3 Group theory revisited.

$n \geq 1$

$S_n :=$ the set of bijections $\{1, \ldots, n\} \to \{1, \ldots, n\}$.

Theorem 4.1

$(S_n, \underbrace{\circ}_{\text{composition}})$ is a group.

$$S_n = \mathrm{Sym}(\{1, \dots, n\})$$

The ~~assbessed~~ assessed ~~course~~ coursework 1

$$S_3$$

<u>Prop 4.2</u>

S_n is an abelian group

$n \leq 2$

& is <u>NOT</u> abelian otherwise.

Pf $n=1$ $S_1 = \{1\}$

the identity bijection sending 1 to 1.

$n=2$ $S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$

they are NOT matrices!!

$= \{ \underset{\substack{\parallel \\ 1}}{(1)(2)}, (1\ 2) \}$

To check that this is abelian,

$$1 \circ (1\ 2) = (1\ 2) \circ 1.$$

but this is obvious!

$\underline{\underline{n \geq 3}}$ In this case,

S_n contains $f = (1\ 2)$

$g = (2\ 3)$

the bijection $\{1, \ldots, n\} \to \{1, \ldots, n\}$

$1 \mapsto 2$

$2 \mapsto 1$

$3 \mapsto 3$

$\vdots$

$n \mapsto n$

$$(1\,2\,3) = f \circ g \neq g \circ f = (1\,3\,2)$$

$$\begin{array}{ccccc} 1 & \overset{g}{\mapsto} & 1 & \overset{f}{\mapsto} & 2 \\ 2 & \mapsto & 3 & \mapsto & 3 \\ 3 & \mapsto & 2 & \mapsto & 1 \\ 4 & \mapsto & 4 & \mapsto & 4 \\ \vdots & & \vdots & & \vdots \end{array}$$

$$\begin{array}{ccccc} 1 & \overset{f}{\mapsto} & 2 & \overset{g}{\mapsto} & 3 \\ 2 & \mapsto & 1 & \mapsto & 1 \\ 3 & \mapsto & 3 & \mapsto & 2 \\ 4 & \mapsto & 4 & \mapsto & 4 \\ \vdots & & \vdots & & \vdots \end{array}$$

Therefore S_n is NOT abelian.

Subgroups

Def Let $(G, *)$ be a group.

$\Gamma \subseteq G$ a subset

We say that Γ is a subgroup if $(\Gamma, *|_\Gamma)$ is a group.

Or equivalently, it satisfies

(G0) if $a, b \in \Gamma$

then $a * b \in \Gamma$

(G1) if $a, b, c \in \Gamma$,

$$(a*b)*c = a*(b*c)$$

This always holds for free

by seeing them as elements

of G.

(G2) P has the identity element e_P

(i.e. $a * e_P = e_P * a = a$ $\forall a \in P$)

In fact, $e_P = e$ (the identity element of G guaranteed by (G2) for G)

Why?

Because

$e_P * e_P = e_P$ ⓐ

OTOH, the identity e of G

makes! $e_\Gamma = e_\Gamma * e$ [illegible]

By [illegible] [illegible],

$$e_\Gamma * e_\Gamma = e_\Gamma * e$$

By Prop 14.

$$e_\Gamma = e.$$

(G3) Every element γ of Γ has an inverse in Γ.

The inverse of γ exists in G

but (G3) here demands that
it has to be an element in Γ.

Rk Not every subset of G
is a subgroup of G.

Examples $(\mathbb{Z}_6, +)$

How many subsets of $\mathbb{Z}_6$?

2^6

However there are only 4 subgroups of $\mathbb{Z}_6$.

All subgroups need to have $[0]$

$$[0] = e$$

$\{[0]\}$ $\qquad \mathbb{Z}_6 =$

$\{[0], [1], [2], [3], [4], [5]\}$

$[1]+[1]$ in $(G, \circ)$

$$\{\lceil 0\rceil, \lceil 2\rceil, \lceil 4\rceil\}$$

$\lceil 2\rceil + \lceil 2\rceil$ in $(\mathbb{Z}_6)$

$$\{\lceil 0\rceil, \lceil 3\rceil\}$$

$$\{\lceil 0\rceil, \lceil 4\rceil, \lceil 2\rceil\}$$

$$\{\lceil 0\rceil, \lceil 5\rceil, \underset{\substack{\| \\ \lceil 4\rceil}}{\lceil 10\rceil}, \underset{\substack{\| \\ \lceil 3\rceil}}{\lceil 9\rceil}, \lceil 2\rceil, \underset{\substack{\| \\ \mathbb{Z}_6}}{\lceil 2\rceil}\}$$

What are subgroups of $\mathbb{Z}_{12}$?

There are 2^{12} subsets.

The subgroups are.

$\{[0]\}$

$\mathbb{Z}_{12}$

$= \{[0], [1], \ldots [11]\}$

$\{[0], [2], [4], [6], [8], [10]\}$

$$\{ [\bar{0}], [\bar{3}], [\bar{6}], [\bar{9}] \}$$

$$\{ [\bar{0}], [\bar{4}], [\bar{8}] \}$$

$$\{ [\bar{0}], [\bar{6}] \}$$

Prop 43

A non-empty subset Γ of G

is a subgroup

$\Leftrightarrow \quad \forall\, g, h \in P$

$$g * h^{-1} \in P$$

P

the inverse of h

in G.

<u>Pf</u> Look at notes!

<u>Theorem 44</u> (Lagrange's theorem)

G a finite group

($|G| < \infty$)

H a subgroup.

Then $|H|$ divides $|G|$

Rk If $G = \mathbb{Z}_n$,

for any divisor d of n,

there always is a subgroup

$H \trianglelefteq \mathbb{Z}_n$ s.t. $|H| = d$.

$\parallel$

$\{ \lceil \frac{n}{d} \rceil, \lceil \frac{2n}{d} \rceil, \lceil \frac{3n}{d} \rceil, \ldots, \lceil \frac{(d-1)n}{d} \rceil \}$