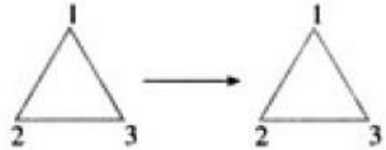
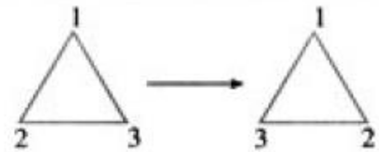
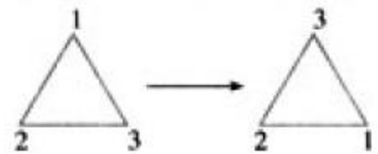
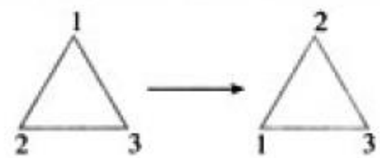
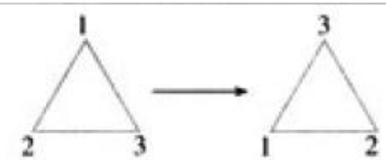
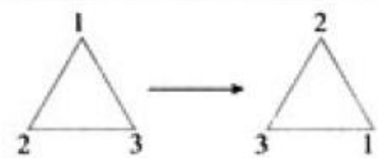
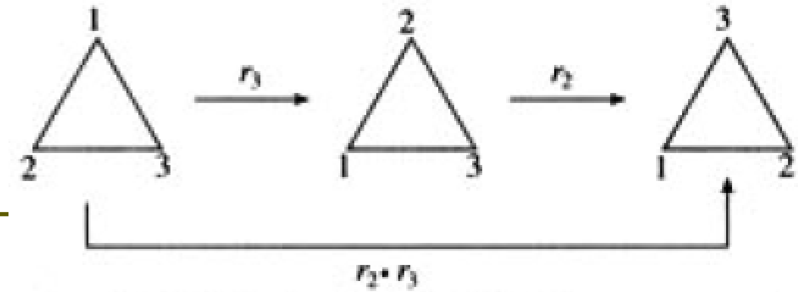
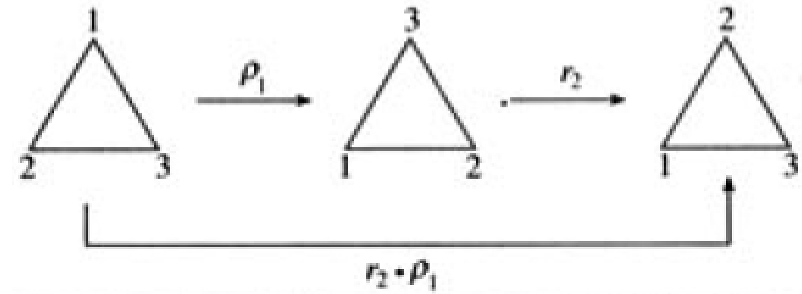
第十七章群

- 群的定义与性质
- 子群
- 循环群
- 变换群和置换群
- 群的分解
- 正规子群和商群
- 群的同态与同构
- 群的直积

对称变换	图形的变换	顶点的变换
恒等变换 I		$\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$
反射变换 r_1		$\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$
反射变换 r_2		$\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$
反射变换 r_3		$\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$
旋转变换 ρ_1		$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$
旋转变换 ρ_2		$\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$

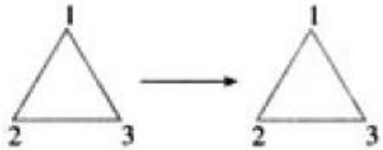
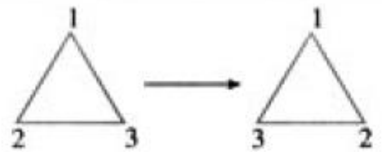
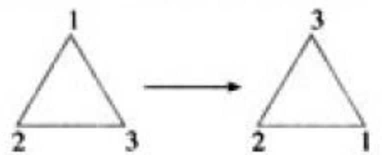
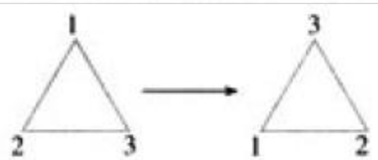
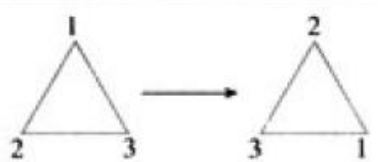


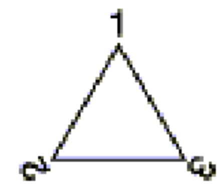
$r_2 \cdot r_3 = \rho_1$

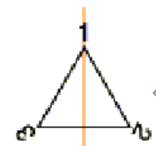


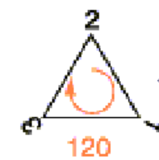
$r_2 \cdot \rho_1 = r_3$

$\cdot$	I	ρ_1	ρ_2	r_1	r_2	r_3
I	I	ρ_1	ρ_2	r_1	r_2	r_3
ρ_1	ρ_1	ρ_2	I	r_3	r_1	r_2
ρ_2	ρ_2	I	ρ_1	r_2	r_3	r_1
r_1	r_1	r_2	r_3	I	ρ_1	ρ_2
r_2	r_2	r_3	r_1	ρ_2	I	ρ_1
r_3	r_3	r_1	r_2	ρ_1	ρ_2	I

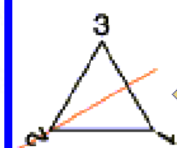
恒等变换 I		$\begin{bmatrix}1&2&3\\1&2&3\end{bmatrix}$
反射变换 r_1		$\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix}$
反射变换 r_2		$\begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}$
反射变换 r_3		$\begin{bmatrix}1&2&3\\2&1&3\end{bmatrix}$
旋转变换 ρ_1		$\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}$
旋转变换 ρ_2		$\begin{bmatrix}1&2&3\\3&1&2\end{bmatrix}$



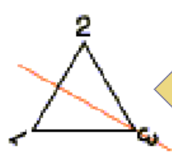
 $\Leftrightarrow \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$



$\Leftrightarrow \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

 $\Leftrightarrow \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

$\Leftrightarrow \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

 $\Leftrightarrow \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$

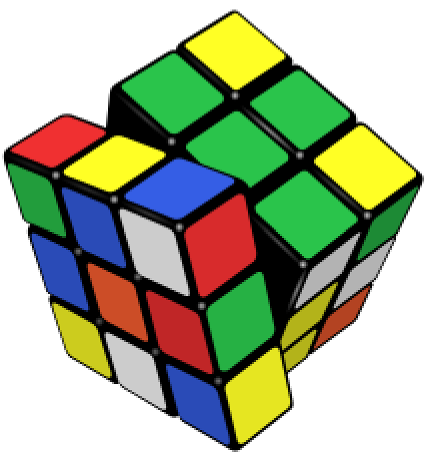
$\Leftrightarrow \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

群与对称性

- 台湾交大应用数学系郭君逸魔方与群论12个PPT（15节课）

  http://www.youku.com/playlist_show/id_3675769.html

- https://en.wikipedia.org/wiki/Rubik%27s_Cube_group



$$|G| = 43,252,003,274,489,856,000$$
$$= 2^{27}3^{14}5^{3}7^{2}11$$

The largest order of an element in *G* is 1260.

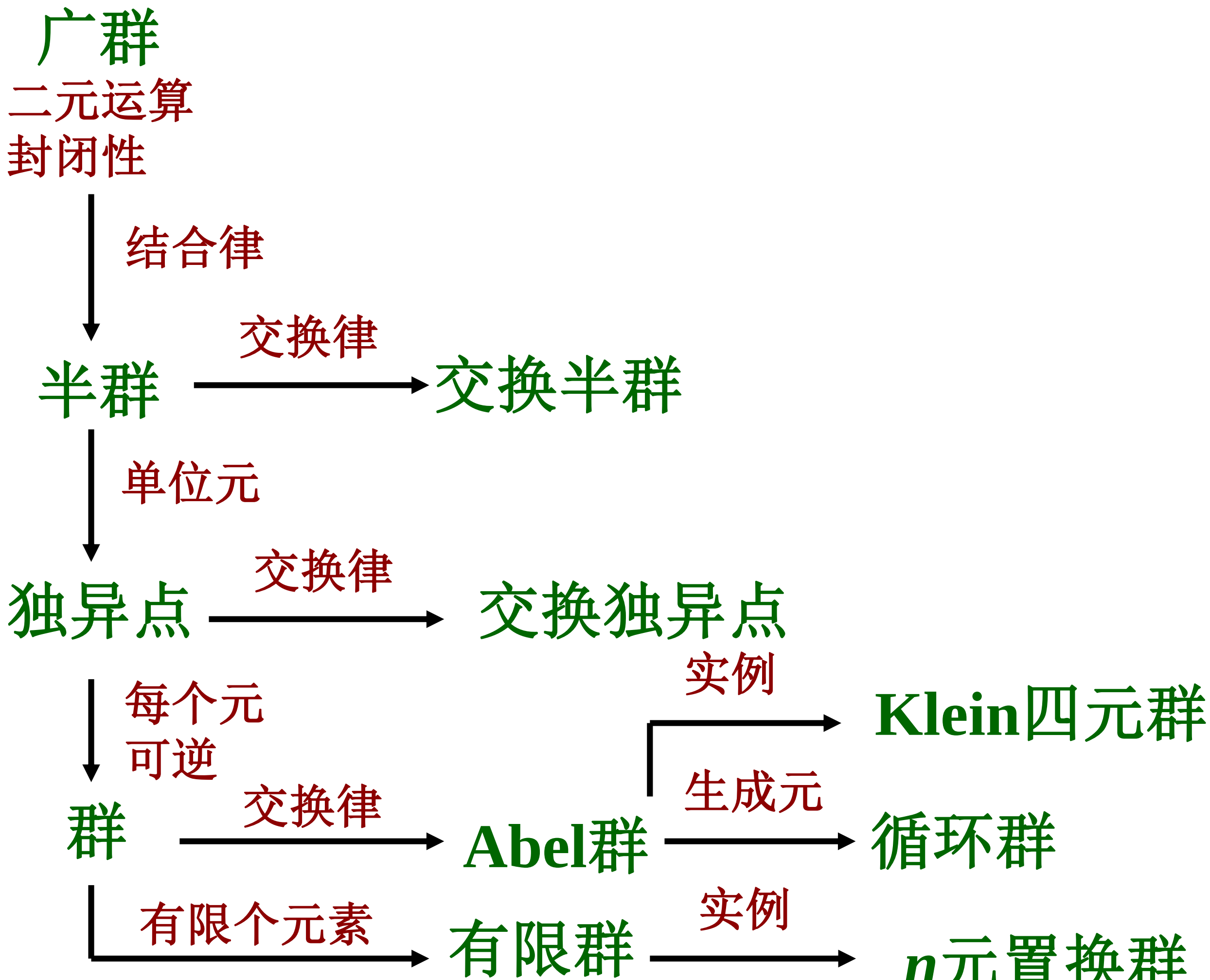
***G* is non-abelian.**

God's Number for Rubik's Cube is 20. (July 2010)

17.1 群的定义与性质

- 群的定义
  - 定义与实例
  - 等价定义
  - 相关术语
- 群的性质
  - 幂运算规则
  - 群方程有唯一解
  - 消去律
  - 运算表的置换性质
  - 元素的阶的性质
- 习题分析

半群与群


广群
二元运算
封闭性
结合律
半群
交换律
交换半群
单位元
独异点
交换律
交换独异点
每个元
可逆
群
交换律
Abel群
实例
Klein四元群
生成元
循环群
有限个元素
有限群
实例
n元置换群

群的定义1

可以将群看成代数系统<G, ∘, $^{-1}$, e>

定义 称非空集合G为一个群，如果在G中定义了一个二元运算∘, 且满足:

1. 结合律：$(a \circ b) \circ c = a \circ (b \circ c), \forall a, b, c \in G;$
2. 存在单位元：$\exists e \in G, \text{s.t. } e \circ a = a \circ e = a, \forall a \in G;$
3. 存在逆元：$\forall a \in G, \exists a^{-1} \in G, \text{s.t. } a^{-1} \circ a = a \circ a^{-1} = e.$

群的定义2

定理1 (等价定义) $<G, \circ>$, $\circ$可结合，若存在右单位元e，且每个元素a相对于e存在右逆元a'，则G是群。

证 先证e为左单位元. $\forall a \in G$，有$aa' = e$，且

$$ee = e \quad (e\text{为右单位元})$$

$$\Rightarrow e(aa') = (aa') \Rightarrow (ea)a' = aa'$$

$$\Rightarrow ea = a \quad (\text{右乘}a'\text{的右逆元})$$

再证a'为a的左逆元，即$a'a = e$, 亦即证a是a'的右逆元。设a'的右逆元为a''，需证$a'' = a$。事实上，

$$a'' = ea'' = (aa')a'' = a(a'a'') = ae = a.$$

群的术语

平凡群 只含单位元的群$\{e\}$

交换群 Abel群

有限群与无限群

群G的阶 G的基数，通常有限群记为$|G|$

元素a的n次幂

$$a^n = \begin{cases} e & n = 0 \\ a^{n-1}a & n > 0 \\ (a^{-1})^m & m = -n, n < 0 \end{cases}$$

元素a的阶$|a|$：使得$a^k=e$成立的**最小正整数**k

说明：有限群的元素都是有限阶，为群的阶的因子；

反之，元素都是有限阶的群不一定是有限群.

群的性质1

定理2 幂运算规则

1. $(a^{-1})^{-1}=a$
2. $(ab)^{-1}=b^{-1}a^{-1}$
3. $a^n a^m=a^{n+m}$
4. $(a^n)^m=a^{nm}$
5. 若G为Abel群，则$(ab)^n=a^n b^n$

说明：

等式1和2的证明用到逆元定义和唯一性

等式3和4的证明使用归纳法并加以讨论

等式2可以推广到有限个元素之积.

群的性质2

定理3 方程$ax=b$和$ya=b$在群G中有解且有唯一解.

证 $a^{-1}b$是$ax=b$的解.

假设c为解，则

$$c=ec=(a^{-1}a)c=a^{-1}(ac)=a^{-1}b$$

定理4 (逆命题) 设G是半群，如果对任意$a,b\in G$，方程$ax=b$和$ya=b$在G中有解，则G为群.

证 找右单位元和任意元素的右逆元.

任取$b\in G$, 方程$bx=b$的解记为e.

$\forall a\in G, yb=a$的解记为c, 即$cb=a$.

$$ae=(cb)e=c(be)=cb=a$$

故e为右单位元.

$\forall a\in G$, 方程$ax=e$有解，得到a的右逆元.

群的性质3

定理5（消去律）$ab=ac \Rightarrow b=c$, $ba=ca \Rightarrow b=c$

定理6 设G是有限半群，且不含零元. 若G中消去律成立，则G是群.

证 设$G=\{a_1,a_2,\ldots,a_n\}$，任取$a_i \in G$，有

$$a_iG=\{a_ia_j \mid j=1, 2, \ldots, n\}$$

由封闭性知, $a_iG \subseteq G$, 假设$|a_iG|<n$, 则存在j, k使得$a_ia_j=a_ia_k$, 根据消去律，$a_j=a_k$, 矛盾！所以$a_iG=G$.

任取a_i, a_j, 由a_i, $a_j \in G \Rightarrow a_j \in a_iG \Rightarrow$方程$a_ix=a_j$有解。

同理，方程$ya_i=a_j$有解。因此，G是群。

注：$<Z_5, \otimes>$不是群，因为有零元0；$<Z^+, \cdot>$也不是群，无限.

群的性质4

定理7 有限群*G*的运算表中每行、每列都是*G*的置换，即 $aG=G$, $Ga=G$.

说明 运算表的行列构成置换的不一定是群，反例：

	0	1	2
0	1	2	0
1	0	1	2
2	2	0	1

思考：

3元集上的不同的二元运算有多少个？

3元集上二元运算表有多少个，使得每行每列能够构成置换？

3元集上有多少个不同的运算表代表群？

3元集上同构的群有多少个？

群的性质5

定理8 G为群，$a \in G$, 且$|a| = r$, 则

(1) $a^k = e \Leftrightarrow r|k$

(2) $|a| = |a^{-1}|$

(3) 若$|G| = n$, 则$r \leq n$.

证 (1)充分性. $a^k = a^{rl} = (a^r)^l = e^l = e$

必要性. $k = rl + i,\ l \in Z,\ i \in \{0, 1, \ldots, r-1\}$

$$\Rightarrow e = a^k = a^{rl+i} = a^i \Rightarrow i = 0 \Rightarrow r|k.$$

(2) $\left(a^{-1}\right)^r = e \Rightarrow |a^{-1}|$存在, 令$|a^{-1}| = t$, 则$t|r$. 同理$r|t$.

(3) 假设$r > n$, 令$G' = \{e, a, a^2, \ldots, a^{r-1}\}$, 则$G'$中元素两两不同，否则与$|a| = r$矛盾。从而$|G'| > n$，与$G' \subseteq G$矛盾.

习题课一

重要结果

(1) $|a| = 1或2 \Leftrightarrow a = a^{-1}$

(2) $|a| = |a^{-1}|,\ |ab| = |ba|,\ |a| = |bab^{-1}|$

(3) $|a| = r \Rightarrow |a^t| = \frac{r}{(t,r)}$

(4) $|a| = n, |b| = m, ab = ba \Rightarrow |ab| \mid [n,m]$;

若$(n,m) = 1$, 则$|ab| = nm$.

(1)(2)(4)的证明留做思考题

符号(n, r)与$[n, r]$

$(\boldsymbol{n},\ \boldsymbol{r})$

定义：　$\boldsymbol{n}$与$\boldsymbol{r}$的最大公约数

性质：　$\exists \boldsymbol{u}, \boldsymbol{v} \in \boldsymbol{Z}\ \mathbf{s.t.}\ \boldsymbol{un} + \boldsymbol{rv} = (\boldsymbol{n},\ \boldsymbol{r})$

$(\boldsymbol{n},\ \boldsymbol{r}) = \mathbf{1}, \boldsymbol{n}$与$\boldsymbol{r}$互质（互素）

$\exists \boldsymbol{u}, \boldsymbol{v} \in \boldsymbol{Z}\ \mathbf{s.t.}\ \boldsymbol{un} + \boldsymbol{rv} = \mathbf{1}$

$[\boldsymbol{n},\ \boldsymbol{r}]$

定义：$\boldsymbol{n}$与$\boldsymbol{r}$的最小公倍数

性质：$[\boldsymbol{m}, \boldsymbol{n}] = \dfrac{\boldsymbol{mn}}{(\boldsymbol{m}, \boldsymbol{n})}$

证明方法

证明元素的阶相等或求元素的阶的方法

证$|x| = |y|$:

令$|x| = r, |y| = s,$

验证$(x)^s = e \Rightarrow r|s$

验证$(y)^r = e \Rightarrow s|r$

求$|x|$:

找到满足$x^n = e$的n, 分析n的因子.

证明群的一些基本性质的方法

工具---幂运算规则、结合律、消去律、群方程的解

例题

例1 设G为群，若$\forall x \in G$有$x^2 = e$, 则G为Abel群.

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

分析 $x^2 = e \Leftrightarrow x = x^{-1}$

幂运算规则

例2 若群G中只有唯一2阶元，则这个元素与G中所有元素可交换.

证 设2阶元为$x, \forall y \in G$,

$$\left|yxy^{-1}\right| = |x| = 2 \Rightarrow yxy^{-1} = x \Rightarrow yx = xy$$

分析 $|yxy^{-1}| = |x|$

例题

例3 若G为偶数阶群，则G中必存在2阶元.

证 若$\forall x \in G, |x| > 2$，则$x \neq x^{-1}$

由于$|x| = |x^{-1}|$，大于2阶的元素成对出现，总数有偶数个。G中1阶和2阶元总共也有偶数个，由于1阶元只有单位元，因此2阶元有奇数个，从而命题得证。

分析 $|x| = |x^{-1}|$

$$x^2 = e \Leftrightarrow x = x^{-1}$$

例题

例4 G为群，$a\in G$，$|a|=r$, 证明$|a^t|=r/(t,r)$

证 令$|a^t|=s$, 设$(t,r)=d$, 则$t=dp, r=dq$,

$(p,q)=1, r/(t,r)=r/d=q$

下面只要证$s=q$

$(a^t)^q=(a^t)^{r/d}=(a^r)^{t/d}=e^p=e\Rightarrow s|q$

$(a^t)^s=e\Rightarrow a^{ts}=e\Rightarrow r|ts\Rightarrow dq|dps\Rightarrow q|ps$

$\Rightarrow q|s$（p,q互素）

分析 相互整除

$|a|=r$, $a^k=e$当且仅当$r|k$

例题

例5 设G是群，$x, y \in G$, y为2阶元，$x \neq e$, 且$x^2y=yx$, 求$|x|$.

解：$x^2y=yx \Rightarrow yx^2y=x$

$\Rightarrow (yx^2y)(yx^2y)=x^2$

$\Rightarrow yx^4y=x^2=yxy$

$\Rightarrow x^4=x \Rightarrow x^3=e$

$\Rightarrow |x|=3 \qquad (x \neq e)$

分析 关键是导出关于$x^k=e$的等式

根据$x^k=e \Leftrightarrow |x| \mid k$，

使用幂运算规则，结合律，消去律，$|x|=2 \Leftrightarrow x=x^{-1}$

17.2 子群

- 子群定义
- 子群判别定理
- 重要子群的实例
  - 生成子群
  - 中心
  - 正规化子
  - 共轭子群
  - 子群的交
- 子群格

子群定义

定义 设G为群, H是G的非空子集，若H关于G中运算构成群，则称H为G的子群，记作$H \le G$.

如果子群H是G的真子集，则称为真子群，记作$H < G$.

说明：子群H就是G的子代数.

假若H的单位元为e', 且x在H中相对e'的逆元为x',

则

$$xe' = x = xe \Rightarrow e' = e$$

$$xx' = e' = e = xx^{-1} \Rightarrow x' = x^{-1}$$

子群判定定理一

定理1 G是群，H是G的非空子集，则

$$H \leq G \Leftrightarrow \forall a, b \in H, ab \in H, b^{-1} \in H.$$

证：只证充分性.

H非空，存在$a \in H$，

由条件2，$a^{-1} \in H$，

由条件1，有$aa^{-1} \in H$，即$e \in H$.

子群判定定理二和三

定理2 G是群，H是G的非空子集，则

$$H \le G \Leftrightarrow \forall a,b \in H, ab^{-1} \in H.$$

证 充分性. $H\neq\varnothing\Rightarrow\exists b\in H$

$$b\in H\Rightarrow bb^{-1}\in H\Rightarrow e\in H$$

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

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

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

定理3 G是群，H是G的非空有限子集，则

$$H \le G \Leftrightarrow \forall a,b \in H, ab \in H.$$

证明见教科书.

重要子群的实例

a生成的子群 $\langle a \rangle = \{a^k | k \in Z\},\ a \in G$

B生成的子群 $\langle B \rangle = \cap \{H | H \le G, B \subseteq H\}, B \subseteq G$

$\langle B \rangle = \{b_1^{e_1} b_2^{e_2} \dots b_n^{e_n} | b_i \in B, e_i = \pm 1, i = 1, 2, \dots, n, n \in Z^+\}$

中心 $C = \{a \in G | \forall x \in G, ax = xa\}$

a的正规化子 $N(a) = \{x \in G | xa = ax\}, a \in G$

H的正规化子 $N(H) = \{x \in G | xHx^{-1} = H\}, H \subseteq G, H$非空

共轭子群 $xHx^{-1} = \{xhx^{-1} | h \in H\}$，其中$H \le G, x \in G$

子群的交

$A, B \le G$,则

(1) $A \cap B \le G$

(2) $A \cup B \le G \Leftrightarrow A \subseteq B$或$B \subseteq A$

If $H \le G$, then the largest subgroup in which H is normal is the subgroup $N(H)$.

关于子群的证明

求证：中心C为G的子群.

$C=\{a\in G \mid \forall x\in G, ax=xa\}$

证 由于e属于C, 故C非空.

任取$x, y\in C$，对于任意$a\in G$有

$(xy^{-1})a=x(y^{-1}a)=x(a^{-1}y)^{-1}=x(ya^{-1})^{-1}$

$=x(ay^{-1})=(xa)y^{-1}=(ax)y^{-1}=a(xy^{-1})$

因此xy^{-1}属于C. 由判定定理2，命题得证.

子群的证明(续)

设$H, K \le G$, 则

(1) $H \cap K \le G$.

(2) $H \cup K \le G \Leftrightarrow H \subseteq K$或$K \subseteq H$.

证 (1) 略.

(2) 只证必要性.

假若 $\exists h(h \in H, h \notin K), \exists k(k \in K, k \notin H)$,

则$hk \notin H$，否则$k = h^{-1}(hk) \in H$, 矛盾.

同理$hk \notin K$, 从而$hk \notin H \cup K$,

但是$h, k \in H \cup K$, 与$H \cup K \le G$矛盾.

AB构成子群的条件

命题 设$A, B \le G$，定义$AB=\{ab|a\in A, b\in B\}$, 则

(1) $AB\le G \Leftrightarrow AB=BA$

(2) $AB\le G \Rightarrow AB=\langle A\cup B\rangle$.

证 (1)习题16.

(2) $A\subseteq AB, B\subseteq AB \Rightarrow A\cup B\subseteq AB \Rightarrow \langle A\cup B\rangle \subseteq AB$

$\forall ab\in AB$，其中$a\in A, b\in B \Rightarrow a, b\in A\cup B$

$\Rightarrow a, b\in \langle A\cup B\rangle \Rightarrow ab\in \langle A\cup B\rangle$

例 Klein四元群$G=\{e, a, b, c\}$,

$\langle a\rangle=\{e, a\}, \langle b\rangle=\{e, b\}, \langle c\rangle=\{e, c\}$

$\langle a\rangle\langle b\rangle=\{e, a, b, c\}$

$\langle \{a, e\}\cup\{b, e\}\rangle=\langle\{a, b, e\}\rangle=\{e, a, b, c\}$

	e	*a*	*b*	*c*
e	*e*	*a*	*b*	*c*
a	*a*	*e*	*c*	*b*
b	*b*	*c*	*e*	*a*
c	*c*	*b*	*a*	*e*

子群格

格的偏序集定义：

$<S,\preccurlyeq>$, S 的任何二元子集都有最大下界、最小上界.

G为群，$S=\{H|H\leq G\}$, 偏序集$<S,\leq>$构成格，

称为G的子群格

Klein四元群，Z_{12}的子群格.