Foreword

Usage

- Notes are presented in two columns: main notes on the left, and sidenotes on the right. Main notes will have a larger margin.
- The following is the color code for the notes:

Blue	Definitions
Red	Important points
Yellow	Points to watch out for / comment for incompletion
Green	External definitions, theorems, etc.
Light Blue	Regular highlighting
Brown	Secondary highlighting

- The following is the color code for boxes, that begin and end with a line of the same color:

Blue	Definitions
Red	Warning
Yellow	Notes, remarks, etc.
Brown	Proofs
Magenta	Theorems, Propositions, Lemmas, etc.

- Hyperlinks are underlined in magenta. If your PDF reader supports it, you can follow the links to either be redirected to an external website, or a theorem, definition, etc., in the same document. Note that this is only reliable if you have the full set of notes as a single document, which you can find on:
  `https://japorized.github.io/TeX_notes`

6 Lecture 6 May 14th 2018

6.1 Subgroups (Continued 2)

6.1.1 Alternating Groups

Recall that $\forall \sigma \in S_n$, with $\sigma \neq \varepsilon$, σ can be uniquely decomposed (up to the order) as disjoint cycles of length at least 2. We will now present a related concept.

Definition 13 (Transposition)
A ***transposition*** $\sigma \in S_n$ *is a cycle of length* 2, *i.e.* $\sigma = \begin{pmatrix} a & b \end{pmatrix}$, *where* $a, b \in \{1, ..., n\}$ *and* $a \neq b$.

Example 6.1.1
We have that[1]

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

Also, we can show that[2]

$$\begin{pmatrix} 1 & 2 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix} \tag{6.1}$$

Observe that the factorization into transpositions are **not unique or disjoint**. However, the following property is true.

Theorem 10 (Parity Theorem)
If a permutations σ *has* 2 *factorizations*

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_r = \mu_1 \mu_2 \dots \mu_s,$$

[1] If we apply the permutations on the right hand side, we have that

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 \\ & & \downarrow & & \\ 1 & 2 & 3 & 5 & 4 \\ & & \downarrow & & \\ 1 & 4 & 3 & 5 & 2 \\ & & \downarrow & & \\ 2 & 4 & 3 & 5 & 1 \end{array}$$

[2]

Exercise 6.1.1
Show that Equation 6.1 is true.

Exercise 6.1.2
Play around with the same idea and create a few of your own transpositions. Note that you will only be able to get an odd number of tranpositions (why?).

where each γ_i and μ_j are transpositions, then $r \equiv s \mod 2$.

Proof

This is the bonus question in A2. Proof shall be included after the end of the assignment.

Definition 14 (Odd and Even Permutations)

A permutation σ is even (or odd) if it can be written as a product of an even (or odd) number of transpositions. By Parity Theorem 10, a permutation must either be even or odd, but not both.

Theorem 11 (Alternating Group)

For $n \geq 2$, let A_n denote the set of all even permutations in S_n. Then

1. $\varepsilon \in A_n$
2. $\forall \sigma, \tau \in A_n \ \ \sigma\tau \in A_n$ *and* $\exists \sigma^{-1} \in A_n$ *such that* $\sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma$
3. $|A_n| = \frac{1}{2}n!$

Note

*From items 1 and 2, we know that A_n si a subgroup of S_n. A_n is called the **alternating subgroup of degree** n.*

Proof

1. *We have that* $\varepsilon = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}$. *Thus ε is even and so $\varepsilon \in A_n$.*
2. *$\forall \sigma, \tau \in A_n$, we may write*

$$\sigma = \sigma_1\sigma_2 \dots \sigma_r \quad \text{and}$$
$$\tau = \tau_1\tau_2 \dots \tau_s,$$

where σ_i, τ_j are transpositions, and r, s are even integers. Then

$$\sigma\tau = \sigma_1\sigma_2 \dots \sigma_r\tau_1\tau_2 \dots \tau_s$$

is a product of $(r+s)$ transpositions, and thus $\sigma\tau$ is even. THus $\sigma\tau \in A_n$.

For the inverse, note that since σ_i is a transposition, we have that $\sigma_i^2 = \varepsilon$ and thus $\sigma_i^{-1} = \sigma_i$. It follows that

$$\begin{aligned}\sigma^{-1} &= (\sigma_1\sigma_2\dots\sigma_r)^{-1}\\ &= \sigma_r^{-1}\sigma_{r-1}^{-1}\dots\sigma_2^{-1}\sigma_1^{-1}\\ &= \sigma_r\sigma_{r-1}\dots\sigma_2\sigma_1\end{aligned}$$

which is an even permutation and

$$\sigma\sigma^{-1} = \sigma_1\sigma_2\dots\sigma_r\sigma_r\dots\sigma_2\sigma_1 = \varepsilon.$$

Thus $\exists\sigma^{-1} \in A_n$ such that it is the inverse of σ.

3. *Let O_n denote the set of odd permutations in S_n. Then we have $S_n = A_n \cup O_n$, and by the Parity Theorem, we have that $A_n \cap O_n = \emptyset$. Since $|S_n| = n!$, to prove that $|A_n| = \frac{1}{2}n!$, it suffices to show that $|A_n| = |O_n|$.*

   Let $\gamma = \begin{pmatrix}1 & 2\end{pmatrix}$ and $f : A_n \to O_n$ such that $f(\sigma) = \gamma\sigma$. Since σ is even, $\gamma\sigma$ is odd, and so f is well-defined.

   Also, if $\gamma\sigma_1 = \gamma\sigma_2$, then by Cancellation Laws, $\sigma_1 = \sigma_2$, and hence f is injective.

   Finally, $\forall\tau \in O_n$, we have that $\gamma\tau = \sigma \in A_n$. Note that

   $$f(\sigma) = \gamma\sigma = \gamma\gamma\tau = \tau.$$

   Therefore, f is surjective.

   It follows that $|A_n| = |O_n|$. □

For the proof of 3, we know that $|S_n| = n!$, which is twice of the suggested order of A_n. Since we took out the even permutations of S_n, we just need to make the rest of the permutations, the odd permutations, into a set and prove that A_n and this new set has the same size. One way to show this is by creating a bijection between the two.

Also, note that the set of all odd permutations of S_n is not a group, since

- there is no identity element in this set; and
- this set is not closed under map composition.

We have shown that ε is an even permutation, and so by the Parity Theorem, it cannot be an odd permutation, and there is only one identity in S_n. The set is not closed under map composition since if we compose two odd permutations, we would get an even permutation, which does not belong to this set.

6.1.2 Order of Elements

Notation

If G is a group and $g \in G$, we denote

$$\langle\, g \,\rangle = \{g^k : k \in \mathbb{Z}\}.$$

Note that $1 = g^0 \in \langle\, g \,\rangle$.

If $x = g^m, y = g^n \in \langle\, g \,\rangle$ *where* $m, n \in \mathbb{Z}$, *then*

$$xy = g^m g^n = g^{m+n} \in \langle\, g \,\rangle$$

and we have $\exists x^{-1} = g^{-m} \in \langle\, g \,\rangle$ *such that*

$$xx^{-1} = g^m g^{-m} = g^0 = 1.$$

Along with the **Subgroup Test**, we have the following proposition:

Proposition 12 (Cyclic Group as A Subgroup)
If G *is a group and* $g \in G$, *then* $\langle\, g \,\rangle$ *is a subgroup of* G.

Definition 15 (Cyclic Groups)
Let G *be a group and* $g \in G$. *Then we call* $\langle\, g \,\rangle$ *the* ***cyclic subgroup*** *of* G *generated by* g. *If* $G = \langle\, g \,\rangle$ *for some* $g \in G$, *then we say that* G *is a* ***cyclic group***, *and* g *is a* ***generator*** *of* G.