

§ Group theory revisited.

$$n \geq 1$$

$S_n :=$ the set of bijections
 $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$

Theorem 41

(S_n, \circ) is a group.

composition

$$\mathcal{S}_n = \mathcal{S}_{/M}(\{1, \dots, n\})$$

The assessed course work 1

\mathcal{S}_3

Prop 42

\mathcal{S}_n is an abelian group

$$n \leq 2$$

\mathcal{S}_n

is NOT abelian otherwise.

$$\underline{\underline{\text{Pf}}}$$

$$\underline{\underline{n=1}} \quad S_1 = \{ \underset{\uparrow}{1} \}$$

the identity bijection

sending 1 to 1.

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

\uparrow

they are NOT matrices!!

$$= \left\{ \begin{array}{c} (1)(2), \\ \parallel \\ 1 \end{array} \begin{pmatrix} 1 & 2 \end{pmatrix} \right\}$$

To check that this is abelian,

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

but this is obvious!

$n \geq 3$ In this case,

S_n contains $f = (1\ 2)$

$g = (2\ 3)$

the bijection $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$

$1 \mapsto 2$

$$2 \mapsto 1$$

$$3 \mapsto 3$$

⋮

$$n \mapsto n$$

$$(1\ 2\ 3)$$

//

$$f \circ g$$

~~X~~

$$g \circ f$$

//

$$(1\ 3\ 2)$$

	g		f	
1	↦	1	↦	2
2	↦	3	↦	3
3	↦	2	↦	1
4	↦	4	↦	4
⋮		⋮		⋮

	f		g	
1	↦	2	↦	3
2	↦	1	↦	1
3	↦	3	↦	2
4	↦	4	↦	4
⋮		⋮		⋮

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

$$(G0) \text{ if } a, b \in P$$

$$\text{then } a * b \in P$$

$$(G1) \text{ if } a, b, c \in P,$$

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

This always holds for free

by seeing them as elements
of G .

(G2) Γ has to identity element

$$e_\Gamma$$

(i.e. $a * e_\Gamma = e_\Gamma * a = a$

$$\forall a \in \Gamma$$

In fact,

$e_\Gamma = e$ (the identity
element of G)

Why?

guaranteed by (G2)

Because

for G

$$e_\Gamma * e_\Gamma = e_\Gamma \quad (\text{a})$$

OTOH, the identity e of G

makes

$$e_P = e_P * e$$

$$\textcircled{e}$$

By $\textcircled{e} \textcircled{ee}$,

$$e_P * e_P = e_P * e$$

By
Prop 14.

$$e_P = e.$$

(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 .

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

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

How many subsets of \mathbb{Z}_6 ?

26

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

All subgroups need to have

$$[0]$$

$$\parallel$$
$$e$$

$$\{ [0] \}$$

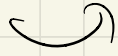
$$\mathbb{Z}_6$$

\parallel

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

$$[1] + [1] \text{ in } (50)$$

$\{ [0], [2], [4] \}$



$[2] + [2]$ in (G)

$\{ [0], [3] \}$

$\{ [0], [4], [2] \}$

$\{ [0], [5], [10], [9], [2], [2] \}$
" " " " "
 $[4] [3] \frac{1}{2}$

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

There are 2^{12} subsets.

The subgroups are.

$$\{[0]\}$$

$$\mathbb{Z}_{12}$$

$$\{[0], [2], \dots, [11]\}$$

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

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

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

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

Prop 43

A non-empty subset Γ

of G

is a subgroup

$$\Leftrightarrow \forall g, h \in \mathcal{P}$$

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

\mathcal{P}

the inverse of h

in G .

Pf Look at notes.

Theorem 44 (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 of \mathbb{Z}_n s.t. $|H| = d.$

||

$\left\{ \frac{1}{d} \langle H \rangle, \frac{2}{d} \langle H \rangle, \dots, \frac{d-1}{d} \langle H \rangle \right\}$