More on Order of elements, cyclic subgroups.

To understand why ThmA is true, we will need to recall few facts of arithmetic which will be soon useful in order to introduce a new family of gps, and later a new type of algebraic structure.

We will need:

- Least integer principle: Every nonempty set of positive integers contains a least element
- Division algorithm: If $a, b \in \mathbb{Z}$ with $b>0$, then there exist unique integers q and r such that

$$a = bq + r \quad \text{with} \quad 0 \leq r < b.$$

The assumption in ThmA is that $\exists$ distinct r, s with $g^r = g^s$. Suppose $r<s$.
Then multiplying both sides by g^{-r} we get:

$$g^{-r} g^r = g^{-r} g^s$$

which thanks to the laws of exponents becomes

$$e = g^{s-r}$$

So $s-r$ is a positive integer satisfying $g^{s-r} = e \Rightarrow \exists$ a least positive integer with this property. We denote it with $o(g) = n$

It is clear (again, law of exponents!) that for all multiples of the order $t = kn$ $g^t = e$ holds.

The fact that it only holds for integers of this form relies on the division algorithm:

if $g^t = e$ then $g^{nq+r} = e$ for unique q, r with $0 \leq r < n$

$$g^{nq} g^r = e$$

$g^{nq} = e$ by above reasoning $\Rightarrow g^r = e$ contradicting minimality of n among positive integers with this property.

Announcement: the first in-class test will take place on Wednesday, October 9 (Lecture 10)

1.6 Subgroups of S_4

S_4 is a non-abelian group of order 24 (=4!). We can represent its element as cycles / products of disjoint cycles. They can have the following "shapes"

- transpositions (ab)
- 3-cycles (abc)
- 4-cycles (abcd)
- products of disjoint transpositions (ab)(cd)*

Knowing the structure of the elements as products of disjoint cycles will help us identify subgroups.

order 2 subgroups

- Any transposition together with the identity forms a subgroup of S_4 of order 2:

  $\langle(12)\rangle, \langle(13)\rangle, \langle(14)\rangle, \langle(23)\rangle, \langle(24)\rangle, \langle(34)\rangle$

- There are elements* other than simple transpositions which have order 2: each of them with the identity forms a subgroup of order 2:

  $\langle(12)(34)\rangle, \langle(13)(24)\rangle, \langle(14)(23)\rangle$

order 3 subgroups

- we have seen that 3-cycles have order 3 - therefore the cyclic subgroups generated by 3-cycles have order 3:

  $\langle(123)\rangle, \langle(124)\rangle, \langle(234)\rangle$ (why are we not considering $\langle(132)\rangle, \langle(142)\rangle$ .. ?)

order 4 subgroups

- All cyclic groups generated by 4-cycles (which generate different subgroups, re)

  $\langle(1234)\rangle$, $\langle(13)(24)\rangle$, $\langle(1243)\rangle$

- Groups of 4 elements consisting of the identity and elements of order 2 which combine to other elements of order 2:

  $\{e, (12), (34), (12)(34)\}$; $\{e, (13), (24), (13)(24)\}$; $\{e, (14), (23), (14)(23)\}$;

  $\{e, (12)(34), (13)(24), (14)(23)\}$ [can you write any of these as generated by one element?]

order 5 ??

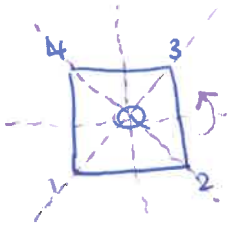
order 6

- $S_3 \leq S_4$ has order 6. Also the symmetric groups which permute 3-elements sets other than [3]:
- $S(\{1,2,4\})$, $S(\{1,3,4\})$, $S(\{2,3,4\})$

order 8

Consider a square and name its vertices 1,2,3,4:

How can we describe the group of symmetries of Q in terms of permutations?



Or in other words, which permutations applied to the vertices of Q give us symmetries of Q?

- the rotations of $\pi/2, \pi, 3\pi/2$ correspond to the 4-cycle (1234) its 2-nd and 3rd power
- flipping along the various axes corresponds to the transpositions or double transpositions:
  (13), (24), (14)(23), (12)(34)

$\rightsquigarrow \{e, (1234), (1234)^2 = (13)(24), (1234)^3 = (1423), (13), (24), (14)(23), (12)(34)\} \leq S_4$
is a subgroup of order 8.

[The groups of symmetries of regular n-gons are called Dihedral groups. This is the dihedral group of order 8.]

Order 9, 10, 11 ..??

Order 12

$A_4 \leq S_4$ has order 12

order between 13 and 23?

Order 24

$S_4 \leq S_4$, trivially.

What do we notice in terms of relationship order of group / order of subgroups?