"Appendix to Lecture 3"

Given a permutation, say in cycle notation, we sometimes want to write it as product of 2-cycles (so-called transpositions). This is always possible and not hard. For instance,

$\sigma = (123456)(789) \in S_9$

can be rewritten as $\sigma = (12)(23)(34)(45)(56)(78)(89)$

or $\sigma = (16)(15)(14)(13)(12)(79)(78)$

As we see already from this example, one can write every permutation in various ways as product of sole transpositions. In both cases, σ has been rewritten as product of 7 transposition. As any transposition composed with itself gives the identity, our σ can easily be written as product of $7+2$, $7+4$ transpositions and so on.
So, writing a permutation as a product of transpositions is in no way canonical.
What is "invariant" is the parity of the number of transpositions that can be used to write a permutation as product of transposition:

Fact If a permutation $\sigma \in S_n$ can be written as a product of an odd (resp. even) number of transposition, then every decomposition of σ as product of transpositions will have an odd (resp. even) number of transpositions.

This fact allows us to give the following definition.

Definition · A permutation $\sigma \in S_n$ is called *odd* if it can be written as a product of an odd number of transpositions.
· A permutation $\sigma \in S_n$ is called *even* if it can be written as a product of an even number of transpositions

Example $e \in S_n$ is always an even permutation.

1.4.1 Cayley table: a useful tool for finite groups

If $(G,\star)$ is a finite group, we can use a table which describes the group structure. This table is known as the Cayley table of the group. Rows and columns of the Cayley table are labelled by group elements (typically in the same order → and ↓). The (ij) entry of the table is the result of (i-th label)$\star$(j-th label) [in this order].

For example, it is easy to check that $\{1,-1,i,-i\}$ forms a group under multiplication. Its (multiplication) table is:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Note that:

- every element appears exactly once in every raw and in every column.

This is a general feature of Cayley tables and reflects the fact that in groups the "cancellation laws" hold [See Problem 2]

- This table is symmetric with respect to the main diagonal.

This is a feature of Cayley tables of abelian groups. In fact, a group is abelian if and only if its Cayley table is symmetric.

Finally, note that the 2×2 sub-table

$\cdot$	1	-1
1	...	...
-1	...	...

is itself the Cayley table of the smaller group $\{1,-1\}$ which lies in $\{1,-1,i,-i\}$. We shall say that $(\{1,-1\},\cdot)$ is a subgroup of $(\{1,-1,i,-i\},\cdot)$.

1.4.2 Subgroups

Definition Let $(G,\star)$ be a group. A subset H of G is a subgroup of G if $(H,\star)$ is a group. [When the operation is clear from the context, we will write $H\leq G$ for a subgroup H of G].

Examples (1) We saw that $(\{1,-1\},\cdot)\leq(\{1,-1,i,-i\},\cdot)$.

(2) As $\{1,-1\}\leq\mathbb{R}^\times$, $(\{1,-1\},\cdot)\leq(\mathbb{R}^\times,\cdot)$ also holds.

(3) $(\mathbb{Z},+)\leq(\mathbb{Q},+)\leq(\mathbb{R},+)\leq(\mathbb{C},+)$.

Non-examples

- The odd integers with addition are a subset of $(\mathbb{Z},+)$ but not a subgroup. Why?
- The set $\{(23),(123)\}\subseteq S_3$ is not a subgroup. Why?

[Notation. If we are dealing with more than one group, say $(G,*)$, $(H,\blacktriangle)$, we write e_G for the identity of G and e_H for the identity of H.]

The following facts are not obvious, but they follow easily from the definitions.

Fact
- If $H \leq G$ is a subgroup then $e_H = e_G$
- If $a \in H$ then the inverse of a in H is the same as the inverse of a in G.

The definition of a subgroup doesn't help much when it comes to recognising whether a subset of a group is a subgroup. The fact that the axioms of group are already satisfied by the ambient set (in fact, group) makes it easier to check whether a subset of a group is also a subgroup. This is similar to what happens for vector spaces and their subspaces. For groups, the following fact / criterion holds.

Fact / criterion Let $(G,*)$ be a group and $H \subseteq G$ a subset. Then H is a subgroup if and only if:

- H is nonempty and
- for all $a,b \in H$ $\bar{a}^1 * b \in H$.

Note: the second condition is the short form combining two conditions: (*) { → for all $a,b \in H$ $a * b \in H$, and → for all $a \in H$ also $\bar{a}^1 \in H$.

You can use •• above or both (*) equivalently.

Example (1) The subset $\{e, (123), (132)\} \subseteq S_3$ is a subgroup:

- it is nonempty ✓
- $(123)(123) = (132)$ and $(123)^{-1} = (132)$ therefore the second condition is satisfied.

This is a special type of subgroup of S_n, we will see that it belongs to a family of subgroups.

(2) The set {all 2×2 matrices with rational entries and determinant 1} is a subgroup of the group $(GL(2,\mathbb{Q}),\cdot)$. We denote this group $SL(2,\mathbb{Q})$ (special linear gp).

why?
- it is non-empty: for instance $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in SL(2,\mathbb{Q})$
- if A, B have determinant 1 then $\det(A^{-1}) = 1$ too and $\det(A^{-1}B) = \det(A^{-1})\det(B) = 1$, so $A^{-1}B \in SL(2,\mathbb{Q})$

and therefore it is a subgroup.