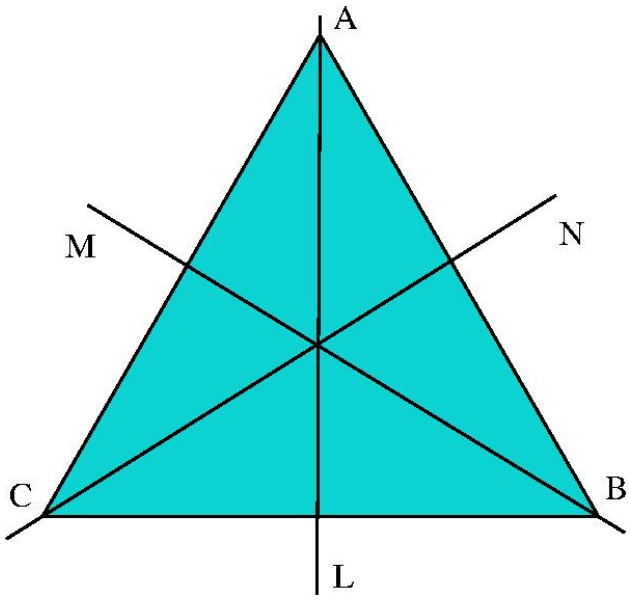
Lecture 18: Cayley's Theorem



$\circ$	id	R_{120}	R_{240}	T_L	T_M	T_N
id	id	R_{120}	R_{240}	T_L	T_M	T_N
R_{120}	R_{120}	R_{240}	id	T_M	T_N	T_L
R_{240}	R_{240}	id	R_{120}	T_N	T_L	T_M
T_L	T_L	T_N	T_M	id	R_{240}	R_{120}
T_M	T_M	T_L	T_N	R_{120}	id	R_{240}
T_N	T_N	T_M	T_L	R_{240}	R_{120}	id

Each row in the table for D_6 details the permutation of the six elements that results from composing everything on the left with the element that labels the row. So we associate to each element of D_6 a different permutation of six objects (which happen to be the six elements of D_6). By taking this view we can interpret D_6 as a subgroup of S_6. This is Cayley's Theorem.

Isomorphism

An isomorphism between groups $(G, \star_G)$ and $(H, \star_H)$ is a bijective function $\phi : G \to H$ with the property that

$$\phi(x \star_G y) = \phi(x) \star_H \phi(y), \text{ for all } x, y \in G.$$

This means that ϕ matches the elements of G with those of H, in a way that matches the group operations too. The groups become identical after relabelling their elements according to the matching.

Example The group of complex 4th roots of unity under multiplication is isomorphic to group of integers modulo 4 under addition.

$(G_4, \times)$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

$(\mathbb{Z}_4, +)$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Cayley's Theorem - statement and outline proof

Theorem (Cayley, 1854) Let G be a group of order n. Then G is isomorphic to a subgroup of S_n.

Outline proof G acts on the set of its own elements by left multiplication. For $g \in G$, we write ϕ_g for the permutation of the elements of G defined by left multiplication by g.

$$\phi_g(x) = gx, \text{ for } x \in G.$$

If $h \in G$ and $h \neq g$, then $\phi_h \neq \phi_g$.
The mapping $g \to \phi_g$ associates to every element of G a permutation of the n elements of G, and these permutations satisfy

$$\phi_{gh}(x) = ghx = g(hx) = \phi_g\phi_h(x), \text{ for all } g, h, x \in G.$$

Moreover ϕ_{id} is the identity permutation and $\phi_{g^{-1}}$ is the inverse of ϕ_g, so the set of all ϕ_g, where $g \in G$, is a group of permutations of n objects that is isomorphic to G.

Lecture 18: Group Homomorphisms

Definition Let G and H be groups, with operations $\star_G$ and $\star_H$ respectively. A function $\phi : G \to H$ is a group homomorphism if

$$\phi(x \star_G y) = \phi(x) \star_H \phi(y),$$

for all elements x, y of G.

Examples of Group Homomorphisms

1. The Determinant The function $\det : \mathrm{GL}(2,\mathbb{R}) \to \mathbb{R}^\times$ is a group homomorphism, since for any matrices A, B in $\mathrm{GL}(2,\mathbb{R})$,

$$\det(AB) = \det(A) \times \det(B).$$

   Note that the multiplication in the left hand side of the above equation is multiplication of 2×2 matrices and the "$\times$" on the right hand side refers to multiplication of real numbers.

2. The logarithm function Let $\mathbb{R}^\times_{>0}$ denote the group of all positive real numbers under multiplication, and let $x, y \in \mathbb{R}^\times_{>0}$. Then $\log(x)$, $\log(y)$ and $\log(x+y)$ are real numbers, and

$$\log(xy) = \log(x) + \log(y).$$

   The function log is a group homomorphism from $\mathbb{R}^\times_{>0}$ to $(\mathbb{R}, +)$, the group of all real numbers under addition. (Note that the choice of base of log does not matter here).

Lemma: $\phi(\mathrm{id}_G) = \mathrm{id}_H$

Let $\phi : G \to H$ be a group homomorphism, and let $x \in G$. Then

$$\phi(x \star_G \mathrm{id}_G) = \phi(x) \star_H \phi(\mathrm{id}_G).$$

Also $\phi(x \star_G \mathrm{id}_G) = \phi(x)$.
In H we have

$$\begin{aligned} \phi(x) \star_H \phi(\mathrm{id}_G) &= \phi(x) \\ \implies \phi(x)^{-1} \star_H \phi(x) \star_H \phi(\mathrm{id}_G) &= \phi(x)^{-1} \star_H \phi(x) \\ \implies \phi(\mathrm{id}_G) &= \mathrm{id}_H . \end{aligned}$$

DefinitionThe kernel of a group homomorphism $\phi : G \to H$ is the subset of G consisting of all those elements whose image under ϕ is id_H.
The image of ϕ is the subset of H consisting of all $\phi(x)$, where $x \in G$.

Examples again

1. $\det : \mathrm{GL}(2,\mathbb{R}) \to \mathbb{R}^\times$
   The kernel is $\{A \in \mathrm{GL}(2,\mathbb{R}) : \det A = 1\}$. This is the special linear group $\mathrm{SL}(2,\mathbb{R})$. It is a subgroup of $\mathrm{GL}(2,\mathbb{R})$.
   The image of det includes all elements of $\mathbb{R}^\times$.
2. The kernel of $\log : \mathbb{R}^\times_{>0} \to (\mathbb{R},+)$ is

$$\{x \in \mathbb{R}_{>0} : \log(x) = 0\} = \{1\}.$$

   The kernel consists only of the identity element of $\mathbb{R}^\times_{>0}\}$. The image of log is the entire group $(\mathbb{R},+)$.

The kernel and image of a group homomorphism $\phi : G \to H$ are subgroups of G and H respectively.

The kernel is a subgroup

Let $\phi : G \to H$ be a homomorphism of groups. The kernel of ϕ is

$$\ker \phi = \{x \in G : \phi(x) = \mathrm{id}_H\}.$$

- $\mathrm{id}_G \in \ker \phi$ - we saw this a couple of slides back
- Suppose $x, y \in \ker \phi$. Then

$$\phi(x \star_G y) = \phi(x) \star_H \phi(y) = \mathrm{id}_H \star_H \mathrm{id}_H = \mathrm{id}_H,$$

  so $x \star_G y \in \ker \phi$ and $\ker \phi$ is closed under $\star_G$.
- Suppose $x \in \ker \phi$. Then

$$\mathrm{id}_H = \phi(x^{-1} \star_G x) = \phi(x^{-1}) \star_H \phi(x) = \phi(x^{-1}) \star_H \mathrm{id}_H = \phi(x^{-1}).$$

  So $x^{-1} \in \ker \phi$.

So $\ker \phi$ is a subgroup of G.