Lecture 8 

## 1.8 Groups: isomorphisms and Cayley's thm.

Example Let us consider three groups of order 6: $C_6 = \langle \xi_6 \rangle$, $(\mathbb{Z}_6, +)$, $S_3$.

- $C_6$ and $\mathbb{Z}_6$ are both cyclic (and in particular abelian). One choice of the generators is $\xi_6$ for $C_6$ and $1$ for $\mathbb{Z}_6$.
- $S_3$ is non-abelian, it cannot be generated by a single permutation.

$\langle a \mid a^6 = e \rangle$

| $*$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $e$ |
| $a^2$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $e$ | $a$ |
| $a^3$ | $a^3$ | $a^4$ | $a^5$ | $e$ | $a$ | $a^2$ |
| $a^4$ | $a^4$ | $a^5$ | $e$ | $a$ | $a^2$ | $a^3$ |
| $a^5$ | $a^5$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ |

If we observe the Cayley table of this "abstract" group, we see that substituting "a" with "1" or with "$\xi_6$" gives exactly the Cayley table of $\mathbb{Z}_6$ and of $C_6$, respectively. This is a way to see that the group structure of $\mathbb{Z}_6$ and $C_6$ is essentially the same.
We will say that $\mathbb{Z}_6$ and $C_6$ are isomorphic and write $(\mathbb{Z}_6, +) \cong (C_6, \cdot)$.

There is no way, instead, to match the multiplicative structure of this abstract group with that of $S_3$. For instance, no substitution would result in a non-commutative structure such as that of $S_3$. We will say that $S_3$ is not isomorphic to $\mathbb{Z}_6$ (or $C_6$).

An isomorphism is a special type of homomorphism, which is a map between groups which "preserves" the operation.

Definition (1) A homomorphism between two groups $(G, *)$ and $(H, \diamond)$ is a map $\varphi: G \to H$ such that $\varphi(g * g') = \varphi(g) \diamond \varphi(g')$ $\forall g, g' \in G$.

(2) A homomorphism which is a bijection is called isomorphism

In this context we simply say "homomorphism" and "isomorphism" since we're only talking about groups. In general one should specify the (algebraic) structure in question.

Examples (1)
$$\varphi: \mathbb{Z}_n \to C_n, \quad k \mapsto \xi_n^k$$
(where $\xi_n$ is a generator of $C_n$)

is an isomorphism.

(2)
$$\exp: \mathbb{R} \to \mathbb{R}_{>0}, \quad x \mapsto e^x$$
is a homomorphism (in fact, an isomorphism: $\ln$ is its inverse)

(indeed: $\exp(x \underset{=}{+} y) = e^{x+y} = e^x e^y = \exp(x) \underset{=}{\cdot} \exp(y)$ )

Properties (1) "Preserving" the operation implies that identity and inverses are preserved. That is, if $\varphi: G \to H$ is a homomorphism then $\varphi(e_G) = e_H$ and $\varphi(g^{-1}) = (\varphi(g))^{-1}$

(2) Isomorphisms preserve orders. If $G \cong H$ and $\varphi: G \to H$ is an isomorphism then
$o(\varphi(g)) = o(g)$ $\forall g \in G$

(3) If $G \cong H$ then $G$ is abelian $\Leftrightarrow$ $H$ is abelian.

**Example / definition** The quaternion group $Q_8$. This is a non-abelian group of order 8.

Its elements are $\{\pm 1, \pm i, \pm j, \pm k\}$ and the operation is a multiplication with "rules"

the complex numbers $\pm 1, \pm i$

$$i^2 = j^2 = k^2 = -1 \ , \qquad ij = k$$

All other products can be deduced from these. The Cayley table is

| $\cdot$ | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ | $-j$ | $j$ | $-k$ | $k$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ | $k$ | $-k$ | $-j$ | $j$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ | $-k$ | $k$ | $j$ | $-j$ |
| $j$ | $j$ | $-j$ | $-k$ | $k$ | $-1$ | $1$ | $i$ | $-i$ |
| $-j$ | $-j$ | $j$ | $k$ | $-k$ | $1$ | $-1$ | $-i$ | $i$ |
| $k$ | $k$ | $-k$ | $j$ | $-j$ | $-i$ | $i$ | $-1$ | $1$ |
| $-k$ | $-k$ | $k$ | $-j$ | $j$ | $i$ | $-i$ | $1$ | $-1$ |

> This group was "invented" in 1843 by Hamilton. He got the idea for the multiplication rules as he was walking on Broom bridge in Dublin. Legend says he scratched them in the stone..

We have met at least two other groups of order 8: $\mathbb{Z}_8$ and the group of symmetries of a square $D_4$. These three groups are pairwise non-isomorphic (see Problem 9).

Also, we have seen that $D_4 \leq S_4$ (or better, $D_4$ is isomorphic to a subgroup of $S_4$).

The theorem of Cayley on finite groups says that this can be realised for all finite groups with a "canonical" construction (different, though, from the one we used for $D_4$ in $S_4$).

**Theorem (Cayley)** Let $(G, *)$ be a (finite) group and $S(G)$ the group of permutations on $G$. Then $G$ is isomorphic to a subgroup of $S(G)$.

or, we could write

Let $(G, *)$ a group of order $n$. Then $G$ is isomorphic to some subgroup of $S_n$.

The isomorphism in Cayley's thm is "canonical", but often non-optimal. (For instance, through the geometric representation of $D_4$ we found an isomorphism with a subgroup of $S_4$, while Cayley's thm would have given us only an isomorphism with a subgroup of $S_8$).

**Fact**

$Q_8$ is the smallest group for which Cayley's construction is optimal, i.e. $S_8$ is the smallest permutation group for which $Q_8 \leq S_8$ ($Q_8 \nleq S_k$ for $k \leq 7$).

The idea Cayley's theorem is that multiplication by an element in a group $G$ corresponds to a permutation of all elements of the group. It is easy to see this looking at a Cayley table. For instance, if in the table above we label the elements 1 to 8 from left to right, we could say that left multiplication by: $i$ gives rise to the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 7 & 8 & 6 & 5 \end{pmatrix} = (1324)(5768)$$

" $j$ " "

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 8 & 7 & 2 & 1 & 3 & 4 \end{pmatrix} = (1526)(3847)$$

and so on..

As an exercise, you can compute all permutations of $S_8$ corresponding to elements of $Q_8$ in this way and verify that they form a subgroup.