+1}$ , we have to pick an automorphism of the left subtree, and the right, and then choose if we switch the trees or not. So the  $|\text{Aut}(G_{n+1})| = 2|\text{Aut}(G_n)|^2 = 2^{2^{n+1}-1}$ . Now we can give generators for this group. Label the vertices as follows:



We want the automorphism group of this graph to be isomorphic to the Sylow 2-subgroup of  $S_{2^n}$ . We proceed by “forgetting” information. Notice that each graph automorphism induces a permutation of the bottom  $2^n$  elements of the tree, and that distinct automorphisms induce distinct permutations. Define  $\varphi : \text{Aut}(G_n) \rightarrow S_{2^n}$  by  $\varphi(f) = (f(2^n) \cdots f(2^{n+1} - 1))$ . We can see clearly that this is a group homomorphism as the operation is the same on both sides (both being function composition). Thus  $\text{Aut}(G_n) \cong H \leq S_{2^n}$  with  $|H| = 2^{2^n-1}$ , and we are done.