Lecture 2

Last time:

① Notion of a group (S, m)

(i) identity $\longrightarrow e \in S$

(ii) $\forall b \in S, \exists b^{-1} \in S$ ← inverse ellement

(iii) $(a\, b)\, c = a\, (b\, c)$ ← associative law

② Examples ← $(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{Q}, +),$
$(\mathbb{C}, +), (\mathbb{Z}/n\mathbb{Z}, +)$

invertible elements in $S^\times$

③ S ← monoid (no (ii)) $\Rightarrow S^\times$ ← group

Examples: $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

$\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$

$$(\mathbb{Z}/n\mathbb{Z})^\times = ?$$

First guess: $(\mathbb{Z}/n\mathbb{Z})^\times \overset{???}{=} \{1, 2, \dots, n-1\}$

For example, $n = 3 \Rightarrow (\mathbb{Z}/3\mathbb{Z})^\times = \{1, 2\}$

$1^{-1} = 1, \quad 2^{-1} = 2$

ask

For $n = 4$:

$\cdot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

$\Rightarrow (\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$

ask.

before

For $n = 9$

$\cdot$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	4	6	8	1	3	5	7
3	3	6	0	3	6	0	3	6
4	4	8	3	7	2	6	1	5
5	5	1	6	2	7	3	8	4
6	6	3	0	6	3	0	6	3
7	7	5	3	1	8	6	4	2
8	8	7	6	5	4	3	2	1

See that:

$(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$

Exercise (will be in PSet)

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{a \in \{1, \dots, n-1\} ; \gcd(a,n) = 1\}$$

Examples: $(\mathbb{Z}/6\mathbb{Z})^{\times} = \{1, 5\}$

$(\mathbb{Z}/12\mathbb{Z})^{\times} = \{1, 5, 7, 11\}$

ask

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

note: $1^2 = 5^2 = 7^2 = 11^2 = 1$

ask

p - prime $\Rightarrow (\mathbb{Z}/p\mathbb{Z})^{\times} = \{1, 2, \dots, p-1\}$

All groups that we had so far were commutative (abelian): $ab = ba$

Let's construct our first example of non commutative group

Group of permutations

Let $T \leftarrow$ nonempty set

such σ are called permutations

$$S_T := \{ \sigma : T \to T \mid \sigma \leftarrow \text{bijective} \}$$

can multiply permutations: $\sigma, \tau \in S_T$

$$\sigma \bullet \tau := \sigma \circ \tau$$

$$T \ni t \mapsto \sigma(\tau(t))$$

Claim: $(S_T, \bullet) \leftarrow$ is a group.

Proof: (i) identity $e \leftarrow$ permutation id_T

that sends $t \mapsto t$.

(ii) inverse: start with $\sigma: T \to T$

$\sigma:$ $a \mapsto b$, $c \mapsto d$, $e \mapsto f$, $\vdots$ then $\sigma^{-1}:$ $b \mapsto a$, $d \mapsto c$, $f \mapsto e$, $\vdots$

"reverse" arrows

Formally:

For $t \in T$, $\sigma^{-1}(t) = s$ s.t. $\sigma(s) = t$

such s • exists (σ: surjective)
• unique (σ: injective)

(iii) $(\sigma \circ \tau) \circ f \overset{?}{=} \sigma \circ (\tau \circ f)$

both of them are given by:

$t \mapsto \sigma(\tau(f(t)))$

indeed:

$$((\sigma \circ \tau) \circ f)(t) = (\sigma \circ \tau)(f(t)) = \sigma(\tau(f(t)))$$

$$(\sigma \circ (\tau \circ f))(t) = \sigma((\tau \circ f)(t))$$

Assume now that T ← finite.

Then can identify $T = \{1, 2, \dots, n\}$.

$S_{\{1,2,\dots,n\}}$ ← will denote by S_n

group of permutations of indices $1, \dots, n$

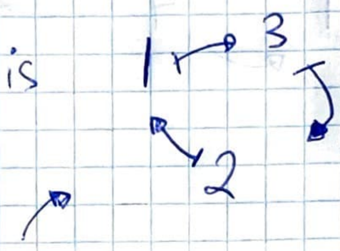
symmetric group

$\sigma \in S_n$ ← ~~determined by~~ can be written as $\begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$

for example $\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$ is

$1 \mapsto 3$
$2 \mapsto 1$
$3 \mapsto 2$

An extremely useful way of writing permutations is using <u>cycle notation</u>

For example: $\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$ is 

<u>cycle</u>

Will use the following notation:

$$(1\ 3\ 2)$$

(in general $(a_1 \dots a_n) \leftrightarrow$ $\left.\begin{array}{l} a_1 \mapsto a_2 \\ a_2 \mapsto a_3 \\ \vdots \\ a_{n-1} \mapsto a_n \\ a_n \mapsto a_1 \end{array}\right)$

Permutation may contain <u>more</u> than one cycle.

Ex: $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{bmatrix}$

is $1 \rightleftarrows 4$ $\qquad$ $\begin{tikzcd} 2 \arrow[r, bend left] & 5 \arrow[d, bend left] \\ & 3 \arrow[ul, bend left] \end{tikzcd}$

So $\sigma = (14)(253)$

Claim: every permutation σ can be written in cycle notation.

Remarks:

1. Cycle notation isn't unique

$(253) = (325) = (532)$ ← all of them represent $\begin{tikzcd} 2 \arrow[r] & 5 \arrow[d] \\ & 3 \arrow[ul] \end{tikzcd}$

these two elements commute

$(14)(253) = (253)(14)$

(2) It is very convenient to omit 1-cycles from the notation.

For example $\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$ in cycle notation is $(13)(2)$ but we simply write it as (13).

The only exception is the identity permutation $\begin{bmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{bmatrix}$, we denote it by 1.

<u>Warning</u>: (12) may refer to both $\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \in S_2$ or $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \in S_3$!

Product in cycle notation

$\sigma \circ \tau$ "First do τ, then σ" !

Example: $\underbrace{(1452)}_{\sigma} \circ \underbrace{(341)(25)}_{\tau} = (135)$

$$\begin{array}{l}
\quad\ \ \tau \qquad \sigma \\
1 \mapsto 3 \mapsto 3 \\
3 \mapsto 4 \mapsto 5 \\
5 \mapsto 2 \mapsto 1
\end{array} \Bigg\} \ \underline{\underline{(135)}}$$

$2 \mapsto 5 \mapsto 2 \qquad (2)$

$4 \mapsto 1 \mapsto 4 \qquad (4)$

Exercise: $(341)(25) \circ (1452) = (234)$.

We see that $\sigma \circ \tau \neq \tau \circ \sigma$ so S_5 is <u>not</u> commutative

$n(n-1)\cdot\ldots\cdot 2\cdot 1$

Group S_n has $n!$ elements. Let's consider $n=3$ in more detail.

Let's describe explicitly the group S_3.

Set $x := (123)$; $y := (12)$.

We have:

relations

$$x^3 = 1, \quad y^2 = 1, \quad yx = x^2y \qquad (*)$$

$$(12)(123) = (1)(23) = (132)(12)$$

$$S_3 = \{1, \underset{(123)}{x}, \underset{(132)}{x^2}, \underset{(12)}{y}, \underset{(13)}{xy}, \underset{(23)}{x^2y}\}$$

S_3 is the group generated by x, y subject to relations $(*)$.

For example, if we want to compute

$$xy\cdot x^2y = xyx^2y = x\underbrace{yx}_{x^2y}xy = \underbrace{x^3}_{=1}yxy = \underbrace{yx}_{x^2y}y = x^2y^2 = x^2$$

We also see that S_3 is not commutative:

$$yx = x^2y \neq xy$$
$$\quad (23) \qquad (13)$$

Exercise: if G is group that contains < 6 elements, then G is commutative.

So S_3 is "smallest" non-commutative group

Why symmetric groups are important?

Because other groups are contained in them as subgroups.

Definition: a subset H of a group G is a subgroup if it has the following properties:

- Closure: $a, b \in H \Rightarrow ab \in H$
- Identity: $1 \in H$
- Inverses: $a \in H \Rightarrow a^{-1} \in H$

Claim: if $H \subset S$ subgroup then the product on S defines the group structure on H

proof identity ✓, inverse ✓

associativity holds for H as it holds for S

Proposition: let G be a group. Then G is a subgroup of the group of permutations S_G.

proof. We construct an embedding:

$$\begin{aligned} G &\xhookrightarrow{\varphi} S_G \quad \text{denote it by } \sigma_g \\ g &\longmapsto (h \mapsto gh) \end{aligned}$$

1) σ_g is bijective because has inverse given by $\sigma_{g^{-1}}$

2) φ is injective.

Our goal is to check that $\sigma_g = \sigma_{g'}$

$$\Downarrow$$

$$g = g'$$

Note that $g = \sigma_g(1) = \sigma_{g'}(1) = g'$ ✓

3) φ is identifies multiplication in G with multiplication in S_G.

In other words need to check:

$$\varphi(\underbrace{g \cdot h}_{\text{mult. in } G}) = \varphi(g) \underbrace{\cdot}_{\text{mult. in } S_G} \varphi(h)$$

Indeed:

$$e \xmapsto{\varphi(gh)} (gh)e \qquad \Big| \qquad e \mapsto he \mapsto g(he) \quad \varphi(g)\cdot\varphi(h)$$

equal by associative law

Examples of subgroups

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

this is a chain of subgroups

$$\mathbb{Z}^\times \subset \mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times$$

Another interesting example:

elements with absolute value 1

$$S \subset \mathbb{C}^\times \quad \{\, a+bi \in \mathbb{C}^\times \mid a^2+b^2=1 \,\}$$

Exercise: S forms a subgroup of $(\mathbb{C}^\times, \cdot)$

Cyclic subgroups

S ← group ; $x \in S$ ← element

The cyclic subgroup of S generated by x is:

$$\langle x \rangle := \{ \dots, x^{-2}, x^{-1}, 1, x, x^2, \dots \}$$

Examples: $S = \mathbb{Z}$, $x = n$, then

$$\langle n \rangle = n\mathbb{Z}$$ ← infinite

$S = (\mathbb{R}, \cdot)$; $x = -1 \Rightarrow \langle -1 \rangle = \{\pm 1\}$

consists of two elements

Goal: understand, how $\langle x \rangle$ can look like.