Week 1 Summary

- Slogan: numbers measure size, groups measure symmetry
- A group is a set G together with an operation $*: G \times G \to G$ satisfying:

$$(A) \quad (a*b)*c = a*(b*c) \quad \forall a,b,c \in G$$

$$(Id) \quad \exists e \in G: \quad a*e = e*a = a \quad \forall a \in G$$

$$(Inv) \quad \forall a \in G \; \exists b \in G: \quad a*b = b*a = e$$

we denote our group $(G,*)$.

- The set of symmetries of a polygon together with composition forms a group.
- Many familiar sets of numbers are groups (with one of the familiar operations):
  $(\mathbb{C}^\times, \cdot)$; $(\mathbb{Z}, +)$; $(\mathbb{Q}_{>0}, \cdot)$ ...
- Groups can be finite (if the underlying set is finite) or infinite. The order of a group $(G,*)$ is the cardinality of G.
- Two elements a, b of a gp commute if $a*b = b*a$.
- Groups in which all elements commute are called commutative or Abelian.
  (they are called non-abelian otherwise).

Lecture 3

1.3 A fundamental example: Permutation groups

We will now introduce a family of finite groups which will constitute a fundamental example throughout our study of groups. These groups arise as groups of bijections of a given (finite) set. We shall see later on that in some sense these groups are "the" example, as every finite group can be thought of – in a very precise sense – as a subgroup of a permutation group. (This is a famous theorem of Cayley)
We shall also see soon that we already met (in disguise) some permutation groups.

Definition Let S be a finite (nonempty) set.

- A **permutation** of S is a bijection from S onto S.
- We will denote $\mathrm{Sym}(S)$ the set of all permutations of S.

Facts – A map $f: S \to S$ has an inverse if and only if it is a bijection
– The composition of maps is associative.

With these definitions and facts at hand, we can give the following

Theorem / Definition The set of all permutations of a nonempty set S is a group with respect to composition. We call this group the **symmetric group on S**, denoted $(\mathrm{Sym}(S), \circ)$.

When $S = \{1, \dots, n\} =: [n]$ is the set of the first n positive integers, we typically write S_n for $\mathrm{Sym}([n])$.

Example • $S = \{v_1, v_2, v_3\}$
An element in $\mathrm{Sym}(S)$ is f defined by $\begin{cases} f(v_1) = v_2 \\ f(v_2) = v_3 \\ f(v_3) = v_1 \end{cases}$, with inverse $\begin{cases} f^{-1}(v_1) = v_3 \\ f^{-1}(v_2) = v_1 \\ f^{-1}(v_3) = v_2 \end{cases}$

If g is $\begin{cases} g(v_1) = v_2 \\ g(v_2) = v_1 \\ g(v_3) = v_3 \end{cases}$. Then $f \circ g$ is given by: $\begin{cases} (f\circ g)(v_1) = f(g(v_1)) = f(v_2) = v_3 \\ (f\circ g)(v_2) = f(g(v_2)) = f(v_1) = v_2 \\ (f\circ g)(v_3) = f(g(v_3)) = f(v_3) = v_1 \end{cases}$

Can you express $(f\circ g)^{-1}$ in terms of f^{-1} and g^{-1}? How?

When $S = [n]$, there is a convenient way to represent permutations. In this case we typically write S_n for $\mathrm{Sym}([n])$, and for a bijection of $[n]$ onto itself we use two-line arrays of the form

$$\begin{pmatrix} 1 & 2 & \dots & k-1 & n \\ f(1) & f(2) & \dots & f(k-1) & f(n) \end{pmatrix}.$$

(we will often use greek letters for elements of S_n)

For instance, if in the example above we identify $\{V_1, V_2, V_3\}$ with $\{1,2,3\}$ then

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & \end{pmatrix}$$

Inverses and compositions are easily identified:

- if $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ to get the inverse we simply read the two-lines array from below and reorder i

$$\rightsquigarrow f^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$ as we expected from the example above.

- if f and g are as above then $f \circ g$ is obtained by "chasing" the image of $1, \dots n$ going from the right to the left in the composition

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

The identity element of S_n is then $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$

For $n=3$, S_3 consists of 6 elements:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

For $n=1$ and $n=2$ S_n is very small (order 1 and 2 respectively), and commutative.
For $n=3$, it is <u>not</u> commutative (you can easily check that $g \circ f$ from the example above is not the same element as $f \circ g$).

The following holds.

Theorem
- The <u>order</u> of S_n is $n!$
- For $n \geq 3$, S_n is <u>non-Abelian</u>.

Elements of S_n can be also represented using the so-called <u>cycle notation</u>. This notation is more compact and proves particularly useful when looking at certain group-theoretic features.

If $a_1 \dots a_k \in S$ then $(a_1 \dots a_k)$ denotes the permutation for which

a_1 has image a_2
a_2 " " a_3
$\vdots$
a_{k-1} has image a_k and a_k "goes back" to a_1

All elements of S not appearing in the <u>k-cycle</u> are left unchanged by the permutation.

A one-cycle is the permutation sending every element to itself.

Examples • $n=6$ and $\alpha=(2534)$, then in the two-line notation we have:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 2 & 3 & 6 \end{pmatrix}$$

[note that 1 and 6 are fixed pts as they don't appear in the 4-cycle]

• $n=6$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 1 & 5 \end{pmatrix}$

To write β in cycle notation we begin with $1 \mapsto 4 \mapsto 6 \mapsto 5$ noting that these first four constitute a first cycle: β moves elements outside this cycle, too. The smallest choice outside this four-cycle is 2 which has image 3, which has in turn image 2: $2 \mapsto 3$

Therefore β consists of the product of one 4-cycle and the 2-cycle:

$\beta = (1465)(23)$ note: cycles are composed just as any permutations. We will omit the "$\circ$".

⚠ When using the cycle notation, it should be clear from the context what "n" we are dealing with, as this information is not explicit in this notation. For instance, in the example above $\alpha \in S_6$, but also $\alpha \in S_5$ and $\alpha \in S_n$ for $n \geq 7$.

Inverses and compositions with cycle notation: • if $\alpha = (a_1 \dots a_k)$ then $\alpha^{-1} = (a_k a_{k-1} \dots a_1)$

•• composition is easily explained through an example.

If $\alpha=(2534)$ and $\beta=(1465)(23)$ as above, then to obtain an expression for $\alpha\circ\beta$:

$\alpha\circ\beta = (2534)(1465)(23)$

Start with 1, move to its image going right within its cycle (so: $1 \mapsto 4$), then move to the cycle to its left and find the image of 4 (so: $4 \mapsto 2$).
All in all: $1 \mapsto 2$.
Then find "the rightmost 2". In this case it is in the cycle (23). Chase its image going right within a cycle and scrolling cycles to the left.
In our case: $2 \mapsto 3 \mapsto 4$; so $2 \mapsto 4$
and so on:
(124635) It already contains all elements, so we're done!

We will use the following fact:

Theorem Any permutation of a finite set is either a cycle or it can be written as a product of pairwise disjoint cycles. This decomposition is unique up to the order of the cycles.