Lecture 1 Groups, permutation groups, isomorphisms, subgroups

Why groups/rings/fields?

* Describe symmetry uniformly
* Compare symmetries in different contexts
* Extract the "most fundamental common structures" in all scenarios

Example: Pell's equation $x^2 - Dy^2 = 1$ D square free integer >1

analogy in a pure abstract level

general sol'ns come from computing $\pm(x_0+\sqrt{D}y_0)^N$ for $N \in \mathbb{Z}$

($\mathbb{Z} \times \mathbb{Z}_2$ form a group)

Elliptic curve $\{(x,y)\in\mathbb{Q}^2 \mid y^2 = x^3 - Dx\} \cup \{\infty\}$ is like $\mathbb{Z}^? \times (\text{torsion})$

Definition A group (群) is a pair of
* a nonempty set G, and
* a binary operation $\star : G \times G \longrightarrow G$

such that (1) $(a\star b)\star c = a\star(b\star c)$

(2) $\exists$ an element $e \in G$, called the identity (单位元)

such that s.t. $\forall a \in G$, $a\star e = e\star a = a$.

(3) for each $a \in G$, $\exists$ an element $a^{-1}\in G$, called an inverse (逆) of a

s.t. $a\star a^{-1} = a^{-1}\star a = e$.

• The group G is called abelian or commutative (阿贝尔群或交换群) if $a\star b = b\star a$

named after Abel.

• $\#G$ or $|G|$ is called the order (阶) of a group (possibly infinite)

Examples. $(\mathbb{Z},+)$, $(\mathbb{Q}\setminus\{0\},\cdot)$

- $(\mathbb{Z}_n, +)$ Here $\mathbb{Z}_n = \{\text{residue classes modulo } n\}$
- $(\mathbb{Q}\setminus\{-1\}, \star)$ $\quad a \star b := ab + a + b$

  (This is in fact $(\mathbb{Q}\setminus\{0\}, \cdot)$, shifted by 1)

- Given two groups $(G, \star)$ and $(H, \circ)$, form their direct product (直积)

$$(G \times H, *) \qquad (g,h) * (g',h') := (g \star g', h \circ h')$$

(In algebra, we don't use g' to denote derivatives.)

Basic properties: If G is a group,

(i) the identity element is unique.

(b/c if e and e' are both identity elements, $e = e \star e' = e'$.)

(ii) the inverse of $a \in G$ is unique

(iii) $(a^{-1})^{-1} = a$

(iv) $(a \star b)^{-1} = b^{-1} \star a^{-1}$ $\quad$ (similar in the case of matrices)

(v) $a \star u = a \star v \Rightarrow u = v$ $\quad$, $\quad u \star b = v \star b \Rightarrow u \star v$

b/c $a^{-1} \star a \star u = a^{-1} \star a \star v$

Important convention:

Multiplicative convention: not knowing whether G is abelian or not

write $\cdot$ for $\star$ and 1 for identity

e.g $(a_1 \cdot \cdots \cdot a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$; $\quad g^n = \underbrace{g \cdots g}_{n \text{ times}}$

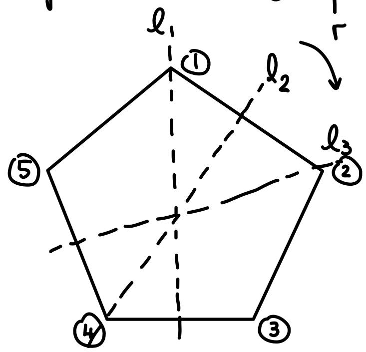
Additive convention: when we are using that G is abelian

write $+$ for $\star$, $\quad$ 0 for identity, and $-a$ for inverse of a

e.g. $a + b = b + a \qquad na = a + \cdots + a$

n times

<u>Example</u> Dihedral group (二面体群) D_{2n} = symmetry group of a regular n-gon



elements: $\begin{cases} e = \text{identity}, \quad r = \text{rotation } \frac{2\pi}{5}, \quad r^2 = \text{rotation } \frac{4\pi}{5}, \dots \\ s = s_1 = \text{reflection about } l_1, \quad s_2 = \text{reflection about } l_2, \dots \end{cases}$

$\# D_{2n} = 2n$

How to write this group efficiently?

$$D_{2n} = \left\{ \begin{matrix} e, r, r^2, \cdots, r^{n-1} \\ s = s_1, rs, r^2 s, \dots \end{matrix} \right\}$$

rs means first reflect about l_1 and then rotate (e.g. $1 \mapsto 1 \to 2$) so this is s_2

$$= \left\langle r, s \;\middle|\; \begin{matrix} r^n = 1, \; s^2 = 1 \\ \underline{srs = r^{-1}} \end{matrix} \right\rangle$$

$srs = r^{-1}$: rotation on the back of the paper = rotation counterclockwise.

Notation means the set of words in r, s, r^{-1}, s^{-1}, subject to the given relations

<u>Rmk</u>: $srs^{-1} = r^{-1} \Rightarrow sr^i s = \underbrace{srs\,srs \cdots srs}_{i \text{ copies of } srs} = \underbrace{r^{-1} \cdots r^{-1}}_{i \text{ of these}} = r^{-i}$

<u>Definition</u> A subset $S = \{s_1, \dots, s_n\}$ of G is called a <u>set of generators</u> (生成元) if every element of G can be written as <u>finite</u> products of $s_1, \dots, s_n, s_1^{-1}, \dots, s_n^{-1}$.

An equality consisting of generators and their inverses is called a <u>relation</u> (生成关系)

We write $G = \langle s_1, \dots, s_n \mid R_1, \dots, R_m \rangle$ if all relations in G can be deduced from $R_1, \dots, R_m$

E.g. $\mathbb{Z}_6 = \langle \underset{\text{for } 2}{r}, \underset{\text{for } 3}{s} \mid r^3 = s^2 = 1, rs = sr \rangle$ (always use multiplicative convention)

Example: Symmetry group / Permutation group (对称群 / 置换群)

Definition. Let Ω be a set. Then $S_\Omega := \{\text{bijections } \sigma: \Omega \to \Omega\}$ has a structure of a group

* identity element $= id: \Omega \to \Omega$
* multiplication: composition $\sigma\tau: \Omega \xrightarrow{\tau} \Omega \xrightarrow{\sigma} \Omega$
* inverses: inverse of the map.

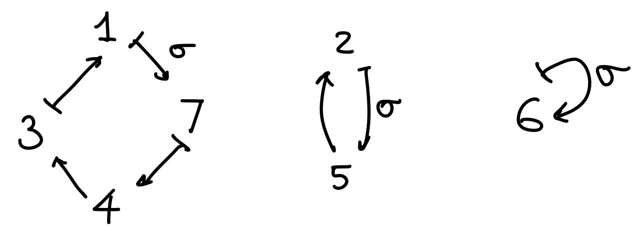
S_Ω is called the symmetry group / permutation group of Ω

When $\Omega = \{1, 2, \cdots, n\}$, we write S_n instead.

* Elements in S_n:

Expression 1:
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 1 & 3 & 2 & 6 & 4 \end{pmatrix}$$

Expression 2:



Write $\sigma = (1743)(25)\cancel{(6)}$ ⟵ called the cycle decomposition of σ.

* More generally, call $(a_1 a_2 \cdots a_r)$ a cycle (here $a_1, \cdots, a_r$ are distinct)

it means $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_r \mapsto a_1$

& fixes other a_i's.

Then $\sigma = (1743)(25)$ means to compose two maps $1 \mapsto 7 \mapsto 4 \mapsto 3 \mapsto 1$

$2 \mapsto 5 \mapsto 2$.

* In general, * every element of S_n can be written as product of disjoint cycles
* disjoint cycles commutes with each other.

E.g. $\sigma^2 = (1743)^2 (25)^2 = (14)(73)$.

$$\sigma^{-1} = (1743)^{-1}(25)^{-1} = (1347)(25)$$

- S_n is noncommutative unless $n=2$.

Exercise: ① S_n is generated by "transpositions" (ij)

② S_n is generated by "adjacent transpositions" $(i\ i{+}1)$

③ ———————— (12), $(123\cdots n)$

* Group isomorphisms

Definition Two groups $(G,\star)$ and $(H,*)$ are isomorphic (同构) if there exists a bijection $\phi: G \xrightarrow{\sim} H$ s.t. $g,h \in G$

① $\phi(g \star h) = \phi(g) * \phi(h)$

② $\phi(e_G) = (e_H)$ (Exercise: ① => ②③)

③ $\phi(g^{-1}) = \phi(g)^{-1}$

We write $G \cong H$ or $G \xrightarrow[\simeq]{\phi} H$

Example: $\exp: (\mathbb{R},+) \to (\mathbb{R}_{>0},\cdot)$ is an isom

$\mathbb{Z}_n \longrightarrow \mu_n = \{$all n^{th} roots of unity in $\mathbb{C}\}$

$a \longmapsto \zeta_n^a = e^{2\pi i a/n}$

Rmk: Isomorphic groups are considered "same"

Basic question in group theory: classify groups with certain properties, up to isomorphisms

e.g. all groups of order 6 are isomorphic to either $\mathbb{Z}_6$ or S_3

In particular, $D_6 \simeq S_3$ (by identifying the symmetry of $\triangle$ with the symmetry of its three vertices)

& $D_6 \not\cong \mathbb{Z}_6$ b/c D_6 is not commutative

Definition A group H is called *cyclic* (循环群) if it can be generated by one element,

i.e. $\exists\, x \in H$, s.t. $H = \{x^n \mid n \in \mathbb{Z}\}$ or sometimes $H = \langle x \rangle$

There are two kinds of cyclic groups (up to isomorphism)

① $\# H = n$, then $H = \{1, x, x^2, \cdots, x^{n-1}\}$ cyclic group of order n

(This H is isomorphic to $\mathbb{Z}_n$: $\phi: H \xrightarrow{\sim} \mathbb{Z}_n$)

$x^a \longmapsto a$

② $\# H = \infty$, then $H \cong \mathbb{Z}$

Parellel development of vector spaces vs. groups

Vector spaces	Groups
direct sums	direct products
linear isomorphisms	isomorphisms
subspaces	subgroups

Definition A subset H of a group G is a *subgroup* (子群), denoted by $H < G$, if

① $e \in H$

② $\forall a, b \in H$, $a \cdot b \in H$

③ $\forall a \in H$, $a^{-1} \in H$

Alternative def'n A nonempty subset $H \subseteq G$ is a subgroup if and only if

$$\forall\, a, b \in H \Rightarrow ab^{-1} \in H$$

(Taking $a = b \Rightarrow e \in H$, taking $a = 1 \Rightarrow b^{-1} \in H$, $a(b^{-1})^{-1} = ab \in H$.)

Definition Let G be a group and A a subset

$$\begin{aligned}\langle A\rangle &:= \text{subgroup of } G \text{ generated by } A \quad (\text{由}A\text{生成的子群}) \\ &= \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_r^{\varepsilon_r} \mid \text{for } a_1,\dots,a_r \in A,\ \varepsilon_1,\dots,\varepsilon_r \in \{\pm 1\}\} \\ &= \bigcap_{\substack{\text{subgps } H<G \\ \text{s.t. } A\subseteq H}} H\end{aligned}$$

Rmk: When G is abelian, and $A=\{a_1,\dots,a_r\}$

$$\langle A\rangle = \{a_1^{d_1}\cdots a_r^{d_r} \mid d_1,\dots,d_r \in \mathbb{Z}\}$$

Definition. Let G be a group and $x\in G$

Define the order (阶) of x in G, denoted $|x|$, as follows:

① if $\exists$ integers $a\neq b$ s.t. $x^a = x^b$, pick a pair a,b with $n=a-b$ positive but minimal.

then $x^n = 1$ & $\langle x\rangle = \{1, x, \dots, x^{n-1}\}$; define $|x| = \#\langle x\rangle$

② if $\nexists$ such integers $\langle x\rangle = \{1, x, x^2, \dots, x^{-1}, x^{-2}, \dots\} \simeq \mathbb{Z}$; define $|x| = \infty$.

Lattices of subgroups

E.g.

$$\begin{tikzcd}[column sep=small]
\mathbb{Z}/p^n\mathbb{Z} \arrow[d, dash] \\
\langle p\rangle = \{0, p, 2p, \dots\} \arrow[d, dash] \\
\langle p^2\rangle \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
\langle p^n\rangle = \{0\}
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
& \mathbb{Z}/12\mathbb{Z} \arrow[dl, dash] \arrow[dr, dash] & & \\
\{0,3,6,9\} = \langle 3\rangle \arrow[dr, dash] & & \langle 2\rangle = \{0,2,4,6,8,10\} \arrow[dl, dash] \arrow[dr, dash] & \\
& \langle 6\rangle = \{0,6\} \arrow[dr, dash] & & \langle 4\rangle = \{0,4,8\} \arrow[dl, dash] \\
& & \{0\} &
\end{tikzcd}$$