Lecture 3

Last time:

- group of permutations S_T (T-set)
- structure of S_n ← symmetric group (cycle notation, how to multiply permutations)
- generators / relations presentation of S_3

$$S_3 = \langle x, y \rangle / \; x^3 = y^2 = 1, \; yx = x^2 y$$

x = (123), y = (12) ← one presentation

Another presentation: $s_1 = (12)$; $s_2 = (23)$

Exercise: $S_3 = \langle s_1, s_2 \rangle / \; s_1^2 = s_2^2 = 1, \; s_1 s_2 s_1 = s_2 s_1 s_2$

$(12)(23)(12) = (12)(132)$
$= (13)$
$= (23)(231) = (23)(12)(23)$

Thm $S_n = \langle s_1, \dots s_{n-1} \rangle / \; s_i^2 = 1, \; s_i s_j = s_j s_i, \; |i-j| > 1, \; s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$

$s_i = (i \; i+1)$ → try to check relations →

More examples of generators/relations presentation

$\mathbb{Z} = \langle x \rangle \quad (x = 1)$

φ

No relations

$\mathbb{Z}/n\mathbb{Z}$ ← generated by $\underline{1}$, so $x = 1$

$\underbrace{1 + 1 + \ldots + 1}_{n} = 0 \Rightarrow$ have relation $x^n = 1$

Exercise: $\mathbb{Z}/n\mathbb{Z} = \langle x \rangle / x^n = 1$

Why symmetric groups are important?

Because other groups are contained in them as subgroups

Definition a subset $H \subset S$ of a group S is a subgroup if it has the following prop.:

- Closure: $a, b \in H \Rightarrow ab \in H$
- Identity: $e \in H$
- 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 SG.

proof. We construct an embedding:

$$G \xrightarrow{\varphi} SG$$

denote it by σ_g

$$g \longmapsto (h \longmapsto gh)$$

1) σ_g ← bijective because has inverse

given by $\sigma_{g^{-1}}$

2) φ ← injective ↓

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

$\Leftarrow$

$g = g'$

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

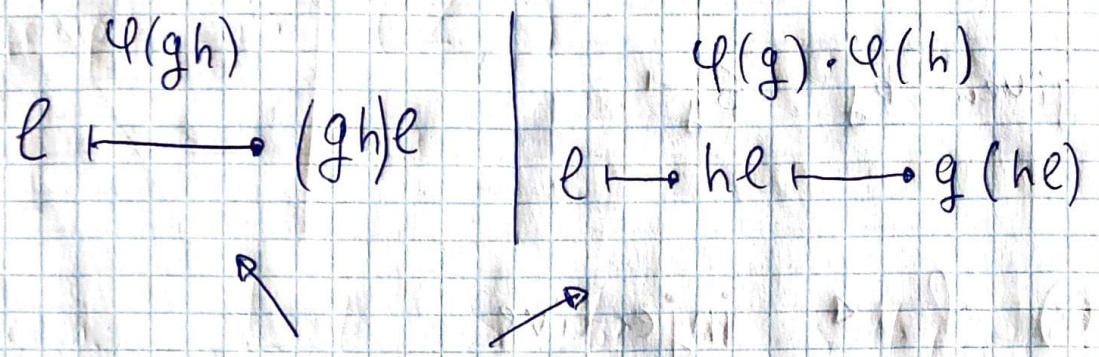
3) φ ← identifies multiplication in G with multiplication in S_G.

In other words need to check:

$$\varphi(g \cdot h) = \varphi(g) \circ \varphi(h)$$

mult. in G ↑ mult. in S_G

Indeed:



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.

First of all, let's describe all subgroups in $(\mathbb{Z}, +)$.

Theorem Let S be a subgroup of $\mathbb{Z}$. Either S is the trivial subgroup $\{0\}$, or else it has the form $\mathbb{Z}a$, where a is the smallest positive integer in S.

Proof

- $0 \in S$, if $S = \{0\}$ $\Rightarrow$ V (by the def. of a subgroup)
- if $\exists n \in S$, $n \neq 0$ $\Rightarrow$ $n, -n \in S$

so S contains some positive integer

Let a = smallest positive integer in S

- Goal: show that $S = \mathbb{Z}a$.

1) $\mathbb{Z}a \subset S$

↳ $a \in S \Rightarrow a + a = 2a \in S \dots$

$\Rightarrow ka \in S \quad \forall k \in \mathbb{Z}_{>0}$

If $ka \in S \Rightarrow -ka \in S$.

We conclude that $\mathbb{Z}a \subset S$

2) $S \subset \mathbb{Z}a$

Pick $n \in S$ and divide with remainder:

$$n = qa + r$$

$q \in \mathbb{Z}$ $\quad$ $r \in \{0, 1, \dots, a-1\}$

$qa \in S \Rightarrow -qa \in S \Rightarrow \underbrace{n - qa}_{r} \in S$

Note now that $r < a \Rightarrow r = 0$

use that a - smallest positive in S

We conclude that $n = qa \in \mathbb{Z}a$

So, $S \subset \mathbb{Z}a$

1) + 2) $\Rightarrow$ $S = \mathbb{Z}a$, as desired

Corollaries of Thm

Pick $a, b \in \mathbb{Z}$ nonzero

$S := \mathbb{Z}a + \mathbb{Z}b = \{ra + sb \mid r, s \in \mathbb{Z}\}$

S subgroup of $\mathbb{Z}$ (generated by a and b)

By Thm, $S = \mathbb{Z}d$ ← some positive number

Corollary 1

(a) $d \mid a$, $d \mid b$

(b) if $e \mid a$ and $e \mid b \Rightarrow e \mid d$

(c) $\exists$ integers r, s s.t. $d = ra + sb$

Proof

(c) $\Leftarrow$ follows from the equality $S = \mathbb{Z}d$ and the definition of S

(a) $a, b \in S = \mathbb{Z}d \Rightarrow d \mid a, d \mid b$

(b) if $e \mid a, e \mid b \Rightarrow e \mid \underbrace{(ra + sb)}_{d}$

Note: number d is nothing else but the $\gcd(a, b)$.

So, we just proved that $\exists r, s$ such that $\gcd(a, b) = ra + sb$ ← this is a nontrivial thing!

Corollary 2

Elements a, b are coprime iff $\exists r, s$ s.t. $ra + sb = 1$

Another subgroup of $\mathbb{Z}$ that one can associate to a pair $a, b \in \mathbb{Z}$ is $\mathbb{Z}a \cap \mathbb{Z}b =: S$

Again we know by Thm that:

$S = m\mathbb{Z}$ ← some positive integer

Exercise / Corollary 3

i.e. $\Rightarrow m = \text{l.c.m.}(a, b)$

(a) $a|m$, $b|m$

(b) if $a|n$, $b|n \Rightarrow m|n$

Corollary 4

Let $d = \gcd(a,b)$, $m = \text{lcm}(a,b)$.

Then $\underline{ab = dm}$.

proof $\frac{b}{d} \in \mathbb{Z} \Rightarrow a \mid \frac{ab}{d}$

similarly $b \mid \frac{ab}{d}$

By Cor 3(b), $m \mid \frac{ab}{d} \overset{(*)}{\Rightarrow} \underline{dm \mid ab}$

Now write $d = ra + sb$, then

$$dm = \underbrace{ram + sbm}_{\text{divisible by } ab} \quad \text{?}$$

$\Rightarrow ab \mid dm$ (**)

It follows from (*) + (**) that $\underline{dm = ab}$

Upshot ← just used groups to prove something about numbers!

this is another indication that the notion of a group/subgroup is important

Cyclic subgroups

$x \in S$ ← some group

$$\langle x \rangle = \{ x^k \mid k \in \mathbb{Z} \}$$

Proposition Let $S \subset \mathbb{Z}$ be the set of all $k \in \mathbb{Z}$ s.t. $x^k = 1$. Then

(a) S ← subgroup of $\mathbb{Z}$,

(b) $x^r = x^s$ iff $r - s \in S$,

(c) suppose S ← not the trivial group. Then $S = n\mathbb{Z}$, and
by Thm

$$\langle x \rangle = \{1, x, x^2, \ldots, x^{n-1}\}$$

all of them are distinct

multiplication rule as in $(\mathbb{Z}/n\mathbb{Z}, +)$

(d) suppose $S = \{0\}$, then

$\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$ ← identifies with the group $(\mathbb{Z}, +)$

Proof (a) $x^k = 1,\ x^\ell = 1 \Rightarrow x^k \cdot x^\ell = x^{k+\ell}$

$\parallel$

1

So if $k, \ell \in S \Rightarrow k+\ell \in S$ ✓

$x^0 = 1 \Rightarrow 0 \in S$ ✓

if $x^k = 1 \Rightarrow (x^k)^{-1} = 1^{-1} = 1$

$\parallel$

x^{-k}

So $k \in S \Rightarrow -k \in S$ ✓

(b) If $x^r = x^s$ —multiply by x^{-s}→ $x^{r-s} = 1$

If $x^{r-s} = 1$ —multiply by x^s→ $x^r = x^s$

Rem! in general $a, b, c \in S$ a group then

$ab = ac$ iff $b = c$ (cancellation law)

(c) $S = n\mathbb{Z}$, follows from (a) that $\{1, x, \dots, x^{n-1}\}$ distinct

Multiplication is as in $(\mathbb{Z}/n\mathbb{Z}, +)$ because $x^n = 1$

(d) x^k, $k \in \mathbb{Z}$ ← are all distinct by (a)

(use that $S = \{0\}$)

Multiplication: $x^k \cdot x^\ell = x^{k+\ell}$

as in $(\mathbb{Z}, +)$

Group $\langle x \rangle = \{1, x, \ldots, x^{n-1}\}$ as in (c)

is called cyclic group of order n.

Definition

If $x \in S$, then the order of x is the number of elements in $\langle x \rangle$

can be ∞

In other words ← order of x is the minimal $n \in \mathbb{Z}_{\geq 0}$ s.t. $x^n = 1$