SUMMER TERM ABSTRACT ALGEBRA HANDOUT IV: SYMMETRIC GROUPS AND LEARNING PROOFS

SAMIR SIKSEK

1. Orientation

This is the final abstract algebra handout for this term. You're meant to tackle it in Weeks 7 and 8. In this handout we revise symmetric groups. We're going to revise the main definitions and theorems, and also how to compute with permutations. But we'll also revise/study the proofs. **I'm asking you to make a special effort to know the proofs**.

What's the point of knowing proofs? Of course a proof convinces us of the theorem's truth. It's true that we can become convinced by reading the proof, checking that it's correct, and then forgetting the proof and just remembering the theorem. But this is dangerous. It separates what's true from why it's true. If you do this, then after a while the maths you know will be a collection of 'facts' and sometimes memory can play tricks; is the 'fact' really true or have you misremembered? Have you missed out a crucial hypothesis? This will not happen if the proof is at your mental finger-tips. You just go through the steps of the proof in your mind (or on paper) and that will allow you to reconstruct the hypotheses and verify the conclusion of the theorem.

Much of the process of creating maths is about recycling arguments that you've seen before and adapting them to new settings. These arguments are contained in the proofs; the statements of the theorems do not contain any arguments. So knowing proofs also helps you discover or create new maths.

When I say 'know proofs' and 'remember proofs' I don't mean rote memorization. I mean that you understand a proof and remember its key points well enough so that you can reproduce it. We'll talk more about that later.

2. Symmetric Groups

We revise some basic facts about symmetric groups and permutations. For more details see Chapter XIV of the lecture notes.

Definition. Let A be a set. We let $\mathrm{Sym}(A)$ be the set of bijections $\sigma : A \to A$. This is called the **symmetric group on** A. An element $\sigma \in \mathrm{Sym}(A)$ is called a permutation of A.

Theorem 1. *Let A be a set. Then $(\mathrm{Sym}(A), \circ)$ is a group where*

Date: May 28, 2020.

- $\circ$ *denotes composition of functions;*
- *the identity element is the bijection*

$$\mathrm{id}_A \ : \ A \to A, \qquad \mathrm{id}_A(a) = a \text{ for all } a \in A.$$

- *the inverse of* $\sigma \in \mathrm{Sym}(A)$ *is the unique bijection* $\sigma^{-1} \in \mathrm{Sym}(A)$ *that satisfies*

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id}_A.$$

Proof. This theorem is an easy exercise. Most of the facts that you need concerning bijections and their inverses is actually in Sections 6.3 and 6.4 of your Foundations lecture notes. □

Definition. Let $n \geq 1$. Let $S_n = \mathrm{Sym}(\{1, 2, 3, \ldots, n\})$. We call S_n the n**-th symmetric group**.

Theorem 2. $\#S_n = n!$.

Proof. The proof of this is so intuitive that you have no excuse not to know it. The elements of S_n are the bijections from $\{1, 2, \ldots, n\}$ to itself. However, as $\{1, 2, \ldots, n\}$ is finite, a function $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is a bijection if and only if it is an injection. This is sometimes called the **pigeon-hole principle** (Proposition 6.7 of your Foundations lecture notes).

Thus S_n is the set of injections $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$. Let σ be such an injection. There are n choices for $\sigma(1)$. Once we have chosen $\sigma(1)$ we must impose $\sigma(2) \neq \sigma(1)$ since σ is an injection. So there are $n - 1$ choices for $\sigma(2)$, and similarly $n - 2$ choices for $\sigma(3)$, ..., and 1 choice for $\sigma(n)$. Thus the number of elements of S_n is

$$n \times (n-1) \times (n-2) \times \cdots \times 1 = n!.$$

□

3. Matrix Notation for Permutations

Let $a_1, a_2, \ldots, a_n$ be the numbers $1, 2, \ldots, n$ in some order. We shall use the notation

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

to denote the permutation (i.e. element of S_n) that sends 1 to a_1, 2 to a_2, ..., and n to a_n.

Example 3. Let

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \qquad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \in S_4.$$

Although we're representing elements of S_4 as 2×4 matrices, never forget that these are bijections from $\{1, 2, 3, 4\}$ to itself. To find out what ρ, μ do just look at the columns:

$$\rho(1) = 3, \qquad \rho(2) = 1, \qquad \rho(3) = 2, \qquad \rho(4) = 4, \tag{1}$$

$$\mu(1) = 1, \qquad \mu(2) = 4, \qquad \mu(3) = 2, \qquad \mu(4) = 3.$$

Now let us compute $\rho\mu$. This means $\rho \circ \mu$ but we don't usually write the composition symbol $\circ$. By definition of function composition, $(\rho\mu)(a) = \rho(\mu(a))$; i.e. we apply μ first then ρ. So

$$\begin{aligned}(\rho\mu)(1) &= \rho(\mu(1)) = \rho(1) = 3;\\ (\rho\mu)(2) &= \rho(\mu(2)) = \rho(4) = 4;\\ (\rho\mu)(3) &= \rho(\mu(3)) = \rho(2) = 1;\\ (\rho\mu)(4) &= \rho(\mu(4)) = \rho(3) = 2.\end{aligned}$$

Thus

$$\rho\mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Let's compute ρ^{-1}. From (1),

$$1 = \rho^{-1}(3), \qquad 2 = \rho^{-1}(1), \qquad 3 = \rho^{-1}(2), \qquad 4 = \rho^{-1}(4).$$

Thus

$$\rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}.$$

Exercise 1. With ρ and μ as above, compute $\mu\rho$ and μ^{-1}.

4. Cycle Notation for Permutations

Definition. Let $a_1, a_2, \ldots, a_k$ be distinct elements of the set $\{1, 2, \ldots, n\}$. The permutation that sends a_1 to a_2, and a_2 to a_3, and a_3 to a_4, $\ldots$, and a_{k-1} to a_k and a_k to a_1, **and** fixes all other elements of $\{1, 2, \ldots, n\}$ is denoted by $(a_1, a_2, \ldots, a_k)$ and called a cycle of length k.

Example 4. Let $\mu = (1, 4, 5) \in S_5$. When you try to visualize μ in your head, what mental picture do you see? Perhaps you see the picture in Figure 1. This picture is incomplete, because although it tells you what μ does to 1, 4, 5, and it doesn't convey that μ fixes 2 and 3.

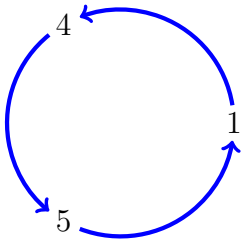

Figure 1. An incomplete picture for the cycle $(1, 4, 5) \in S_5$. The picture tells you that $(1, 4, 5)$ cyclically permutes 1, 4, 5, but it doesn't tell you what happens to 2 and 3.

The complete picture for $\mu = (1, 4, 5) \in S_5$ is given by Figure 2.

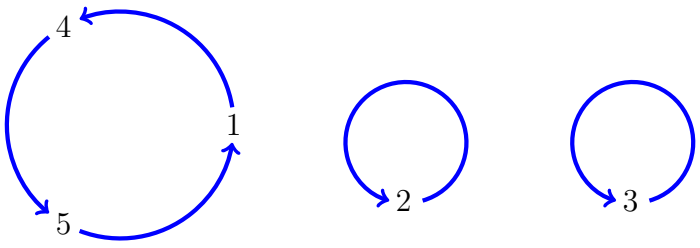

FIGURE 2. A complete picture for the cycle $(1, 4, 5) \in S_5$. It cyclically permutes 1, 4, 5, but fixes 2, 3.

Example 5. Note that there is some ambiguity in cycle notation, namely:

$$(a_1, a_2, \ldots, a_k) = (a_2, a_3, \ldots, a_k, a_1) = (a_3, a_4, \ldots, a_k, a_1, a_2) = \cdots \tag{2}$$

Why? Because they are identical as functions from $\{1, 2, \ldots, n\}$ to itself. Thus

$$(1, 3, 4, 2) = (3, 4, 2, 1) = (4, 2, 1, 3) = (2, 1, 3, 4).$$

However, this is not the same as $(1, 4, 3, 2)$. **For two cycles to be equal they need to cycle through precisely the same numbers in the exactly same order, but the starting point does not matter.**

Example 6. A cycle of length 1 is just the identity element id of S_n. Indeed, (a) just sends a to itself, and sends every member of $\{1, 2, \ldots, n\} \setminus \{a\}$ to itself, so it is just the identity map. Hence

$$(1) = (2) = (3) = \cdots = (n) = \mathrm{id}.$$

Definition. We call cycles $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ **disjoint** if $a_i \neq b_j$ for all i, j.

Theorem 7. *Disjoint cycles commute.*

Proof. Let $\sigma = (a_1, a_2, \ldots, a_k)$ and $\tau = (b_1, b_2, \ldots, b_\ell)$, and suppose they are disjoint. We're required to show that $\sigma\tau = \tau\sigma$. This means $\sigma\tau$ and $\tau\sigma$ are the same function $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$; i.e. we want to prove that $\sigma(\tau(x)) = \tau(\sigma(x))$ for all $x \in \{1, 2, \ldots, n\}$. The proof of this is just a calculation, and we split it into three cases.

Case 1. $x \neq a_i$ for all i, and $x \neq b_j$ for all j. Then $\sigma(x) = x$ and $\tau(x) = x$. Hence $\sigma(\tau(x)) = x = \tau(\sigma(x))$.

Case 2. $x = a_i$ for some i. As the cycles are disjoint $x \neq b_j$ for all j. Note that

$$\begin{aligned} \sigma(\tau(x)) &= \sigma(\tau(a_i)) \\ &= \sigma(a_i) \qquad a_i \text{ is fixed by } \tau \text{ as it doesn't equal any of the } b_j \\ &= a_{i+1} \qquad \text{because } \sigma = (a_1, a_2, \ldots, a_k). \end{aligned}$$

Here we interpret $a_{k+1} = a_1$. Also

$$\begin{aligned}\tau(\sigma(x)) &= \tau(\sigma(a_i)) \\ &= \tau(a_{i+1}) \qquad \text{because } \sigma = (a_1, a_2, \ldots, a_k) \\ &= a_{i+1} \qquad a_{i+1} \text{ is fixed by } \tau \text{ as it doesn't equal any of the } b_j.\end{aligned}$$

Hence $\sigma(\tau(x)) = \tau(\sigma(x))$.

Case 3. $x = b_j$ for some j. This is similar to Case 2.

This completes the proof. □

Strategy for 'remembering' proofs. Some students memorize proofs for exams, and often end up writing complete rubbish because they have misremembered some of the steps. A better and safer strategy is the following.

(I) Understand the proof.
(II) Ask yourself what the keys steps or ideas are.
(III) Make an effort to remember those key steps.

For me the key steps in the above proof are

- we want to show $\sigma(\tau(x)) = \tau(\sigma(x))$;
- we divide into three cases according to whether x doesn't appear in either, or appears in σ or appears in τ;
- After that it's just calculation.

Try this strategy as you're going through the proofs in this handout. Then come back the next day and try to write down the proofs without looking them up. It might seem pointless—you don't have exams coming up and if you don't remember a proof you can google it. But remembering the key points of proofs and how they fit together is an important part of mathematical fluency, and will improve your understanding and confidence.

Theorem 8. *Every permutation can be written as a product of disjoint cycles.*

We'll delay the proof a little till we've seen an example and practiced writing permutations as products of disjoint cycles.

Example 9. Let

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 5 & 7 & 2 & 4 & 1 & 6 & 8 & 11 & 10 & 9 \end{pmatrix},$$

which we want to write as a product of disjoint cycles. We start with 1 and apply ρ to it repeatedly:

$$1 \mapsto 3 \mapsto 7 \mapsto 6 \mapsto 1. \tag{3}$$

If we're just looking at the set $\{1, 3, 7, 6\}$ then ρ and the cycle $(1, 3, 7, 6)$ do exactly the same thing. However (3) does not tell us what ρ does to 2. We start at 2 and apply ρ repeatedly:

$$2 \mapsto 5 \mapsto 4 \mapsto 2. \tag{4}$$

Thus on the set $\{2,5,4\}$, the permutation ρ and the cycle $(2,5,4)$ do the same thing. Note that $(2,5,4)$ is the identity on $\{1,3,7,6\}$ and $(1,3,7,6)$ is the identity on $\{2,5,4\}$. Hence the product (or composition) $(1,3,7,6)(2,5,4)$ does the same thing as ρ on $\{1,3,7,6\} \cup \{2,5,4\} = \{1,2,3,4,5,6,7\}$. The product $(1,3,7,6)(2,5,4)$ and the permutation ρ both have the effect

$$1 \mapsto 3 \mapsto 7 \mapsto 6 \mapsto 1, \qquad 2 \mapsto 5 \mapsto 4 \mapsto 2. \tag{5}$$

We continue: (5) doesn't tell us what ρ does to $8,9,10,11$. Note on the set $\{8,9,10,11\}$, the effect of ρ is

$$8 \mapsto 8, \qquad 9 \mapsto 11 \mapsto 9, \qquad 10 \mapsto 10,$$

which is the same as $(8)(9,11)(10)$.

Putting it all together, ρ and $(1,3,7,6)(2,5,4)(8)(9,11)(10)$ agree on $\{1,2,\ldots,11\}$ so they must be equal:

$$\rho = (1,3,7,6)(2,5,4)(8)(9,11)(10).$$

Since cycles of length 1 are equal to the identity, we usually omit them, so we write

$$\rho = (1,3,7,6)(2,5,4)(9,11).$$

Note that there are many ways to write the answer correctly. First, as the cycles are disjoint they commute, so we could have written for example

$$\rho = (2,5,4)(1,3,7,6)(9,11).$$

Also, because of the ambiguity in the cycle notation (2) we could also write (again for example)

$$\rho = (5,4,2)(7,6,1,3)(11,9).$$

Remark. We did the example in way too much detail, just to make the thought process clear. But you can just follow the arrows in your head and simply write down the answer.

Exercise 2. Let

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 2 & 8 & 11 & 4 & 10 & 1 & 5 & 3 & 9 & 6 \end{pmatrix}$$

Write ρ as a product of disjoint cycles.

We're about to prove Theorem 8, but we first need a couple of lemmas.

Lemma 10. *Let $\rho \in S_n$ and $a \in \{1,2,\ldots,n\}$. Then there is some $u \geq 1$ such that $a, \rho(a), \rho^2(a), \ldots, \rho^{u-1}(a)$ are all distinct, but $\rho^u(a) = a$.*

Proof. Consider the sequence

$$a, \quad \rho(a), \quad \rho^2(a), \quad \rho^3(a), \ldots$$

Every term in this infinite sequence is contained in the finite set $\{1,2,\ldots,n\}$. Thus the sequence must contain repetition. Let $\rho^u(a) = \rho^v(a)$ be the first instance of repetition in the sequence, where $0 \leq v < u$. Apply ρ^{-v} to both

sides. We obtain $\rho^{u-v}(a) = a$. Note that $0 < u - v \leq u$. If $u - v < u$, then $\rho^{u-v}(a) = a$ is in fact an earlier instance of repetition in the sequence, which contradicts our assumption. Therefore, $u - v = u$ and so $v = 0$. Hence $\rho^u(a) = a$. As this is the earliest repetition, $a, \rho(a), \ldots, \rho^{u-1}(a)$ are distinct. □

Definition. Let $\rho \in S_n$ and $a \in \{1, 2, \ldots, n\}$. Let u be as in the statement of Lemma 10. Denote

$$\mathrm{Orb}_\rho(a) = \{a, \rho(a), \rho^2(a), \ldots, \rho^{u-1}(a)\};$$

this is called the **orbit of** a **under** ρ.

Example 11. In Example 9, the orbits of ρ are

$$\mathrm{Orb}_\rho(1) = \mathrm{Orb}_\rho(3) = \mathrm{Orb}_\rho(7) = \mathrm{Orb}_\rho(6) = \{1, 3, 7, 6\}$$
$$\mathrm{Orb}_\rho(2) = \mathrm{Orb}_\rho(5) = \mathrm{Orb}_\rho(4) = \{2, 5, 4\}$$
$$\mathrm{Orb}_\rho(8) = \{8\}, \qquad \mathrm{Orb}_\rho(9) = \mathrm{Orb}_\rho(11) = \{9, 11\}, \qquad \mathrm{Orb}_\rho(10) = \{10\}.$$

Lemma 12. *Let $\rho \in S_n$, and a, $b \in \{1, 2, \ldots, n\}$. Then the orbits* $\mathrm{Orb}_\rho(a)$, $\mathrm{Orb}_\rho(b)$ *are either equal or disjoint.*

Proof. Let u be the smallest positive integer such that $\rho^u(a) = a$, and let v be the smallest positive integer such that $\rho^v(b) = b$. Thus

$$\mathrm{Orb}_\rho(a) = \{a, \rho(a), \rho^2(a), \ldots, \rho^{u-1}(a)\}, \quad \mathrm{Orb}_\rho(b) = \{b, \rho(b), \rho^2(b), \ldots, \rho^{v-1}(b)\}.$$

Suppose $\mathrm{Orb}_\rho(a) \cap \mathrm{Orb}_\rho(b) \neq \emptyset$. Then $\rho^i(a) = \rho^j(b)$ for some $0 \leq i < u$ and $0 \leq j < v$. Without loss of generality, $j \leq i$. Thus $b = \rho^k(a)$ where $k = i - j < u$. Thus $b \in \mathrm{Orb}_\rho(a)$. Hence $\rho^t(b) = \rho^{k+t}(a) \in \mathrm{Orb}_\rho(a)$ for all t, so $\mathrm{Orb}_\rho(b) \subseteq \mathrm{Orb}_\rho(a)$. However, $a = \rho^{u-k}(b)$, so $a \in \mathrm{Orb}_\rho(b)$ and so in a similar way $\mathrm{Orb}_\rho(a) \subseteq \mathrm{Orb}_\rho(b)$. Hence the two orbits are equal. □

Lemma 13. *Let $\rho \in S_n$. The orbits of ρ form a partition of $\{1, 2, \ldots, n\}$.*

Proof. Note that $a \in \mathrm{Orb}_\rho(a)$. Thus the orbits are non-empty and their union is $\{1, 2, \ldots, n\}$. By Lemma 12, any two orbits are either disjoint or equal. Thus the orbits form a partition of $\{1, 2, \ldots, n\}$. □

Exercise 3. Let ρ be as in Exercise 2. Determine the orbits of ρ and check that they form a partition of $\{1, 2, \ldots, 11\}$.

Proof of Theorem 8. Let ρ be an element of S_n. Let $C_1, C_2, \ldots, C_k$ be the distinct orbits of ρ. Choose $a_i \in C_i$. Then for each $i = 1, 2, \ldots, k$ there is a positive integer u_i such that

$$C_i = \mathrm{Orb}_\rho(a_i) = \{a_i, \rho(a_i), \rho^2(a_i), \ldots, \rho^{u_i-1}(a_i)\}.$$

Let

$$\mu_i = (a_i, \rho(a_i), \rho^2(a_i), \ldots, \rho^{u_i-1}(a_i)).$$

This is a cycle of length u_i. Note that for $i \neq j$, the cycles μ_i, μ_j are disjoint, since C_i, C_j are disjoint by Lemma 12.

Consider the effect ρ has on the elements of C_i; this is the same as the effect μ_i has on the elements of C_i. However, for $j \neq i$, the cycle μ_j fixes all the elements of C_i. Thus the product $\mu_1\mu_2\cdots\mu_{i-1}\mu_i\mu_{i+1}\cdots\mu_k$ has the same effect as μ_i on the elements of C_i, and therefore the same effect as ρ on the elements of C_i. As $\{1, 2, \ldots, n\} = C_1 \cup C_2 \cup \cdots \cup C_n$, then ρ has the same effect on $\{1, 2, \ldots, n\}$ as the product of disjoint cycles $\mu_1\mu_2\cdots\mu_k$. In other words, $\rho = \mu_1\mu_2\cdots\mu_k$. □

Exercise 4. Let ρ and τ be the following permutations:

$$\rho = (1, 3)(2, 4, 5), \qquad \tau = (1, 2, 3, 4, 5).$$

Determine ρ^3 and $\tau^{-1}\rho$, writing your answers as products of disjoint cycles.

Exercise 5. Show that S_n is non-abelian for $n \geq 3$. What about S_2?

Exercise 6. (i) Let G be an abelian group. Let g, h be elements of G having finite orders r, s. Show that the order of gh divides $\mathrm{lcm}(r, s)$. Make sure it is clear where you have used the fact that G is abelian.

(ii) Give a counterexample to show that the corresponding statement need not hold for non-abelian groups. **Hint.** Try S_3.

(iii) Can you find an infinite group G with elements g, h of finite order such that gh has infinite order? **Hint.** Revise the section on rotations and reflections in Handout III.

5. The Parity of a Permutation

Definition. A **transposition** is a cycle of length 2. Thus it has the form (a, b) where $a \neq b$.

Theorem 14. *Every permutation can be written as a product of transpositions.*

Proof. The proof of this theorem is so easy that you have no excuse not to know it. First we know that every permutation can be written as a product of cycles (Theorem 8). So all we have to do is show that that every cycle can be written as a product of transpositions. To see this, simply check the formula:

$$(a_1, a_2, \ldots, a_k) = (a_{k-1}, a_k)(a_{k-2}, a_k)\cdots(a_2, a_k)(a_1, a_k). \tag{6}$$

□

Definition. We call a permutation **even** if it is a product of an even number of transpositions, and **odd** if it a product of an odd number of transpositions.

The following theorem is really saying that the definition is a sensible one.

Theorem 15. *A permutation is either even or odd, but can't be both.*

In Term 1 we proved Theorem 15 using permutation polynomials. That's a great proof. But to stop boredom from creeping in we'll give another proof of Theorem 15. First you need to do this exercise.

Exercise 7. Let a, b, c, d be pairwise distinct members of the set $\{1, 2, \ldots, n\}$. Verify the following identities:

(7a) $$(c, d)(a, b) = (a, b)(c, d)$$

(7b) $$(b, c)(a, b) = (a, c)(b, c)$$

(7c) $$(a, c)(a, b) = (a, b)(b, c)$$

(7d) $$(a, b)(a, b) = \mathrm{id}$$

Note that $(u, v) = (v, u)$ for $u \neq v$. Thus we could've swapped the numbers appearing in any of these transpositions and we would still have the same identity. For example, (7b) can also be written as $(c, b)(a, b) = (a, c)(b, c)$.

Remark. What are the identities (7a)–(7d) really saying? They are saying that if I have any product of two transpositions $\varepsilon \cdot \delta$ and a occurs in δ, then I can either replace $\varepsilon \cdot \delta$ by $\varepsilon' \cdot \delta'$ where a appears only in ε', or I can replace $\varepsilon \cdot \delta$ by id. To see this we need only convince ourselves that the identities (7a)–(7d) cover all possible cases:

(a) ε, δ have no numbers in common; we use (7a).
(b) ε, δ have exactly one number in common, and that isn't a; we use (7b).
(c) ε, δ have exactly one number in common, and that is a; we use (7c).
(d) ε, δ have both numbers in common; we use (7d).

The Transposition Game. Given a product of transpositions we are going to play a game. We let a be the largest number appearing in any of the transpositions. The identities (7a)–(7d) are our **allowable moves**, which we apply to pairs consecutive transpositions where a appears in the right hand transposition. Note that (7a)–(7c) move a so that it appears only in left hand transposition. Also (7d) removes two of the occurrences of a. The objective of the game is:

- either make a disappear altogether;
- or have only one occurrence of a which appears in the left-most transposition.

Let's see some examples.

Example 16. We apply the allowable moves repeatedly to the product $(4, 3)(5, 1)(2, 3)(5, 2)(1, 5)$. Here throughout $a = 5$ (the biggest number appearing in the transpositions). We use the under-brace to highlight which

pair of consecutive transpositions we're applying the move to.

$$\begin{aligned}
(4,3)(5,1)(2,3)\underbrace{(5,2)(1,5)} &= (4,3)(5,1)(2,3)\underbrace{(5,1)(1,2)} && \text{using move (7c)}\\
&= (4,3)(5,1)\underbrace{(2,3)(5,1)}(1,2)\\
&= (4,3)(5,1)\underbrace{(5,1)(2,3)}(1,2) && \text{using move (7a)}\\
&= (4,3)\underbrace{(5,1)(5,1)}(2,3)(1,2)\\
&= (4,3)(2,3)(1,2) && \text{using move (7d).}
\end{aligned}$$

We stop now as we've got rid of the 5.

Let's do a slightly different example. Consider the product $(4,3)(4,1)(2,3)(5,2)(1,5)$.

$$\begin{aligned}
(4,3)(4,1)(2,3)\underbrace{(5,2)(1,5)} &= (4,3)(4,1)(2,3)\underbrace{(5,1)(1,2)} && \text{using move (7c)}\\
&= (4,3)(4,1)\underbrace{(2,3)(5,1)}(1,2)\\
&= (4,3)(4,1)\underbrace{(5,1)(2,3)}(1,2) && \text{using move (7a)}\\
&= (4,3)\underbrace{(4,1)(5,1)}(2,3)(1,2)\\
&= (4,3)\underbrace{(5,4)(1,4)}(2,3)(1,2) && \text{using move (7b)}\\
&= \underbrace{(4,3)(5,4)}(1,4)(2,3)(1,2)\\
&= \underbrace{(5,3)(4,3)}(1,4)(2,3)(1,2) && \text{using move (7b).}
\end{aligned}$$

We stop now because 5 is present only in the left-most transposition.

Exercise 8. It's your turn to play the transposition game:

(i) $(1,5)(4,3)(2,5)(2,4)(3,5)$.
(ii) $(4,5)(4,3)(2,5)(2,4)(3,5)$.

Lemma 17. *Let $\tau_1, \tau_2, \ldots, \tau_r$ be transpositions in S_n, and let a be the largest number appearing in any of these transpositions. Then the product $\tau_1\tau_2\cdots\tau_r$ is equal to a product $\mu_1\mu_2\cdots\mu_s$ of transpositions where*

(I) $s \leq r$ and $s \equiv r \pmod 2$.
(II) ***Either***
(i) a appears in μ_1, but not in $\mu_2, \ldots, \mu_s$;
or
(ii) or a does not appear in any of the μ_i, and $s < r$.

Proof. This should be clear, except for a couple of points. Note that applying any of the identities (7a)–(7c) preserves the number of transpositions, since they simply replace the product of two transpositions by another product of two transpositions. However, (7d) replaces the product of two transpositions by id, and so reduces the number of transpositions by 2. Thus $s = r - 2t$, where s is the final number of transpositions, and t is the number of times

we have applied (7d). In particular $s \leq r$ and $s \equiv r \pmod 2$. Moreover, if a disappears altogether then we must have applied (7d) at least once, so $t \geq 1$ so $s < r$. □

Lemma 18. *Let $\tau_1, \ldots, \tau_r$ be transpositions belonging to S_n. Suppose*

$$\tau_1 \tau_2 \cdots \tau_r = \mathrm{id}.$$

Then r is even.

Proof. The proof is by strong induction on r. If $r = 0$ then r is even and there is nothing to prove. Note that $r = 1$ is impossible, since a transposition τ swaps two numbers and so can't be the identity. We suppose $r \geq 2$.

Let a be the largest number appearing in the transpositions $\tau_1 \tau_2 \cdots \tau_r$. By Lemma 17 there exists transpositions $\mu_1, \mu_2, \ldots, \mu_s$ such that

$$\mu_1 \mu_2 \cdots \mu_s = \tau_1 \tau_2 \cdots \tau_r = \mathrm{id}, \tag{8}$$

where moreover, either a appears only in μ_1 or a does not appear in any of the μ_i.

Suppose a appears only in μ_1. Then $\mu_j(a) = a$ for $j = 2, 3, \ldots, s$. Write $\mu_1 = (a, b)$, with $b \neq a$. Thus

$$\begin{aligned} a =& \mathrm{id}(a) \\ &= (\mu_1 \mu_2 \cdots \mu_s)(a) \qquad \text{from (8)} \\ &= (\mu_1 \mu_2 \cdots \mu_{s-1})(\mu_s(a)) \\ &= \mu_1 \mu_2 \cdots \mu_{s-1}(a) \qquad \mu_s(a) = a \\ &= \cdots \\ &= \mu_1(a) = b \end{aligned}$$

giving a contradiction as $a \neq b$.

It follows that a does not appear in any of the μ_i. In particular, we are in case (ii) of Lemma 17. Hence $s < r$. Applying the inductive hypothesis to $\mu_1 \mu_2 \cdots \mu_s = \mathrm{id}$ tells us that s is even. But again by part (I) of Lemma 17 we know that $r \equiv s \pmod 2$. Hence r is even. This completes the proof. □

We're ready to prove Theorem 15.

Proof of Theorem 15. Suppose $\rho \in S_n$ can be written as

$$\rho = \varepsilon_1 \varepsilon_2 \cdots \varepsilon_k = \delta_1 \delta_2 \cdots \delta_\ell$$

where the ε_i and the δ_j are transpositions. We're required to show that k and ℓ are both even or both odd. Now

$$\begin{aligned} \mathrm{id} &= \rho \rho^{-1} \\ &= (\varepsilon_1 \varepsilon_2 \cdots \varepsilon_k) \cdot (\delta_1 \delta_2 \cdots \delta_\ell)^{-1} \\ &= \varepsilon_1 \varepsilon_2 \cdots \varepsilon_k \cdot \delta_\ell^{-1} \cdots \delta_2^{-1} \delta_1^{-1} \\ &= \varepsilon_1 \varepsilon_2 \cdots \varepsilon_k \cdot \delta_\ell \cdots \delta_2 \delta_1 \qquad (\delta^{-1} = \delta \text{ for any transposition } \delta). \end{aligned}$$

We have written the identity as a product of $k+\ell$ transpositions. Hence $k+\ell$ is even by Lemma 18. Therefore k, ℓ are either both odd or both even. $\square$

Remark. It might seem that the proof of Theorem 15 in this handout is very hard to learn. After all, you must have extremely good memory to be able to memorize the identities (7a)–(7d). But do they really need to be memorized? If you know the objective of these identities, is it not possible to reproduce them? The idea is that we have a product of two transpositions $(?,?)(a,b)$. I want to rewrite this as either the identity, or a product of two transpositions, where a appears only in the left transposition. The case where I get the identity is easy to remember or figure out: $(a,b)(a,b) = \mathrm{id}$, which is saying that if you swap twice you get the identity. Another case which is easy to remember is when the two transpositions are disjoint $(c,d)(a,b) = (a,b)(c,d)$ because disjoint cycles commute. What about the other cases? Do I even remember how many other cases there are? In the other cases we have $(?,?)$ is not the same as (a,b) and not entirely disjoint from (a,b), so it has one number in common. So we have exactly two other cases where that number is a or that number is b:

$$(a,c)(a,b) = (a,?)(?,?), \qquad (b,c)(a,b) = (a,?)(?,?).$$

We don't want a to appear in the transposition on the right, so question marks are all bs and cs. It's not hard anymore to figure out what the question marks must be. As you can see, if you remember the ideas, you can work out the details for yourself.

Exercise 9. Let ρ be a cycle of length k. Show that ρ even if k is odd, and ρ is odd if k is even.

Exercise 10. Let ρ, $\sigma \in S_n$.

(i) Show that the identity $\mathrm{id} \in S_n$ is even.
(ii) Show that $\rho\sigma$ is even if and only if ρ and σ are both even or both odd.
(iii) Show that ρ^{-1} has the same parity as ρ.

Exercise 11. Let $\sigma \in S_n$ be an odd permutation. Show carefully that the order of σ is even.

6. The Alternating Group

Definition. We let $A_n = \{\sigma \in S_n \ : \ \sigma \text{ is even}\}$. This is called the **$n$-th alternating group**.

Theorem 19. *A_n is a subgroup of S_n of index 2. The cosets of A_n in S_n are A_n and*

$$\{\sigma \in S_n \ : \ \sigma \textit{ is odd}\}.$$

Proof. The fact that A_n is a subgroup of S_n follows immediately from Exercise 10.

Write

$$A'_n = \{\sigma \in S_n \ : \ \sigma \text{ is odd}\}.$$

We **claim** that, for all $\rho \in S_n$,

$$\rho A_n = \begin{cases} A_n & \text{if } \rho \text{ is even} \\ A'_n & \text{if } \rho \text{ is odd.} \end{cases}$$

Once we have proved our claim, we will know that A_n has precisely two cosets in S_n, and these are A_n and A'_n. Thus in particular, the index of A_n in S_n is 2.

Let's prove the claim. Suppose ρ is even. Then $\rho \in A_n$. Hence ρA_n and A_n have the element ρ in common. But cosets are either disjoint or equal. Thus $\rho A_n = A_n$. Suppose next that ρ is odd. We want to show that $\rho A_n = A'_n$. Equivalently we want to show that $\tau \in \rho A_n$ if and only if $\tau \in A'_n$. Of course, any element τ of ρA_n has the form $\tau = \rho\sigma$ where σ is even. As ρ is odd, $\tau = \rho\sigma$ is odd (part (ii) of Exercise 10). Thus $\tau \in A'_n$. Conversely, suppose $\tau \in A'_n$, and so τ is odd. Let $\sigma = \rho^{-1}\tau$. As ρ is odd, so is ρ^{-1} (part (iii) of Exercise 10) and so $\sigma = \rho^{-1}\tau$ is even. Hence $\sigma \in A_n$, so $\tau = \rho\sigma \in \rho A_n$. It follows that $\rho A_n = A'_n$, completing the claim's proof. □

Lagrange's theorem immediately allows us to deduce the following.

Corollary 20. $\#A_n = n!/2$.

Exercise 12. Let ρ and τ be the following permutations:

$$\rho = (1,3)(2,4,5), \qquad \tau = (1,2,3,4,5).$$

Write ρ, τ as products of transpositions. Which of them belongs to A_5?

Exercise 13. Show that A_n is non-abelian for $n \geq 4$. What about A_2 and A_3?

Exercise 14. Let

$$H_1 = \{\sigma \in A_4 : \sigma^3 = 1\}, \qquad H_2 = \{\sigma \in A_4 : \sigma^7 = \sigma^{-5}\}.$$

Which of these is a subgroup of A_4. Justify your answers.

Exercise 15. Let f be a polynomial in variables $x_1, \ldots, x_4$. Let σ be a permutation in S_4. We define $\sigma(f)$ to be the polynomial $f(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$. (For example, if $f = x_1 + x_2^2 + x_3x_4$ and $\sigma = (1,4)(2,3)$ then σ swaps x_1 and x_4, and swaps x_2 and x_3; thus $\sigma(f) = x_4 + x_3^2 + x_2x_1$.) Define $\mathrm{Stab}(f) = \{\sigma \in S_4 : \sigma(f) = f\}$. This is called the **stabilizer of** f.

(a) Show that $\mathrm{Stab}(f)$ is a subgroup of S_4.
(b) Write down the elements of $\mathrm{Stab}(f)$ for the following polynomials in $x_1, \ldots, x_4$:
  (i) $f = x_1x_2 + x_3 + x_4$.
  (ii) $f = x_4^2 + x_1x_2x_3$.
(c) Write down a polynomial f in x_1, x_2, x_3, x_4 such that $\mathrm{Stab}(f) = A_4$.

(d) Show that there is no polynomial f in $x_1, \ldots, x_4$ such that $\mathrm{Stab}(f)$ has order 5.

(e) **Prove or disprove** the following statement: if f and g are polynomials in $x_1, \ldots, x_4$, and $\sigma \in \mathrm{Stab}(f+g)$, then $\sigma \in \mathrm{Stab}(f)$ and $\sigma \in \mathrm{Stab}(g)$.

7. D_n is a subgroup of S_n

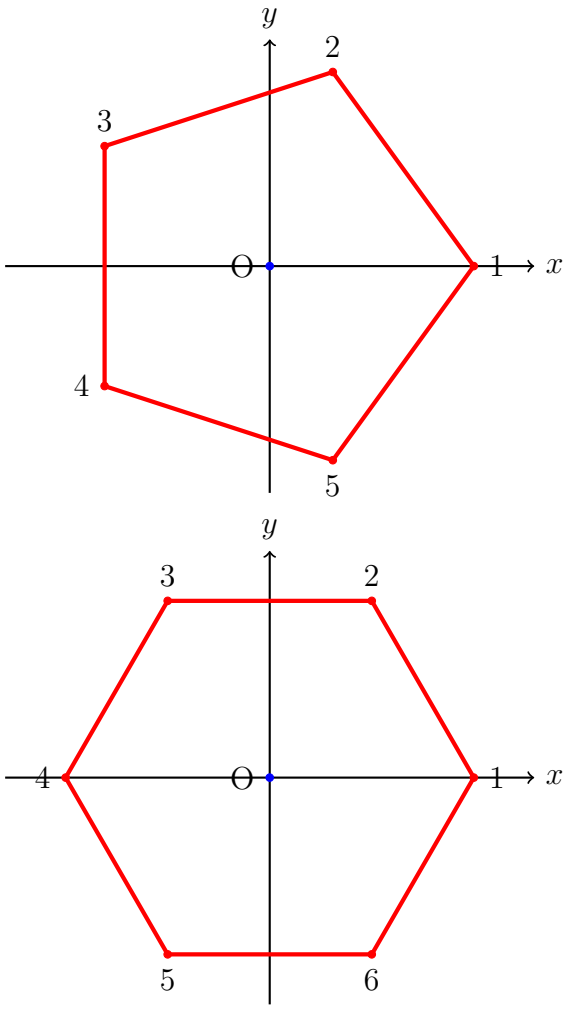

FIGURE 3. We place the regular n-gon in the plane so that its centre coincides with the origin, and its vertex 1 lies on the positive x-axis. In these pictures, $n = 5$ (top) and $n = 6$ (bottom).

Recall that D_n is the group of symmetries of the regular n-gon. We give the vertices of the n-gon labels $1, 2, \ldots, n$ (going anticlockwise). A symmetry of the n-gon of the n-gon permutes $1, 2, \ldots, n$ and so can be identified as an element of S_n.

For example, in D_4, we used ρ_1 to denote anticlockwise rotation around the centre of the square through $90°$. Thus ρ_1 sends vertex 1 to vertex 2, vertex 2 to vertex 3, vertex 3 to vertex 4, and vertex 4 to vertex 1. So we write $\rho_1 = (1, 2, 3, 4)$.

Recall our conventions of Handout 3. We place the regular n-gon in the plane with its centre coinciding with the origin, and vertex 1 is on the positive x-axis. See Figure 3 for illustrations. We used the symbol r to denote anticlockwise rotation of the n-gon through an angle of $2\pi/n$, and the symbol s to denote reflection of the n-gon in the x-axis. Moreover,

$$D_n = \{1, r, r^2, \ldots, r^{n-1}\} \cup \{s, rs, r^2s, \ldots, r^{n-1}s\}.$$

Exercise 16. (i) Write r and s as products of disjoint cycles.
(ii) For which values of n is D_n a subgroup of A_n?

8. Permutation Types

A permutation $\rho \in S_n$ is said to have **permutation type** $[\alpha_1, \alpha_2, \ldots, \alpha_n]$ if, when written as a product of disjoint cycles, ρ has α_1 cycles of length 1, α_2 cycles of length 2, $\ldots$, α_n cycles of length n. For example, in S_{11}, the permutation $\rho = (1, 7)(3, 4, 5)(6, 11)$ has permutation type $[4, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0]$. If you're puzzled by the 4 (four cycles of length 1) it is because ρ fixes 2, 8, 9, 10 and so can be written as $\rho = (2)(8)(9)(10)(1, 7)(3, 4, 5)(6, 11)$.

For example, possible permutation types for an element of S_4 are

$$[4, 0, 0, 0], \quad [2, 1, 0, 0], \quad [0, 2, 0, 0], \quad [1, 0, 1, 0], \quad [0, 0, 0, 1].$$

Examples of permutations having these types are

$$(1)(2)(3)(4), \quad (1)(2)(3, 4), \quad (1, 2)(3, 4), \quad (1)(2, 3, 4), \quad (1, 2, 3, 4)$$

respectively. We write $p(n)$ for the number of permutation types in S_n (this is called the **n-th partition number**. From the above $p(4) = 5$.

Exercise 17. (i) Compute $p(n)$ for $n = 2, 3, 4, 5, 6$.
(ii) Show that $[\alpha_1, \alpha_2, \ldots, \alpha_n]$ is a permutation type for some element of S_n if and only if

$$\alpha_1 + 2\alpha_2 + 3\alpha_3 \cdots + n\alpha_n = n. \tag{9}$$

Exercise 18. Give a recipe for determining the parity (evenness or oddness) of $\rho \in S_n$ in terms of its permutation type $[\alpha_1, \alpha_2, \ldots, \alpha_n]$.

Hardy and Ramanujan proved an asymptotic formula for $p(n)$:

$$p(n) \sim \frac{\exp(\pi\sqrt{2n/3})}{4n\sqrt{3}}. \tag{10}$$

What does the notation $\sim$ mean? Let $\{a(n)\}_{n=1}^{\infty}$ and $\{b(n)\}_{n=1}^{\infty}$ be sequences. We say that they are **asymptotic** and write $a(n) \sim b(n)$ if $\lim_{n\to\infty} \frac{a(n)}{b(n)} = 1$.

Exercise 19. (Optional, but I really think you should try it)

(i) Write a program that computes $p(n)$ given n (using any programming language you like). Here are a couple of tips.
   (a) The last thing you want to do is write down all $n!$ permutations and then compute their types. The number $p(n)$ is the number of solutions to the equation (9) in non-negative integers $\alpha_1, \alpha_2, \ldots, \alpha_n$.
   (b) From the Hardy–Ramanujan asymptotic you can see that $p(n)$ grows very quickly. Thus you should not expect your program to run in reasonable time for big values of n. If you can compute $p(50)$ in less than a minute then you're doing really well.

(ii) Let $\mathrm{HR}(n)$ be the right-hand side of (10). Plot $p(n)/\mathrm{HR}(n)$ against n for a few values of n. Does it look like it is converging to 1?

9. Student led astray by lecturer (topic for reflection)

During a 2020–2021 Zoom lecture, the lecturer gets muddled and writes out an incorrect proof (such blunders do occasionally happen in the heat of the lecture). In the module's end-of-year open book exam a student reproduces the incorrect proof word for word and symbol for symbol. What mark should the student get? (I originally wrote "What mark does the student deserve?", but the word "deserve" conveys connotations of guilt, and I rephrased as I didn't want to prejudice your deliberations before they have even commenced.)