Notes on Group Theory

Betelgeuse Nebula 2023

version 2.0

Fundamentals

How to Define a Group

① elements   eg. $\{0, 1, 2, 3, 4\}$

② define multiplication   eg. $a \cdot b := (a+b) \bmod 5$

The definitions must satisfy:

① Closure ☆ $\forall a, b \in G,\ ab \in G$.

② Associativity (结合律) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

③ Existence of the identity $I \cdot g = g,\ g \cdot I = g$.

④ Existence of a unique inverse for every element.

→ actually these can be weaken to left identity & left inverse.

☆ abelian group: $a \cdot b = b \cdot a$

non-abelian group: not communicative

Subgroup

def: ① subset   ② same multiplication definition.   writes $H \subset G$

- cyclic subgroup

  For any $g \in G$, the sequence $\{I, g, g^2, \cdots, g^{k-1}\}$ forms a subgroup Z_k, where $g^k = I$.

- Lagrange's thm

  G has n elements, H has m elements, if $H \subset G$, then $m \mid n$.

☆ The "once and only once rule" in multiplication table of a finite group:

Statement 1° Every element appears once and only once in every row or column.

Statement 2° $\{g_i g_1, g_i g_2, \cdots, g_i g_n\}$ and $\{g_1 g_i, g_2 g_i, \cdots, g_n g_i\}$ are permutations of $\{g_1, g_2, \cdots, g_n\}$

Direct Product of Groups

writes: $H := F \otimes G$

elements in H: (f, g) where f is in F, g is in G.

multiplication in H: $(f, g) \underset{\text{H dot}}{\cdot} (f', g') = (f \underset{\text{F dot}}{\cdot} f', g \underset{\text{G dot}}{\cdot} g')$

identify & inverse $I_H = (I_F, I_G)$, $(f, g)^{-1} = (f^{-1}, g^{-1})$

Presentations

Using few elements (aka. generators) and some restrictions to define (present) the group. All the elements can be obtained by multiplying the generators.

Note: absolute presentation: not ambiguous presentation

Example

$Z_8 = \langle a \mid a^8 = I \rangle$ absolute: $Z_8 = \langle a \mid a^8 = I, a^4 \neq I \rangle$

$Z_2 \otimes Z_2 = \langle a, b \mid a^2 = b^2 = I, ab = ba \rangle$

Homomorphism (同态) & Isomorphism (同构)

def of homomorphism: a map $f: G \to G'$, if $f(g_1) \cdot f(g_2) = f(g_1 \cdot g_2)$

G' dot   G dot

more mathematical description: a structure-preserving map between two algebra structures. { elements, 二元运算 }

def of isomorphism: a bijective homomorphism, exactly the same group.

Examples

— $f: Z_{pq} \to Z_p \otimes Z_q$ when p & q are relative primes.

def
① in Z_{pq}, $x \cdot y = x + y \bmod pq$, $x, y = 0, 1, \cdots, pq-1$.
② in $Z_p \otimes Z_q$, $(a,b)\cdot(c,d) = (a+c \bmod p,\ b+d \bmod q)$, $a, c = 0, 1, \cdots, p-1$, $b, d = 0, 1, \cdots, q-1$.
③ $f(x) = (x \bmod p,\ x \bmod q)$

is a bijection (only when $\gcd(p,q) = 1$)

Then
$$
\begin{aligned}
f(x\cdot y) &\overset{①}{=} f(x+y \bmod pq) \\
&\overset{③}{=} (x+y \bmod p,\ x+y \bmod q) \\
&= ((x \bmod p + y \bmod p) \bmod p,\ (x \bmod q + y \bmod q) \bmod q) \\
&\overset{②}{=} (x \bmod p,\ x \bmod q)\cdot(y \bmod p,\ y \bmod q) \\
&\overset{③}{=} f(x)\cdot f(y)
\end{aligned}
$$

So f is an Isomorphism!

— $f: SO(2) \to U(1)$, $f[R(\phi)] = e^{i\phi}$

Isomorphism!

Finite Group

Permutation Group S_n

☆ Any element in S_n (any permutation) can be written as the product of cycles, then being decomposed to transpositions.

Example $\quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix} = \underbrace{(142)}_{1 \to 4 \to 2 \to 1}(35) = \underbrace{(14)(42)}_{\text{first } 4 \leftrightarrow 2, \text{ then } 1 \leftrightarrow 4}(35)$

Caylay's Thm

- Any finite group G of n order (n elements) is isomorphic to a subgroup of S_n.

pf? : List G as $\{g_1, g_2, \cdots, g_n\}$, show g_i as $\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_ig_1 & g_ig_2 & \cdots & g_ig_n \end{pmatrix}$ is a permutation.

— All the group of 2 order are identical to S_2 & Z_2.

Square Root of Identity

Thm: In a group of even order, there exists at least one element other than I, that also squares to the identity.

pf: I inverse to itself, so at lease one other element also inverse to itself.

Equivalence & Equivalence Class

def of equivalence: In a group G, two elements g & g' are said to be equivalence ($g \sim g'$) if there exists another element f st. $g' = f g f^{-1}$.

Note: Equivalence implies that the two elements are essentially the same, playing the same role, being similar transformation in linear algebra.

• Transitivity $\begin{cases} g \sim g' \\ g' \sim g'' \end{cases} \Rightarrow g \sim g''$

☆ All elements in a group can be divided into several classes (equivalence classes), where any two elements in the same class are equivalent.

Properties

1. In an abelian world, everybody is in a class by himself or herself. Show this.
2. In any group, the identity is always proudly in its own private class of one. Show this.
3. Consider a class c consisting of $\{g_1, \cdots, g_{n_c}\}$. Then the inverse of these n_c elements, namely, $\{g_1^{-1}, \cdots, g_{n_c}^{-1}\}$, also form a class, which we denote by $\bar{c}$. Show this.

Example

[illegible]. The even permutations form the subgroup A_4, with $4!/2 = 12$ elements. Given the preceding remarks, the even permutations fall into four equivalence classes:

$\{I\}$, $\{(12)(34), (13)(24), (14)(23)\}$, $\{(123), (142), (134), (243)\}$, and $\{(132), (124), (143), (234)\}$

Quanternionic Group (四元数群) Q

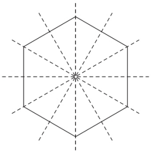
Q has 8 elements: $\pm 1, \pm i, \pm j, \pm k$. They satisfy

$$\begin{cases} i^2 = j^2 = k^2 = -1 \\ ij = k = -ji \\ jk = i = -kj \\ ki = j = -ik \end{cases}$$

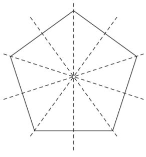
using algebraric multiplication.

Dihedral Group (二面体群) D_n

set of transformations that leave the n-sided regular polygon invariant.



n even

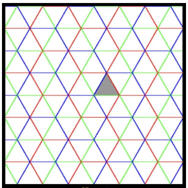


n odd

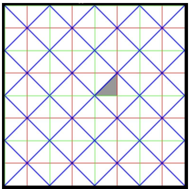
elements of D_n $\begin{cases} \text{Rotation of } \frac{2\pi}{n} \\ \text{reflection through a median} \end{cases}$

Coxeter Group $\langle a_1, \cdots a_k \mid (a_i)^2 = I, (a_i a_j)^{n_{ij}} = I, n_{ij} \geq 2, i \neq j \rangle$

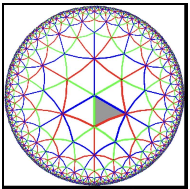
反射群的抽象表示，不限于欧氏空间。



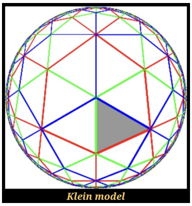
Affine A2



Affine B2



Poincaré model



Klein model

Invariant Subgroup & Simple Group

(不变子群/正规子群)

Invariant subgroup is a special kind of subgroup. Similarity transformations (generate by the group element G) leave the invariant group unchanged.

def of invariant subgroup: (premise, H is a subgroup of G)

If $H = g^{-1} H g$ for all $g \in G$, then H is called a invariant subgroup (of G),

no need to be in the same order

writing $H \triangleleft G$

def of simple group: A group is called simple if it doesn't have any invariant subgroup. (excluding G itself and $\{I\}$)

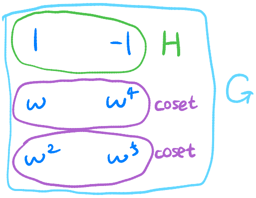
properties:

- In a direct product group $G = E \otimes F$, $E \otimes I_F$ & $I_E \otimes F$ are invariant subgroups.

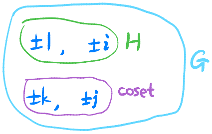
Cosets (陪集) & Quotient Group (商群)

Examples

1) $G = Z_6$
   $H = Z_2 \triangleleft G$



2) $G = Q$ (quotient group)
   $H = Z_4 = \{\pm 1, \pm i\}$, $H \triangleleft G$



def of cosets: First we have $H \triangleleft G$. For all the elements in G, $g_1, g_2, \cdots, g_n$, we can write a set

$g_iH = \{g_ih_1, g_ih_2, \cdots, g_ih_n\}$ for each g_i, but some of them are exactly the same set.

若重复的集合仅计一次，那么恰好剩余

$$N(Q) = \frac{N(G)}{N(H)}$$ 个集合，不重不漏地划分了 G，

这 $N(Q)$ 个均有 $N(H)$ 个元素的集合定义为陪集(cosets)，

除 H 外的 $N(Q)-1$ 个陪集都不是群。

def of quotient group Q: The (left) cosets form a group — quotient group,

where $(g_aH)(g_bH) = (g_ag_bH)$, $I_{quotient} = I_GH = H$.

writes $Q = G/H$

Derived Subgroup

In physics, a commutator of A & B is defined as $[A, B] = AB - BA$.

Similarly, we define $\langle a, b \rangle \equiv (ba)^{-1}ab$ measuring how much ab differ from ba.

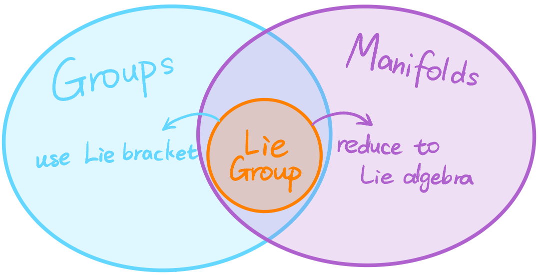
def of derived subgroup: 由 $\langle a,b \rangle$ 组成(除去重复者), 其中 a, b 遍历 G 中所有元素, 二元运算与 G 中保持一致。

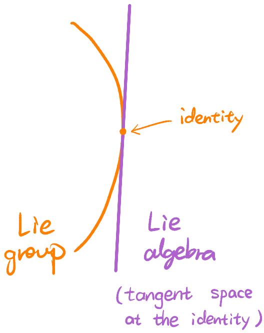
Note: The larger D is, the "more" G is nonabelian.

Derive subgroup is an invariant subgroup.

Lie Group & Lie Algebra

in matrix language





Manifolds: all neighbourhoods look like flat space.

Lie Group

O(n)

(real)

orthogonal (正交的):

$$R^T R = I$$

SO(n)

(real)

special orthogonal:

$$R^T R = I$$
$$|R| = 1$$

U(n)

(complex)

orthogonal:

$$R^T R = I$$

SU(n)

(complex)

special orthogonal:

$$R^T R = I$$
$$|R| = 1$$

Rotation

$$\left.\begin{array}{r}\text{Linear transformations} \\ \vec{u}' = R\,\vec{u} \\ \text{Invariance of dot product} \\ \vec{u}^T\vec{v} = \vec{u}'^T\vec{v}'\end{array}\right\} \Longrightarrow R^TR = I$$

(orthogonal matrix) $\xrightarrow{\text{form}}$ orthogonal group 正交群 $O(n)$

property: Rs are continuously related to the identity.

Reflection

$$R^TR = I \Longrightarrow \det R = \begin{cases} +1, & \text{rotations} \\ -1, & \text{reflections} \end{cases}$$

rotations $\longrightarrow$ special orthogonal group 特殊正交群 $SO(n)$

Generator

consider a rotation close to the identity (2 dimension)

$$R(\theta) = I + \theta J + O(\theta^2) = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + \theta \begin{pmatrix} & 1 \\ -1 & \end{pmatrix} + O(\theta^2)$$

$$\approx I + \theta J \quad (\approx e^{\theta J})$$

then for a finite angle θ, we have

$$R(\theta) = \lim_{N\to\infty}\left[R\left(\frac{\theta}{N}\right)\right]^N = \lim_{N\to\infty}\left(1 + \frac{\theta J}{N}\right)^N = e^{\theta J}$$

In higher dimentions, definition of generators are,

$$\left(J_{(mn)}\right)^{ij} = \delta^i_m \delta^j_n - \delta^j_m \delta^i_n$$

that is, row m col n = 1, row n col m = -1, only exist while $m \neq n$.

Then, an N dimentional infinitesimal rotation is given by

$$R \simeq I + \sum_{m \neq n} \theta_{(mn)} \boxed{\mathcal{J}_{(mn)}} \quad \text{generators}$$

$$= I + \sum_{m \neq n} \theta_{(mn)} \; i \boxed{J_{(mn)}} \quad \text{this is Hermitean matrices: } J^{\dagger} = J$$

Commutator & Lie Algebra

commutator between A & B : $[A, B] = AB - BA$.

property: $(I+A)\cdot(I+B)\cdot(I+A)^{-1} = (I+B) + [A, B]$

$$[J_a, J_b] = i \boxed{C_{abc}} J_c$$

Structure constants,

telling the multiplicative structure of infinitesimal rotation

For $SO(3)$, $C_{abc} = \varepsilon_{abc}$

(J_a, J_b, J_c are defined as $J_{(23)}, J_{(31)}, J_{(12)}$)

Table: the way to get another element	
Lie group	multiplication
Lie algebra	commutator

Lie Group & Lie Algebra

Given two finite rotations g & h

$$g = \exp\left(\sum_{i}^{\frac{D(D-1)}{2}} \varphi_i \mathcal{J}_i\right), \quad f = \exp\left(\sum_{i}^{\frac{D(D-1)}{2}} \psi_i \mathcal{J}_i\right)$$

When it's hard to calculate $g \cdot h$, we can ask Lie algebra for help, assuming $g = e^{X}$, $h = e^{Y}$, $g \cdot h = e^{Z}$, then

$$X = \ln g = \sum_i \varphi_i J_i, \quad Y = \ln h = \sum_i \psi_i J_i,$$

$$Z = \ln(g\cdot h) = \ln\left(e^X \cdot e^Y\right)$$

$$= \ln\left[\left(I + X + \tfrac{1}{2}X^2 + \tfrac{1}{6}X^3 + \cdots\right)\left(I + Y + \tfrac{1}{2}Y^2 + \tfrac{1}{6}Y^3 + \cdots\right)\right]$$

$$= \ln\left(I + X + Y + XY + \tfrac{1}{2}X^2 + \tfrac{1}{2}Y^2 + \tfrac{1}{6}X^3 + \tfrac{1}{2}X^2Y + \tfrac{1}{2}XY^2 + \tfrac{1}{6}Y^3 + \cdots\right)$$

$$= \left(X + Y + XY + \tfrac{1}{2}X^2 + \tfrac{1}{2}Y^2 + \tfrac{1}{6}X^3 + \tfrac{1}{2}X^2Y + \tfrac{1}{2}XY^2 + \tfrac{1}{6}Y^3\right)$$

$$-\tfrac{1}{2}\left(X + Y + XY + \tfrac{1}{2}X^2 + \tfrac{1}{2}Y^2 \cancel{+ \tfrac{1}{6}X^3 + \tfrac{1}{2}X^2Y + \tfrac{1}{2}XY^2 + \tfrac{1}{6}Y^3}\right)^2$$

$$+\tfrac{1}{3}\left(X + Y \cancel{+ XY + \tfrac{1}{2}X^2 + \tfrac{1}{2}Y^2} \cancel{+ \tfrac{1}{6}X^3 + \tfrac{1}{2}X^2Y + \tfrac{1}{2}XY^2 + \tfrac{1}{6}Y^3}\right)^3 + \cdots$$

$$= X + Y + XY + \tfrac{1}{2}(X^2 + Y^2) - \tfrac{1}{2}(X^2 + Y^2) - XY - (X+Y)\left[XY + \tfrac{1}{2}(X^2+Y^2)\right] + \tfrac{1}{3}(X^3 + Y^3) + XY(X+Y) + \cdots$$

$$Z = X + Y + \tfrac{1}{2}[X, Y] + \tfrac{1}{12}[X - Y, [X, Y]] + \cdots$$

This is Baker-Campbell-Hausdorff formula, implying the relation between Lie group and Lie algebra.

Lie group

Lie algebra

(tangent space at I)