Week 2 Summary (through an exercise) + Facts from homework.

Let $A_n := \{\text{even permutations}\} \subseteq S_n$ (bijections of $\{1 \dots n\}$; it is a group under composition (of bijections): the symmetric group)

every permutation can be written as product of 2-cycles, or transpositions. There are many ways to do this, but for a permutation the no. of transpositions will always be even (we call this an even permutation) or always be odd (we call this an odd p.)

Example for $n=4$: $(13)(24) \in A_4$; $(123) = (12)(23) \in A_4$; $e = (12)(12) \in A_4$ ...

Exercise Show that A_n is a subgroup (a subset of a group which is a group) of S_n (of order $\frac{n!}{2}$)

To show that $A_n \subseteq S_n$, we use the criterion from last week:

> $H \subseteq G$ is a subgroup
> $\Leftrightarrow$ it is nonempty and
> - for all $g \in H$ $g^{-1} \in H$
> - for all $g, h \in H$ $g \cdot h \in H$.

→ A_n is non-empty as the identity $e = (12)(12)$ is always an even permutation.

→ Let $\alpha \in A_n$. This means α = product of an even no. of transpositions.

Then by Problem 2(i), α^{-1} is the product of the same transp. in reverse order

$\Rightarrow \alpha^{-1}$ again product of even no. of transp. $\Rightarrow \alpha^{-1} \in A_n$

→ Let $\alpha, \beta \in A_n$. Then $\alpha \cdot \beta$ can be written as product of an even no. of transpositions (simply those of α and those of β together..)

$\Rightarrow \alpha\beta \in A_n$.

Therefore, $A_n \subseteq S_n$.

We will prove the statement about the order in few lectures.

1.5 Groups: generation

If $(G,*)$ is a group, then we can, for an element $g \in G$, take the $*$ operation with itself: $g*g$; and iterate: $(g*g)*g$ (which we know is also equal to $g*(g*g)$). In fact, when multiplying an element with itself, associativity ensures the same familiar behaviour of "powers of numbers".

Integral powers of group elements are defined as follows:

if $g \in G$ then:

- $g^0 = e$
- $g^1 = g$
- $g^2 = g*g$, and
- $g^{n+1} = g^n * g$, inductively, for each positive integer n.

Also: $\cdot\ g^{-n} = (g^{-1})^n$ for each positive integer n.

The familiar laws of exponents hold: $-\ g^m * g^n = g^{m+n}$, and

$-\ (g^m)^n = g^{mn}$ for all integers m,n.

Example (1) - a practical rule for powers of k-cycles.

Let $\alpha = (12345) \in S_5$. Then α^2 can be obtained reading the cycle from left to right and writing every 2nd element:

$\alpha^2 = (12345)(12345) = (13524)$

similarly for higher powers: $\alpha^3 = (14325)$, $\alpha^4 = (15234)$ ...

(2) Elements of A_3:

$A_3 = \{e, (123), (132)\}$

we immediately notice that $(123)^2 = (132)$ and $(132)^2 = (123)$

Also $(123)^3 = (123)^6 = \dots = e$

we can try many different exponents, we will always get one of the three elements of A_3.

we will say that A_3 is the cyclic group generated by (123) (or (132)).

Definition If $(G,*)$ is a group and $g \in G$ then $\langle g \rangle$ will denote the set of all integral powers of G:

$$\langle g \rangle := \{ g^n : n \in \mathbb{Z} \}$$

By our observation in Example (2), we have $\langle (123) \rangle = \{e, (123), (132)\}$

The fact that the set of all integer powers of a group element is itself a group is no coincidence. The following holds.

Theorem If $(G,*)$ is a group and $g \in G$ then $\langle g \rangle$ is a subgroup of G.

Terminology.
The subgroup $\langle g \rangle$ is called the subgroup **generated** by g. Subgroups H of a group G which are of the form $H = \langle h \rangle$ for some $h \in H$ are called **cyclic subgroups**

Examples
- $\langle 1 \rangle$ (seen as a subgroup of $(\mathbb{Z},+)$) consists of all "integer multiples of 1". That is, $\langle 1 \rangle = (\mathbb{Z},+)$ is a cyclic group (also $\langle -1 \rangle = (\mathbb{Z},+)$).
- In our very first example (rotations of a regular hexagon) the group $R(H) = \langle \rho_{\pi/3} \rangle$

How do we describe subgroups generated by an elements? What can their order be?
We have seen very different examples: $\langle (123) \rangle$ is a subgroup of S_n of order 3; $\langle \rho_{\pi/3} \rangle$ has order 6, but $\langle 1 \rangle = (\mathbb{Z},+)$ [and you can check that $\langle 2 \rangle \leq (\mathbb{Z},+)$, $\langle 3 \rangle \leq (\mathbb{Z},+)$.. are also so]
The difference is whether there exist or not two **different** exponents for which the two integer powers of the element coincide. If so, the subgroup generated by the element is finite, its order equal the smallest exponent for which the power of the element is the identity, and (and only) exponents which are multiples of the order give the identity. This long list of properties is summarised in the thm below:

Theorem Let $(G,*)$ be a group and $g \in G$. Suppose there exist $r \neq s \in \mathbb{Z}$ such that $g^r = g^s$. Then
(i) There is a smallest positive integer n such that $g^n = e$.
(ii) If $t \in \mathbb{Z}$ then $g^t = e$ if and only if n divides t
(iii) the elements $g^0 = e, g, g^2 \ldots, g^{n-1}$ are distinct and $\langle g \rangle = \{g^0, g, \ldots g^{n-1}\}$

We write $o(g)$ for the **smallest positive integer** n in (i) and call it the **order of the element** g.
By (iii) above we have that the order of g and the order of $\langle g \rangle$ coincide: $|\langle g \rangle| = o(g)$.
If the hypothesis of the theorem is not satisfied, then all powers of the element g are distinct (this can only happen if $|G| = \infty$). $\langle g \rangle$ is still a subgroup, but has ∞ order.

Examples (1) $\langle (1234) \rangle \leq S_4$ is a group of order 4 (what are its elements?)
(2) $\langle i \rangle \leq (\mathbb{C}^\times, \cdot)$ is also a group of order 4 (but in this case the ambient gp is ∞!)
* Have we met this group?

(3) $\langle 2 \rangle \leq (\mathbb{Q}^\times, \cdot)$ is an infinite cyclic group. Why? How do its elements look like?