# 13th Lecture: 23/2

**Permutations.** We will focus on permutations of finite sets. Recall that $S_n$ denotes the group of permutations of $\{1, 2, \ldots, n\}$. We will henceforth also employ the more compact notation $[n] := \{1, 2, \ldots, n\}$.

**Definition 13.1.** Let $n, k \in \mathbb{Z}_+$ with $k \leq n$. A permutation $\pi \in S_n$ is called a *$k$-cycle* if there is a subset $\{x_1, x_2, \ldots, x_k\}$ of $[n]$ of size $k$ such that

$$\pi(x_1) = x_2, \;\; \pi(x_2) = x_3, \; \ldots, \; \pi(x_{k-1}) = x_k, \;\; \pi(x_k) = x_1; \quad \pi(i) = i \; \forall \, i \in [n] \backslash \{x_1, x_2, \ldots, x_k\}. \tag{13.1}$$

**Notation 13.2.** The $k$-cycle $\pi$ given by (13.1) will be denoted

$$\pi = (x_1 \, x_2 \, \ldots \, x_k).$$

Observe that

$$(x_1 \, x_2 \, \ldots \, x_k) = (x_2 \, x_3 \, \ldots \, x_k \, x_1) = \cdots = (x_k \, x_1 \, x_2 \, \ldots \, x_{k-1}).$$

When writing a cycle with this notation, the *convention* is to always place the smallest number in the leftmost position.

When composing permutations, we will adopt the default multiplicative notation for group operations. Hence $\pi_1 \pi_2$ is the function $\pi_2 \circ \pi_1$. When using cycle notation, this means that we "follow each number from left to right". For example,

$$(12)(13) = (13)(23) = (23)(12) = (123), \quad (13)(12) = (23)(13) = (12)(23) = (132).$$

**Observation 13.3.** Suppose $\pi_1$ and $\pi_2$ are cycles on disjoint subsets $\{x_1, \ldots, x_k\} \cap \{y_1, \ldots, y_l\} = \phi$ of $[n]$. Then it is clear that they commute, $\pi_1 \pi_2 = \pi_2 \pi_1$. It follows that every element of $S_n$ can be uniquely written as a product of pairwise disjoint cycles, provided we adopt the following conventions:

1. As already mentioned above, each cycle is written with its smallest number to the left.
2. Disjoint cycles are written from left to right in order of increasing smallest number.
3. Fixed points are written as 1-cycles.

**Example 13.4.** Let $\pi \in S_{10}$ be given as a function $[10] \rightarrow [10]$ by

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\pi(i)$ | 3 | 5 | 10 | 4 | 7 | 1 | 2 | 9 | 8 | 6 |

Then, in cycle notation, we have

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

**Notation and Terminology 13.5.** Recall that the order of an element $g$ in a group $G$ is the smallest $n \in \mathbb{Z}_+ \cup \{\infty\}$ such that $g^n = 1$ and that, if $G$ is finite, then the order of any element is a divisor of $|G|$, by Corollary 9.15. We denote the order of $g \in G$ by $|g|$. This notation makes sense since $|g|$ is also the size of the cyclic subgroup of $G$ generated by $g$, i.e.: $|g| = | < g > |$.

Now suppose $\pi \in S_n$ is written in the conventional manner (Obs. 13.3) as a product of disjoint cycles, as $\pi = \pi_1 \pi_2 \ldots \pi_t$. Since the order of a $k$-cycle is clearly $k$ (see Prop.

13.6(i) below), we have $\sum_{i=1}^{t} |\pi_i| = n$ and so the cycle lengths/orders form a partition of $n$. The set $\{|\pi_1|, |\pi_2|, \ldots, |\pi_t|\}$ of cycle lengths is called the *cycle structure* of $\pi$. Thus, for each $1 \leq k \leq n$, there are $p(n, k)$ possible cycle structures for a permutation $\pi \in S_n$ which is a product of $k$ pairwise disjoint cycles when using the conventional notation in Observation 13.3.

**Proposition 13.6.** *(i) If $\pi \in S_n$ is a $k$-cycle then $|\pi| = k$.*
*(ii) More generally, if $\pi_1, \pi_2, \ldots, \pi_t$ are pairwise disjoint $k_i$-cycles, $i = 1, \ldots, t$, then*

$$|\pi_1\pi_2 \ldots \pi_t| = \mathit{LCM}(|\pi_1|, |\pi_2|, \ldots, |\pi_t|) = \mathit{LCM}(k_1, k_2, \ldots, k_t).$$

*(iii)*

$$(x_1\, x_2\, \ldots\, x_k)^{-1} = (x_1\, x_k\, x_{k-1}\, \ldots\, x_2).$$

PROOF: (i) It is clear that the order of a $k$-cycle is just $k$ - in other words, a cyclic shift of $k$ numbers must be performed $k$ times to get back the initial configuration.

(ii) First note that, for *any* two commuting elements $g_1$ and $g_2$ of *any* finite group $G$, $|g_1g_2|$ will be a divisor of LCM($|g_1|$, $|g_2|$). For, since the $g_i$ commute, $(g_1g_2)^s = g_1^s g_2^s$ for any $s \in \mathbb{Z}_+$ and thus $g_1^s = g_2^s = 1 \Rightarrow (g_1g_2)^s = 1$.

Now let $\pi = \pi_1 \ldots \pi_t$ be a product of pairwise disjoint cycles. If $s$ is not a multiple of LCM($|\pi_1|, \ldots, |\pi_t|$) then there will be some $i$ for which $\pi_i^s \neq 1$. But the remaining cycles never interact with $\pi_i$ since they only move around disjoint sets of numbers. Hence $\pi^s$ can't be the identity function either.

(iii) This is obvious. Think of $\pi$ as a clockwise shift with $x_1$ at 12-o'clock. Then $\pi^{-1}$ is instead an anti-clockwise shift with $x_1$ still at 12-o'clock.

Recall that the Stirling numbers of the second kind $S(n, k)$ counted the number of ways to place $n$ distinguishable balls in $k$ identical bins so that no bin was left empty. It's natural to ask: what are Stirling numbers of the *first* kind ? Well, here's the answer:

**Definition 13.7.** Let $n, k \in \mathbb{Z}_+$ with $k \leq n$. The *Stirling number of the first kind* $s(n, k)$ is the number of permutations $\pi \in S_n$ which are a product of exactly $k$ pairwise disjoint cycles, using the conventions of Observation 13.3.

We then have the following analogue of Theorem 6.3:

**Theorem 13.8.**

$$\begin{aligned} \forall\, n \in \mathbb{Z}_+ :\ & s(n, n) = 1, \\ \forall\, n \in \mathbb{Z}_+ :\ & s(n, 1) = (n-1)!, \\ \forall\, n \in \mathbb{Z}_+,\ 2 \leq k \leq n :\ & s(n+1, k) = n \cdot s(n, k) + s(n, k-1). \end{aligned} \tag{13.2}$$

PROOF: (i) If $\pi \in S_n$ is a product of $n$ p.d. cycles, then each cycle must have length $1$ and hence $\pi$ can only be the identity permutation. This proves that $s(n, n) = 1\ \forall\, n$.

(ii) If $\pi \in S_n$ has just one cycle, then this cycle has length $n$ (recall the convention that fixed points are included as cycles of length one) and hence $\pi = (1\, x_2\, x_3\, \ldots\, x_n)$, where $x_2x_3 \ldots x_n$ is an arbitrary permutation of $23 \ldots n$. Hence there are $(n-1)!$

possibilities for $\pi$. Another way to look at it is that $s(n,\,1) = \frac{n!}{n}$ since there are are $n$ possible choices of the "base point" for a given $n$-cycle.

(iii) Fix $n,\,k$ and consider the following two options for a permutation $\pi \in S_{n+1}$ which is a product of $k$ p.d. cycles:

*Case 1:* $\pi(1) = 1$. Then $\pi = \pi_1\pi^*$, where $\pi_1 \in S_1$ and $\pi^*$ is some permutation of $2,\,3,\,\dots,\,n+1$. Thus $\pi^*$ can be considered as an element of $S_n$. If $\pi$ has $k$ p.d. cycles then $\pi^*$ has $k-1$ p.d. cycles. There are thus $s(n,\,k-1)$ possibilities for $\pi^*$ and hence also for $\pi$.

*Case 2:* $\pi(1) \neq 1$. Firstly, there are $n$ options for $\pi(1)$. Hence, by AP and MP, in order to prove (13.2) it remains to prove that, for any given $i \in \{2,\,\dots,\,n+1\}$, if $\pi(1) = i$ then there are $s(n,\,k)$ possibilities for $\pi$. We will do so by describing a simple 1-1 correspondence $\pi \leftrightarrow \pi^*$, where $\pi$ is a permutation of $1,\,\dots,\,n+1$ with $k$ p.d. cycles and satisfying $\pi(1) = i \neq 1$ for some fixed $i$, while $\pi^*$ is an *arbitrary* permutation of $2,\,\dots,\,n+1$ with $k$ p.d. cycles.

We write $\pi$ using conventional cycle notation and it will look like

$$\pi = (1\,i\,\dots)\sigma$$

where $\sigma$ is some product of $k-1$ p.d. cycles on some subset of $\{2,\,3,\,\dots,\,n+1\}$. We then just set

$$\pi^* := (i\,\dots)\sigma$$

and it is clear that $\pi \leftrightarrow \pi^*$ is a 1-1 correspondence and that $\pi^*$ can be *any* permutation of $2,\,\dots,\,n+1$ with $k$ p.d. cycles.

**Remark 13.9.** It is now natural to ask what is the relationship between Stirling numbers of the first and second kinds. In words, there is a many-to-one correspondence between the permutations counted by the numbers $s(n,\,k)$ and the distributions of balls into bins counted by the numbers $S(n,\,k)$. But "how many" depends on the cycle structure of a permutation. Let's just do an example. Let $\pi \in S_7$ be given by

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

So $\pi$ is a product of two disjoint cycles. The obvious corresponding distribution of 7 distinguishable balls into 2 identical bins is that one bin receives balls 1,2,3,4 and the other gets balls 5,6,7. That the bins are identical corresponds to the fact that the cycles commute: $(1\,2\,3\,4)(5\,6\,7) = (5\,6\,7)(1\,2\,3\,4)$. However, there are many different permutations which correspond to the same distribution of balls, namely any permutation of the form $\sigma = \sigma_1\sigma_2$, where $\sigma_1$ is some cycle on $1, 2, 3, 4$ and $\sigma_2$ is some cycle on $5, 6, 7$. From the argument in the proof of Theorem 13.8(ii), there are $(4-1)! = 3! = 6$ possibilities for $\sigma_1$ and $(3-1)! = 2! = 2$ possibilities for $\sigma_2$. Hence there are $6 \cdot 2 = 12$ different permutations in $S_7$ which all correspond to the same distribution of balls into bins as $\{1,\,2,\,3,\,4\} \cup \{5,\,6,\,7\}$.

**Definition 13.10.** A 2-cycle is called a *transposition*. If $\pi = (i\,j)$ we say that $\pi$ *transposes* $i$ and $j$.

**Proposition 13.11.**

$$(1\,2\,3\,\ldots\,k) = (1\,2)(1\,3)\ldots(1\,k).$$

PROOF: By staring.

It follows that every permutation on a finite set can be written as a product of transpositions (this is also "intuitively obvious"). Note, by the way, that a transposition is its own inverse. Hence, if we write a permutation as a product of transpositions then its inverse is just the same product of transpositions backwards:

$$\pi = \tau_1\tau_2\ldots\tau_r \;\Leftrightarrow\; \pi^{-1} = \tau_r\ldots\tau_2\tau_1. \tag{13.3}$$

However, it is also clear that there are, in general, many different ways to perform a given permutation as a composition of transpositions. This motivates the next definition:

**Definition 13.12.** A permutation on a finite set is said to be *even* (resp. *odd*) if it can be written as a product of an even (resp. odd) number of transpositions.

**Theorem 13.13.** *A permutation cannot be both even and odd.*

PROOF: There are various ways to explain this (see Remark 13.14 below), but we will do so using the concept of *permutation matrix*, which you have already encountered in linear algebra. Recall that every $\pi \in S_n$ corresponds to left-multiplication by a matrix $M_\pi \in \mathbb{M}_n(\mathbb{R})$

$$\begin{pmatrix} \pi(1) \\ \pi(2) \\ \cdot \\ \cdot \\ \cdot \\ \pi(n) \end{pmatrix} = M_\pi \begin{pmatrix} 1 \\ 2 \\ \cdot \\ \cdot \\ \cdot \\ n \end{pmatrix}.$$

The matrix $M_\pi$ is obtained from the identity matrix $I_n$ by a permutation of its rows, namely: the $i$:th row of $M_\pi$ is the $\pi(i)$:th row of $I_n$, for each $i = 1, \ldots, n$. Now recall from linear algebra that

(a) If we permute two rows of $I_n$ then we get a matrix with determinant $-1$.
(b) For any two $n \times n$ matrices $A$ and $B$ one has det$(AB)$ = det$(A)\cdot$ det$(B)$.
(c) Composition of linear transformations corresponds to matrix multiplication.

From (c) it follows that $M_{\pi_1\pi_2} = M_{\pi_2\circ\pi_1} = M_{\pi_2}M_{\pi_1}$. Then from (a) and (b) it follows that

$$\pi \text{ is an even permutation} \Leftrightarrow \det(M_\pi) = +1$$
$$\pi \text{ is an odd permutation} \Leftrightarrow \det(M_\pi) = -1.$$

In particular, a permutation can't be both odd and even, v.s.v.

**Remark 13.14.** In the textbook, Theorem 13.13 is proven using the concept of inversion. For $1 \leq i < j \leq n$, the permutation $\pi \in S_n$ is said to *invert* the pair $(i,\, j)$ if $\pi(i) > \pi(j)$. The number of *inversions* in $\pi$, denoted inv$(\pi)$, is the number of pairs it inverts. One first shows that, if $\tau$ is a transposition, then inv$(\tau)$ is always an odd number. From there one deduces that

$$\pi \text{ is an even permutation} \Leftrightarrow \text{inv}(\pi) \text{ is an even number}$$
$$\pi \text{ is an odd permutation} \Leftrightarrow \text{inv}(\pi) \text{ is an odd number.}$$

For details, see Vol. 2, Sats 5.1.

**Notation 13.15.** Since a sum of two even numbers is even, a product of two even permutations is also even (since we just concatenate transpositions). In other words, the set of even permutations in $S_n$, for a fixed $n$, is closed under the group operation and hence is a subgroup of $S_n$. This subgroup is denoted $A_n$, and usually referred to as the *alternating group of order* $n$.

**Proposition 13.16.** $|A_1| = 1$ *and, for each* $n \geq 2$, $|A_n| = n!/2$.

PROOF: If $n = 1$ then the only permutation is the trivial one, which is a product of zero transpositions, hence even.

Now let $n \geq 2$ be fixed. To simplify notation, set $H := A_n$ and $G := S_n$. We already noted above that $H$ is a subgroup of $G$. Hence, by Proposition 9.10, $G$ can be partitioned into (right) cosets of $H$. One such coset is $H$ itself. Secondly, if $\pi$ is any odd permuation then $H\pi \neq H$ since every element of $H\pi$ is of the form $\sigma\pi$ where $\sigma$ is even, hence $\sigma\pi$ will always be odd. Now what we want to show is that $|H| = \frac{1}{2}|G|$, hence that there are exactly two cosets of $H$ in $G$. It thus just remains to show that, if $\pi_1$ and $\pi_2$ are any two odd permutations, then $H\pi_1 = H\pi_2$. But this is also obvious since $H\pi_1 = H\pi_2 \Leftrightarrow H = H\pi_1\pi_2^{-1} \Leftrightarrow \pi_1\pi_2^{-1} \in H$. But $\pi_1$ and $\pi_2$ are both odd, hence so also is $\pi_2^{-1}$ (see (13.3)) and thus $\pi_1\pi_2^{-1}$ will be even, v.s.v.

**Remark 13.17.** The alternating groups are important objects in the study of finite groups. For example the group $A_5$ is the group of symmetries of an icosahedron, one of the Platonic solids. For each $n \geq 5$, the group $A_n$ is *simple*. A group $G$ is said to be simple if it has no *normal* subgroups except itself and $\{1\}$. A subgroup $H$ of a group $G$ is said to be normal if left- and right-cosets of $H$ coincide: in the notation of Homework 2, Exercise 10, if $G = N_G(H)$. In an abelian group, every subgroup is normal, but this is rarely the case in non-abelian groups[1]. The most important property of a normal subgroup is that its cosets can be "multiplied": since left- and right- cosets coincide we have

$$(Hx)(Hy) \overset{\text{assoc.}}{=} H(xH)y = H(Hx)y \overset{\text{assoc.}}{=} HH(xy) \overset{H \text{ subgp.}}{=} Hxy.$$

[1] There are some examples of non-abelian groups in which every subgroup is normal.

It turns out that the cosets thereby form a group, called the *quotient group*[2] $G/H$.

Informally then, a normal subgroup $H$ of $G$ yields a "factorisation" of $G$ into subgroup $H$ and quotient group $G/H$. A simple group is therefore the closest analogy in group theory to the notion of a prime number in arithmetic. One of the most famous problems solved during the 20th century was that of classifying *all* finite simple groups. The so-called *Classification of the Finite Simple Groups* is generally regarded as one of the most complicated proofs of the "pre-computer age". It wasn't accomplished by one person in one paper, but rather was the result of the combined efforts of many authors over a period of perhaps 30 years, up to the early 1980s. Since then, efforts have been made to write down a complete proof in one place, but even the shortest complete proofs are still several thousand pages long.

**Example 13.18. (Femtonspelet)** You've probably all seen the case $n = 4$ of this well-known children's game. You have an $n \times n$ square with $n^2 - 1$ tiles, each showing one of the numbers $1$ through $n^2 - 1$. You can move the tiles around with the help of the "empty tile" and the goal is to get the tiles in the right order, that is, in increasing order from left to right and top to bottom, with the empty tile in the bottom right-hand corner. Usually, this is also the location of the empty tile at the outset. So the question is: for which starting configurations can one solve the game ?

To answer this, we assume the empty tile is indeed in the bottom right-hand corner at the outset and consider the initial configuration of numbered tiles as an element $\pi \in S_{n^2}$. In words:

- for $1 \leq i \leq n^2 - 1$, $\pi(i)$ is the number on the tile in position $i$, where we read positions in increasing order from left to right and top to bottom
- $\pi(n^2) = n^2$, meaning that the empty tile is in the bottom-right position.

Now note that each move involves sliding one of the numbered tiles adjacent to the empty tile into the latter position. In terms of permutations of $[n^2]$, this is a transposition. This transposition must move the empty tile and, since in the final configuration it is supposed to be back where it started, the total number of moves performed in a solution of the game must be an even number. Hence, the initial configuration must be given by an even permutation $\pi$. In particular, this means that there are initial configurations (at least half of all possible configurations, by Proposition 13.16) for which the game can't be solved.

It remains to answer whether the game *can* always be solved if the initial configuration is an even permutation in $S_{n^2}$. Note that this is not immediately obvious, since each move is a transposition involving the empty tile, hence, when considered in terms of permutations of $[n^2]$, is a transposition involving a specific number, namely $n^2$. In other words, we are not allowed to write $\pi$ in any way we like as a product of transpositions, but only transpositions each of which involves the number $n^2$. It nevertheless turns out that a solution is always possible. We hop over the proof, but see Projektövning 5.22 in Vol. 2 for the case $n = 4$.

[2] In particular, one can always form the quotient of an abelian group by a subgroup, since all subgroups are in that case normal. This is analogous to the construction of *quotient spaces* in linear algebra (addition of vectors is always commutative).