GROUP HOMO-MORPHISMS

Def? **Group homomorphisms**

Let $(G_1, \circ)$ & $(G_2, +)$ be groups.

Let $f: G_1 \to G_2$ be any fn

Consider $a, b, c \in G_1$ s.t. $a \cdot b = c$ &

Consider $f(a \cdot b) = f(c)$.

If $f(a \cdot b) = f(a) + f(b)$ then f is called a homomorphism. i.e. f preserves the alg. structure of G_1 within G_2.

eg. $G_1 = \{e, a, a^2\}$, $G_2 = \{0, 1, 2\}$

Consider $(G_1, \circ)$, $a \cdot a^2 = e$, $\{G_2, +\}$, $1+2 = 0$

& $f: G_1 \to G_2$: $e \mapsto 0$, $a \mapsto 1$, $a^2 \mapsto 2$

Then $f(a \cdot a^2) = f(e) = 0 = 1+2$
$= f(a) + f(a^2)$

$f(a \cdot a) = f(a^2) = 2 = 1+1 = f(a) + f(a)$

f is a hom.

$g: G_1 \to G_2$: $e \mapsto 0$, $a \mapsto 2$, $a^2 \mapsto 1$

$g(a \cdot a^2) = g(e) = 0 = 2+1 =$
$g(a) + g(a^2)$

$g(a \cdot a) = g(a^2) = 1 = 2+2$
$= g(a) + g(a)$: g hom

$h: G_1 \to G_2$: $e \mapsto 1$, $a \mapsto 0$, $a^2 \mapsto 2$

$h(a \cdot a) = h(a^2) = 2$

$h(a) + h(a) = 0+0 = 0 \neq 2$

h not hom.

In fact f & g are both bijections

Def: a gp hom $f: G_1 \to G_2$ that is a bijection is called an isomorphism. → important

if f is injective : monomorphism } Not important
if f is surjective : epimorphism }

if $f: G_1 \to G_1$ is a hom. of this is called an endomorphism

if $f: G_1 \to G_1$ is an isomorphism it is an automorphism (study later)

homomorphisms are usually written φ (or ψ)
They allow us to study the structure of gps w/o concerning ourselves w/ the specific elts.

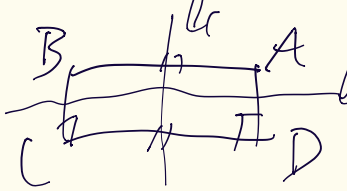
Theorem: The cyclic gp C_n is isomorphic to $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ w/ $+ \pmod n$

Proof: Let $C_n = \langle a \rangle$, $a^n = e$
Let $\varphi: C_n \to \mathbb{Z}_n : \varphi(a^i) = i \pmod n$
Then $\varphi(a^i a^j) = \varphi(a^{i+j}) = (i+j) \bmod n = i \bmod n + j \bmod n$
$= \varphi(a^i) + \varphi(a^j)$. φ Clearly bijective
Hence φ an isomorphism $\square$

HW Prove $C_\infty = \mathbb{Z}$

eg some isomorphism of Symmetries of torus.

Aletsar: 42–55

Consider 

Rotation by $\pi = 180°$

$R = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$

Flips along l_1: $F_1 = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$ & l_2: $F_2 = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$

Note $R^2 = e$, $F_1^2 = e$, $F_2^2 = e$

Cayley table:

	e	R	F_1	F_2
e	e	R	F_1	F_2
R	R	e	F_2	F_1
F_1	F_1	F_2	e	R
F_2	F_2	F_1	R	e

Consider $C_4 = \langle \alpha \rangle$, $\alpha^4 = e$

Cayley table:

	e	α	α^2	α^3
e	e	α	α^2	α^3
α	α	α^2	α^3	e
α^2	α^2	α^3	e	α
α^3	α^3	e	α	α^2

	e	α^2	α	α^3
e	e	α^2	α	α^3
α^2	α^2	e	α^3	α
α	α	α^3	α^2	e
α^3	α^3	α	e	α^2

Thm: $G_1 \cong G_2$ iff their Cayley tables have same structure after relabelling

HW Prop

Theorem (hom. & identity)
Let $(G,\cdot)$ & $(H,+)$ be gps w/ $e_G \in G$ & $e_H \in H$
Let $\varphi: G \to H$ be hom. Then $\varphi(e_G) = \varphi(e_H)$

Proof: Note $e_G \cdot e_G = e_G$. So

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) + \varphi(e_G)$$

Add $\varphi(e_G)^{-1}$ to both sides

$$= \varphi(e_G)$$

$$e_H \quad \varphi(e_G) - \varphi(e_G) = \varphi(e_G) + \varphi(e_G) - \varphi(e_G) = \varphi(e_G)$$

□

Corollary: $\varphi: G \to H$ hom. Then $\varphi(g^{-1}) = \varphi(g)^{-1}$

Proof: $\varphi(e_G) = \varphi(g \cdot g^{-1}) = \varphi(g) + \varphi(g^{-1}) = e_H$

So $\varphi(g^{-1}) = \varphi(g)^{-1}$ □

Important method for checking hom is order:
Recall $\operatorname{ord}(g) = \min\{n > 0 \mid g^n = e\}$
Thm: Let $\varphi: G \to H$ be a hom. Then
$\operatorname{ord}(\varphi(a)) \mid \operatorname{ord}(g)$
in H in G

Proof: let $\operatorname{ord}(g) = n$, $g^n = e_G$
Then $e_H = \varphi(e_G) = \varphi(g^n) = \varphi(g \cdots g) = \varphi(g) \cdots \varphi(g) = \varphi(g)^n$

So $ord(\varphi(g)) \leq n$, $\varphi(g)^n = e_H$. Let $m = ord(\varphi(g))$

$\varphi(g)^m = e_H$, $\varphi(g)^{m+1} = \varphi(g)$, $\varphi(g)^{m+i} = \varphi(g)^i$, $i = 1, \dots, m-1$

So if $\varphi(g)^n = e_H$ then $n = mk$ so $m \mid n$

Corollary: $\varphi: G \to H$ hom & injective then $ord(g) = ord(\varphi(g))$ $\forall g \in G$ □

Proof: $n = ord(g)$, $\varphi(g^n) = \varphi(g) \dots \varphi(g) = \varphi(g)^n$

injective so only elt mapping to e_H is e_G

So if $\varphi(g)^m = e_H$ then $\varphi(g^m) = e_H$ so $g^m = e_G$

Hence $n \mid m$. from bfor $m \mid n$ so $m = n$ □

Application: If two groups have elts of different orders $\nexists$ a hom between them

eg1 $C_4 = \langle \alpha \rangle$, $\alpha^4 = e$: $ord(\alpha) = 4$ $ord(\alpha^3) = 4$

$ord(\alpha^2) = 2$ $ord(e) = 1$

Plane symmetries of  F_2 $ord(\pi) = 2$

$ord(F_1) = 2$

Different alg. structure F_1 $ord(F_2) = 2$

(Different orders) so no hom.

between C_4 & V_4. → Called Klein 4 group

Ex. Consider $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$
(in $\mathbb{Z}_2$, $1+1=0$)

So $(1,0)+(1,0) = (0,0) = (0,1)+(0,1) = (1,1)+(1,1)$

each non identity $(0,0)$ elt has order 2.

This is a candidate for isomorphism w/ V_4, but is not enough to prove.

Consider $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to V_4$:
$(0,0) \mapsto e$
$(0,1) \mapsto F_1$
$(1,0) \mapsto F_2$
$(1,1) \mapsto R$
} Clear bijection

For a small gp check Cayley table

Then $\varphi((0,1)+(1,0)) = \varphi((1,1)) = R$

$\varphi((0,1)) \cdot \varphi((1,0)) = F_1 \cdot F_2 = R$

$\varphi((1,1)+(1,0)) = \varphi((0,1)) = F_1$

$\varphi((1,1)) + \varphi((1,0)) = R \cdot F_2 = F_1$

In general have to show $\varphi(ab) = \varphi(a)\varphi(b)$ some how?

SUBGROUPS

Subgroups

Consider a gp $(G,\cdot)$ & a subset $H \subseteq G$.
Sometimes $(H,\cdot)$ will be a gp w/ the same operation.
This is called a subgp.

eg The group of rotations of an n-gon is a subgroup of all symmetries of the n-gon

eg if $g \in G$ then $\langle g \rangle = \{e, g, g^1, g^2, \dots\}$ is a subgp of G, called a cyclic subgp.

Theorem: (Basic properties of subgps)
i) If H is a subgp of G then $e_H = e_G$
ii) if $a \in H$ then $a^{-1}_G = a^{-1}_H$

Proof: i) Consider $e_H \cdot e_G = e_H = e_G$
ii) if $a \in H$ then $a \cdot e = a$

$$a^{-1}_H \cdot a = e$$

$$a^{-1}_H = a^{-1}_H \cdot a \cdot a^{-1}_G = e \cdot a^{-1}_G = a^{-1}_G \quad \square$$

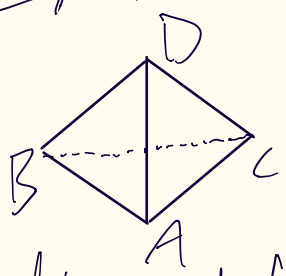
Lec 57-62

Lets discuss types of gps in more detail
We have seen cyclic gps $C_n = \langle \alpha \rangle = \{\alpha^0, \alpha^1, \dots, \alpha^{n-1}\}$
We have seen gps of symmetries of regular n-gons
ie. Rotations & Reflections: These are called Dihedral gps

We have seen gps of permutations of n elts $\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & & a_n \end{pmatrix}$. These are called symmetric gps

Let us introduce another important gp.

Example: Consider a regular tetrahedron (all sides same length)

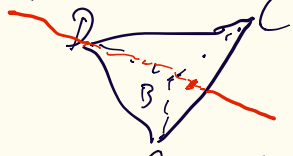


The base is ΔABC

Note we could have ΔACB as a base

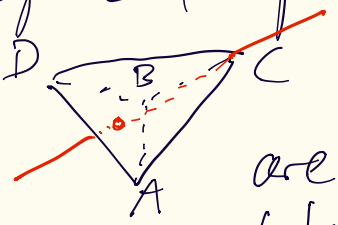
We differentiate between the two and say they have different orientation.

Now consider the transformations that preserve the tetrahedron. eg rotation about the axis passing through D & ΔABC



by $0°, 120°$, or $240°$

These form a cyclic subgroup of S_4 of order 3. $\begin{pmatrix} A & B & C & D \\ \to & & & D \end{pmatrix}$

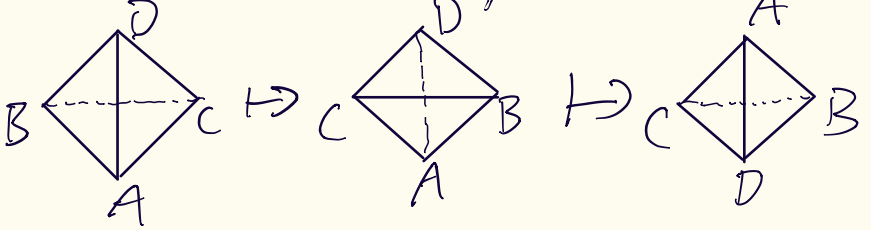


Rotations about from another cyclic subgp.

Note the identities are of course the same.

The four possible axes rotations then make up the identity & 8 other elts of A_4. Are there others?

Yes: consider



i.e. $(AD)(BC)$. These preserve orientation

there are 3 such operations

S_4 → All permutations of $\{A, B, C, D\}$

Note that $\begin{pmatrix} A & B & C & D \\ C & A & B & D \end{pmatrix} = (A\,C\,B)(D) = (AB)(CB)$

Together we have 12 orientation preserving transformations

HW Prove these 12 form a subgp of S_4

Note: How many elts in S_4? $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 \text{ choices} & 3 \text{ choices} & 2 \text{ choices} & 1 \text{ choice} \end{pmatrix}$: $4! = 24$

So there are 12 other transf. preserving $\triangle ABCD$

HW Find them. Show they don't preserve orientation
Show they do not form a subgp. Write all elts as products of transpositions.

HW Find all subgps of S_4

Definition: A regular n-simplex is the smallest (i.e. fewest # of edges) regular polyhedron that may be built in n-1-dimensions that cannot also be built in $n-2$ dim.

eg: a point in 0-dim.
the segment in 1-dim.
$\triangle$ in 2-dim
tetrahedron in 3-dim
5-cell in 4-dim
etc.

i.e. in 2 dim the simplex has 3 vertices we call this the 3-simplex. In literature it is often called 2-simplex

Def: The group S_n of permutations of $1 \ldots n$ is the group of symmetric

transformations of an n-simplex.

This is where the name of S_n, the symmetric group, arises.

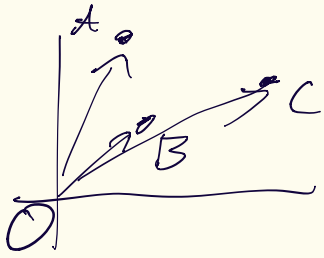
The orientation preserving transformations of the n-simplex form a subset of S_n denoted A_n.

Theorem. A_n is a group for all n, called the alternating group.

Note that we haven't defined clearly what orientation is.

ORIENTATION

Consider an n-simplex in $(n-1)$-dim whose vertices are affine vectors eg $A-O$, $B-O$, $C-O$



Any labelling of the vertices $1 \dots n$ gives an ordering of the vectors $v_1 \dots v_n$

The <u>orientation</u> of the ordering is the sign of the determinant $\det(v_1 \dots v_n)$.

Lemma: transpositions reverse orientation.

Proof: A transposition swaps two vertices i & j. This has the effect of swapping two vectors v_i & v_j in $(v_1 \dots v_i \dots v_j \dots v_n) \mapsto (v_1 \dots v_j \dots v_i \dots v_n)$

This swaps the sign of the determinant. $\square$

Hence the orientation preserving perms in S_4 must be even. In other words a cycle preserves orientation iff it is even.
Since parity is multiplicative permutation product is a binary operation from $A_n \times A_n \to A_n$ & so A_n is a gp.
This proves the theorem.
Put explicitly for easier recall:

Proof: Orientation preserving transp. have even parity, and as parity is mult., $\cdot : A_n \times A_n \to A_n$ is a binary op.
The empty transp. is the identity (exactly as in no nontriv. cycles)
& written as transpositions, inverses are in A_n as inverses are reverse of sequence of transpositions, so clearly even.
This completes the proof. □

HW: Show $|S_n| = 2 \cdot |A_n|$
ie. #even perms = #odd perms
HW Find $|S_n|$

CAYLEY'S THEOREM

We pay particular attention to symmetric groups. Symmetric groups are the groups of all permutations of a set, usually written

S_n = Permutations of $1, \ldots, n$.

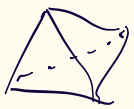
Such a permutation can be written in "cycle" notation, which we study in detail later.

eg $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$ means

$1 \mapsto 2$
$2 \mapsto 1$
$3 \mapsto 3$
$4 \mapsto 5$
$5 \mapsto 4$

Def'n An n-simplex is the smallest polyhedron one can form in n-dimensions, but not in (n-1)-dim.

eg △ - simplex in 2-D □ - not (△ is smaller)

 simplex in 3-D, can't be formed in >D

— simplex in 1-D, but not in 2D as it's "too" simple.

Note the n-simplex has (n+1) vertices & edges.

Symmetric groups arise from simplices

Def'n Symmetric group S_n is the group of symmetric transformations of an $(n-1)$-simplex

HW: Prove both definitions are equivalent.

Symmetric are central objects of study in group theory:

Theorem (Cayley's Theorem)

Every group is isomorphic to a subgroup of some symmetric group.

Proof: Abstract Algebra II