LN IX a

§5.1 continued

Let $(G,\cdot)$ be a group.

$g \in G$. If there is no $n \geq 1$ such that $g^n = e$ then g is of infinite order.

If there is a finite $n \geq 1$ with $g^n = e$. then the smallest such n is called the order of g

Lemma: If g has finite order n then $g^r = g^s \Longleftrightarrow r \equiv s \mod n$.

Proof is similar as ~~the~~ in the case of permutations.

- If G is finite every element has finite order
- $Gl(n, \mathbb{R})$ invertible $n \times n$ matrices

$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = A$ has infinite order.

$$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \forall n \geq 1.$$

- The same matrix over the field $\mathbb{Z}_p$, p prime,

$$A = \begin{pmatrix} [1]_p & [1]_p \\ [0]_p & [1]_p \end{pmatrix}.$$

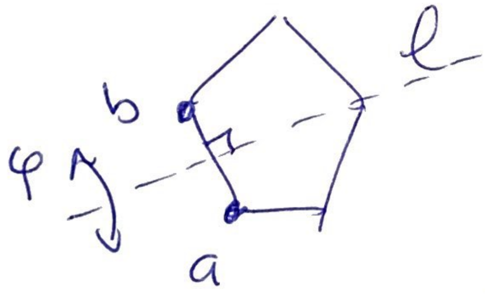
$$A^p = \begin{pmatrix} [1]_p & [p]_p \\ [0]_p & [1]_p \end{pmatrix} = \begin{pmatrix} [1]_p & [0]_p \\ [0]_p & [1]_p \end{pmatrix}$$

$= id.$

A subset $H \subset G$ is called a subgroup of G if it is itself a group with the same operation as G.

Ex] $(2\mathbb{Z}, +) \subset (\mathbb{Z}, +)$

Ex] The symmetries of the pentagon which fixe a specific side $[a,b]$ = $\{id, \varphi\}$ where φ is the reflection wrt. ~~axis~~ line $\ell \perp [a,b]$



How to decide whether a subset is a subgroup?

<u>Prop</u> $(G, \cdot)$ group and $H \subset G$.
The following statements are equivalent.

1) $H \subset G$ is a subgroup

2) $h \in H \Rightarrow h^{-1} \in H$ and
$h, k \in H \Rightarrow hk \in H$

3) $h, k \in H \Rightarrow hk^{-1} \in H$.

Pf) We need to prove.

$$1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 1).$$

<u>1) ⇒ 2)</u> ok

<u>2) ⇒ 3)</u> $h, k \in H \overset{2}{\Rightarrow} h \in H$ and $k^{-1} \in H$
$\overset{2}{\Rightarrow} hk^{-1} \in H$

<u>3) ⇒ 1)</u> We need to show all group properties.

- associativity

If $a,b,c \in H$ and $(ab)c \in H$ $a(bc) \in H$ then $(ab)c = a(bc)$.

- identity

$h \in H \xRightarrow{3)} \cancel{hh}^{-1} \in H$. So $e \in H$.

hh^{-1}

- inverse

$\left.\begin{matrix} g \in H \\ e \in H \end{matrix}\right\} \xRightarrow{3)} eg^{-1} \in H$. But $eg^{-1} = g^{-1}$.

- closed

$g, h \in H$. then $h^{-1} \in H$

So 3) $g(h^{-1})^{-1} \in H$

But $g(h^{-1})^{-1} = gh \in H$. $\square$.

Ex) $A(n) \subset S(n)$ subset of even permutations.

Check 3) : $\pi, \sigma \in A(n)$

$sgn(\pi), sgn(\sigma) = 1$

$$\mathrm{sgn}(\sigma)\,\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma\sigma^{-1})$$
$$= \mathrm{sgn}(\mathrm{id}) = 1$$

So $\mathrm{sgn}(\sigma^{-1}) = 1$: $\sigma^{-1} \in A(n)$.

$$\mathrm{sgn}(\pi\sigma^{-1}) = \mathrm{sgn}(\pi)\,\mathrm{sgn}(\sigma^{-1}) = 1 \cdot 1 = 1$$

So $\pi\sigma^{-1} \in A(n)$

<u>Lemma</u>: $H, K \subset G$ subgroups.
then $H \cap K \subset G$ subgroup.

<u>Pf)</u> Check 3).

$x, y \in H \cap K$.

3): $x y^{-1} \in H$ because H subgroup
$x y^{-1} \in K$ ——— K ——— $\Rightarrow$

$x y^{-1} \in H \cap K$ $\square$.

<u>Lemma</u> $g \in G$

$$\langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \} \subset G \text{ subgroup}$$

"cyclic subgroup generated by g"

Pf) $g^i, g^j \in \langle g \rangle$

$$g^i (g^j)^{-1} = g^i g^{-j} = g^{i-j} \in \langle g \rangle$$

So $\langle g \rangle \subset G$ satisfies 3)

$\langle g \rangle$ is a subgroup $\square$.

Project V

Two groups are isomorphic if one can be obtained from the other by "relabeling" the elements.

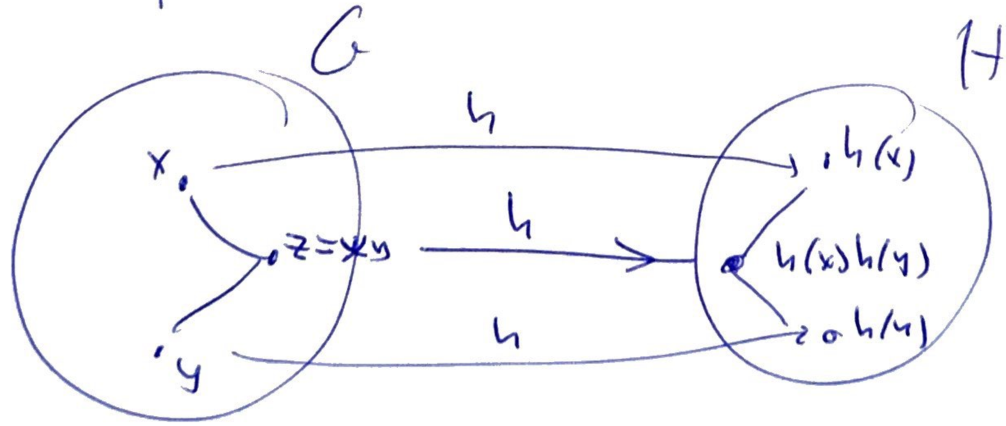
~~Formally~~ Isomorph means they are in essence the same.

Formally. G is isomorph to H if there exists a bijection h.

$$h: G \to H$$

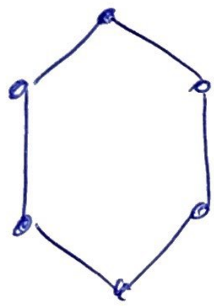
such that $h(xy) = h(x)h(y) \; \forall x, y \in G$.

h "preserves" the operation



There are many finite groups.

One typical example: G is a symmetry group of the hexagon.



each element of G permutes the vertices of the hexagon.

So $G \subset S(6)$. G is isomorph to a subgroup of $S(6)$.

$\# G = 12$

$\# S(6) = 720 \; (= 6!)$

G is a proper subgroup

<u>Thm</u>: Every finite group is (isomorph to) a subgroup of some $S(n)$.

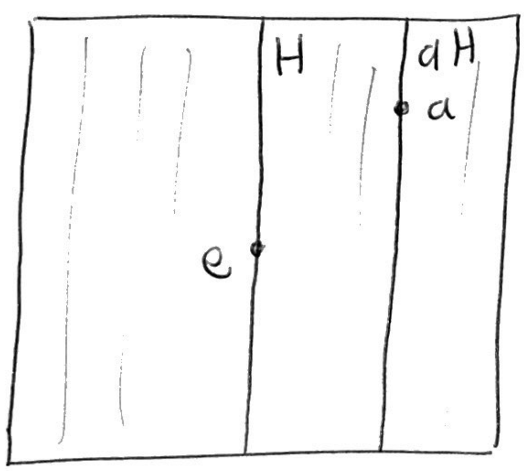
§5.2

Cosets

$H \subset G$ subgroup. $a \in G$

left coset: $aH = \{ah \mid h \in H\}$.

(right coset: $Ha = \{ha \mid h \in H\}$)



G

cosets of H are "translates" of H which fill the whole group.

$$G = \bigcup_{a \in G} aH$$

Lemma: $aH \cap bH = \phi$

or

$aH = bH$

Pf] $aH \cap bH = \phi$: ok.

Suppose $c \in aH \cap bH$.

$\exists h_1 \quad c = ah_1$

$\exists h_2 \quad c = bh_2$

Let $x \in aH$, $x = ah$.

$$x = ah = (ch_1^{-1})h = c(h_1^{-1}h)$$

$$= (bh_2)(h_1^{-1}h) = b(h_2 h_1^{-1} h) \in bH.$$

So $aH \subset bH$

Similarly one shows $bH \subset aH$ $\square$.

If G is finite: $\exists a_1 \cdots a_m$.

$$G = a_1 H \cup a_2 H \cup \cdots \cup a_m H \quad \text{with}$$

$$a_i H \cap a_j H = \phi.$$

<u>Lemma</u> $H \subset G$, G finite, $a \in G$

$\# aH = \# H$.

<u>Pf</u>] Define $\phi : H \to aH$ by

$\phi : h \mapsto ah$.

<u>Claim</u>: ϕ is a bijection.

<u>Pf</u>] Suppose $\phi(h_1) = \phi(h_2)$. $\Longleftrightarrow$

$ah_1 = ah_2$ $\Longleftrightarrow$

$a^{-1}(ah_1) = a^{-1}(ah_2)$ $\Longleftrightarrow$

$h_1 = h_2$.

Suppose $x \in aH$. $\Longrightarrow$

$\exists h \in H$ $x = ah$. $\Longrightarrow$

$\phi(h) = x$ $\Longrightarrow$

ϕ is onto

$\square$

Thm (Lagrange) G finite group

$H \subset G$ subgroup.

Suppose H has m distinct (left) cosets

$$G = a_1 H \cup a_2 H \cup \cdots \cup a_m H.$$

Then

$$\# G = m \# H.$$

In particular, $\# H / \# G$.

Pf) $\# G = \# a_1 H + \# a_2 H + \cdots + \# a_m H$

$= m \cdot \# H$ $\square$.

Corollary $\mathrm{order}(g) \mid \# G$.

Corollary $\# G =$ prime

then G is cyclic.

Corollary p prime $[a]_p \neq 0$

(Fermat) $[a]_p^{p-1} = [1]_p$.

Pf) $[a]_p \in G_p \subset \mathbb{Z}_p$.

$[a]_p$ has order k.

$$[a]_p^k = [1]_p$$

$\langle [a]_p \rangle \subset G_p$ subgroup

So $k \mid p-1$, $\# \langle [a]_p \rangle = k$.

$$p-1 = q \cdot k.$$

Hence,

$$[a]_p^{p-1} = \left([a]_p^k\right)^q = [1]_p^q = [1]_p.$$

$\square$.

<u>Corollary</u> (Euler)

$n \geq 1$ $\quad 0 \neq [a]_n \in G_n \subset \mathbb{Z}_n$.

$$\phi(n) = \# G_n.$$

Then

$$[a]_n^{\phi(n)} = [1]_n.$$

Pf] $[a]_n \in G_n$ has order $k \geq 1$ $[a]_n^k = [1]_n$.

$\langle [a]_n \rangle \subset G_n$ subgroup

$\# \langle [a]_n \rangle = k$

$k \mid \# G_n$ $\quad kq = \phi(n)$

So $[a]_n^{\phi(n)} = \left([a]_n^k\right)^q = \left([1]_n\right)^q$

$= [1]_n$ $\square$.

<u>Example</u> Let Sym_5 be the symmetry group of the pentagon. Each symmetry can be seen as a permutation of the vertices. So

$$Sym_5 \subset S(5).$$

Observe $\#\mathrm{Sym}_5 = 10$

$$\# S(5) = 5! = 120$$

Indeed, (Lagrange), $10 \mid 120$.

Maybe Sym_5 can be seen as a subgroup of $S(4)$. ?

No, this is not true;

$$\left.\begin{array}{l} \#\mathrm{Sym}_5 = 10 \\ \# S(4) = 4! = 24 \end{array}\right\} \quad 10 \nmid 24$$

10 does not devide 24.