2.1 群的定义

2023年9月19日 17:15

群的定义

(第一定义) 设G为非空集合，若G上存在二元运算(称为乘法)满足：

1° 封闭性. i.e. $\forall a,b\in G.\ ab\in G$

2° 结合律. i.e. $\forall a,b,c\in G,\ a(bc)=(ab)c$

3° 存在左单位元. i.e. $\exists e\in G,\ \forall a\in G,\ ea=a$.

4° 存在左逆元. i.e. $\forall a\in G,\ \exists a^{-1}\in G.\ a^{-1}a=e$.

则称G关于该运算构成一个群.

(第二定义) 第一定义中的3°, 4°合并为：

$\forall a,b\in G$, 方程$ax=b$和$ya=b$在G上都有解.

(第三定义) 第一定义中的3°加强为：

存在单位元. i.e. $\exists e\in G,\ \forall a\in G,\ ea=ae=a$.

第一定义中的4°加强为：

存在逆元. i.e. $\forall a\in G,\ \exists a^{-1}\in G.\ a^{-1}a=aa^{-1}=e$.

存在左单位元 $\Rightarrow$ 左单位元也是右单位元
存在左逆元 $\Rightarrow$ 左逆元也是右逆元

类似地：利用 $ea=((a^{-1})^{-1}a^{-1})a=(a^{-1})^{-1}e$ 又左程代到右

$ae=e(ae)=(ea)e=(((a^{-1})^{-1}a^{-1})a)e=((a^{-1})^{-1}(a^{-1}a))e=((a^{-1})^{-1}e)e$
$=(a^{-1})^{-1}e)e=(a^{-1})^{-1}e=(a^{-1})^{-1}(a^{-1}a)=((a^{-1})^{-1}a^{-1})a=ea=e$
$aa^{-1}=e(aa^{-1})=((a^{-1})^{-1}a^{-1})(aa^{-1})=(a^{-1})^{-1}(a^{-1}a)a^{-1}=(a^{-1})^{-1}ea^{-1}=(a^{-1})^{-1}a^{-1}=e$

第三定义 $\Rightarrow$ 第二定义

$\forall a,b\in G$, $ax=b$有解 $x=a^{-1}b$
$ya=b$有解 $y=ba^{-1}$

第二定义 $\Rightarrow$ 第一定义 (要证上，两个方程一个有解即可)

[法1] $\forall a,b\in G,\ \exists y\in G,\ s.t.\ ya=b$
同样也存在 $y'\in G,\ s.t.\ y'b=a$
于是 $(y'y)a=y'(ya)=y'b=a$. 即存在左单位元$y'y$
记$y'y=e$, $\exists a^{-1}\in G,\ a^{-1}a=e$, 即存在左逆元.

[法2] $\forall a\in G,\ \exists e\in G.\ s.t.\ ea=a$
对上述e, $\forall b\in G,\ \exists c\in G,\ s.t.\ ac=b$
于是 $eac=ac\Rightarrow eb=b$, e是左单位元
$\exists a^{-1}\in G,\ s.t.\ a^{-1}a=e$, 存在左逆元

单位元、逆元是唯一的
$(e=ee'=e',\ a^{-1}a=e=(a^{-1})'a \xrightarrow{\text{消去律}} a^{-1}=(a^{-1})')$

群的性质

1° 群中消去律成立, 即 $\forall a,b,c\in G$.
$ab=ac\Rightarrow b=c$ (左消去律)
$ba=ca\Rightarrow b=c$ (右消去律) (左或右乘a^{-1})

2° $(ab)^{-1}=b^{-1}a^{-1}$ ($abb^{-1}a^{-1}=e$)

特殊的"群"

半群 设S是一个非空集合, 若它有一个运算满足结合律.
则S关于这个运算构成半群

有限半群G构成群的充要条件是两个消去律成立

证明：(只需证两个消去律成立则群的第二定义的3°成立)
设$G=\{a_1,\cdots,a_n\}$, $\forall i,j,k:\ 1\le i,j,k\le n$, $a_ia_j=a_ia_k\Rightarrow a_j=a_k\Rightarrow j=k$
因此若$j\neq k$, 则$a_ia_j\neq a_ia_k$. 故$\forall a\in G$, $G=\{aa_1,\cdots,aa_n\}$
于是$\forall b\in G$, $\exists i:\ 1\le i\le n$, s.t. $aa_i=b$. 即方程$ax=b$有解.
对$ya=b$同理.

有单位元(既是左单位元，又是右单位元)的半群称为幺半群

如果一个半群既有左单位元，又有右单位元，则二者必相等且唯一
($e=ee'=e'$)

加群：运算用$+$表示, 单位元用0表示, 逆元用$-a$表示.
一般指交换群

整数加群$(\mathbb{Z},+)$

模n剩余类加群$(\mathbb{Z}/\sim,+)$ 本质相同 n次单位根群
其中$x\sim y\Leftrightarrow x\equiv y\ (\mathrm{mod}\ n)$
$[x]+[y]=[x+y]$

一般线性群$(GL_n(F)$, 矩阵乘法) 当$n>1$时, 非交换
(n级全体可逆矩阵)

8阶非交换群(四元数群)
$G=\{1,i,j,k,-1,-i,-j,-k\}$

加群	乘群
$0a=0$	$a^0=e$
$na=\underbrace{a+\cdots+a}_{n个}$	$a^n=\underbrace{a\cdots a}_{n个}$

单位元是唯一的, 且不存在非单位元的"单位因子"
群中没有所谓"单位"

2.2 群的阶

2023年9月21日 11:54

群的阶

使得 $\forall a\in G,\ a^m=e$ 的最小正整数 m 称为群 G 的阶

群中元素的阶 (以乘群为例)

对群 G 中的一个元素 a，使得 $a^m=e$ 的最小正整数 m 称为 a 的阶，记作 $|a|$. 如果不存在这样的 m，称 a 为无限阶的.

- 周期群：每一个元素的阶都有限
- 无扭群：除单位元外，每一个元素的阶都无限　Q_+ 乘群
- 混合群：其它　Q^* 乘群

Th1 有限群中每一个元素的阶都是有限的

证明：设 $G=\{a_1,\cdots,a_n\}$，

则 $\forall a_i,\ a_i,a_i^2,\cdots,a_i^{n+1}$ 中至少有两个相同

不妨设 $a_i^{r_1}=a_i^{r_2}$，$1\le r_1<r_2\le n+1$

于是 $a_i^{r_2-r_1}=e$

无限群中也可能每一个元素的阶都有限
如全体有次单位根对普通乘法作成的群三并)
$(i=1,2,\cdots)$

Th2 设 G 中元素 a 的阶为 n，则 $a^m=e\Leftrightarrow n\mid m$

Co2-1 如果存在整数 m 使得 $a^m=e$，则 $|a|$ 有限

Th3 若 G 中元素 a 的阶是 n，则 $|a^k|=\frac{n}{(k,n)}$ $(k\in\mathbb{Z})$

证明：设 $(k,n)=d$，则 $(a^k)^{\frac{n}{d}}=(a^n)^{\frac{k}{d}}=e$，$\frac{k}{d}\in\mathbb{Z}$.

设 $(a^k)^t=e$，由 Th2，$n\mid kt$

设 $k=k_1d$，$n=n_1d$，则 $(k_1,n_1)=1$，

从而 $n_1d\mid k_1dt$. 于是 $n_1\mid t$

故 $n_1=\frac{n}{d}\le t$，$|a^k|=\frac{n}{(k,n)}$

Co3-1 在群中设 $|a|=st$，则 $|a^s|=t$，其中 s,t 是正整数

$\underbrace{a\cdots a}_{s个a}\cdots\underbrace{a\cdots a}_{s个a}=e$　$t个(s个a)$

Co3-2 在群中若 $|a|=n$，则 $|a^k|=n\Leftrightarrow(k,n)=1$

Th4 设群中元素 $|a|=m$，$|b|=n$，则若 $ab=ba$ 且 $(m,n)=1$ 时，$|ab|=mn$

证明：$(ab)^{mn}\overset{交换}{=}(a^m)^n\cdot(b^n)^m=e$

设 $(ab)^s=e$. 则 $e=(ab)^{sm}\overset{\Delta}{=}(a^m)^s\cdot b^{ms}=b^{ms}$

由 Th2，$n\mid ms$. 因为 $(m,n)=1$，$n\mid s$

同理，$m\mid s$. 从而 $mn\mid s$. $mn\le s$.

故 $|ab|=mn$.

若不满足可交换
反例：在 $GL_2(\mathbb{Q})$ 中令 $A=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$，$B=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$
则 $|A|=4$，$|B|=3$
但 $AB=\begin{pmatrix}1&1\\0&1\end{pmatrix}$，$|AB|=\infty$
Jordan 块

Th5 设 G 为交换群，且 G 中所有元素有最大阶 m，则 G 中每个元素的阶都是 m 的因数，从而 $\forall x\in G$，有 $x^m=e$

证明：设 $a\in G$，$|a|=m$，则 $a^m=e$

假设 $\exists b\in G$，$|b|=n$，$n\nmid m$

则 $\exists$ 素数 p，s.t.

$m=p^{k_1}m_1$，$p\nmid m_1$

$n=p^{k_2}n_1$，$p\nmid n_1$，$k_1<k_2$

由 Co2 知，$|a^{p^{k_1}}|=m_1$，$|b^{n_1}|=p^{k_2}$

由于 $(m_1,p^{k_2})=1$ 且 G 是交换群，由 Th4，

$|a^{p^{k_1}}b^{n_1}|=m_1p^{k_2}>m$，矛盾

具有相同阶的元素

1° $|ab|=|ba|$

证明：设 $|ab|=n$，则

$(ba)^{n+1}=\underbrace{ba\cdots ba}_{n+1个ba}=b(ab)^na=ba$

由消去律，$(ba)^n=e$

设 $|ba|=m$，$m\in\mathbb{Z}^+$，同理 $(ab)^m=e$

由 Th2，$n\mid m$ 且 $m\mid n$，故 $m=n$.

2° $|A|=|A^{-1}|=|CAC^{-1}|$

证明：$(A^n)^n=(A^n)^{-n}$，iff. $A^n=e$ 时 $(A^{-1})^n=e$

$(CAC^{-1})^n=CA^nC^{-1}$，iff. $A^n=e$ 时 $(CA^nC^{-1})^n=e$

例：设 a 是群 G 中唯一一个阶为 2 的元素，则 a 可与 G 中所有元素交换.

证明：$\forall x\in G$，由于 $|xax^{-1}|=|a|=2$，

而 a 是群 G 中唯一一个阶为 2 的元素，

$xax^{-1}=a$，从而 $xa=ax$

利用"唯一"的方法：
构造满足相同条件的元素，
则二者相等

2.3 子群

2023年10月5日 23:48

定义 设G是一个群，H是G的一个非空子集. 如果H本身对G的乘法也作成一个群，则称H为G的一个子群，记作 $H \leq G$

- 平凡子群
  - 只由单位元作成的子群 $\{e\}$（或记为e）
  - G
- 非平凡子群/真子群：其它　记为 $H < G$

Th1 设G是群，$H \leq G$. 则H的单位元就是G的单位元，H中元素a在H中的逆元就是在G中的逆元.

证明：设H中单位元为e'，则 $e'e' = e' = e'e$（H，G）

由消去律（G），$e' = e$

设H中元素a在H中的逆元为a'，则 $aa' = e = aa^{-1}$（H，G）

由消去律（G），$a' = a^{-1}$

子集成群的充要条件

Th2.1 群G的非空子集H作成子群的充要条件是

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

（说明验证子群只需验证封闭性和有逆元）

合并

Proof. 必要性. 1)显然，2)由Th1亦显然.

充分性.

H中的代数运算就是G中的代数运算，结合律显然成立.

又因为 $e = aa^{-1} \in H$，H中有单位元. 证毕

Th2.2 群G的非空子集H作成子群的充要条件是

$a, b \in H \Rightarrow ab^{-1} \in H$　（$a^{-1}b \in H$ 亦可）

Proof. 由Th2.1必要性显然成立.

充、令 $b = a$，则有 $e = aa^{-1} \in H$

令 $a = e$，则有 $b \in H \Rightarrow b^{-1} \in H$

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

由Th2，$H \leq G$　证毕

Th3 群G的有限子集H作成子群的充要条件是H对G的乘法封闭，即 $a, b \in H \Rightarrow ab \in H$

Proof 充、H中G的乘法结合律成立，H作成半群.

$\forall a, b, c \in H$，若 $ac = bc$，将a, b, c看作G中的元素，可得 $a = b$，从而消去律在H中成立（另一个同理）

由"有限半群构成群的充要条件是两个消去律成立"（§2.1 Th1），H作成群.

例：特殊线性群 $SL_n(F) = \{A \in GL_n(F) \mid |A| = 1\}$ 是一般线性群 $GL_n(F)$ 的一个子群

（$\forall A, B \in SL_n(F)$，$|A||B^{-1}| = 1$，$AB^{-1} \in SL_n(F)$）

中心元与交换子群

定义 群 G 中元素 a 如果与 G 中的每一个元素都可交换，则称 a 是群 G 的一个**中心元**

若 G 的中心元只有 e，称 G 为**无中心群**

G 的全体中心元作成的集合 $C(G)$ 称为 G 的**中心**，G 是交换群 iff. $C(G)=G$

Th4 G 的中心 $C(G)$ 是 G 的一个子群

Proof. 因为 $e\in C(G)$，$C(G)$ 非空

$\forall a,b\in C(G)$，$\forall x\in G$，$ax=xa$，$bx=xb$

$abx=axb=xab$，

对 $ax=xa$ 两边左右都乘 a^{-1}，得 $xa^{-1}=a^{-1}x$

故 ab，$a^{-1}\in C(G)$ ☐

群的子集的乘积和逆

Def. 设 A,B 是群 G 的两个非空子集，规定

$AB=\{ab\mid a\in A,b\in B\}$，称为 A 与 B 的**乘积**

$A^{-1}=\{a^{-1}\mid a\in A\}$，称为 A 的**逆**

运算律 $(AB)C=A(BC)$，$A(B\cup C)=AB\cup AC$　　$A=B\Rightarrow AC=BC$，$CA=CB$

$(AB)^{-1}=B^{-1}A^{-1}$，$(A^{-1})^{-1}=A$　　$\not\Leftarrow$

于是对于群的子集，

$\forall a,b\in H,\ ab\in H\Leftrightarrow HH=H$

$\forall a\in H,\ a^{-1}\in H\Leftrightarrow H^{-1}=H$

$\forall a,b\in H,\ ab^{-1}\in H\Leftrightarrow HH^{-1}=H$

Th5 设 H 是 G 的一个非空子集，则

$H\le G\Leftrightarrow HH=H$ 且 $H^{-1}=H$

$\Leftrightarrow HH^{-1}=H$（由 Th2）

特别，如果 H 有限，

$H\le G\Leftrightarrow HH=H$（由 Th3）

（实际上，右端条件都可弱化为包含式）

Th6 设 H,K 是 G 的两个子群，则

$HK\le G\Leftrightarrow HK=KH$

$HK=KH\not\Leftarrow$ H 中元素与 K 中元素可交换

Proof. $(\Rightarrow)$ $HK\le G\Rightarrow (HK)^{-1}=HK$

$\Leftrightarrow K^{-1}H^{-1}=HK$

$\xrightarrow{H,K\le G\Rightarrow H^{-1}=H,K^{-1}=K}KH=HK$

$(\Leftarrow)$ $HK(HK)^{-1}=HKK^{-1}H^{-1}$

$\xrightarrow{H,K\le G\Leftrightarrow HH^{-1}=H,KK^{-1}=K}HKH$

$=HHK=HK$

$\Leftrightarrow H\le G$

Co 交换群的任二子群之积仍为子群

特别，当 $A=\{a\}$ 时，AH 可写为 aH.

除了群子集的基本运算性质，还满足

$b\in H\Leftrightarrow ab\in aH$

$H=K\Leftrightarrow aH=aK$

$H\le K\Leftrightarrow aH\le aK$

如果 φ 保乘法，则 $\varphi(aN)=\varphi(a)\varphi(N)$

交集、并集构成子群的条件

设 $H\le G$，$K\le G$. 则

1) $H\cap K\leq G$

2) $H\cup K\leq G \Leftrightarrow H\subseteq K$ 或 $K\subseteq H$

或 $\xrightarrow{\text{反面}}$ 且

用反证避免分类

Proof. 1) $\forall a,b\in H\cap K\subseteq H$, $ab^{-1}\subseteq H$

同理 $ab^{-1}\in K$, 故 $ab^{-1}\in H\cap K$

所以 $H\cap K\leq G$

2) ($\Rightarrow$) 假设RHS不成立, 则 $\exists h\in H-K\subseteq H\cup K$, $k\in K-H\subseteq H\cup K$

从而 $hk\notin H$ 且 $hk\notin K$, $hk\notin H\cup K$, 矛盾

($\Leftarrow$) $H\cup K=H$ 或 $H\cup K=K$.

显然

2.4 循环群

2023年10月10日 16:13

生成的子群

Def. 设M是群G的一个非空子集，称群G的包含M的子群之交为由M生成的子群，记为$\langle M\rangle$.
把M叫作这个子群的生成系
当|M|有限时，可简记作$\langle a_1,\cdots,a_n\rangle$

由于子群的交仍是子群，
$\langle M\rangle$是G的子群.
$\langle M\rangle$是包含M的最小子群

如果群G可以由一个元素a生成，即$\langle a\rangle=G$，
则称G为由a生成的一个循环群，a是G的
一个生成元
易知$\langle a\rangle=\{a^k\mid k\in\mathbb{Z}\}$
循环群必是交换群.

有限群的生成元

循环群的分类

$\langle a\rangle$是无限循环群

1) $|a|=\infty$

$\langle a\rangle=\{\cdots,a^{-2},a^{-1},a^0=e,a,a^2,\cdots\}$

2) $\langle a\rangle$有两个生成元，a和a^{-1}

无限循环群和整数加群同构

$\langle a\rangle$是n阶循环群

1) $|a|=n$

$\langle a\rangle=\{e=a^n,a,a^2,\cdots,a^{n-1}\}$

n阶循环群和n次单位根群U_n同构

2) a^k是$\langle a\rangle$的生成元 iff. $(k,n)=1$

$\langle a\rangle$一共有$\varphi(n)$个生成元

$\varphi(n)$: Euler函数
表示小于n的与n互素的正整数的个数

Co. n阶群G是循环群 $\Leftrightarrow$ G有n阶元素(a)

循环群的子群

循环群的子群也是循环群

证明：设$H\leq\langle a\rangle$，若$H\neq\{e\}$，是循环群

证明：设 $H \leq \langle a \rangle$，若 $H=\{e\}$，是循环群

若 $H \neq \{e\}$，$\forall b \in H$，有 $b=a^m$，$m \in \mathbb{Z}$.

则 $a^{|m|} \in H$，故 H 中必包含 a 的正整数次幂

令 $m_0 = \min\limits_{a^{|m|} \in H} |m|$

任取 $a^s \in H$，作带余除法得

$s = m_0 q + r$，$0 \leq r < m_0$，则 $a^s = (a^{m_0})^q a^r$

因为 $(a^{m_0})^q \in H$，$a^r \in H$.

由于 m_0 的最小性，$r=0$.

从而 $a^s = (a^{m_0})^q$，$q \in \mathbb{Z}$ ☑

无限循环群有无限多个子群（$\langle e \rangle, \langle a \rangle, \langle a^2 \rangle, \cdots$ 全互不相同）

若 $\langle a \rangle$ 为 n 阶循环群，对 n 的每个正因数 k，

$\langle a \rangle$ 有且仅有一个 k 阶子群 $\langle a^{\frac{n}{k}} \rangle$

Proof. $|a|=n$，$k|n$，设 $n=kq$，则 $\langle a^{\frac{n}{k}} \rangle = \langle a^q \rangle$

是 $\langle a \rangle$ 的子群

下证唯一性.

设 $\langle a \rangle$ 有 k 阶子群 $H' = \langle a^m \rangle$ qq

由 2.2 Th 3 知，$|a^m| = \frac{n}{(n,m)} = k$，从而 $q = \frac{n}{k} = (n,m)$

于是 $q|m$，$a^m \in \langle a^q \rangle$，$\langle a^m \rangle \subseteq \langle a^q \rangle$ 包含+阶相等

又因为 $|\langle a^m \rangle| = |\langle a^q \rangle|$，$\langle a^m \rangle = \langle a^q \rangle$ ☑

2.5 变换群

2023年10月10日 17:28

Def. 设M是一个非空集合，则由M的一些变换关于变换的乘法作成的群称为M的一个**变换群**

由M的若干个双射变换关于变换的乘法作成的群称为**双射变换群**

由M的若干个非双射变换关于变换的乘法作成的群称为**双射变换群**

非双射变换群的例子

1. 设$|M|>0$，取定$a\in M$，$\tau:x\to a$，$\{\tau\}$作成非双射变换群
2. 设$M=\{(x,y)\mid x,y\in\mathbb{R}\}$，任取$a\in\mathbb{R}$，$\tau_a:(x,y)\longrightarrow(x+a,0)$，则$\{\tau_a\mid a\in\mathbb{R}\}$是非双射变换群.

记由全体M的双射作成的集合为$S(M)$，这是一个变换群，称为M上的**对称群**，当$|M|=n$时，称为n元对称群(S_n)

(根据双射的性质，$S(M)$满足封闭性，结合律.
恒等变换是单位元，逆变换是逆元)

S_n对任意M是同构的
$|S_n|=n!$
可用$1,\cdots,n$表示M中的元素(有限情形)
将映射写为$\sigma=\begin{pmatrix}1&2&\cdots&n\\ \sigma(1)&\sigma(2)&\cdots&\sigma(n)\end{pmatrix}$

Th1 设G是集合M上的一个变换群，则
M是双射变换群$\Leftrightarrow$恒等变换$\in G$(并且是单位元)

Proof. ($\Rightarrow$) 设ε是G的单位元，则任取$\sigma\in G$，$\sigma\varepsilon=\sigma$
从而$\forall y\in M$，设$\sigma(x)=y$，则
$\varepsilon(y)=\varepsilon(\sigma(x))=\varepsilon\sigma(x)=\sigma(x)=y$
故ε是恒等变换
($\Leftarrow$) $\forall\sigma\in G$，$\exists\sigma^{-1}\in G$，$\sigma^{-1}\sigma=\sigma\sigma^{-1}=\varepsilon$
$\forall x,y\in M$，$\sigma(x)=\sigma(y)\Rightarrow\sigma^{-1}\sigma(x)=\sigma^{-1}\sigma(y)\Rightarrow x=y$(单)
$\forall y\in M$，令$x=\sigma^{-1}(y)$，则$\sigma(x)=\sigma\sigma^{-1}(y)=y$(满)
故σ是双射 ☑

意即没有M的变换群既含有M的双射变换，又含有M的非双射变换.

事实上，非双射变换群也不含单/满射

Th2 设G是集合M上的一个变换群，则
G是双射变换群$\Leftrightarrow$$G$含有$M$的单(满)射变换

Proof. ($\Rightarrow$)显然
($\Leftarrow$) 先证G的单位元是恒等变换，设单位元为ε.
若G含有M的满射变换，证明同Th1($\Rightarrow$)
若G含有M的单射变换，设为σ，则
$\forall x,y\in M$，若$\sigma(x)=\sigma(y)$，则$x=y$
又由于$\sigma(x)=\sigma(\varepsilon(x))$，$\sigma(\varepsilon(x))=\sigma(y)$，则$\varepsilon(x)=y$
而$\forall x\varepsilon(x)\neq x$，$\varepsilon$是恒等变换.
由Th1，G是双射变换群. ☑

本质：

σ(满)
$\varepsilon\sigma$

保证ε必须映射到自身
若非满，无论d映射到什么，都不影响$\varepsilon\sigma=\sigma$
$a\to c$
$b\nearrow d$等

σ(单)
$a\to a'$
$b\to b'$
$\sigma\varepsilon$

没有别的元素经σ作用和$\sigma(a)$相等
要使$\sigma\varepsilon=\sigma$，ε只能是恒等变换

Th3 (Cayley定理)任何一个群都与一个双射变换群同构

Proof. 设G是一个群，任取$a\in G$，令G上的变换$\tau_a:x\to ax$.
$\forall x,y\in G$，若$\tau_a(x)=\tau_a(y)$，即$ax=ay$，则$x=y$(单)
$\forall y\in G$，令$x=a^{-1}y$，则$\tau_a(x)=a(a^{-1}y)=y$(满)
故τ_a是双射.
令$H=\{\tau_a\mid a\in G\}$，下证H作成群
$\forall\tau_a,\tau_b\in H$，因为$a,b\in G$，$ab\in G$.
所以$\forall x\in G$，$\tau_a\tau_b(x)=\tau_a(\tau_b(x))=a(bx)=abx$
故$\tau_a\tau_b=\tau_{ab}\in H$，满足封闭性

$\forall \tau_a, \tau_b \in H$，因为 $a, b \in G$，$ab \in G$.
所以 $\forall x \in G$，$\tau_a\tau_b(x) = \tau_a(\tau_b(x)) = a(bx) = abx$
故 $\tau_a\tau_b = \tau_{ab} \in H$，满足封闭性.
令 $b = a^{-1} \in G$，得 $\tau_a\tau_{a^{-1}} = \tau_e$.
由定义知 τ_e 是恒等变换，由 Th1，τ_e 是 $S(G)$ 的单位元.
故 $H \leq S(G)$ 四

构造 G 到 H 的映射 $\varphi: a \to \tau_a$，显然 φ 是双射.
因为 $\forall a, b \in G$，$\varphi(ab) = \tau_{ab} = \tau_a\tau_b = \varphi(a)\varphi(b)$
故 $H \cong G$.

Co 任何 n 阶有限群都与 S_n 的一个子群同构 （但事实上 S_n 的子群并不容易研究…）

2.6 置换群

2023年10月17日 15:58

Def n元对称群 S_n 的一个子群称为一个n元**置换群**
置换群中的元素(双射)称为一个**置换**
任何一个有限群都与一个置换群同构
一般讨论 $n>1$ 的置换群.

如果一个置换 σ 将 $i_k \to i_1$, $i_1 \to i_2$, ..., 其它数码(如果有)不变, 则称 σ 是一个 **k-轮换(循环)置换**, 记为 $\sigma=(i_1\cdots i_k)$
1-循环即是恒等变换, 2-循环也叫**对换**
参与循环的数码中, 没有公共数码的循环称为**不相连循环**

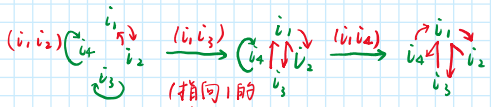
Th1 不相连循环相乘时可交换

Th2 每个置换都可以表示为不相连循环之积 (1) (表法唯一)
每个循环都可以表示为对换之积 (2) (表法不唯一)
从而每个置换都可以表示为对换之积

Proof. (1) 任意 σ 可以改写为
$\sigma=\begin{pmatrix} i_{11}i_{12}\cdots i_{1k_1}\cdots i_{s1}\cdots i_{sk_s} a_1\cdots a_l \\ i_{12}i_{13}\cdots i_{11}\cdots i_{s2}\cdots i_{sk_s} a_1\cdots a_l\end{pmatrix}$, 其中
i_{11} 是任一不满足 $\sigma(x)=x$ 的数码(如果有)
$i_{1,n+1}=\sigma(i_{1n})$, i_{1k_1} 是作迭代时第一个满足 $\sigma(n)=i_{11}$ 的数码
j_{11} 是任一不满足 $\sigma(x)=x$ 且不在 $i_{11}\cdots i_{1k_1}$ 中的数码(如果有)
$i_{21}\cdots i_{2k_2}$ 的类系同 i 系的数码.
因为 σ 是双射, i 系和 i 系必没有公共的数码.
j_{21} 是任一不满足 $\sigma(x)=x$ 且不在 $i_{11}\cdots i_{1k_1}, i_{21}\cdots i_{2k_2}$ 中的数码(如果有)
$i_{31}\cdots i_{3k_3}$ 的类系同 j 系的数码.
因为 σ 是双射, j 系和 i 系, i_3 系两两之间必没有公共的数码.
以此类推, 因为总数码数有限, 最后剩余有限个数码满足 $\sigma(x)=x$, 即 $a_1\cdots a_l$

于是 $\sigma=(i_{11}\cdots i_{1k_1})\cdots(i_{s1}\cdots i_{sk_s})$

(2) $(a)=(ab)(ab)$, $b\neq a$
$(i_1\cdots i_k)=(i_1 i_k)(i_1 i_{k-1})\cdots(i_1 i_2)$



Th3 每个置换表示为对换的乘积时, 对换个数的奇偶性一定.

Proof. 设置换 $\sigma=\sigma_1\cdots\sigma_m$ 是n元置换群上的一个置换,
$\sigma_1,\cdots,\sigma_m$ 是对换.
对排列 $i_1\cdots i_n$ 的每个数码施对换 $(i_s i_t)$, 即将 i_s 与 i_t 在排列中的位置对换. 因此对排列 $1\cdots n$ 的每个数码施置换 σ, 即依次将 $\sigma_m,\cdots,\sigma_1$ 中的数码进行对换.
因为每次对换都会改变排列的逆序数奇偶性, 所以对换个数的奇偶性一定, 与排列 $\sigma(1)\cdots\sigma(n)$ 的逆序数奇偶性相同.

一个置换若分解成奇数个对换的乘积, 则称为**奇置换**, 否则称为**偶置换**.

恒等变换是偶置换
互逆的置换同奇偶

1° 恒等置换是偶置换
2° 奇奇=偶偶=偶, 奇偶=偶奇=奇
3° 奇、偶置换各占一半, 即都有 $\frac{n!}{2}$ 个

奇偶排列各半 两种证明方法:
1. 偶排列集 A_n 与奇排列集 B_n 间存在双射 σ: $A_n \to B_n$, $i_1 i_2\cdots i_n \to i_s i_2\cdots i_n$
2° n级全1矩阵的行列式 $=\sum_{i_1\cdots i_n}(-1)^{\tau(i_1\cdots i_n)}=0$

S_n 中全体偶置换作成一个 $\frac{n!}{2}$ 阶子群, 称为n元**交错群**, 记为 A_n

Th4 一个n元置换群 G 中的置换或全为偶置换,

【2° n级全1矩阵的行列式 $=\sum_{i_1\cdots i_n}(-1)^{\tau(i_1\cdots i_n)}=0$

Th4 一个n元置换群G中的置换或全为偶置换，或奇、偶置换各占一半，其全体偶置换作成一个群.

证明数量相等，常建立双射

Proof. G中必包含恒等变换ε，故G中必包含偶置换
令 $G=\{\varepsilon\}$，则G中置换全为偶置换.
假设G中有奇置换σ，设G中偶、奇置换的集合为A, B.
对 $\forall\tau\in B$，$\sigma\tau\in G$. 由于στ是偶置换，$\sigma\tau\in A$.
故可作 $B\to A$ 的映射 $\varphi:\tau\to\sigma\tau$
$\forall v\in A$，令 $\tau=\sigma^{-1}v$，由于σ^{-1}也是奇置换，τ是偶置换.
于是 $\varphi(\tau)=v$，从而φ可逆，φ是双射.
故 $|A|=|B|$
偶置换关于乘法封闭，且B有限，故作成群 □

置换的阶的判别方法

Th5 k-循环的阶为k，
不相连循环乘积的阶为各因子的阶的最小公倍数

Proof. $1\le m<k$ 时有 $(i_1\cdots i_n)^m=(i_1\,i_{m+1}\cdots i_{n-m+1})\neq(1)$
而 $(i_1\cdots i_n)^k=(1)$，故 $(i_1\cdots i_n)$ 的阶是k.
设 $\sigma_1,\cdots,\sigma_s$ 分别是阶为 $k_1,\cdots,k_n$ 的不相连循环，
且 $t=[k_1,\cdots,k_s]$. 由于 $k_i\mid t$，故 $\sigma^t=(1)$.
由Th1，$(\sigma_1\cdots\sigma_s)^t=\sigma_1^t\cdots\sigma_s^t=(1)$
另一方面，设 $(\sigma\cdots\sigma_s)^r=(1)$，则 $\sigma_1^r\cdots\sigma_s^r=(1)$
由于 $(i_1\cdots i_n)^r\neq(1)$ 时，$(i_1\cdots i_n)^m=(i_1\,i_{m+1}\cdots i_{n-m+1})$
是 $(i_1\cdots i_n)$ 的一个排列，故当 $\sigma_j^r\neq(1)$ 时，
σ_j^r 仍是 σ_j 中数码的一个循环，从而 $\sigma_1^r,\cdots,\sigma_s^r$
仍是不相连循环，$\sigma_1^r\cdots\sigma_s^r\neq(1)$. 于是 $\sigma_1^r=\cdots=\sigma_n^r=(1)$.
当 $r<t$ 时，显然不满足上述条件 □

Th6 设n元置换 $\tau=\begin{pmatrix}1&2&\cdots&n\\ i_1&i_2&\cdots&i_n\end{pmatrix}$，则对任意n元置换σ，
有 $\sigma\tau\sigma^{-1}=\begin{pmatrix}\sigma(1)&\cdots&\sigma(n)\\ \sigma(i_1)&\cdots&\sigma(i_n)\end{pmatrix}$ $(\sigma\tau\sigma^{-1}(\sigma(j))=\sigma\tau(j)=\sigma(i_j))$
于是当τ表示为不相连循环之积时，也可以迅速得出 $\sigma\tau\sigma^{-1}$
表示为不相连循环之积的表法

eg. $K_4=\{(1),(12)(34),(13)(24),(14)(23)\}$ 作成交错群 A_4 的一个交换子群，称为 Klein 四元群.

eg. 当n≥3时，n元对称群 S_n 只有唯一的中心元恒等变换，即 S_n 是一个无中心群

Proof. 当n≥3时，$\forall\varphi\neq(1)\in S_n$，$\exists i$，$\varphi(i)=j\neq i$
设 $\sigma=(jk)$，$k\neq i$，则 $\sigma\varphi(i)=k$，$\varphi\sigma(i)=j$，$\sigma\varphi\neq\varphi\sigma$ □

2.7 陪集、指数和Lagrange定理

2023年10月19日 10:26

陪集

Def. 设 $H\leq G$, $a\in G$, 则称群 G 的子集
$aH=\{ax\mid x\in H\}$ / $Ha=\{xa\mid x\in H\}$
为群 G 关于子群 H 的一个左/右陪集 (coset)

(1) 陪集一般不是 G 的子群(除 H 本身, 元单位元)
(2) 由 G 的两个不同元素可能生成 H 的同一个左(右)陪集
(3) H 的一个左陪集 aH 一般不等于相应的右陪集 Ha
(4) G 关于 H 的左(右)陪集和 H 具有相同的势

例: $H=\{(1),(12)\}\leq S_3$
$(13)H=\{(13),(123)\}$
$H(13)=\{(13),(132)\}$

可以将陪集理解为平移/放缩

左陪集的性质(右陪集有对应的性质)

1° $a\in aH$ ($e\in H$)

2° $a\in H\Leftrightarrow aH=H$
($\Rightarrow$) $\forall h\in H$, $ah, a^{-1}h\in H$, 从而 $h=a(a^{-1}h)\in aH$, 故 $aH=H$.
($\Leftarrow$) 由1°显然

3° $b\in aH\Leftrightarrow aH=bH$
($\Rightarrow$) 设 $b=ax$, $x\in H$, 则 $\forall h\in H$, $ah=b(x^{-1}h)\in bH$. $bh=a(xh)\in aH$
($\Leftarrow$) 由1°显然 (或直接由2°, $bH=axH=aH$)

4° $aH=bH$, 即 a,b 同在一个左陪集中 $\Leftrightarrow a^{-1}b\in H$ (或 $b^{-1}a\in H$) (逆元在左)
$aH=bH\Leftrightarrow H=a^{-1}aH=a^{-1}bH\overset{2°}{\Leftrightarrow}a^{-1}b\in H$

5° $aH=bH$ 及 $aH\cap bH=\varnothing$, 二者必居其一且仅居其一
由1°, aH 非空, 故二者至少, 只需证若 $aH\cap bH\neq\varnothing$, 则 $aH=bH$.
设 $c\in aH\cap bH$, 则 $c\in aH$, $c\in bH$.
由3°, $aH=cH=bH$.

由5°, 用 $aH, bH,\cdots$ 表示 H 在 G 中所有不同的左陪集, 则
$G=aH\sqcup bH\sqcup\cdots$
称上式为群 G 关于子群 H 的左陪集分解,
$\{a,b,\cdots\}$ 为 G 关于 H 的一个左陪集代表系
由2°, $aH, bH\cdots$ 中有且仅有一个就是 H

6° $aH\leq G\Leftrightarrow a\in H$
($\Rightarrow$) $aH\leq G\Rightarrow e\in aH\overset{2°}{\Rightarrow}aH=eH=H\overset{1°}{\Rightarrow}a\in aH=H$
($\Leftarrow$) $a\in H=eH\overset{2°}{\Rightarrow}aH=eH=H\leq G$

7° $|aH|=|bH|=|H|$
设 $\varphi: \begin{matrix}H\to aH\\ x\to ax\end{matrix}$, φ 显然是满射
$\forall x',y'\in aH$, 设 $x'=ax$, $y'=ay$.
若 $x'=y'$, 由消去律, $x=y$, 故 φ 也是单射
从而 $|aH|=|H|$, 对 b 同理.

Th1 设 $H\leq G$, 令
$L=\{aH\mid a\in G\}$, $R=\{Ha\mid a\in G\}$
则 $|L|=|R|$ (左右陪集之集合的势相等)

Proof. 设 $\varphi: \begin{matrix}L\to R\\ aH\to Ha^{-1}\end{matrix}$. 因为群中每个元都是某元的逆元, φ 是满射.
$\forall Ha^{-1}, Hb^{-1}\in R$, 若 $Ha^{-1}=Hb^{-1}$,
由4°, $a^{-1}(b^{-1})^{-1}\in H$, 即 $a^{-1}b\in H$.
再逆用4°, 可知 $aH=bH$, 故 φ 是单射. 证

Co 当 $\{a,b,\cdots\}$ 是 G 关于 H 的一个左陪集代表系时,
$\{a^{-1},b^{-1},\cdots\}$ 是 G 关于 H 的一个右陪集代表系

指数

Def. 群 G 关于子群 H 的互异的左(右)陪集个数,
称为 H 在 G 中的指数, 记为 $(G:H)$

$(G:H)=|L|=|R|$, 可能有限, 也可能无限

J.L. Lagrange 定理

Th2 设 H 是有限群 G 的一个子群, 则
$$(G:H)=\frac{|G|}{|H|}$$
从而有限群 G 的子群的阶和指数都是 G 的阶的因数

Proof. 设 $(G:H)=s$, $G=a_1H\sqcup\cdots\sqcup a_sH$ 是 G 关于 H 的左陪集分解.
由左陪集的性质7°, $|a_1H|=\cdots=|a_sH|=|H|$
从而 $|G|=|H|\cdot s$ 证

Co1 有限群G的子群的阶整除G的阶

Co2 有限群中每个元素的阶都整除群的阶
(|a|=|<a>|整除|G|)
因此素数阶群必为循环群.

Co3 设G是一个有限群, K≤H≤G, 则
(G:H)(H:K)=(G:K)

Proof1. 由 Lagrange 定理立得

Proof2. 设 $A=\{a_1, a_2, \cdots\}$ 是 G 关于 H 的一个左陪集代表系
$B=\{b_1, b_2, \cdots\}$ 是 H 关于 K 的一个左陪集代表系
则 $G=a_1H\cup a_2H\cup\cdots$, $H=b_1K\cup b_2K\cup\cdots$
显然, $\forall a_i$, 有 $a_ib_{j_1}K\cap a_ib_{j_2}K=\emptyset$, $j_1\neq j_2$ (否则违反消去律)
又, $\forall x\in a_iH$, 设 $x=a_ih$, $h\in H$. 则 $h\in b_jK$. 从而 $x=a_ih\in a_ib_jK$
于是 $a_iH=a_ib_1K\cup a_ib_2K\cdots$
从而 $G=\bigcup_{i,j} a_ib_jK$,
即 $\{a_ib_j \mid a_i\in A, b_j\in B\}$ 是 G 关于 K 的一个左陪集代表系 (以上对无限群亦成立)
所以 (G:H)(H:K)=(G:K)

Th3 设 H, K 分别是群 G 的两个有限子群, 则
$$|HK|=\frac{|H||K|}{|H\cap K|}$$

Proof. 因为 $H\cap K\leq H$, 设 $(H:H\cap K)=m$,
$H=\bigcup_{i=1}^{m} h_i(H\cap K)$ 是 H 关于 $H\cap K$ 的一个左陪集分解
从而 $HK=\bigcup_{i=1}^{m} h_i(H\cap K)K$.

因为 $e\in H\cap K$, $\forall k\in K$, $k=ek$, 故 $K\subseteq(H\cap K)K$;
$\forall h\in H\cap K\subseteq K$, $k\in K$, 有 $hk\in K$, 故 $(H\cap K)K\subseteq K$.
于是 $(H\cap K)K=K$.
根据左陪集分解的性质4°, $h_i^{-1}h_j\notin H\cap K$, 记为
因为 $h_i, h_j\in H$, $h_i^{-1}h_j\in H$. 故可知 $h_i^{-1}h_j\notin K$
再逆用4°, 及由5°, 得 $h_iK\cap h_jK=\emptyset$
所以 $HK=\bigcup_{i=1}^{m} h_iK$, 从而 $|HK|=m|K|$. □
⚠ HK未必是子群

Co1 $|HK|=|H||K|\Leftrightarrow H\cap K=\{e\}$

Co2 设 p, q 是两个素数且 $p<q$, 则 pq 阶群 G 至多有一个 q 阶子群

Proof. 假设有两个不同的 q 阶子群 H, K, 因为 $H\cap K\leq H$, $|H\cap K|\mid|H|$.
从而 $|H\cap K|=1$ 或 q.
若 $|H\cap K|=q$, 说明 $H=K$, 所以 $H\cap K=\{e\}$.
由 Co1, $|HK|=|H||K|=q^2>pq=|G|$, 与 $HK\subseteq G$ 矛盾!

事实上, 有且仅有一个 q 阶子群 (How to prove?)

例: 15阶群至多含有一个5阶子群

Proof. 假设有不同的5阶子群 H, G
因为 $H\cap G\leq H$, $|H\cap G|=5$ 或 1, 而 $H\neq G$. 故 $|H\cap G|=1$
由 Th5, $|HK|=\frac{|H||G|}{|H\cap G|}=\frac{5\times5}{1}=25>15$, 矛盾!

33阶群必有3阶子群.

Proof. 33阶群中除单位元外, 元素的阶为3或11或33
如含有33阶元素 a, $G=\langle a\rangle$, 显然.
如除e外全为11阶元, 任取 $a\in G\setminus\{e\}$, 令 $H=\langle a\rangle$.
再任取 $b\in G\setminus H$, 令 $K=\langle b\rangle$. 则 $\langle a\rangle\cap\langle b\rangle=\{e\}$
于是 $|HK|=121>33$
故 $\exists a\in G$, $|a|=3$, 从而 $|\langle a\rangle|=3$

eg. 6阶群要么是6阶循环群, 要么是 S_3

6阶循环群 $\cong$ ($T_r: a^m\to a^{m+r}$)
$\{(1), (123456), (135)(246), (14)(25)(36), (153)(264), (165432)\}\leq S_6$
$S_3=\{(1), (12), (13), (23), (123), (132)\}$, 显然是不同的
假设 G 不是6阶循环群, 即没有6阶元素.
则 G 中除 e 都是2或3阶元素.

假设 G 中没有3阶元素. 则 $\forall a\in G$, $a^2=e$.
若 G 中仅有3个不同的2阶元素. 易证 $G\cong\{e, a, b, ab\}$
若 G 中至少有4个不同的2阶元素,
当 $\{e, a, b, ab\}$ 作成群时. 设 $c\notin\{e, a, b, ab\}$, $c^2=e$.
则易证 G 中至少有8个元素 e, a, b, c, ab, ac, bc, abc
于是与 $|G|=6$ 矛盾.

设3阶元 $a\in G$, 则 $\langle a\rangle\leq G$.
任取 $b\in G\setminus\langle a\rangle$, 由于 $(G:\langle a\rangle)=\frac{6}{3}=2$, $G=\langle a\rangle\cup b\langle a\rangle$
即 $G=\{e, a, a^2, b, ba, ba^2\}$.
假设 $|b|=3$, 则 $b^2a=b(ba)\in G$.
依次令 e, a, …, $ba^2=b^2a$, 均可得出矛盾. 故 $|b|=2$.
显然 $ab\neq e, a, a^2, b$. 假设 $ab=ba$, 则
$(ba)^2=b(ab)a=b^2a^2=a^2$, $(ba)^3=b(ab)(ab)a=b^3a^3=b$
与 $|ba|=2$ 或3矛盾. 故 $ab=ba^2$.
经验证, G 确是群
并且 $G\cong S_3$, 由映射 $\varphi=\begin{pmatrix} e & a & a^2 & b & ba & ba^2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}$

$\because |ba| = 2$或3矛盾. 故 $ab = ba^2$.

经验证, G确是群.

并且 $G \cong S_3$, 由映射 $\varphi = \begin{pmatrix} e & a & a^2 & b & ba & ba^2 \\ (1) & (132) & (123) & (12) & (13) & (23) \end{pmatrix}$

3.1 群的同态与同构的简单性质

2023年10月24日 16:40

同态与同构 见第一章

Th1 设G是一个群，$\bar{G}$是一个有代数运算的集合.
如果$G \overset{满}{\sim} \bar{G}$，则$\bar{G}$是一个群.

Proof. 设φ是$G \to \bar{G}$的同态满射.则
$\forall \bar{a}, \bar{b} \in \bar{G}$, $\exists a, b \in G$, $\varphi(a)=\bar{a}$, $\varphi(b)=\bar{b}$, 且$\varphi(ab)=\bar{a}\bar{b}$
由同态映射的性质，M中对应运算满足结合律.
令$\bar{a}=\bar{e}=\varphi(e)$，则有$\bar{e}\bar{b}=\varphi(eb)=\varphi(b)=\bar{b}$，故$\bar{e}$是$\bar{G}$的单位元. (单位元、逆元对存在)
令$\bar{b}=\overline{a^{-1}}=\varphi(a^{-1})$，则有$\bar{a}\,\overline{a^{-1}}=\varphi(aa^{-1})=\varphi(e)=\bar{e}$. 故有逆元. □

eg. $\bar{G}=\{0,1,2,3\}$关于运算$a*b=r$(r是$a+b$被4除的余数)
作成群，因为$\mathbb{Z} \overset{满}{\sim} \bar{G}$，$\varphi: x \mapsto x'$，$x'$是$x$被4除的余数

注：若$G \sim \bar{G}$，$\bar{G}$是群，不能推G是群

Th2 (同态在子群上仍成立)
设φ是群$G \to$群$\bar{G}$的同态映射，则
i) 当$H \leq G$时，$H \overset{\varphi}{\sim} \varphi(H)$，且$\varphi(H) \leq \bar{G}$
ii) 当$\bar{H} \leq \bar{G}$时，$\varphi^{-1}(\bar{H}) \leq G$，且$\varphi^{-1}(\bar{H}) \sim \bar{H}$

Proof. i) $\forall \bar{a}, \bar{b} \in \varphi(H)$，设$\bar{a}=\varphi(a)$, $\bar{b}=\varphi(b)$, $a, b \in H$.
则$\bar{a}\bar{b}=\varphi(ab) \in \varphi(H)$，即$\varphi(H)$对$G$的乘法封闭. 于是$H \sim \varphi(H)$.
由Th1，$\varphi(H)$作成G的子群.
ii) 由于$e \in \bar{H}$，$\varphi^{-1}(\bar{H})$非空.
$\forall a, b \in \varphi^{-1}(\bar{H})$，设$\varphi(a)=\bar{a}$, $\varphi(b)=\bar{b}$.
则$\varphi(ab^{-1})=\bar{a}\bar{b}^{-1} \in \bar{H}$，故$ab^{-1} \in \varphi^{-1}(\bar{H})$，由i)知$\varphi^{-1}(\bar{H}) \leq G$.
由i)，$\varphi^{-1}(\bar{H}) \overset{\varphi|\varphi^{-1}(H)}{\sim} \varphi[\varphi^{-1}(\bar{H})]=\bar{H}$.

Th3 (单射的充要条件)
设群$G \overset{满}{\sim}$群$\bar{G}$，φ是单射的充要条件是：
$\bar{G}$的单位元$\bar{e}$的原像只有e. (如运算为加法，即$\operatorname{Ker}\varphi=\{e\}$)

Proof. 必：显然.
⇐) 设$a, b \in G$, $a \neq b$. 假设$\varphi(a)=\varphi(b)$，则
$\varphi(a)[\varphi(b)]^{-1}=\bar{e}$，即$\varphi(ab^{-1})=\bar{e}$，从而$ab^{-1}=e$.
这与$a \neq b$矛盾.

3.2.1 正规子群和商群

2023年10月24日 17:23

正规子群

Def. 设 $N\le G$，如果对 $\forall a\in G$ 都有
$$aN=Na$$
则称 N 是 G 的一个正规子群(不强调子群)，记为 $N\trianglelefteq G$
若 $N\trianglelefteq G$ 且 $N\neq G$，记为 $N\lhd G$
aN(或 Na)可简称为群 G 的由 a 生成的陪集

- 平凡正规子群 e.G　　单群：只有平凡正规子群
- 非平凡正规子群　其它

交换群的所有子群都是正规子群
群 G 的中心是正规子群.

设 $N\trianglelefteq G$，又 $N\le H\le G$，则 N 也是 H 的一个正规子群
但正规子群不具有传递性，即
$N\trianglelefteq H\trianglelefteq G\not\Rightarrow N\trianglelefteq G$　(eg3.)

$aN=Na\Leftrightarrow aNa^{-1}=N$　(对 a 求集运算)
($\Rightarrow$) $\forall n_1\in N$，$\exists n_2,n_3\in N$：$an_1=n_2a$，$an_3=n_1a$
从而 $an_1a^{-1}=n_2aa^{-1}=n_2\in N$
$n_1=n_1aa^{-1}=an_3a^{-1}\in aNa^{-1}$
故 $aNa^{-1}=N$
($\Leftarrow$) $\forall n_1\in N$，$\exists n_2,n_3\in N$，$an_1a^{-1}=n_2$，$an_3a^{-1}=n_1$
从而 $an_1=n_2a\in Na$，$n_1a=an_3\in aN$
故 $aN=Na$

设 $N\le G$，则 $N\trianglelefteq G\Leftrightarrow\forall a\in G$，$aNa^{-1}=N$.

弱化条件 → 检验子群是否是正规子群

Th1 设 $N\le G$，则 $N\trianglelefteq G\Leftrightarrow aNa^{-1}\subseteq N\ (\forall a\in G)$

Proof. ($\Rightarrow$) 若 $N\trianglelefteq G$，则 $\forall a\in G$，$aNa^{-1}=N$，显然
($\Leftarrow$) $\forall a\in G$，若 $aNa^{-1}\subseteq N$，则 $aN\subseteq Na$.
$a^{-1}Na\subseteq N$，则 $Na\subseteq aN$
故 $aN=Na$.

(不能直接由 $|aN|=|Na|$ 得出 $aN=Na$，在无限情况下，有已含关系且势相等不能得出集合相等，如整数集与偶数集)

eg1 n 次交错群 $A_n\lhd S_n$　($\forall\sigma\in S_n$，由于 $\sigma\tau\sigma^{-1}$ 奇偶性相同，$\sigma A_n\sigma^{-1}\subseteq A_n$)

eg2 四元数群 $G=\{1,i,j,k,-1,-i,-j,-k\}$ 是非交换群.
但它的真子群 $\langle1\rangle$，$\langle i\rangle$，$\langle j\rangle$，$\langle k\rangle$ 都是正规子群.
对置换，可利用 2.6 Th6 计算 $\sigma N\sigma^{-1}$

(非交换且任何子群都是正规子群的群称为 Hamilton 群)

最小的 Hamilton 群 (1,2,3,5,7 阶循环群 4 阶的群必为 $\{e,a,b,ab\}$ 6 阶群必为 S_3 或 (循环群)

eg3 Klein 四元群 $K_4=\{f(1),(12)(34),(13)(24),(14)(23)\}$
$K_4\trianglelefteq S_4$　($K_4\setminus\{f(1)\}$ 是 S_4 中全部的二阶偶置换，$\forall\sigma\in K_4\setminus\{f(1)\}$，$\forall\sigma\in S_4$，$(\sigma\times\sigma^{-1})(\sigma\times\sigma^{-1})=(1)$，即 $\sigma\times\sigma^{-1}$ 也是二阶偶置换)
$B_4=\{f(1),(12)(34)\}\trianglelefteq K_4\trianglelefteq S_4$，但 $B_4\not\trianglelefteq S_4$

Th2 (同态保正规子群)
设 φ 是群 G 到群 $\bar G$ 的一个同态满射，则
1) $N\trianglelefteq G\Rightarrow\varphi(N)\trianglelefteq\bar G$
2) $\bar N\trianglelefteq\bar G\Rightarrow\forall N\in\varphi^{-1}(\bar N)$，$N\trianglelefteq G$.

Proof. 1) $\forall\bar a\in\bar G$，设 $\bar a=\varphi(a)$，
则 $\bar a\varphi(N)=\varphi(a)\varphi(N)=\varphi(aN)=\varphi(Na)=\varphi(N)\bar a$.
2) $\bar N$ 中有个元素都有原像，$\varphi^{-1}(\bar N)$ 非空.
$\forall N\in\varphi^{-1}(\bar N)$，$\forall a\in G$：
$\varphi(aN)=\varphi(a)\bar N=\bar N\varphi(a)=\varphi(Na)$

Th3 群 G 的一个正规子群与一个子群的乘积是子群.
两个正规子群的乘积仍是正规子群.
即设 $N\trianglelefteq$ 群 G，$H\le G$.
则 $NH=HN\le G$，$NP=PN\trianglelefteq G$

Proof. 1) $NH=HN$ 显然.
$\forall n_1,n_2\in N$，$h_1,h_2\in H$：$(n_1h_1)^{-1}=h_1^{-1}n_1^{-1}\in HN=NH$
故 $(n_1h_1)(n_2h_2)^{-1}\in NH$.
2) $\forall a\in G$，$aNP=NaP=NPa$.

商群

陪集的乘法：在条件 $N\trianglelefteq G$ 下，
$(aN)(bN)=a(Nb)N=a(bN)N=(ab)N$

(设 $aN=a'N$，则 $a'\in aN$，从而 $a'b\in aNb=abN$，于是 $(a'b)N=(ab)N$.
故陪集的乘法是良定义的)

Def. 设 $N\trianglelefteq G$，则 N 的全体陪集对于陪集的乘法作成一个群，称为 G 关于 N 的商群，记为 G/N

Proof. 陪集的乘法是集乘法的特殊情况，故满足结合律.
显然 N 是单位元，$a^{-1}N$ 是 aN 的逆元.

商群的阶：$|G/N|=(G:N)=\dfrac{|G|}{|N|}$　(Lagrange)

(A.L.Cauchy 定理) 设 G 是 pn 阶有限交换群，其中 p 是一个素数，则 G 有 p 阶元素.　不用交换 → 若素数 $p\mid|G|$，则 G 中有 p 阶元.

[注1]

定理1.10.1 (Cauchy 定理)　设素数 p 是 $|G|$ 的因子，则 G 中存在 p 阶元.
证　考虑集合 $X=\{(a_1,\cdots,a_p)\mid a_i\in G,a_1\cdots a_p=e\}$，并设 $\sigma=(12\cdots p)\in S_p$. 容易看出 $|X|=|G|^{p-1}$，因此 $p\mid|X|$. 考虑 p 阶循环群 $\langle\sigma\rangle$ 在 X 上的作用:
$$\sigma\cdot(a_1,\cdots,a_p)=(a_{\sigma(1)},\cdots,a_{\sigma(p)}).$$
由于 p 是素数，每个 $\langle\sigma\rangle$ 的轨道的元素个数只能是 1 或 p. 记不动点的全体为 X_0. 因每个非不动点所在轨道都有 p 个元素，而 $p\mid|X|$，因此 $p\mid|X_0|$. 显然，X_0 中的元素都形如 $(a,\cdots,a)$，其中 $a^p=e$. 又 $(e,\cdots,e)\in X_0$，故 X_0 非空，所以 X_0 中存在元素 $(a,\cdots,a)$ 使得 $a\neq e$. 于是 a 为 p 阶元.　□

[注2] Sylow ??

C. 设 G 是 pq 阶交换群，p,q 是互异素数，则 G 是循环群. (可推广至 $|G|=p_1\cdots p_n$)

Proof. G 有 p 阶元素 a，q 阶元素 b，由 2.2 Th4，$|ab|=pq$

3.3 群同态基本定理

2023年10月26日 11:53

设N是群G的任一正规子群，则$G\sim G/N$

设φ是群G到群$\bar{G}$的一个同态映射，$\bar{G}$的单位元在φ下所有逆像作成的集合称为φ的**核**，记作$Ker\varphi$

群同态基本定理

设φ是群G到群$\bar{G}$的一个同态满射，则$Ker\varphi \trianglelefteq G$，且$G/Ker N\cong \bar{G}$

Proof.

Co1 设G，$\bar{G}$是有限群，$G\sim\bar{G}$，则$|\bar{G}||G|$

设G，$\bar{G}$是两个群，$G\sim\bar{G}$，若G是循环群，则$\bar{G}$也是循环群 (且G的生成元对应的$\bar{G}$中元素也是$\bar{G}$的生成元)

Proof. 设$G=\langle a\rangle$，$G\overset{\varphi}{\sim}\bar{G}$，$\varphi(a)=\bar{a}$. 显然$\langle\bar{a}\rangle\subseteq G$.
$\forall \bar{x}\in\bar{G}$，设$\varphi(x)=\bar{x}$，$x=a^m$，由同态，$\bar{x}=\varphi(a^m)=\bar{a}^m$.
故$\bar{G}\subseteq\langle\bar{a}\rangle$. 而$\bar{G}=\langle\bar{a}\rangle$ 囧

Co 循环群的商群也是循环群

3.4 群的同构定理

2023年10月31日 16:24

(第一同构定理) 设 φ 是群 G 到群 $\bar{G}$ 的一个同态满射, $N \trianglelefteq G$.
并且 $\ker\varphi \subseteq N$, 则 $G/N \cong \bar{G}/\bar{N}$ $(\bar{N} = \varphi(N))$

Proof. 令 $f: G/N \mapsto \bar{G}/\bar{N}$
$aN \longrightarrow \bar{a}\bar{N}$ $(\bar{a} = \varphi(a))$
$\forall aN, bN \in G/N$

所以 f 是良定义的, 且是单射

[法2] 令 $\tau: G \mapsto \bar{G}/\bar{N}$
$a \longrightarrow \bar{a}\bar{N}$

(第二同构定理) 设 G 是群, 又 $H \leq G$, $N \trianglelefteq G$, 则 $H \cap N \trianglelefteq H$, 并且 $HN/N \cong H/(H \cap N)$

(注: $N \leq HN \leq G$, $N \trianglelefteq G \Rightarrow N \trianglelefteq HN$
$H \cap N \leq H \leq G$, $H \cap N \trianglelefteq G \Rightarrow H \cap N \trianglelefteq H$?)

Proof.

例: $K_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$
证明 $S_4/K_4 \cong S_3$ (S_n 是 n 元对称群)

Proof. $K_4 \trianglelefteq S_4$, $S_3 \leq S_4$, 由 Th2,
$S_3K_4/K_4 \cong S_3$ $(K_4 \cap S_3 = \{e\})$

3.5 群的自同构群

2023年11月2日 10:27

Def. 设M是一个有代数运算的集合，则M的全体自同构关于变换的乘法作成一个群，称为M的自同构群

Proof.

群G的自同构群记为$Aut\,G$　　双射+同态

例：$Aut\,K_4 \cong S_3$

(1)对右(1)，其它三个元素任意排列)

无限循环群的自同构群是一个二阶群　　为什么要生成元？

n阶循环群的自同构群是一个$\varphi(n)$阶群

内自同构

Def. 设G是一个群，$a\in G$，则
$\sigma_a: x\to axa^{-1}$ 是G的一个自同构，称为G的一个内自同构

Proof. $\sigma_a(x)=\sigma_a(y)\Leftrightarrow axa^{-1}=aya^{-1}\Leftrightarrow x=y$，单
$\forall \bar{x}\in G$，令$x=a^{-1}\bar{x}a$，有$\sigma_a(x)=\bar{x}$，满
$\sigma_a(xy)=axya^{-1}=(axa^{-1})(aya^{-1})=\sigma_a(x)\sigma_a(y)$，同态　四

G的全体内自同构作成一个群，称为G的内自同构群，记作$Inn\,G$

Proof. $\forall \sigma_a,\sigma_b\in Inn\,G$，$\forall x\in G$，$\sigma_a\sigma_b(x)=abxb^{-1}a^{-1}=\sigma_{ab}(x)$，封闭
$\forall \sigma_a\in Inn\,G$，$\forall x\in G$，$\sigma_a\sigma_e(x)=\sigma_{ae}(x)=aexe(a)^{-1}=axa^{-1}=\sigma_a(x)$，有单位元
$\forall \sigma_a\in Inn\,G$，$\forall x\in G$，$\sigma_a\sigma_{a^{-1}}(x)=aa^{-1}xa^{-1}a=x=\sigma_e(x)$，有逆元　四

$Inn\,G\trianglelefteq Aut\,G$

Proof. $\forall \tau\in Aut\,G$，$\forall \sigma_a\in Inn\,G$，$\forall x\in G$，
$\tau\sigma_a\tau^{-1}(x)=\tau(a\tau^{-1}(x)a^{-1})=\tau(a)x\tau(a^{-1})=\tau(a)x(\tau(a))^{-1}=\sigma_{\tau(a)}(x)$，
故$\tau\sigma_a\tau^{-1}=\sigma_{\tau(a)}\in Inn\,G$.
于是$\forall\tau\in Aut\,G$，$\tau Inn\,G\tau^{-1}\subseteq Inn\,G$，而$Inn\,G\trianglelefteq Aut\,G$

特征子群

对群G的所有自同构都不变的子群，即满足
$\forall\sigma\in Aut\,G$，都有$\sigma(N)\subseteq N$　的子群N
称为G的一个特征子群

{全特征子群}$\subseteq${特征子群}$\subseteq${正规子群}

对群G的所有自同态都不变的子群，即满足
$\forall$自同态φ，都有$\varphi(H)\subseteq H$　的子群H
称为G的一个全特征子群

群的中心是一个特征子群

$Inn\,G\cong G/C$

作业 1

2023年9月21日 22:18

2023.9.21 1.5 $T_{2,3}$ 1.6 $T_{1,2}$

2.1 $T_{2,4,6}$

1.5 T_2 $f: \mathbb{Q} \longmapsto \mathbb{Q}$, $a \longrightarrow 2a$ 是关于加法的自同构

$\forall a,b \in \mathbb{Q}$, $f(a)+f(b) = 2a+2b = 2(a+b) = f(a+b)$

$\forall a' \in \mathbb{Q}$, $\exists a = \frac{a'}{2}$ 使得 $f(a)=a'$，故 f 是满射

$\forall a,b \in \mathbb{Q}$，若 $f(a)=f(b)$ 即 $2a=2b$，则 $a=b$，故 f 是单射

T_3 $\exists \varphi: M \to \overline{M}$, $\forall a,b \in M$, $\varphi(a) \bar{\circ} \varphi(b) = \varphi(a \circ b)$

若 $\circ$ 满足结合律，则 $\varphi(a\circ(b\circ c)) = \varphi((a\circ b)\circ c)$.

从而 $\varphi(a) \bar{\circ} (\varphi(b) \bar{\circ} \varphi(c)) = (\varphi(a) \bar{\circ} \varphi(b)) \bar{\circ} \varphi(c)$.

由于 φ 是满射，$\bar{\circ}$ 也满足结合律.

1.6 T_1 $\forall a,b \in M$，$a+b$ 仍为整数，有 $4 \mid a+b$ 或 $\neg(4 \mid a+b)$

二者互斥，故 R 为 M 的一个关系

R 不满足反身性. 令 $a=1$，则 $4 \nmid a+a$，$a \not R a$.

R 满足对称性，$aRb \Leftrightarrow 4 \mid a+b \Leftrightarrow 4 \mid b+a \Leftrightarrow bRa$

R 不满足传递性. 令 $a=3, b=1, c=3$，则 aRb 且 bRc，但是 $a \not R c$.

T_2 1) 不满足对称性. 令 $a=1, b=2$，aRb 但 $b \not R a$.

2) 不满足传递性. 令 $a=1, b=0, c=-1$，则 aRb 且 bRc，但 $a \not R c$.

3) 是等价关系

4) 是等价关系

2.1 T_2 N 对 $\circ$ 作成半群

封闭性显然满足.

$\forall a,b,c \in N$, $a\circ(b\circ c) = a+(b+c+bc)+a(b+c+bc)$

$= a+b+c+ab+bc+ca+abc$

$= (a+b+ab)+c+(a+b+ab)c$

$= (a\circ b)\circ c$，满足结合律.

N 对 $\circ$ 不作成幺半群.

令 $b=2$，方程 $a+b+ab=b$ 在 N 上无解

故 N 中不含单位元.

同样 N 对 $\circ$ 不作成群.

T_4 证: 1° 由 G 关于乘法的封闭性，G 关于 $\circ$ 也封闭

2° $\forall a,b,c \in G$, $a\circ(b\circ c) = au(buc)$

$= (aub)uc = (a\circ b)\circ c$，满足结合律

3° 设 u 在 G 中的乘法逆元为 u^{-1}，则 $\forall b \in G$,

$u^{-1}\circ b = u^{-1}ub = b$，故 u^{-1} 为左单位元

4° $\forall b \in G$，设 b 在 G 中的乘法逆元为 b^{-1}，则

$u^{-1}b^{-1}u^{-1}\circ b = u^{-1}b^{-1}u^{-1}ub = u^{-1}$，故存在左逆元.

综上，G 对 $\circ$ 作成一个群.

T_6 证明: $\forall a,b \in G$，由 $a^2=e$, $b^2=e$ 有 $a(bb)a=e$

从而 $(ab)(ba) = e = (ab)(ab)$

由消去律，$ba=ab$. 故 G 为交换群.

2.2 1(1)(3) 3(1)(2) 2.3 3,5,6

T_1 (1) $(a^{-1})^n = (a^n)^{-1}$, iff. $a^n=e$ 时 $(a^{-1})^n = e$

$(cac^{-1})^n = ca^nc^{-1}$, iff. $a^n=e$ 时 $(ca^nc^{-1})^n = e$

(2) 设 $|ab|=n$，则

$(ba)^{n+1} = \underbrace{ba \cdots ba}_{n+1 \text{个} ba} = b(ab)^n a = ba$

由消去律，$(ba)^n = e$

设 $|ba| = m$, $m \in \mathbb{Z}^+$，同理 $(ab)^m = e$

由 Th2, $n \mid m$ 且 $m \mid n$，故 $m=n$.

(3) 由 (2) 显然

T_3 (1) 设有限群 G 中阶为 k 的元素有 $a_1, \cdots, a_n$ ($n \in N$), $k > 2$.

因为 $\forall a \in G$, $|a| = |a^{-1}|$，并且由逆元的唯一性，$a_1^{-1}, \cdots, a_n^{-1}$ 互不相同.

有 $\{a_1, \cdots, a_n\} = \{a_1^{-1}, \cdots, a_n^{-1}\} \triangleq S$

由于 $\forall a \in G$, $|a|>2 \Leftrightarrow a^2 \neq e \Leftrightarrow a \neq a^{-1}$

于是，S 中的每个元素都能与它的逆元配对. 从而 n 是偶数

对 $\forall k>2$，阶为 k 的元素个数都为偶数，而 G 有限.

故 G 中阶大于 2 的元素个数为偶数

(2) 设偶数阶群 $G = \{e, a_1, \cdots, a_n, b_1, \cdots, b_m\}$, $2 \mid 1+n+m$

其中 $|a_i| = 2$, $|b_i| > 2$, $\forall i$.

由 (1) 可知，m 为偶数，则 n 为奇数.

2.3 T_3 Proof. 设 G 是交换群，$H = \{a \mid a \in G, a^n = e, n \in N_+\} \subset G$

$\forall x,y \in H$，设 $x^m = e$, $y^l = e$, $m, l \in N_+$.

则 $(xy^{-1})^{ml} = (x^m)^l ((y^l)^m)^{-1} = e$，故 $xy^{-1} \in H$

所以 $H \leq G$.

根据 "$\exists n \in N_+$, s.t. $a^n = e \Leftrightarrow a$ 的阶有限".

H 即为所有有限阶元素作成的群 ◻

若 G 不是交换群，m 步骤未必能进行，结论未必成立. 反例:

在 $GL_2(\mathbb{Q})$ 中，令 $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$

则 $|a| = 4$, $|b| = 3$，但 $ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $|ab| = \infty$

故所有有限阶元素不能构成子群

T_5 因为 $(m,n)=1$, $\exists u,v \in \mathbb{Z}$, s.t. $um+vn=1$.

故 $a = a^{um+vn} = (a^m)^u (a^n)^v \in H$

T_6 $\forall x,y \in G$, $xy(yx) = xy^2x = x^2 = e$，故 $(xy)^{-1} = yx$

由于 $(xy)^2 = e$, $xy = (xy)^{-1}$.

由逆元的唯一性，$xy = yx$

故 G 是交换群.

任取 $a,b \in G$, s.t. $a \neq e$, $b \neq a$, $b \neq e$.

因为 $|G| > 2$，这是可行的.

由于 $b \neq a$ 且 $b \neq e$，并且 $a^2 = e$，有 $ab \neq e$, $ab \neq a$

由于 $a \neq e$, $ab \neq b$

令 $H = \{e, a, b, ab\}$，显然 e, a, b 两两的积仍在 H 中.

又因为 $(ab)a = a(ab) = a^2b = e$,

$(ab)b = b(ab) = e$. H 关于乘法封闭

根据 "有限子集作成子群的充要条件是关于乘法封闭"，$H \leq G$

2.4 1 2 3 2.5 3

T_1 小于 6 的与 6 互素的正整数有 1, 5

故 $\langle a \rangle$ 的生成元有 a 和 a^5

6 的正因数有 1, 2, 3, 6，故子群有

$\langle a \rangle$, $\langle a^2 \rangle$, $\langle a^3 \rangle$, $\langle e \rangle$

T_2 ($\Rightarrow$) 假设 $|s| \neq |t|$，不妨设 $|s| > |t|$

由于 $a^t \in \langle a^t \rangle = \langle a^s \rangle$, $a^t = (a^s)^k = a^{sk}$, $k \in \mathbb{Z}$.

因为 $|a| = \infty$，不存在 $m \in \mathbb{Z}$ 使得 $a^m = e$，所以 $t = sk$，从而 $|t| = |s||k|$, $k \in \mathbb{Z}$.

若 $|k| \neq 0$, $|k| \geq 1$，从而 $|t| \geq |s|$;

若 $|k| = 0$, $|t| = 0$，从而 $\langle a^s \rangle = \langle a^t \rangle = \langle e \rangle$, $|s| = 0$.

都与 $|s| > |t|$ 矛盾. 故假设不成立.

所以，…

($\Leftarrow$) 若 $s = t$，显然;

若 $s = -t$，则 $\forall (a^s)^k \in \langle a^s \rangle$, $k \in \mathbb{Z}$，有 $(a^t)^{-k} = (a^s)^k$.

从而 $\langle a^s \rangle \subseteq \langle a^t \rangle$. 同理 $\langle a^t \rangle \subseteq \langle a^s \rangle$.

所以 $\langle a^s \rangle = \langle a^t \rangle$

综上，… ◻

T_3 ($\Rightarrow$) 假设 $(s,n) = d_1 \neq d_2 = (t,n)$

则 $(a^s)^{\frac{n}{d_1}} = (a^n)^{\frac{s}{d_1}} = e$. $\frac{n}{d_1}, \frac{s}{d_1} \in N_+$.

设 $(a^s)^k = e$, $k \in N_+$，则 $n \mid sk$，从而 $\frac{n}{d_1} \mid \frac{s}{d_1} \cdot k$

由于 $(\frac{n}{d_1}, \frac{s}{d_1}) = 1$, $\frac{n}{d_1} \mid k$，从而 $k \geq \frac{n}{d_1}$.

故 $|a^s| = \frac{n}{d_1}$，同理 $|a^t| = \frac{n}{d_2}$

因为 $d_1 \neq d_2$, $|a^s| \neq |a^t|$，故 $\langle a^s \rangle \neq \langle a^t \rangle$，矛盾

所以 $(s,n) = (t,n)$

($\Leftarrow$) 设 $(s,n) = (t,n) = d$，则 $\exists u,v \in \mathbb{Z}$, $us + vn = d$

$\forall (a^t)^k \in \langle a^s \rangle$, $k \in \mathbb{Z}$, $tk = dmk = sumk + nvmk$, $m \in N_+$.

则 $(a^t)^k = (a^s)^{umk} + (a^n)^{vmk} = (a^s)^{umk} \in \langle a^s \rangle$

从而 $\langle a^t \rangle \subseteq \langle a^s \rangle$. 同理 $\langle a^s \rangle \subseteq \langle a^t \rangle$

所以 $\langle a^t \rangle = \langle a^s \rangle$ ◻

T_3 G 关于变换的乘法作成群. 证明:

i) $\forall \tau(a_1,b_1), \tau(a_2,b_2) \in G$,

$\tau(a_1,b_1)\tau(a_2,b_2)x = a_1(a_2x+b) + b = a_1a_2x + (a_1b+b)$,

$a_1a_2 \neq 0$ 且 a_1a_2, $a_1b+b \in M$, $\tau(a_1,b_1)\tau(a_2,b_2) \in G$

ii) $\forall \tau(a_1,b_1), \tau(a_2,b_2), \tau(a_3,b_3) \in G$

$\tau(a_1,b_1)(\tau(a_2,b_2)\tau(a_3,b_3))x = a_1a_2a_3x + a_1(a_2b+b)+b$

$= (a_1a_2)(a_3x+b) + (a_1b+b) = (\tau(a_1,b_1)\tau(a_2,b_2))\tau(a_3,b_3)x$

iii) $\forall \tau(a,b) \in G$, $\tau(1,0)\tau(a,b)x = \tau(a,b)x$.

故 $\tau(1,0)$ 是单位元

iv) $\forall \tau(a,b) \in G$, $\tau(\frac{1}{a},0)\tau(a,b)x = x = \tau(1,0)x$

故 $\tau(\frac{1}{a},0) = \tau(a,b)^{-1}$

综上，G 作成群.

因为 $\tau(1,0)$ 是恒等变换，G 是双射变换群.

2.6 T2

2(1) 显然 $x \notin \{i_1, \cdots, i_k\}$ 时，$(i_1 \cdots i_k)(i_k \cdots i_1)(x) = x$

而 $x \in \{i_1, \cdots, i_k\}$ 时，设 $x = i_r$.

$(i_1 \cdots i_k)(i_k \cdots i_1)(x) = (i_1 \cdots i_k)(i_{(r-2+k) \bmod k+1}) = x$

故 $(i_1 \cdots i_k)(i_k \cdots i_1) = (1)$, $(i_1 \cdots i_k)^{-1} = (i_k \cdots i_1)$

(2) 显然 $\begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix} \begin{pmatrix} i_1 & \cdots & i_n \\ 1 & \cdots & n \end{pmatrix} = (1)$

2.7 1,2 3.1 4 3.2 1,2,3

2.7 T_1

Proof. 根据 Lagrange 定理的推论 2，G 中每个元素的阶都整除群的阶. 于是 $x^n = e$

T_2 因为 $H \cap K \leq H, K$，所以 $|H \cap K| \mid m$, $|H \cap K| \mid n$

而 $(m,n) = 1$，故 $|H \cap K| = 1$, $H \cap K = \{e\}$

3.1 T_4 $\forall x \in G$，设 $x = \frac{u}{v}$，u, v 互素唯一

设 n_1, n_2 满足 $2^{n_1} \mid u$, $2^{n_1+1} \nmid u$

$2^{n_2} \mid v$, $2^{n_2+1} \nmid v$

令 $b = \frac{u}{2^{n_1}}$, $a = \frac{v}{2^{n_2}}$. $n = n_1 - n_2$

则 $x = 2^n \frac{b}{a}$，且 n 确定. 故 φ 是良定义的.

$\forall n \in \overline{G}$, $\exists 2^n \in G$. $\varphi(2^n) = n$. 故 φ 满

$\forall 2^{n_1}\frac{b_1}{a_1}, 2^{n_2}\frac{b_2}{a_2} \in G$,

$\varphi(2^{n_1}\frac{b_1}{a_1} \cdot 2^{n_2}\frac{b_2}{a_2}) = \varphi(2^{n_1+n_2}\frac{b_1b_2}{a_1a_2})$

由于 b_1, a_1, b_2, a_2 奇，将 $\frac{b_1b_2}{a_1a_2}$ 化为互素分子分母不会引入偶因数. 故 $\varphi(2^{n_1+n_2}\frac{b_1b_2}{a_1a_2}) = n_1+n_2$

所以 φ 是同态满射

3.2 T_1 设 $H \leq G$, $(G:H) = 2$. 则 $G = H \sqcup aH$, $\forall a \in G \backslash H$

于是 $aH = G \backslash H$. 同理 $Ha = G \backslash H$

故 $aH = Ha$, $\forall a \in G \backslash H$.

当 $a \in H$ 时，显然 $aH = Ha$.

故 $\forall a \in G$, $aH = Ha$, $H \trianglelefteq G$.

T_2

假设 $N \ntrianglelefteq G$，即 $\exists a \in G$, $aN \neq Na$. 从而 $aNa^{-1} \neq N$.

下证 $aNa^{-1} \leq G$.

$\forall n_1, n_2 \in N$, $(an_1a^{-1})(an_2a^{-1}) = a(n_1n_2)a^{-1} \in aNa^{-1}$

$e = aea^{-1} \in aNa^{-1}$

$\forall n_1 \in N$ $(an_1a^{-1})(an_1^{-1}a^{-1}) = e$, $an_1^{-1}a^{-1} \in aNa^{-1}$

综上，$aNa^{-1} \leq G$.

因为 $|aNa^{-1}| = n$，有两个不同的 n 阶子群.

假设矛盾，原命题成立

T_3 考虑 G/H，根据 lagrange 定理，$\forall a \in G$, $(aH)^m = H$

即 $a^mH = H$，所以 $a^m \in H$.

3.3 $T_{1,3,5}$ 3.4 T_1 3.5 T_3

1. ($\Rightarrow$) 设 $G \overset{\varphi}{\sim} \overline{G}$，则 $\varphi(K) = e$.

$\forall x,y \in G$, $\varphi(x) = \varphi(y) = a'$，设 $\varphi(a) = a'$

令 $t = a^{-1}x$，则 $\varphi(t) = \varphi(a^{-1})\varphi(x) = a'^{-1}a' = e'$，故 $t \in K$

从而 $x \in aK$，同理 $y \in aK$.

($\Leftarrow$) $\forall x,y \in aK$，设 $x = at_1$, $y = at_2$，其中 $\varphi(t_1) = \varphi(t_2) = e$

于是 $\varphi(x) = \varphi(a)\varphi(t_1) = \varphi(a)$，同理 $\varphi(y) = \varphi(a)$ ◻

3. 证明: 因为 $N \trianglelefteq G$, $N \subseteq H \leq G$，可知 $N \trianglelefteq H$.

设 $G \overset{\varphi}{\sim} G/N$，则 $\forall aN \in H/N$, $\varphi(a) = aN$，且 $a \in H$.

反过来，$\forall a \in H$, $\varphi(a) = aN \in H/N$. 于是 $H \overset{\varphi}{\sim} H/N$.

5. 证明: 假设存在双射 $\varphi: \mathbb{Q}_+ \to \mathbb{Q}^*$,

设 $\varphi^{-1}(-1) = x$, $\varphi^{-1}(1) = y$，则 $x \neq y$.

但是 $\varphi(2x) = \varphi(x)\varphi(x) = 1 = \varphi(y)\varphi(y) = \varphi(2y)$

这与 φ 是单射矛盾. 故 $\mathbb{Q}_+ \ncong \mathbb{Q}^*$

1. (1) $\forall a \in H \cap K$，显然 $aH = Ha$.

因为 $K' \trianglelefteq K$, $aK' = K'a$

从而 $aH \cap aK' = Ha \cap K'a$

即 $a(H \cap K') = (H \cap K')a$

(2) $(H/K') \cap (K/K') \leq K/K'$,

令 $\varphi: H \cap K / H \cap K' \longmapsto (H/K') \cap (K/K')$

$a(H \cap K') \longrightarrow aK'$

下证 φ 是同构映射.

$\forall a,b \in H \cap K$, s.t. $a(H \cap K') = b(H \cap K')$,

有 $a^{-1}b \in H \cap K' \leq K'$，故 $aK' = bK'$

因为 $a \in H \cap K$, $aK' \in (H/K') \cap (K/K')$.

所以 φ 是 $H \cap K / H \cap K' \to (H/K') \cap (K/K')$ 的映射

$\forall M \in (H/K') \cap (K/K') \subseteq H/K'$，有 $M = aK'$, $a \in H$

同理有 $M = bK'$, $b \in K$，于是 $aK' = bK'$，从而 $a \in bK'$

因为 $K' \trianglelefteq H, K$，可知 $K' \subseteq H \cap K$，故 $a \in H \cap K$.

所以 $\forall M \in (H/K') \cap (K/K')$，有 $M = aK'$, $a \in H \cap K$

从而 $\varphi(N) = M$, $N = a(H \cap K') \in H \cap K / H \cap K'$.

$\forall M, N \in H \cap K / H \cap K'$

设 $M = a(H \cap K')$, $N = b(H \cap K')$, $a, b \in H \cap K$

如果 $\varphi(M) = \varphi(N)$，即 $aK' = bK'$,

则 $a^{-1}b \in K' \leq H \cap K'$，从而 $M = N$.

所以 φ 是双射

又，$\forall M, N \in H \cap K / H \cap K'$, $MN = ab(H \cap K')$

$\varphi(MN) = abK' = (aK')(bK') = \varphi(M)\varphi(N)$

所以 φ 是同构映射. 原命题得证.

3. 假设 G 不是交换群，即 $\exists a, b \in G$, $ab \neq ba$.

令 $\varphi: G \mapsto G$, $x \longrightarrow abxb^{-1}a^{-1}$.

则 ① $\forall x,y \in G$, $\varphi(xy) = abxyb^{-1}a^{-1} = (abxb^{-1}a^{-1})(abyb^{-1}a^{-1}) = \varphi(x)\varphi(y)$

② $\forall y \in G$，令 $x = b^{-1}a^{-1}yab$，有 $\varphi(x) = y$

③ $\forall x,y \in G$，如果 $\varphi(x) = \varphi(y)$ 即 $abxb^{-1}a^{-1} = abyb^{-1}a^{-1}$，由消去律得 $x = y$

所以 φ 是 G 的自同构.

因为 $\varphi(b) = abbb^{-1}a^{-1} = aba^{-1} \neq baa^{-1} = b$,

φ 不是恒等映射，矛盾. 所以 G 是交换群.

现已知 G 是交换群.

假设 $\exists a \in G$, $a^2 \neq e$，则令 $\varphi: G \mapsto G$, $x \longrightarrow x^{-1}$.

因为 $\varphi(a) = a^{-1} \neq a$，$\varphi$ 不是恒等映射.

$\forall x,y \in G$, $\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = \varphi(y)\varphi(x) = \varphi(x)\varphi(y)$

又 φ 显然是双射. 故 φ 是 G 的自同构.

所以 $\mathrm{Aut}\, G \neq \{I\}$，矛盾.

(直观理解: 非交换或有非二阶元(除 e 外)，说明有不完全相同的对称的群)

3.2.2 单群

2024年1月5日 20:14

Def. 阶大于1且只有平凡正规子群的群称为单群

Thl 有限交换群为单群的充要条件是|G|为素数