Group Theory 群论

群 Group

群 : $(G, *, \#)$

- G 是非空集合
- *, # 称为 二元运算

只有满足以下 4 个性质才是群 :
① 封闭性 : $\forall a, b \in G, \quad a * b \in G$ 集合中任意 2 个元素运算都跑不出这个集合
② 结合律 : $\forall a, b, c \in G, \quad a * (b * c) = (a * b) * c \in G$ 群内元素运算顺序不影响结果
③ 单位元 : $\exists e \in G, \ \forall a \in G, \quad a * e = e * a = a$ 单位元和群内任何元素运算都等于该单位元

- 类似整数里的 "1" , 只有 e 不管处于运算的哪边都满足这个条件时, 才成它为单位元 , 否则的话, 称其为 `左单位元 / 右单位元`
  ④ 逆元 : $\forall a \in G, \ \exists b \in G$, 使 $a * b = b * a = e$, a 的逆元记为 a^{-1}
- 类似与 a / b 互为倒数 (a 运算 b = 1)

几个例子 :
(重要) : $(Z_p{}^*, \times)$ **是群吗?**

- 首先 $Z_p{}^*$ 的意思是**正整数模 p**

1. 封闭性 : 相乘后模 p, 还是$(Z_p{}^*)$ 里的元素
2. 结合律 : 模运算下的乘法满足乘法结合律
3. 单位元 : 1
4. 逆元 : 乘法逆元 $a \times b \equiv 1 \pmod{p}$

> $(Z_p{}^*, \times)$ 中的元素是所有与 p 互质的整数，它们的数量为 $\varphi(p) = p - 1$

举个栗子 : $(Z_7{}^*, \times) := \{1, 2, 3, 4, 5, 6\}$

① $(Z, +)$ ✅

1. 封闭性 : 整数相加还是整数
2. 结合律 : 整数相加满足加法结合率
3. 单位元 : 0 (任何整数 + 0 都等与它本身)
4. 逆元 : 互为相反数

② $(Q, \times)$ ❌

1. 封闭性 : 有理数相乘还是有理数
2. 结合律 : 有理数相乘满足结合率
3. 单位元 : 1 (任何整数 $\times 1$ 都 == 它本身)
4. 逆元 : 有理数的倒数 (但是注意 🦐, 0 是没有逆元的 , 所以这个**不是一个群**)

③ $(Q \backslash \{0\}, \times)$ ✅

- 还是有理数乘法群, 只需要把 0 排除在外, 就又是一个群了

群的性质

- 有限群 :
  - G 是有限集合, 如 $(Z_p{}^*, \times)$ 里某实例 $(Z_7{}^*, \times)$ 有 6 个元素
  - $|G|$ 记为 G 的元素个数, 称作群 G 的阶
- 无限群 :
  - G 是无限集合, 比如 $(Z, +)$, $(Q \backslash \{0\}, \times)$
  - 此时群 G 的阶称为**无限阶**
- 定理 1 : 群里的单位元是唯一的 (反证法) ; 只包含一个元素(单位元)的群叫做**平凡群**

- 定理 2 : 群里的每个元素, 都且只有一个**逆元** (反证法)
- 消去律 : $a*b=a*c \quad \Rightarrow \quad b=c$
- 群方程 $a*x=b$, 有唯一解 $x\in G$, $x=a^{-1}*b$
- $(a\ *\ b)^{-1}=b^{-1}\ *\ a^{-1}$ (注意左右有顺序)
- $(a^{-1})^{-1}=a$

有限群:

> 在数学中，Zp ×*表示模p剩余系（即模p同余下的非零元素）上的乘法群，其中p是一个素数。Zp* ×中的元素是所有与p互质的整数，它们的数量为φ(p)=p-1，其中φ是欧拉函数。

Zp ×*是有限群的原因是，首先Zp* ×中的每个元素都有一个逆元，也就是说，对于每个a∈Zp ×，*存在另一个元素b∈Zp* ×，使得a×b ≡ 1 (mod p)。这是因为p是一个素数，因此每个非零元素都是模p的单位元素。因此，Zp* ×是封闭的，结合的，具有单位元素1和逆元素，满足群的四个基本公理。

其次，由于p是素数，因此每个非零元素在Zp ×*中都是互异的。这意味着，Zp* ×中的元素的数量是有限的，具体而言，它的大小为φ(p)=p-1。因此，Zp* ×是一个有限群。

消去律证明 (同时 $\times$ 逆元 a^{-1}):

$$
\begin{aligned}
& a*b=a*c \\
\Rightarrow \quad & a^{-1}*a*b=a^{-1}*a*c \\
\Rightarrow \quad & e*b=e*c \\
\Rightarrow \quad & b=c
\end{aligned}
$$

$(a\ *\ b)^{-1}=b^{-1}\ *\ a^{-1}$ 证明 :

$$
\begin{aligned}
& (a*b)*(b^{-1}*a^{-1}) \\
\Rightarrow\ & a*(b*b^{-1})*a^{-1} \qquad \text{群的运算不一定满足交换律} \\
\Rightarrow\ & a*(b*b^{-1})*a^{-1} \\
=\ & e
\end{aligned}
$$

所以是 $(b^{-1}*a^{-1})$ 而不是 $(a^{-1}*b^{-1})$

Abelian group 阿贝尔群/交换群

定义 : 如果对于群 G 中 $\forall a,b\in G$, 都有下式成立, 则称 G 为阿贝尔群/交换群

$$a*b=b*a \qquad \text{(交换律)}$$

定理 ① : G 是阿贝尔群, $\forall a,b\in G$ 有 $(a\ *\ b)^t=a^t\ *\ b^t$

总得来说, 一个阿贝尔群要满足 5 个性质 : {封闭性, 结合律, 单位元, 逆元, **交换律**}

之前的几个例子 : $(Z_p{}^*,\ \times)$, $(Q\backslash\{0\},\times)$ 等都满足交换律, 所以他们都是阿贝尔群

群的简记符号表示 :

- a^t : a^t 表示的不是 t 次方 , 而是**表示 `t` 个 `a` 一起运算** , 注意这个并不表示 `t` 和 `a` 之间的运算 , 因为 `t` 是整数 , 而 `a` 是 Group 内的元素 (群里的元素不一定是整数, 也有可能是抽象符号)
- a^{-t} : ...
- $(a^t)^m=a^{tm}$: 有了上面 2 个铺垫
- $a^t\ *\ a^m=a^{m+t}$
- $(a^{-1})^t=(a^t)^{-1}=a^{-t}$

定理证明 : 用交换律换来换去即证

Subgroup 子群

定义: 设 $(G,*)$ 是 Group , H 是 G 的非空子集 , 如果 $(H,*)$ 也是一个 Group , 则称 $(G,*)$ 是 $(H,*)$ 的 subgroup

G 的子群:

1. 真子群(非平凡子群): $(H,*)$ 且 $H \neq \{e\}, G$
2. 平凡子群: ① 只由单位圆构成的 Group : $(\{e\},*)$ ② 其自身: $((G,*))$

定理 ① : Group 的单位元也是其 `subgroup` 的单位元 (反证法)

- 比如 $(R,+)$、$(Q,+)$、$(Z,+)$ 每 `next one` 都是 `prev one` 的子群, 但其的单位元**都是 0**
  定理 ② : 元素在 `subgroup` 中, 其逆元也必在该子群中

判断子群 :
方法① 看性质, 是否满足:

1. 非空子集
2. 封闭性
3. 结合律
4. 单位元
5. 逆元

方法② :
- 定理 : `H` 是 Group `G` 的非空子群 , 若对于任意的 $a,b \in H$, 都有 $a * b^{-1} \in H$, 则 `H` 是 `G` 的子群 ;
- 定理 : `H` 是 Group `G` 的非空子群 , 若果 `H` 是有限集 , 而且 G 的运算 $*$ 在 H 上满足封闭性 , 则 `H` 是 `G` 的子集

子群的构造(Abelian group)

法① : G^m 运算 m 次

定理 ① : G 是阿贝尔群, $m \in Z$, 则下式 ↓ 是 G 的子群

$$G^m := \{a^m \mid a \in G\}$$

定理 ① 解释 —— 比如 $m == 3$:

- $G^3 := \{a^3 \mid a \in G\}$ —— 意思就是 G 里的每个元素**自己对自己运算三遍**
- $G^{-3} := \{(a^{-1})^3 \mid a \in G\}$ —— 意思就是 G 里的每个元素的逆元**自己对自己运算三遍**

定理 ① 举例 —— 当 p 是奇素数时, $(Z_p{}^*, \times)$ 是个交换(阿贝尔)乘法群 :
模 p 乘法下, **二次剩余就是它的子群** (因为这相当于 $m == 2$, 二次剩余的集合就是把 $Z_p{}^*$ 里所有的元素都自己做平方模 p):

$$(Z_p{}^*, \times)^2 \in_{subgroup} (Z_p{}^*, \times)$$

拓展一下, 对任意整数 n 的 任意次剩余 m (m 次剩余) :

$$(Z_n{}^*, \times)^m \in_{subgroup} (Z_n{}^*, \times)$$

法② : $a^m = e$

定理 ② : G 是阿贝尔群, $m \in Z$, 则下式 ↓ 是 G 的子群

$$\begin{aligned} G\{m\} &:= \{a \in G \mid a^m = e\} \\ (\ G^m &:= \{a^m \mid a \in G\} \qquad \leftarrow \text{对比上式}) \end{aligned}$$

现在的玩法是, 把对自己做了 m 次运算后, 结果 $== e$ 的都挑出来构成子群

整数群的子群

定理 ① : H 是 Z 的子群, 则存在唯一的非负整数 m , 使得 $H = mZ$

> 如果一个集合**不是 G 的倍数形式, 那它就必然不是整数群 G 的 `subgroup`**

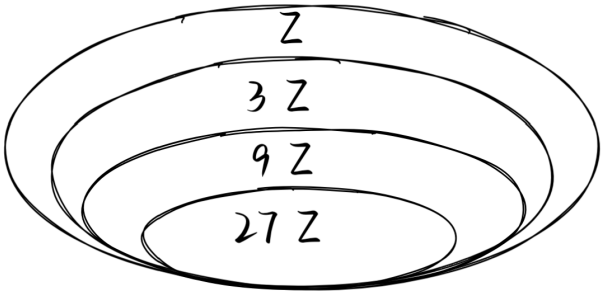
定理 ② : $m1$ 和 $m1$ 是非负整数, 则 $m_2 \mid m_1$, 当且仅当 $m_1 Z \in_{sub-G} m_2 Z$

定理② 举例 : 例如 $3 \mid 9$, $9Z$、$3Z$ 都是 Z 的子群, 因为

$$\begin{aligned} 3Z &= \{0, \pm 3, \pm 6, \pm 9, \ \ldots\} \\ 9Z &= \{0, \pm 9, \ \ldots\} \end{aligned}$$

可见 $9Z \in_{sub-G} 3Z$ ($9Z$ 是 $3Z$ 的子群)

$27Z \in 9Z \in 3Z \in Z$



定理 ③

子群构造子群

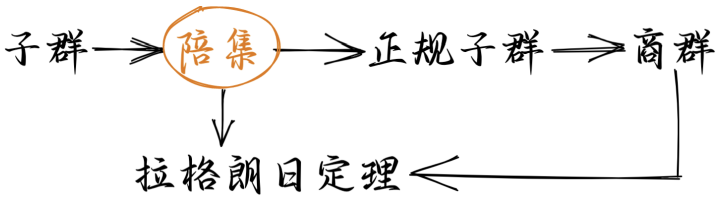
coset 陪集

coset 性质 1~ :

- $a \in [a]_H$: 每个元素必然进入由 `itself` 构造的 `coset` 里
  - 后面有证明
- $[e]_H = H$: 子群 H 本身 is a coset , 它相当于用 `单位元` 和 `H` 构造出来的 coset , 叫做平凡陪集
  - $a \in H \iff [a]_H = H$
- $[a]_H = [b]_H \iff a^{-1} * b \in H \quad (Or \ b^{-1} * a \in H)$
  - 比如 $[2]_{3Z} = [2]_{3Z} \iff 2^1 \cdot 2 \in H\ (3\mathbb{Z})$
  - 后面有证明

陪集定理 : 子群的两个右陪集（或左陪集），要么有完全相同的元素，要么没有任何公共元素。

陪集在下图中的中心位置 :



定义 : H 是群 G 的子群, $a \in G$, 则 :

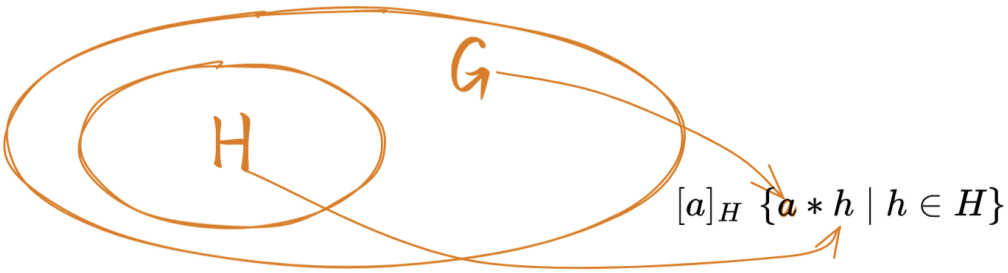
$$\begin{aligned} aH &:= \{a * h \mid h \in H\} \quad : \quad \text{左陪集}(left\ \ cost) \\ Ha &:= \{h * a \mid h \in H\} \quad : \quad \text{右陪集}(right\ \ cost) \end{aligned}$$

称为 H 关于 a 在 G 中的 左(右)陪集 ;

如果 $aH = Ha$, 则称其为 H 关于 a 在 G 中的陪集 (coset) ; **a 叫做代表元 (`representative`)**

元素 a 和 子群 H 构造的陪集**用符号 $[a]_H$ 表示**

画个图如下 :



Coset 的研究目的是以子群 H 为基准, 去观察群里每个元素与 H 之间的关系

举个栗子 : $(Z, +)$ 整数加法群 , 子群 $3Z \in Z$, 则陪集 (coset) :

$$
\begin{aligned}
[0]_{3Z} &= \{0,\ \ 0 \pm 3,\ \ 0 \pm 6,\ \dots,\} \\
[1]_{3Z} &= \{1,\ \ 1 \pm 3,\ \ 1 \pm 6,\ \dots,\} \\
[2]_{3Z} &= \{2,\ \ 2 \pm 3,\ \ 2 \pm 6,\ \dots,\} \\
&\dots
\end{aligned}
$$

因为是加法群, 构造的 cosets 如上, 可以看到 : **每个整数只会存在唯一的一个 coset 中**

所以这种陪集实际上是对整数 Group 进行的划分, 划分的依据是 **和子群 $3Z$ 的关系** :

- 和 $3Z$ 距离是 `0` (在 $3Z$ 中的) 归为一个集合 ;
- 和 $3Z$ 距离是 `1` 的归为一个集合 ;
- 和 $3Z$ 距离是 `2` 归为一个集合 ;

证明 - 性质 1: $a \in [a]_H$: 每个元素必然进入由 `itself` 构造的 `coset` 里

$$
H = \{e\ ,\ \dots.\ \}
$$

$$
\begin{aligned}
[a]_H &= \{a * e\ ,\ \dots.\ \ \} \\
&= \{a\ ,\ \dots.\ \ \}
\end{aligned}
$$

$$
故 \quad a \in [a]_H
$$

证明 - 性质 2: 显然, 略

证明 - 性质 3: $[a]_H = [b]_H \iff a^{-1} * b \in H \quad (Or\ \ b^{-1} * a \in H)$

$$
H = \{e\ ,\ \dots\ , h^1,\ h^2,\ \ \dots\ ,\}
$$

$$
\begin{aligned}
[a]_H &= \{a\ ,\ \dots\ , ah^1\ , ah^2\ \dots\ ,\} \\
[b]_H &= \{b\ ,\ \dots\ , bh^1\ , bh^2\ \dots\ ,\}
\end{aligned}
$$

$$
\begin{gathered}
\because [a]_H = [b]_H\ ,\ \text{且}\ a \in [a]_H\ ,\ \ b \in [b]_H \\
\therefore \text{必有}\ \{b = ah^* \mid h^* \in H\} \\
\text{故} \Rightarrow \ \ a^{-1} * b \in H \quad (Or\ \ b^{-1} * a \in H)
\end{gathered}
$$

(下面是 Chatgpt 写的证明, 我总觉得怪怪的 ....)

在子群 $H = 3\mathbb{Z}$ 中，任意的陪集 $[a]_H$ 可以写成 $[a]_H = a + 3n \mid n \in \mathbb{Z}$ 的形式，其中 a 是 H 中的代表元素。

现在考虑两个陪集 $[a]_H$ 和 $[b]_H$，我们要找到一个例子满足 $[a]_H = [b]_H$ 当且仅当 $a^{-1}b \in H$。

我们可以选择 $a = 3$ 和 $b = 9$ 作为例子。此时 $[3]_H = 3 + 3n \mid n \in \mathbb{Z} = \dots, -6, -3, 0, 3, 6, \dots$ 和 $[9]_H = 9 + 3n \mid n \in \mathbb{Z} = \dots, -3, 0, 3, 6, 9, \dots$，这两个陪集的元素分别是 3 和 9 模 3 的余数。

我们来验证一下 $[3]_H = [9]_H$ 当且仅当 $3^{-1}9 = 3 \cdot 3^{-1} \cdot 3 = 3 \in H$：

- 如果 $[3]_H = [9]_H$，则对于任意的 $n \in \mathbb{Z}$，都存在一个 $m \in \mathbb{Z}$，使得 $3 + 3n = 9 + 3m$，即 $n = m + 2$。因此 $3n = 3(m + 2)$，所以 $3n \in H$，于是 $3^{-1}(9) = 3 \cdot 3^{-1} \cdot 3 = 3 \in H$。
- 如果 $3^{-1}(9) = 3 \in H$，则对于任意的 $n \in \mathbb{Z}$，都有 $9 + 3n = 3(3 + n)$，因此 $9 + 3n \in 3 + 3m \mid m \in \mathbb{Z} = [3]_H$。反过来，如果存在 $m \in \mathbb{Z}$，使得 $3 + 3m = 9 + 3n$，则 $n = m + 2$，于是 $[3]_H = [9]_H$。

因此，我们得到了一个例子，使得在子群 $3\mathbb{Z}$ 中的任意陪集 $[a]_H$ 满足 $[a]_H = [b]_H$ 当且仅当 $a^{-1}b \in H$。

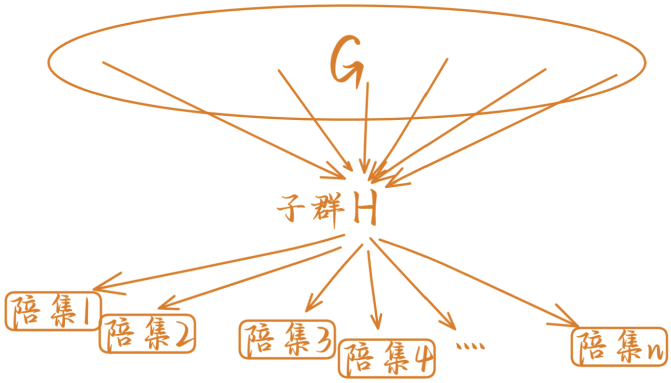
拉格朗日定理-1

> 好吧我承认这 chap 讲了半天也没讲到拉格朗日定理

子群 H 就像一个分类器, 会根据群 G 里的元素与他的关系, 将 G 进行 (互斥地) 划分

- 子群 H 本身就是第一个陪集, 称为平凡陪集
- 单位元在且仅在**子群 H 里** (即陪集 1)

- 其他的所有陪集**都不是子群**, 因为**不含有单位元**



拉格朗日定理：群G的阶g一定是子群H的阶h的整数倍

还是 $3\mathbb{Z}$,

$$
\begin{aligned}
3\mathbb{Z} &= \{0,\ \ 0\pm 3,\ \ 0\pm 6,\ \dots,\} \\
[0]_{3\mathbb{Z}} &= \{0,\ \ 0\pm 3,\ \ 0\pm 6,\ \dots,\} \\
[1]_{3\mathbb{Z}} &= \{1,\ \ 1\pm 3,\ \ 1\pm 6,\ \dots,\} \\
[2]_{3\mathbb{Z}} &= \{2,\ \ 2\pm 3,\ \ 2\pm 6,\ \dots,\} \\
&\dots
\end{aligned}
$$

拿 $[2]_{3\mathbb{Z}}$ 举例 , 同在 $[2]$ 这个陪集里的元素 , 它们的差必然是 `3` 的倍数 (比如 `5` 、 `8`) ,
其实, 2 个元素如果差值是子群 $3\mathbb{Z}$ 里的元素的话 , **就必然在同一个陪集里**

5 & 8 做差值就相当于是 一个元素的逆元(相反数) 与 另一个元素运算

> 所以 a 和 b 在同一个陪集的条件是 $a^{-1}b$ 或是 $b^{-1}a \in H\ (subgroup)$

对上面一句话的解释 : 比如 $a=5, b=8$
那么 $b+a^{-1}\quad means\ \ that\quad 8-5=8+(-5)$

> 为什么 $a==5$,　$a^{-1}==-5$? —— 因为这是个加法群, 单位元是 0 !!!!
> 注意 : $b+a^{-1}$ 也就是 ba^{-1} , 因为 ba^{-1} 表示 b 运算 a^{-1} , 不是乘法 !!!

现在, 你应该完全理解了上一节性质 3 ($[a]_H=[b]_H \iff a^{-1}*b\in H\quad (Or\ \ b^{-1}*a\in H)$) 的含义

这个定理也可以这么写 :

$$
b=ah\quad (或\ \ a=bh)\ ,\ \ \exists h\in H
$$

这种写法说明 a、b 与子群的 "关系 `relationship` " 是相同的

针对元素和子群的关系, 引入一个专门的二元关系 :

$$
a\equiv b\pmod{\{H\}}\quad : 表示\ a/b\ 在(同一个由\ H\ 构造的)陪集里
$$

他表示一种二元关系, 而不是运算!! 注意
他表示用子群 H 构造陪集时, a 和 b 被分到了同一个陪集里 ; 或者说 , a 和 b 与子群的关系相同

$$
\begin{aligned}
&a\equiv b\pmod{\{H\}}\quad means\quad a、b\ 在同一个陪集 \\
\iff\ &b=ah\quad ,\exists h\in H \\
\iff\ &b\in [a]_H\ \ ,\exists h\in H \\
\iff\ &[b]_H=[a]_H
\end{aligned}
$$

以上几种写法都是可以相互替换的 , **故** $[a]_H$ **可以理解成** :

1. 以 a 为代表元 representative 的陪集 coset
2. a 和 H 构造的 coset
3. 以 H 为分类依据时 , a 被分类到的 coset

▪ (mod H) 是一种等价关系

- 自反性 : 对于 $\forall a\in G$, 都有 $a\equiv a\pmod{H}$
- 对称性 : 对于 $\forall a,b\in G$, 都有

    - $a \equiv b \pmod{H} \quad \Rightarrow \quad b \equiv a \pmod{H}$
- 传递性 : 对于 $\forall a, b, c \in G$, 都有
    - $a \equiv b \pmod{H}$, $b \equiv c \pmod{H} \quad \Rightarrow \quad a \equiv c \pmod{H}$

本质上在整数群里, 陪集 和 剩余类 是同一个东西 (历史原因分开讲了) 本质上就是一种等价类

双射、等势

在数论中，双射是指一个函数 $f : A \to B$，其中 A 和 B 是两个集合，满足以下两个条件：

1. 对于 A 中的每个元素 a，都存在 B 中的一个唯一元素 b，使得 $f(a) = b$。
2. 对于 B 中的每个元素 b，都存在 A 中的一个唯一元素 a，使得 $f(a) = b$。

简而言之，双射是一个 “一一对应” 的函数，它将一个集合中的每个元素映射到另一个集合中唯一的元素上，并且每个元素都有一个逆映射。

当集合 A 和 B 之间存在双射时，它们被称为等势（equipotent），也可以说它们具有相同的基数（cardinality）。这意味着两个集合之间存在一种一一对应的关系，使得它们具有相同数量的元素。

例如，集合 $1, 2, 3$ 和集合 a, b, c 之间存在双射，其中函数 f 可以定义为 $f(1) = a$，$f(2) = b$，$f(3) = c$。因此，这两个集合是等势的，它们都有三个元素。

拉格朗日定理-2

定理 : G 是**有限群**, H 是 G 的任意子群 , 则 $|H| | |G|$

- G 的大小 $|G|$ 是 $|H|$ 的倍数
- 或者说, G 的任意子群的阶, 必然是它的阶的因子
- 比如 : $|G| = 15$, 子群的阶只可能是 1, 3, 5, 15, 不可能是其他的

证明 :

....

拉格朗日定理在群论中的一些应用：

1. 确定子群的阶数
2. 确定群的阶数：如果一个群 G 的某个子群 H 的阶数已知，那么可以通过拉格朗日定理得到 G 的阶数。
3. 证明某些元素不可能是群元素：如果一个元素 g 不属于子群 H，那么它一定属于某个左陪集 gH。因此，如果 $|gH| \neq |H|$，那么 g 不可能是群元素。
4. 求解离散对数问题：设 G 是一个阶为 n 的群，g 是它的一个生成元，$h \in G$。如果我们知道 g 和 h 属于同一个循环群，那么可以使用拉格朗日定理来求解离散对数问题，即求解 $g^k = h$ 中的 k 值。
5. 确定群的性质：拉格朗日定理可以用来证明一些群的性质，如阶数为素数的群是循环群，没有平方元素的有限群的阶数必须是 2 或者一个奇素数等等。

≡ (mod H) 是一种等价关系 复习

性质 : 任意 2 个 cosets $[a]_H$ 和 $[b]_H$ 之间存在双射 , 任意陪集 $[a]_H$ 和子群 H 是等势的

> 这告诉我们一个重要性质 :
>
> 1. 同一个子群构造的所有陪集, 它们的大小都是相等的 ;
> 2. 而且 这些陪集的大小都等于子群(subgroup) 的大小 :
>   sizeof(any coset) == sizeof(subgroup) :

商群/正规子群

> md 没看懂

正规子群定义:

> 说实话，要理解为什么要引入 正规子群 Normal subgroups ，就必须对求解多项式的理论进行大量的工作理解。

首先，让我们来看正规子群。在群论中，一个群的正规子群是指一个子群，满足对于任意的群元素 g，其在该正规子群中的像元素 g' 满足 $g'ag'^{-1}$ 仍然属于该正规子群。也就是说，正规子群是满足对于任意群元素 g 和正规子群中的元素 n，都有 gng^{-1} 也在该正规子群中的子

群。正规子群通常被记作 $H \trianglelefteq G$，其中 H 是 G 的子群，$\trianglelefteq$ 表示“正规”。

接下来，我们来看商群。在群论中，给定一个群 G 和它的正规子群 H，则 H 作为 G 的子群的所有左陪集所构成的集合，构成了一个群，称为 G 模 H 的商群。商群的符号通常是 G/H。商群中的元素是由左陪集构成的，也就是 $gH = gh|h \in H$，其中 g 是 G 中的任意一个元素。商群中的运算是将左陪集相乘，即 $(g_1H) \cdot (g_2H) = g_1g_2H$。

通俗来说，正规子群是满足一定条件的子群，可以看做原群中某些元素的“代表”，而商群则是用左陪集表示的，相当于将群元素分成了几个等价类，它们的运算规则是由子群和原群共同决定的。

群同态 homomorphism

同态像: $Im\ \ f := f(G) := \{f(a) \mid a \in G'\}$
同态核: $Ker\ \ f := \{a \in G \mid f(a) = e'\}$

群同态本质上是定义在群和群之间的映射(函数), 类似于在 2 个群之间建立了一条**穿越通道** ,可以将一个群的元素映射成另一个群的某个元素

设 f 是定义在群 G 和 G' 之间的映射(函数) , 群 G 的元素 a 经过它穿越到群 G' 之后, 元素模样会发生变化变成 $f(a)$, 但元素之间的运算规律仍能得到保持

下面给出详细定义: 设群 $(G,\ *)$ 与 $(G,\ \otimes)$, 如果函数 $f:\ G \to G'$ 对于 $\forall a,\ b \in G$ 都有

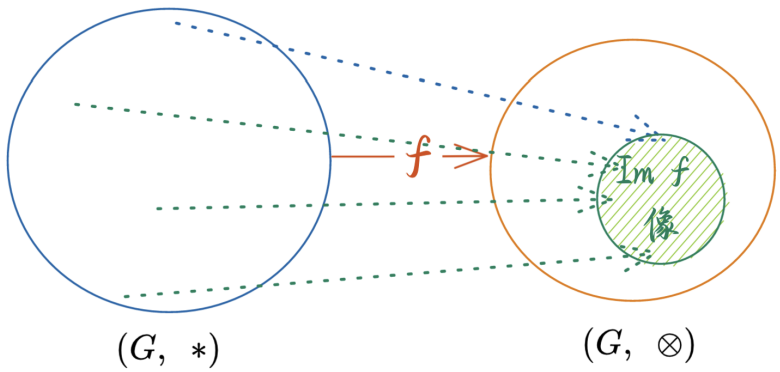
$$f(a * b) = f(a) \otimes f(b)$$

则称 f 为 $(G,\ *)$ 到 $(G,\ \otimes)$ 的群同态

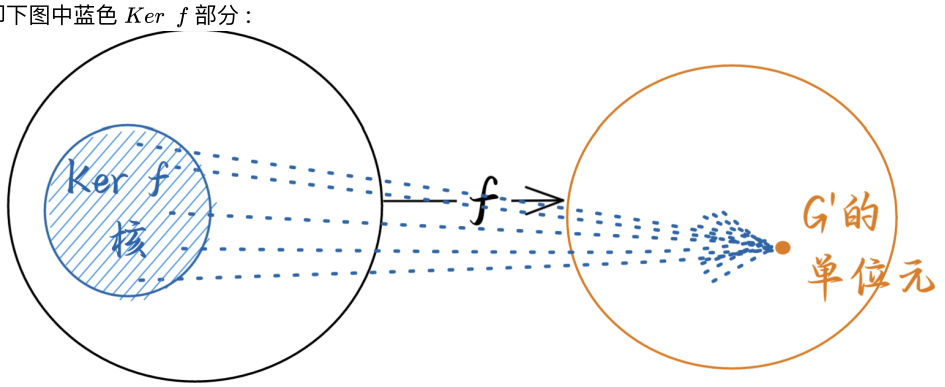
因为群之间的差异, 有的群很容易分析, 有的群则不, 利用 homomorphism 这种映射, 我们就能用一个群的性质去分析另一个

群之间的 homomorphism 可能会有很多个, 不止一个, 也就是说, G 中元素经过 f 之后的落点可能只是 G' 的子集, 即 G' 中的很多元素在 G 中找不到原像, 因此, 就引出 f **的同态像(简称像)** 这种重要集合, 用 $Im\ \ f$ 表示

> 像 就是 G' 中能找到原像的那些元素所构成的子集, 即下图中绿色 $Im\ \ f$



另一个重要集合是**同态核(核 kernel)** , 用 $Ker\ \ f$ 表示, 核这个概念关心的是定义域 G 里的元素: G 中经 f 映射等于 G' 的**单位元** 的那些元素, 即下图中蓝色 $Ker\ \ f$ 部分 :



几个例子 :

① 嵌入映射 (`inclusion map`) : 子群 和 群之间可以定义一个群同态
② 自然映射 (`natural map`) :

$$G \xrightarrow[addd]{f} G/N$$

$$G \xrightarrow[addd]{f} G/N$$

第一同构定理

一个函数, 即是单射, 又是满射, 那么就是一个双射
一个**群同态**还是双射函数, 他就是**群同构**

> 群同构是特殊类型的群同态, 它即是双射, 又满足群同态的性质

循环群 Cyclic Group

定理: 设 G 是群, $a \in G$, 则 :

$$< a > \ := \ \{ \ a^z \mid z \in Z \ \} \quad \text{是由} \ \ a \ \ \text{生成的} \ \ G \ \ \text{的子群}$$

`Cyclic Group` 定义:

- G is a group, IF $G =< g >$, 则称 G 是循环群 , g 是循环群 G 的生成元 (generator)

生成元 : 群里的元素 g , 他自己运算自己玩, 就能产生群里所有的元素 (或者说群里所有元素都能由 g 生成)

> 这个操作叫做用 g 对 G 进行循环移位。

定理 2: 任意循环群 Cyclic Group **都是** `Abelian Group`
证明(非常简单) : 对循环群 $< g >$ 里的任意 2 个元素 $a = g^r$, $b = g^k$, 只需证明 $ab = ba \quad$ 即 $\quad g^r \cdot g^k = g^k \cdot g^r$

定理 3: Cyclic Group 的 `subgroup` 必然是 Cyclic Group

定理 4: 假设 G 是 $< g >$ (Cyclic Group) , H 是其子群 , 则商群 G/H 是循环群

例 1: 整数群 Z 是加法**循环群** (cyclic group!) ± 1 是它的 generator 可以写成 $< 1 >$ 或 $< -1 >$
因为是加法群, 所以 1 或 -1 运算 z 次 , 就可以写成 $1 \cdot z \quad or \quad -1 \cdot z$ 的形式 , 这样就可以得到其他所有整数 :

$$\begin{aligned} Z &= \{ z \mid z \in \mathbb{Z} \} \\ &= \{ z \cdot 1 \mid z \in \mathbb{Z} \} =< 1 > \\ &= \{ (-z) \cdot 1 \mid z \in \mathbb{Z} \} =< -1 > \end{aligned}$$

例 2: $m\,\mathbb{Z}$ 是加法**循环群** : $\pm m$ 是它的 generator 可以写成 $< m >$ 或 $< -m >$
$m / -m$, 它们自己运算, 就可以得到其他元素 (因为 $m\,\mathbb{Z}$ 就表示 m 的倍数的集合)

例 3: ${Z_5}^* = \{1, 2, 3, 4\}$ 是乘法循环群, {2} 和 {3} 都是其 `generator`
(${Z_5}^* =< 2 >=< 3 >$)
如下, 2 自己运算得到 2 , 运算 2 遍得到 4 , 运算 3 遍得到 3 ... :

$$2^1 = 2; \ \ 2^2 = 4; \ \ 2^3 = 3; \ \ 2^4 = 1; \ \ldots$$

> 所以说, 一个循环群可以有很多 `generator` , 所以在公钥密码算法例, 经常会看到 "随机选择一个生成元" 这样的表述 :
> $g \in G \quad Generator \ldots$

- 无限循环群 : 群元素个数无限: ($\mathbb{Z}$, $m\,\mathbb{Z}$)
- 有限循环群 : 群元素个数有限: (${Z_5}^*$)

循环群的性质非常重要，其中最重要的一点是循环群的阶（即元素个数）可以非常大，但是它们的结构相对简单，因此在数学和应用领域都有广泛的应用。特别地，循环群在密码学、编码理论、量子力学等领域中都有重要应用。

举例来说，整数集合 $\mathbb{Z}$ 上的加法群是一个循环群，它的生成元可以是任意整数，例如 1。用 1 进行循环移位就是一直加上 1，可以得到 $\mathbb{Z}$ 中的所有整数。这个群的阶是无限的。另一个例子是模 n 的剩余类集合 `{0, 1, 2, ..., n-1}` 上的乘法群，如果 n 是质数，那么这个群是一个循环群，它的生成元可以是任意一个与 n 互质的数。例如当 n=7 时，3 是一个生成元，因为用 3 不断进行乘法运算可以得到 `{0, 1, 2, 3, 4, 5, 6}` 中的所有数。这个群的阶是 `n-1` 。

元素的阶 (order)

性质1 : 有限循环群的阶是 n , 则生成元 g 的阶也是 n , 且群里元素 $g, g^2, g^3, \ldots, g^n \ \ (= g^0 = e)$ 各不相同

- 有限循环群的元素个数 == 生成元到 e 的距离 , 这很直观 :
- generator 的产量决定了群的大小 (因为产量一旦达到群阶的大小, 再产生的就是以前生成过的元素了)
- 举个例子 : $|Z_5{}^*| = |\{1,2,3,4\}| = 4$, 则 $2^4 \pmod 5 = e = 1$

性质 2: 对于正整数 $d \mid n$, n 阶有限循环群恰好有唯一的 d 阶子群
证明: ...
例: 循环群 G 的阶是 15, 15 的正因子 $\{1,3,5,15\}$, 所以, G 一共有 4 个子群, 它们的阶分别是 $\{1,3,5,15\}$

性质 4: 素数阶 (元素个数为 5/7/11...) 的群必然是有限循环群

循环群的同构

---

what is order ?
如果 n 是使 $a^n = e$ 实现的最小正整数, n 就叫元素 a 的阶

$$a^{min(n)} = e$$

元素的阶 表达的含义是 : 元素 a 自己运算 n 遍就**到达了单位元** e (是不是很类似于**走阶梯**?)
所以这个 n 就可以理解为**元素到单位元 e 的距离**

> 当然, 有的元素不管对自己运算多少遍 , 都接近不了单位元, (这就是吒儿的命吧) , 这种倒霉孩子就是**无限阶的**

区分 群的阶 和 元素的阶 :

1. 一个 *群的阶* 是指其势，即其元素的个数；
2. 元素的阶是元素到单位元 e 的距离

Cryptography

密码学中常用循环群是因为循环群具有一些重要的性质，如：

1. 生成性：循环群中的元素可以通过重复对一个生成元素进行操作而生成。
2. 离散性：循环群中的元素数量有限且离散，这使得循环群中的元素难以被猜测或预测。
3. 难以计算的离散对数问题：在循环群中，对于给定的元素和生成元素，计算出元素的对数是困难的，这是很多密码算法的基础。

一个循环群可以有很多 `generator` , 所以在公钥密码算法例, 经常会看到 "随机选择一个生成元" 这样的表述

循环群 $\mathbb{Z}_7$ $(p = 7)$ 以 3 为生成元的构造方法如下：

首先，我们定义 $\mathbb{Z}_7$ 为整数集合 $0,1,2,3,4,5,6$ 上的模 7 加法运算，即对于任意 $a, b \in \mathbb{Z}_7$，定义 $a + b$ 的值为 a 与 b 在 $\mathbb{Z}_7$ 中相加后对 7 取余的结果：

$$a + b = \begin{cases} a + b - p, & \text{if } a + b \geq p \\ a + b, & \text{if } a + b < p \end{cases}$$

接下来，我们以元素 3 为起点，不断对其进行加法运算，直到得到 $\mathbb{Z}_7$ 中的所有元素，形式化地，生成的集合为：

$\langle 3 \rangle = 3, 6, 2, 5, 1, 4, 0$
$3,\ 3+3,\ 3+3+3 \pmod 7 == 2,\ 3+3+3+3 \pmod 7 == 5 \ldots$

其中，$\langle 3 \rangle$ 表示由元素 3 生成的循环子群。因为群 $\mathbb{Z}_7$ 中所有元素都可以由元素 3 生成，所以 $\langle 3 \rangle$ 是 $\mathbb{Z}_7$ 的一个生成元。

群内元素为 $0,1,2,3,4,5,6$。