群论整理

半群与群

半群与幺半群之定义

半群定义:

若集合$(M,\cdot)$满足:

1. 二元运算$\cdot : M\times M\to M, (a,b)\in a\cdot b$;
2. 结合律$(ab)c=a(bc)=abc$.

则称$(M,\cdot)$为半群。

幺半群定义:

若半群含有单位元e使得对任意$a\in M$满足$ea=ae=1$, 则称$(M,\cdot)$为幺半群.

群的定义

一般定义

若集合$(G,\cdot)$满足:

1. 二元运算$\cdot : G\times G\to G, (a,b)\in a\cdot b$;
2. 结合律$(ab)c=a(bc)=abc$;
3. 存在单位元$e\in G$使得对任意$a\in G$均有$ea=ae=a$;

   > *单位元唯一性：$e=ee'=e'$.*

4. 对任意元素$a\in G$存在逆元a^{-1}使得$a^{-1}=a^{-1}a=e$.

   > *逆元唯一性: $a'^{-1}a'^{-1}aa^{-1}=a$.*

> *Remark. 前两条说明群蕴含半群之性质, 第三条说明群为蕴含幺半群之性质.*

（左）单边定义

若幺半群$(G,\cdot)$满足

1. 存在左单位元$e_l\in G$使得对任意$a\in G$均有$e_la=a$;
2. 对任意元素$a\in G$存在左逆元a^{-1}使得$a_l^{-1}a=e_l$.

> *Remark. 证明思路: 考虑$(g_l^{-1})_l^{-1}g_l^{-1}\cdot gg_l^{-1}$即可.*

> *Remark. 将3, 4两则中“左”换作“右”结论亦然; 同时存在左单位与右逆元者或非然, 于半群$(\{e_l,a\},\cdot)$中置二元运算为取右元即可, 即$a\cdot b=b$.*

消去律判定（有限群情形）

若有限幺半群$(G,\cdot)$满足

1. 左消去律, 即$\forall a,b,c\in G: ca=cb\Leftrightarrow a=b$;
2. 右消去律 (定义同上).

则$(G,\cdot)$为群.

> *Remark. 视左乘映射$f_g: G\to G, x\mapsto gx$, 则映射是一一的, 右乘映射同理.*

子群与陪集

子群相关定义及判准

子群定义

$H \subset G$为$(G, \cdot)$的子群若且仅若$(H, \cdot)$为群. 记作$H \leq G$.

真子群定义

G的子群H为真子群若且仅若$G \neq H$.

子群判别法则

G的子集H为子群, 若且仅若$\forall a, b \in H : ab^{-1} \in H$.

> *Remark.* G*有限时,* G*的子集*H*为子群, 若且仅若*$\forall a, b \in H : ab \in H$*. 对无限群而言,* a *或无法通过自乘以生成逆元, 因而至多推出*H*为半群.*

G的子集H为子群, 若且仅若$\exists A, B \leq G$使得$H = AB = BA$.

陪集定义及其相关性质

陪集划分

设$H \leq G$, 则存在由一组代表元系组成之集合$R \subset G$使得$G = \dot{\cup}_{x \in R} xH$为无交并.

> *Remark: 由是得陪集之等价划分, 从而两个陪集仅有全等与不交之情形.*

Lagrange定理

设$H \leq G$, 记$[G : H]$为陪集之数量, 亦即H的指数. Lagrange定理如是说: $G = |H| \cdot [G \cdot H]$, 且对无穷之情形亦然.

左右陪集之关系

左右陪集可一一对应: 对任意$H \leq G$, H于G下之左陪集R_l与右陪集R_r间存在元素间的一一对应.

Prop. 左右陪集可互相生成: R_l可由$R_r^{-1} := \{r^{-1} : r \in R_r\}$表示.

Prop. H与K具有有限阶指数之子群, 则

$$|HgK| = |H| \cdot [K : g^{-1}Hg \cap K] = |K| \cdot [K : g^{-1}Kg \cap K]$$

证明: 记$HgK = \dot\cup_{1 \leq i \leq t} Hgk_t$, 则$\{k_t\}$为$g^{-1}Hg \cap K$某陪集划分之代表元系. 由Lagrange定理即得.

Prop. 对任意$H \leq G$均存在$R_l = R_r$之情形.

证明: 考虑双陪集分解$G = \dot\cup_{g \in R} AgA$, 故$|AgA|$为$A$的$[A : g^{-1}Ag \cap A]$个陪集之并 (实际上$[A : g^{-1}Ag \cap A] = |A|$或1). 则

$$AgA = \cup_{i=1}^t Aga_i(g) = \cup_{i=1}^t b_i(g)gA$$

因此

$$G = \dot\cup_{r \in R} \dot\cup_{1 \leq i \leq t} b_i(g)ga_i(g)A = \dot\cup_{r \in R} \dot\cup_{1 \leq i \leq t} Ab_i(g)ga_i(g)$$

由此可知**陪集不必强调左右**.

积集公式

对任意群A, B均有$|A| \cdot |B| = |AB| \cdot |A \cap B|$.

证明: 考虑$\varphi \in \hom(A \times B, AB)$, 计算$\dfrac{|A \times B|}{|\ker \varphi|} = |\mathrm{im}\varphi|$即可.

子群覆盖与生成

1. $A, B \subset G$且$|A| + |B| > G$, 则$AB = G$;
2. G一定可由过半的元素生成.
3. 子群的任意并为子群.
4. 有限群中某一子群的共轭子群之并不能覆盖整个群.

> *证明：所有$N \leq G$, 共轭子群占有$\frac{|G|}{|N_G(N)|}(|N|-1)+1$个元素. 若*
>
> $$\frac{|G|}{|N_G(N)|}(|N|-1)=|G|-1$$
>
> *则由互质关系得到$|N_G(N)|=|G|$. 显然矛盾.*
>
> *Remark: 对无穷维情形或不再成立. 考虑代数闭域上的Shur上三角化即可.*

5. 群不等于任意两个真子群之并, 但或能表示为三个真子群之并(如K_4).
6. 未完待续...

元素的阶

基本概念

定义: 元素$g \in G$的阶$o(g) := \inf_{k,k\geq 1,g^k=1} k \in [1,\infty]$.

性质 (设$g \in G$, G为有限群)

1. $o(g) \mid |G|$, 即$g^{|G|}=1$;
2. $o(g^m)=\dfrac{o(g)}{\gcd(o(g),m)} \leq o(g)$;
3. $\forall a,b \in G: o(ab)=o(ba)$;
4. $\forall g \in G: o(g)=o(g^{-1})$;
5. $a,b \in G$且$\gcd(o(a),o(b))=1$且$ab=ba$, 则$o(ab)=o(a)o(b)$;

   > *对非可交换情形或非然, 如D_3中元素$\tau\sigma$.*

6. $\{g \in G: o(g) \mid k\}$不构成G的子群, 如置换群可由对换生成;
7. 未完待续...

Cauchy定理

对任意$|G|$的素因子p, 总存在p阶元. 该定理本质上为弱化的Sylow I定理.

共轭关系

定义

共轭关系与共轭类

G中元素a, b在G中共轭若且仅若存在$g \in G$使得$a = g^{-1}bg$.

共轭类系等价类$[a] := \{b : \exists g \in G \text{ s.t. } g^{-1}bg = a\}$. 显然$G = \dot\cup_{a\in R}[a]$.

中心化子与中心

a的**中心化子**定义为所有与a可交换元素之集合, 即$C_G(a) := \{c \in G : ca = ac\}$.

群G的**中心**$C(G) := \cap_{a\in G}C_G(a) = \{x : gx = xg\,(\forall g \in G)\}$.

类数公式:

$$|G| = \sum_{a\in R}\frac{|G|}{|C_G(a)|} = |C(G)| + \sum_{a\in R\setminus C(G)}\frac{|G|}{|C_G(a)|}$$

Prop. p^k阶群无平凡中心, 这里p为质数. (类数公式推论)

正规化子与正规子群

$M \le G$的正规化子为$\{g \in G : gM = Mg\}$.

正规子群: $H \le G$为正规子群若且仅若$N_G(H) = G$, 亦即$|[H]| = 1$.

$H \lhd G$的等价定义:

1. $N_G(H) = G$;
2. H于G中的共轭子群仅有自身;
3. H的任一左陪集均为右陪集;

   > *Remark: 指数为2的子群一定正规.*

4. G/H为群.

Prop. $C_G(M) \lhd N_G(M)$.

证明: $f_h : M \to M, m \mapsto h^{-1}mh$为$M$的自同构. 对任意$c \in C_G(C)$, 下证明$hch^{-1}$仍然为$M$的中心. 由于对任意$m \in M$皆有$hch^{-1}m(hch^{-1}) = f_h^{-1}(cf_h(m)c^{-1}) = m$, 明所欲证.

> *Remark. 中心与中心化子皆为正规子群.*

> *Remark. 正规子群之正规子群不一定为正规子群, 如$\mathbb{Z}_2 \lhd K_4 \lhd A_4$, 但显然$\mathbb{Z}_2 \not\lhd A_4$.*

群同态相关定理

同态与同构

幺半群/群**同态**定义如是: $\pi : G_1 \to G_2$为同态, 若且仅若对任意g_1, g_2 属于S_1均有$\pi(g_1 g_2) = \pi(g_1)\pi(g_2)$. 记作$\pi \in \hom(G_1, G_2)$, 亦即$\pi$属于$G_1$至$G_2$的同态群.

同构即单且满的同态. 记$\mathrm{aut}(G_1, G_2)$为G_1至G_2的同构, 可视作$\hom(G_1, G_2)$所包含之最大群, 即可逆元之集合.

自同构群$\mathrm{aut}(G, G)$可记作$\mathrm{aut}(G)$. 内自同构为自身元素的共轭作用所对应的同构, 表示为

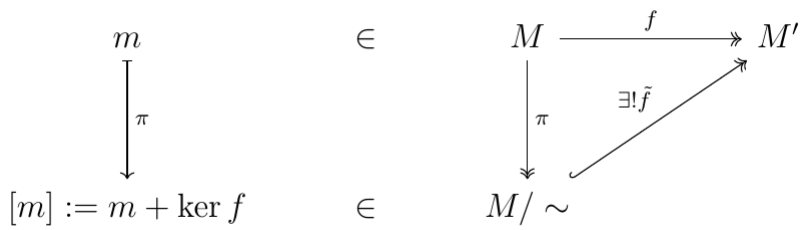
$$\mathrm{inn}(G) := \{f_g : g \in G; f_g : G \to G, x \mapsto g^{-1}xg\}$$

> *Remark.* $\mathrm{inn}(G) \lhd \mathrm{aut}(G)$.

> *Remark:* $\mathrm{inn}(G) \cong G/C(G)$.

同态基本定理

置$f \in \hom(M_1, M_2)$为满同态, 其中$f^{-1}(1)$记作$\ker f$. 显然M_1作为群时有$\ker f \lhd M_1$. 有如下图表交换:

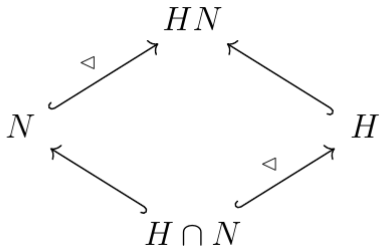


群同态定理

上图中有$G/H \cong \mathrm{im} f$.

第一同构定理

若$H \leq N_G(N)$, 则有图表



与同构$\dfrac{HN}{N} \cong \dfrac{H}{H \cap N}$.

第二同构定理 (子群对应定理)

若$N \subset H \leq G, N \lhd G$, 则$H/N \lhd G/N \Leftrightarrow H \lhd G$. 或曰: 商即子之商.

映射形式

$$
\begin{array}{rccc}
\varphi: & G_1 & \twoheadrightarrow & G_2 \\
& \downarrow & & \downarrow \\
& \{H_1 : \ker\varphi \subset H_1 \leq G_1\} & \overset{1:1}{\twoheadrightarrow} & \{H_2 : H_2 \leq G_2\} \\
& \downarrow & & \downarrow \\
& \{H_1 : \ker\varphi \subset H_1 \lhd G_1\} & \overset{1:1}{\twoheadrightarrow} & \{H_2 : H_2 \lhd G_2\}
\end{array}
$$

若$G_2 = G_1/\ker\varphi$, 则对$\ker\varphi \subset H \lhd G_1$均有$G_1/H \cong \dfrac{G_1/\ker\varphi}{H/\ker\varphi}$.

自由群与表示

自由群

字: 字为某集合X中的元素中通过形式组合得到的形式表达式, 其长度可为零 (得到空字), 可有穷, 也可无穷. 所有此类式子 (包括空字) 组成集合$M(X)$

自由幺半群: 记$(M(X),\tau)$为X上的自由幺半群, 若对到任意幺半群M'的映射τ'存在唯一的同态φ使得下表可交换.

$$\begin{array}{ccc} X & \xrightarrow{\tau} & M(X) \\ \downarrow{\scriptstyle \tau'} & \swarrow{\scriptstyle \exists!\varphi} & \\ M' & & \end{array}$$

自由群: 考虑构造$X\cup X^{-1}$, 其中$X^{-1}:=\{x^{-1}:x\in X\}$. 记$F(X):=M(X\cup X^{-1})$. 记$(F(X),\tau)$为$X$上的自由群, 若对到任意群$F'$的映射$\tau'$存在唯一的同态$\varphi$使得下表可交换.

$$\begin{array}{ccc} X & \xrightarrow{\tau} & F(X) \\ \downarrow{\scriptstyle \tau'} & \swarrow{\scriptstyle \exists!\varphi} & \\ F' & & \end{array}$$

自由群之诠释更宜范畴学之角度, 在此不拟细说.

群表示

我们期望群G能以X上的自由群以及相应的约化方式得到, 自然需验证以下命题:

Prop. 任一群均为自由群之商群. 任一有限群皆为一有限生成自由群之商群.

证明: 令$X=\{x:x\in G\}$, 构造同态映射

$$\pi:F(X)\to G, 1\mapsto e, s_n\cdots s_1\mapsto s_n\cdots s_1$$

即可. 显然G有限时$F(X)$有限生成.

群表示要求取合适之π以表示G, 自然应从$\ker\pi$入手. 取$\ker\pi$为包含所有约束关系之最小正规子群即可, i.e.

$$F(X)/\langle Y\rangle_{\text{正规}}\xrightarrow{\sim}G$$

其中$Y=\{y_1,y_2,\cdots,y_n\cdots\}\subset F(X)$. 取$X,Y$为有限集时, G具有有限表示.

> *Remark:* $\langle Y\rangle_{\text{正规}}=\left\langle x^{-1}Yx:x\in X\right\rangle$.

> *Remark: (Nielsen–Schreier) 自由群之子群仍为自由群.*

> *Remark: (R. Guranlnick & G. Malle) 任意非交换有限单群可由两个共轭元素生成.*

特殊群的表示

二面体群

$$D_n\cong\left\langle a,b:a^n=b^2=(ab)^2=1\right\rangle$$

证明: 记$\pi:F(a,b)\xrightarrow{\sim}D_n$, 不难验证$K:=\left\langle a^n=b^2=(ab)^2=1\right\rangle_{\text{正规}}\subset\ker\pi$, 故
$|F(a,b)/K|\geq 2n$. 而$ab=ba^{n-1}$给出将任一字中b移动至a之前的方案. 因此
$D_n\subset\{b^ia^j:i=0,1,j=0,1,\cdots,n-1\}$. 得证.

四元数群

$$Q_8\cong\left\langle a,b:a^4=1,a^2=b^2,ba=a^3b\right\rangle$$

证明: 记$\pi:F(a,b)\xrightarrow{\sim}Q_8$, 不难验证$K:=\left\langle a^4=1,a^2=b^2,ba=a^3b\right\rangle_{\text{正规}}\subset\ker\pi$, 故
$|F(a,b)/K|\geq 8$. 而$ba=a^3b$给出所有将b移动至a之后的方案. 因此
$Q_8\subset\{a^ib^j:i=0,1,2,3,j=0,1\}$. 得证.

置换群

$$S_n=\left\langle x_1,\ldots,x_{n-1}\mid x_i^2=1(1\leq i\leq n-1),\,x_ix_j=x_jx_i(j<i-1),\,(x_ix_{i+1})^3=1\,(i\leq n-2)\right\rangle$$

证明: 首先$S_n=\langle(i(i+1)):i=1,2,\ldots,n-1\rangle:=\langle x_1,x_2,\ldots,x_{n-1}\rangle$. 有同态

$$\pi:F(S^n)\to S_3,x_i\to(i(i+1))$$

这里$S^n:=\{x_1,\ldots,x_{n-1}\}$.

由于$x_i^2=1,x_ix_j=x_jx_i(j<i-1)$, 及$(x_ix_{i+1})^3=1\,(i\leq n-2)$, 因此$x_i^2$,
$[x_i,x_j](j<i-1)$与$(x_ix_{i+1})^3(i\leq n-2)$被包含之最小正规子群$K_n$包含于$\ker\pi$. 下用数学归纳法说明$|F(S^n)/K_n|=n!$.

不难验证$n=4$时成立. 不妨设n时成立, 即$|F(S^n)/K_n|=n!$. 下证明

$$S_{n+1}=\left\langle x_1^{(n)},\dots,x_n^{(n)}\mid (x_i^{(n)})^2=1(1\le i\le n),\, x_i^{(n)}x_j^{(n)}=x_j^{(n)}x_i^{(n)}(j<i-1),\, \left(x_i^{(n)}x_{i+1}^{(n)}\right)^3=1\,(i\le n-1)\right\rangle$$

先证明

$$S_{n+1}=S_n\cup(x_n^{(n)}S_n)\cup\cdots\cup(x_1^{(n)}\cdots x_n^{(n)}S_n)$$

只需证对每个$i=1,\dots,n$, 左乘$x_i^{(n)}$运算对$x_j^{(n)}\cdots x_n^{(n)}S_n$封闭.

- 当$i<j-1$时, 可将$x_i^{(n)}$一路平移入S_n, 得证.
- 当$i\ge j-1$时, $x_i^{(n)}$可一直平移至状态

  $$\cdots x_{i-2}^{(n)}x_i^{(n)}x_{i-1}^{(n)}x_i^{(n)}x_{i+1}^{(n)}\cdots S_n$$

  由于$x_i^{(n)}x_{i-1}^{(n)}x_i^{(n)}=x_{i-1}^{(n)}x_i^{(n)}x_{i-1}^{(n)}$, 则上式化为

  $$\cdots x_{i-2}^{(n)}x_{i-1}^{(n)}x_i^{(n)}x_{i-1}^{(n)}x_{i+1}^{(n)}\cdots S_n$$

  再将右侧$x_{i-1}^{(n)}$项一直右移即可. 得证.

综上, S_{n+1}至多含有$(n+1)!$个元素; 而$\pi:F(S^{n+1})/K_{n+1}\to S_{n+1}$为满同态, 故$\pi$为单射. 得证.

pq阶群

当$p\nmid q-1$时, $G\cong\langle t:t^{pq}=1\rangle$; 当$p\mid q-1$时, $G\cong\langle a,b:a^p=b^q=1,ba=b^ra\rangle$, 其中$r^p\equiv 1\mod q$而$r\not\equiv 1\mod q$.

证明: 当pq阶群G非Abel群时, $N(q)=1+kq\mid p$, 故$q=1$, 因此$\langle b\rangle\ni a^{-1}ba=b^r$. 同时$N(p)=1+k'p\mid q$, 若$N(p)=1$则$\mathbb{Z}_{pq}\cong G$矛盾, 故$p\mid q-1$. 下验证其群表示为

$$G=\left\langle a,b\mid a^p=b^q=1,a^{-1}ba=b^r\right\rangle$$

其中任取$r^p\equiv 1\mod q$且$r\not\equiv 1\mod q$.

记自由群$F=\langle a,b\rangle$, $G\cong F/\langle P\rangle_{\text{正规}}$. 群同态$\pi:G\to F$之核包括

$$P=\left\langle a^p,b^q,a^{-1}bab^{-r}\right\rangle$$

因此$|\operatorname{im}\pi|=\left|\dfrac{\langle P\rangle_{\text{正规}}}{P}\right|\ge 1$. 另一方面, 考虑陪集划分, G中元素可表示为a^ib^j, 其中$0\le i\le p-1,0\le j\le q-1$, 因此$\operatorname{im}\pi\le pq$. 综上$\left|\dfrac{\langle P\rangle_{\text{正规}}}{P}\right|=1$, 验证完毕.

p^3阶群

$p=2$时, 8阶群无非$\mathbb{Z}_8$, $\mathbb{Z}_2\oplus\mathbb{Z}_4$, $\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$, D_4, Q_8. 其表示分别为

- $\mathbb{Z}_8\cong\langle a:a^8=1\rangle$.
- $\mathbb{Z}_4\oplus\mathbb{Z}_2\cong\langle a,b:a^4=b^4=1,ab=ba\rangle$.
- $\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2\cong\langle a,b:a^2=b^2=c^2=1,abc=bac=acb\rangle$.
- $D_4\cong\langle a,b:a^4=b^2=(ab)^2=1\rangle$.
- $Q_8\cong\langle a,b:a^4=1,a^2=b^2,ba=a^3b\rangle$.

p为奇素数时, p^3阶群分类如下:

- $\mathbb{Z}_{p^3}\cong\left\langle a:a^{p^3}=1\right\rangle$.
- $\mathbb{Z}_{p^2}\oplus\mathbb{Z}_p\cong\left\langle a,b:a^{p^2}=b^{p^2}=1,ab=ba\right\rangle$.
- $\mathbb{Z}_p\oplus\mathbb{Z}_p\oplus\mathbb{Z}_p\cong\langle a,b:a^p=b^p=c^p=1,abc=bac=acb\rangle$.
- $\mathbb{Z}_{p^2}\rtimes\mathbb{Z}_p\cong\left\langle a,b:a^{p^2}=b^p=1,ab=ba^{1+p}\right\rangle$.
- $(\mathbb{Z}_p\times\mathbb{Z}_p)\rtimes\mathbb{Z}_p\cong\langle a^p=b^p=c^p=1,ac=ca,cb=bc,ab=bac\rangle$.

证明: 下仅考虑$p=3$时非Abel之情形.

显然G不含有p^3阶元, 反之$G\cong\mathbb{Z}_{p^3}$矛盾. 同时$|C(G)|=p$, 反之$|C(G)|=p^2$或p^3与Abel群之限定矛盾, $|C(G)|\neq1$显然成立.

若G含有p^2阶元a, 则$H:=\langle a\rangle$正规. 引理证明:

> *Lemma. 阶为p^m的群G的所有p^{m-1}阶子群均正规.*
>
> *考虑$G=\dot\cup_{r\in R}rH$与群作用$\pi:G\to S(R)$, 则$|G|/|\ker\pi|\mid|S(R)|=p!$. 显然$|\ker\pi|=p^{n-1}$, 即$G$所有$p^{n-1}$子群正规.*

记$G/H\cong\langle b\rangle\cong\mathbb{Z}_p$, 则不妨设$b^{-1}ab=a^r$. 故$a^{r^p}=b^{-p}ab^p=a$, 即$r\equiv1\mod p$.

设$r=1+kp$, $k=1,2,\dots,p-1$, k'满足$kk'-1\mid p$, 则$b^{-k'}ab^{k'}=a^{r^{k'}}=a^{1+kk'p}=a^{1+p}$. 不妨设$k'=-1$. 由于$b^p\in H$, 且$o(b)\neq p^3$, 故$o(b^p)=p$或1. 设$b^p=a^{sp}$, 则易知$(b^{-1}a^s)^p=1$, 同时

$$(b^{-1}a^s)^{-1}a(ba^s)=a^s(bab^{-1})a^s=a^{p+1}$$

将$b^{-1}a^s$视作第一小题中之b, a不变. 下证明群表现为

$$\left\langle a,b\mid a^{p^2}=b^p=1,b^{-1}ab=a^{p+1}\right\rangle$$

设自由群$F=\langle a,b\rangle$, 与满同态$\pi:G\to F$. 记

$$P=\left\langle a^{p^2}=b^p=1,b^{-1}ab=a^{p+1}\right\rangle$$

已证明$P\subset\ker\pi$. 注意到G中元素均可用a^ib^j形式表示, 其中$0\le i\le p^2-1,0\le j\le p-1$. 因此$|\ker\pi|\le|P|$, 即$\ker\pi=P$.

若G不包含p^2阶元, 不妨设$G/C(G)\cong\langle a\rangle\oplus\langle b\rangle$, $C(G)\cong\langle c\rangle$. 下证明群表现为

$$\langle a,b,c\mid a^p=b^p=c^p=1,ca=ac,cb=bc,ab=bac\rangle$$

记自由群$F=\langle a,b,c\rangle$, 满同态$\pi:F\to G$, 记

$$P=\left\langle [c,b],[c,a],[a,b]c^{-1}\right\rangle$$

已证$P\subset\ker\pi$. 注意到G中元素都可用$a^ib^jc^k$表示, 其中$1\le i,j,k\le p-1$, 故$|\ker\pi|\le|K|$, 证毕.

非Abel小阶群结构

$1-7$阶群

应当注意, 阶数最小之非Abel群为6阶. 此时有非Abel群$D_3\cong S_3$.

$8-11$阶群

8阶群为p^3阶群, 其分类及表示业已详细论证. 10阶非Abel群显然为D_5.

12阶群

12阶非Abel群为A_4, D_6, T. 生成元阶数为

群	半直积	表示
A_4	$(\mathbb{Z}_2\times\mathbb{Z}_2)\rtimes\mathbb{Z}_3$	$\left\langle a,b:a^3=b^3,a^2=b^2\right\rangle$
D_6	$\mathbb{Z}_2\rtimes\mathbb{Z}_6$	$\left\langle a,b:a^6=b^2=(ab)^2=1\right\rangle$
T	$\mathbb{Z}_3\rtimes(\mathbb{Z}_2\times\mathbb{Z}_2)$	$\left\langle a,b:a^6=1,b^2=a^3,ab=ba^5\right\rangle$

$\lvert o(1)\rvert$	$\lvert o(2)\rvert$	$\lvert o(3)\rvert$	$\lvert o(4)\rvert$	$\lvert o(6)\rvert$	$\lvert o(12)\rvert$

$\lvert o(1)\rvert$	$\lvert o(2)\rvert$	$\lvert o(3)\rvert$	$\lvert o(4)\rvert$	$\lvert o(6)\rvert$	$\lvert o(12)\rvert$
1	3	8	0	0	0
1	7	2	0	2	0
1	1	2	6	2	0

其中$\lvert o(j)\rvert := \lvert\{a \in G : o(a) = j\}\rvert$.

$13-15$阶群

仅有$D_{14} \cong \mathbb{Z}_2 \rtimes \mathbb{Z}_7$非Abel.

16阶及以上群

这是复杂的.

置换群浅谈

置换与轮换

注: 若无特殊强调, 一般略去对S_1与S_2之讨论.

相关定义

置换: 记置换$(a_1\ a_2\ \cdots\ a_n)$为映射$\sigma \in \mathrm{aut}(\Omega)$. 其中

$$\sigma : \Omega \to \Omega, w_{a_i} \mapsto w_{a_{i+1}}, \quad i \in \mathbb{Z}_n$$

变换群$S(\Omega)$为Ω中所有元素(可行)置换之集合. 诸如二面体群, 正多面体群等.

Cayley定理: $S(\Omega)$同构于某一变换群, 即置换群之某一子群.

Remark. 置换运算从右至左.

n阶置换群

n阶置换群S_n定义为集合$\{1,2,\cdots,n\}$所有置换构成之集合. 轮换$(a_1\ a_2\ \cdots\ a_n)$满足$a_i=a_j\Leftrightarrow i=j$. 相关性质如下:

1. $|S_n|=n!$.
2. $o((a_1\ a_2\ \cdots\ a_n))=n$.
3. $C_{S_n}((a_1\ a_2\ \cdots\ a_n))=\prod_{k\geq 1}(b_1^{(k)}\cdots b_{n_k}^{(k)})$, 其中$b_t^{(s)}\neq a_j$恒成立.

> *Remark. 两两不相交之轮换可交换.*

4. 共轭关系: 置τ, $\sigma=\prod_{k\geq 1}(b_1^{(k)}\cdots b_{n_k}^{(k)})$为置换, 则
$$\tau\sigma\tau^{-1}=\prod_{k\geq 1}(\tau(b_1^{(k)})\cdots\tau(b_{n_k}^{(k)}))$$
5. S_n中含有不动点之轮换占比为$\sum_{k=0}^{n}\dfrac{(-1)^k}{k!}$, 即全错排公式.

> *Remark: 一般称二阶轮换为对换.*

一般置换的表示

分解定理: $\forall\sigma\in S(\Omega)$, σ可唯一地写作不交轮换之积.

证明: 考虑轨道分解$\Omega=\dot{\cup}_\omega\langle\sigma\rangle\omega$即可. 亦得其唯一性.

置换可写作对换之积. 因为

$$(a_1\ a_2\ \cdots\ a_n)=\prod_{k=n}^{2}(a_1\ a_k)=\prod_{k=n}^{2}(1\ a_k)(1\ a_2)(1\ a_k)$$

常用恒等式:

1. $(ij)=(1i)(1j)(1i)$;
2. $(ij)(kl)=(ikl)(ijl)$;
3. $(ij)(il)=(ilj)$;
4. $(1jk)=(12k)(12j)^2$;
5. $(2jk)=(12k)^2(12j)$;
6. $(ijk)=(12i)(12k)^2(12j)(12i)^2$.

交错群

交错群A_n定义为S_n中偶置换之集合. 由于S_n中奇置换与偶置换数量相等, 故$2|A_n| = |S_n|$, 因此$A_n \lhd S_n$. 满同态

$$\delta : S_n \twoheadrightarrow \{\pm 1\}$$

是唯一的.

> *Remark: 这类保留符号之同态映射又称作字称.*

置换群共轭类的讨论

型

既有共轭关系: 置τ, $\sigma = \prod_{k\geq 1}(b_1^{(k)} \cdots b_{n_k}^{(k)})$为置换, 则

$$\tau\sigma\tau^{-1} = \prod_{k\geq 1}(\tau(b_1^{(k)}) \cdots \tau(b_{n_k}^{(k)}))$$

由不交轮换分解之唯一性可知, 两置换共轭当且仅当其不交轮换分解形式相同, 一般称型相同. 述诸定理化表达, 置换的型记录了其不交轮换并中不同长度轮换之数量. 若σ之轮换分解中长度为k之轮换数为m_k, 则记录其型为$1^{m_1}2^{m_2}\cdots k^{m_k}$, 一般可省略$1^{m_1}$项.

置换群与交错群的正规子群

$n = 1, 2$之情形

注意到共轭类数量为1的元素等价于中心元素, 故$n \neq 2$时, S_n具有平凡中心$\{1\}$. $n = 2$时有$C(S_2) = S_2$. $A_1, A_2 \cong \{e\}$. 对$n \geq 3$, S_n不可交换.

$n = 3$之情形

型	轮换
1^3	(1)
12	$(12), (23), (13)$
3	$(123), (132)$

容易列举得到S_3的非平凡正规子群仅有$A_3 \cong \mathbb{Z}_3$. 同时$\mathbb{Z}_3$为单群.

$n=4$之情形

型	轮换
1^4	(1)
1^22	$(12),(13),(14),(23),(24),(34)$
13	$(123),(124),(134),(234)$
2^2	$(12)(34),(13)(24),(14)(23)$
4	$(1234),(1243),(1324),(1342),(1423),(1432)$

易验证$\{(1),(12)(34),(13)(24),(14)(23)\}\cong K_4\lhd S_4$. 群同构定理知$\dfrac{S_4}{K_4}\cong\dfrac{S_3}{\{1\}}$.

S_4全部非平凡正规子群为A_4, K_4. 根据第二同构定理知

$$A_4/K_4\lhd S_4/K_4\Leftrightarrow A_4\lhd S_4$$

因此$K_4\lhd A_4$. A_4的非平凡正规子群仅有K_4.

$n\geq 5$之情形

下证明A_n在$n\geq 5$时为单群. 由于A_n有三轮换生成, 且三轮换显然彼此共轭, 故对任意$H\lhd A_n$仅需找出H含有三轮换即可. 先取$\sigma\in S_n$使得σ下的不动点数量$|\{i:\sigma(i)=i\}|$最大.

1. 若σ之分解仅包含轮换, 则至少有两组轮换方可使σ为偶置换. 不妨设σ中存在$(ij)(kl)$形式之两组轮换. 考虑$\tau:=(klr)$, $r\notin\{i,j,k,l\}$, 则换位子$[\tau,\sigma]=\tau\sigma\tau^{-1}\sigma^{-1}\in H$. 注意到$\sigma'$作用下之不动点较$\sigma$者少了$r$, 但多出了$i$与$j$, 这与$\sigma$之定义矛盾.
2. 若σ之轮换分解包含长度大于2之轮换, $\sigma=(ijk)$则显然, $\sigma=(ijkl)$为奇置换, 矛盾. 此外, σ移动了至少五个元素. 仿照1. 中对σ之构造即可.

综上, A_n为单群.

兹断言S_n之非平凡正规子群仅为A_n, 若不然, 令$N\lhd S_n$为S_n的非平凡正规子群. 显然$N\not\subset A_n$, 因此$NA_n=S_n$. 由第一同构定理知

$$\mathbb{Z}_2\cong NA_n/A_n\cong N/(A_n\cap N)$$

注意到$N\lhd S_n$, 故$A_n\cap N\lhd A_n\cap S_n=A_n$. 从而$A_n\cap N=\{1\}$或$A_n$, 显然都不符合.

置换群的自同构群

内自同构群$\mathrm{inn}(S_n)$

对$n\neq 2$而言, $\mathrm{inn}(S_n)\cong S_n/C(S_n)\cong S_n$. 对$n=2$, $\mathrm{inn}(S_2)\cong\{e\}$. 欲探究$\mathrm{aut}(S_n)$与$\mathrm{inn}(S_n)$之关联, 下先证明引理一则.

引理: $\tau\in\mathrm{aut}(S_n)$将对换映至对换, 若且仅若τ为内自同构.

证明: 充分性显然, 因为对任意同构映射f皆有$f(a\,b)f^{-1}=(f(a),f(b))$. 下证明其必要性:

可以观察到τ将不交对换映至不交对换, 将相交对换映射至相交对换, 亦将两两相交的三组对换映至两两相交的三组对换. 今设$\tau((ij)(il))=\tau((ilj))=(i'l'j')$, 则由$\tau((ij)(ir))=(i''r''j'')$及$|\{i'',r'',j''\}\cap\{i',l',j'\}|=2$知$\tau$将$(ij)$映至的像$(\phi(i)\phi(j))$. 同理考虑$\tau((is)(il))$知$\tau$将$(il)$映至的像$(\phi(i)\phi(l))$, 从而求出$\phi(i)$. 如此递推可知$\tau:(a,b)\mapsto(\phi(a),\phi(b))$, 因此$\tau=f_\phi, f_\phi(\sigma)=\phi\sigma\phi^{-1}$为内自同构. 必要性证毕.

记$T_k^{(n)}$由S_n中所有由k组不交对换组成的置换组成. 因此$\mathrm{aut}(S_n)=\mathrm{inn}(S_n)$当且仅当$|T_k^{(n)}|=|T_1^{(n)}|\Leftrightarrow k=1$. 不幸的是$|T_3^{(6)}|=|T_1^{(6)}|=15$恰为唯一的异类.

一般地, $|T_k^{(n)}|=\dfrac{\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2k+2}{2}}{k!}=\dfrac{n!}{2^k k!(n-2k)!}$, $|T_1^{(n)}|=\dfrac{n(n-1)}{2}$.

$$|T_k^{(n)}|/|T_1^{(n)}|=\frac{(n-2)\cdots(n-2k+1)}{2^{k-1}k!}$$

其中$k\leq\dfrac{n}{2}$. $n\leq 6$时逐项验证知$(k,n)=(3,6)$为有价值之1解. 当$n=7,8$时,分子含有5因子而分母不含之, 故比值非1. $n\geq 9$时,

$$|T_k^{(n)}|/|T_1^{(n)}|=\frac{(n-2)\cdots(n-2k+1)}{2^{k-1}k!}=$$
$$\frac{n-3}{k}\cdot\frac{n-2}{2(k-1)}\cdot\frac{n-4}{2(k-2)}\cdots\frac{n-k-1}{2}\cdot(n-k-2)!>1$$

故$n\neq 2,6$时, 有

$$\mathrm{aut}(S_n)=\mathrm{inn}(S_n)\cong S_n\cong\mathrm{aut}(A_n)=\mathrm{inn}(A_n)$$

S_6实则存在外自同构, 且$[\mathrm{aut}(S_6):\mathrm{inn}(S_6)]=2$, 今以篇幅故暂不展示. 外自同构之展现方式诸多. 图论角度上, 构造双射$GQ(2,2)\xrightarrow{\sim}K_6$即可; 代数角度上, 考虑$PGL_2(\mathbb{F}_5)\curvearrowright P^1(\mathbb{F}_5)$即可.

循环群初探

循环群定义及性质

循环群为单一元素生成之群, 其中生成元之阶数为群之阶数, 即$A := \langle a : a^n = 1 \rangle$.

> *Remark. 某一元阶数有限之循环群即有限循环群, 反之为无限循环群.*

循环群可交换. 一般地, 有限循环群同构于$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, 其中$n$为群之阶; 无限循环群同构于$\mathbb{Z}$.

$\mathbb{Z}_n$之子群同构于$\mathbb{Z}_m$, 其中$m \mid n$. 由Abel性之子群一定正规. 因此

$$\mathbb{Z}_n \cong \prod_{i=1}^{n} \mathbb{Z}_{p_i}^{r_i}, \quad n = \prod_{i=1}^{n} {p_i}^{r_i}$$

> *Remark. 素数阶群一定为循环群.*

群循环之充要条件

Prop. 有限子群之阶数两两不同若且仅若群循环.

证明: (必要性) 由于$d(\mid n)$阶元之数量为$\dfrac{n}{\gcd(n,d)}$, 则生成元之数量为$\pi(n) + 1 \neq 0$.

Prop. 有限子群每一子群均为G^m形式若且仅若群循环. (证明同上)

欧拉函数及初等数论定理

欧拉函数$\varphi(n)$定义为$|\{x \in \mathbb{Z}_n : \gcd(x,n) = 1\}|$, 亦即后文所述之$|\mathbb{Z}_n^*|$. 一般地有如下结论:

1. $n = \sum_{m|n} \varphi(n)$, 即将$\mathbb{Z}_n$中元素依阶数分类以计数.
2. (Fermat小定理) $a^{\varphi(n)} \equiv 1 \mod n$, 若$\gcd(a,n) = 1$.
   证明: 视$a \in \mathbb{Z}_n^* \cong \mathrm{aut}(\mathbb{Z}_n)$为一自同构, 则$a^{\varphi(n)}$为恒等映射.
3. (Wilson定理) $(n-1)! \equiv -1 \mod n$.
   证明: 参考一般初等代数书籍即可.
4. 未完待续...

循环群的自同构群

无限阶情形

$\mathbb{Z}$之生成元仅$\{\pm 1\}$尔. 故$\mathbf{aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

有限阶情形

注意到$\forall f \in \mathrm{aut}\ (\mathbb{Z}_n)$都将$\mathbb{Z}_n$中生成元映射至生成元, 同时$\langle f(1) \rangle = \mathbb{Z}_n$, 因此任一自同构映射可由$f(1)$直接确定. 映射之符合无非$\mathrm{aut}\ (\mathbb{Z}_n)$中元素之乘积, 故$\mathrm{aut}\ (\mathbb{Z}_n)$同构于$\{x : \gcd(x, n) = 1\}$于乘法下之群, 记作$\mathbb{Z}_n^*$. 同构关系

$$(\mathrm{aut}\ (\mathbb{Z}_n), +) \cong (\mathbb{Z}_n^*, \cdot)$$

同记$n = \prod_{i=1}^{n} {p_i}^{r_i}$, 则由中国剩余定理知$\mathbb{Z}_n^* \cong \oplus_{i=1}^{n} \mathbb{Z}_{p_i^{r_1}}^*$. 下考虑$\mathbb{Z}_{p^r}^*$之结构即可.

p为奇素数时, 下证明$(\langle 2 \rangle, \cdot) = \mathbb{Z}_{p^k}^*$, 即2为$\mathbb{Z}_{p^k}^*$之原根. 由Fermat小定理知2为$\mathbb{Z}_p^*$之原根, 即$p \mid 2^{p-1} - 1$. 同样可证${p^{n-1}} \mid (2^{p-1})^{p^{n-2}} - 1$与$p^n \mid (g^{p-1})^{2^{n-1}} - 1$, 因此2为原根. 因此$\mathbb{Z}_{p^k}^* \cong \mathbb{Z}_{\varphi(p^k)}$.

> *Remark. 一般地, $\mathbb{Z}_{p^k}^*$之原根数量为$\varphi(\varphi(p^k)) = \varphi(p^{k-1}(p-1))$.*

$p = 2$之情形如下. 首先$\mathbb{Z}_2^* \cong \mathbb{Z}_1$, $\mathbb{Z}_4^* \cong \mathbb{Z}_2$是显然的. 对一般的$\mathbb{Z}_{4 \cdot 2^k}^*$, 考虑正规子群$\{\pm 1\} \lhd \mathbb{Z}_{4 \cdot 2^k}^*$及$|(\langle 3 \rangle, \cdot)| = 2^k$知$\mathbb{Z}_{4 \cdot 2^k}^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^k}$.

> *Remark. (Gauss) $n = 1, 2, 4, p^k, 2p^k$ 时, $\mathbb{Z}_n^*$ 为循环群.*

小节末列举典例一则: $\mathbb{Z}_{360}^* \cong \mathbb{Z}_{2^3}^* \oplus \mathbb{Z}_{3^2}^* \oplus \mathbb{Z}_5^* \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_4$.

半直积与二面体群初探

二面体群之定义

定义: 正二面体群D_n即正多边形于三维空间中以所有$2\pi/n$度旋转与翻转所生成之变换群.

> *Remark: D_n阶数为$2n$. $D_n = \{\tau^i \sigma^j : 1 \le i \le 2, 1 \le j \le n\}$.*

等价定义: 正二面体群D_n为正多边形顶点至自身的保距同构群.

今记旋转变换为σ, 翻转为τ, 则$o(\sigma)=n$, $o(\tau)=2$, $o(\sigma\tau)=o(\tau\sigma)=2$. 记顶点为$\{1,\cdots,n\}$, 则$\sigma=(12\cdots n)$, $\tau=(2n)(3(n-1))\cdots$.

半直积刻画

半直积定义

若$N\lhd G$而$(G/N)\times N\ncong G$, 由于$(G/N)\times N$与G元素等同但不具备同态关系, 下定义半直积.

群的半直积定义如下: 设H, N为群, $\alpha:H\to \mathrm{aut}(N)$为同态. 定义$N\rtimes_\alpha H$为群$H$与$N$于映射$\alpha$下的半直积, 满足:

1. 群$N\rtimes_\alpha H$于形式上等于$N\times H:=\{(n,h):n\in N,h\in H\}$.
2. 二元运算为$(n_1,h_1)(n_2,h_2):=(n_1\alpha(h_1)(n_2),h_1h_2)$.

群$N\rtimes_\alpha H$之幺元为$(1,1)$, 逆元$(n,h)^{-1}=(\alpha(h^{-1})(n^{-1}),h^{-1})$.

半直积诸性态之诠释

注意到$N\lhd N\rtimes H$, 半直积实则$N\lhd G$之等价形式. 通常考虑$hn=(hnh^{-1})n$, 此时$\alpha:H\ni h\mapsto f_h$; $f_h:N\to N, n\to hnh^{-1}$将群中元素映射至自然的自同构.

若$\mu:N\rtimes H\to G,(n,h)\mapsto nh$为同构, 则称$G$为$N$与$H$的半直积. 此时$NH=G$, $N\cap H=\{1\}$.

> *Remark: 若$N\cap H=\{1\}$且$N\subset N_G(H)$, 则$nh=hn$及$\ker\alpha=N$是自明的.*

二面体群之半直积刻画

$D_n\cong\mathbb{Z}_2\rtimes_\alpha\mathbb{Z}_n$, 其中对$\mathbb{Z}_2$中非平凡元$\tau$定义$\alpha(\sigma):n\to -\sigma$即可.

特别地, n为偶数时$\{1,\sigma^{n/2}\}\lhd D_n$. 有$D_n\cong D_{n/2}\times\mathbb{Z}_2$.

二面体群之自同构群

一般地, $\mathrm{inn}(D_n) \cong D_n/C(D_n)$. 考虑$\tau\sigma^k = \sigma^k\tau$知当$n$为奇数时有$C(D_n) = \{1\}$, n为偶数时有$C(D_n) = \{1, \sigma^{n/2}\}$. 下证明$\mathrm{aut}(D_n) \cong \mathrm{hol}(\mathbb{Z}_n) := \mathbb{Z}_n \rtimes \mathrm{aut}(\mathbb{Z}_n)$.

考虑

$$\pi : \mathbb{Z}_n \to \mathrm{aut}(D_n), i \mapsto f_i; \quad f_i : \tau \mapsto \sigma^i\tau, \sigma \mapsto \sigma$$

及形式上等同于$\mathrm{aut}(\mathbb{Z}_n)$之映射集

$$\pi^* : \mathbb{Z}_n^* \to \mathrm{aut}(D_n), i \mapsto g_i, \quad g_j : \tau \mapsto \tau, \sigma \mapsto \sigma^j$$

注意到$\pi(\mathbb{Z}_n) \lhd \mathrm{aut}(D_n)$, 故

$$\mathrm{aut}(D_n) \cong \mathrm{hol}(\mathbb{Z}_n) := \mathbb{Z}_n \rtimes \mathrm{aut}(\mathbb{Z}_n)$$

其阶数为$n\varphi(n)$.

群作用与计数原理

作用

半群在集合上之作用

作用$f : M \times \Omega \to \Omega$为$M \times \Omega$至$\Omega$之映射, 满足$f(g, f(g', x)) = f(gg', x)$, 即结合律.

群在集合上之作用

半群在集合上之作用之定义延拓至群 (添加单位元与逆元) 即可. 特别地, 作用$\rho : G \times \Omega \to \Omega$之集合即$\hom(G, S(\Omega))$.

若$|\ker\rho| = 1$, 则作用忠实. 应注意到$\ker\rho \lhd G$.

三类典型作用

左正则作用

$f: G \to S(G)$满足$f(g) = f_g; f_g: G \to G, h \mapsto gh.$

f为单射, 因而忠实.

左诱导作用

设G在子群H导出左陪集R. $f: G \to S(R)$满足$f(g) = f_g; f_g: G \to G, h \mapsto gh.$

$\ker f = \cap_{x \in G}: xHx^{-1}$, 即$H$中所包含之$G$中最大正规子群.

左共轭作用

设$A \subset G$. 令$\Omega := \{xAx^{-1}\}$. $f: G \to S(\Omega)$, $f(g) = f_g; f_g: xAx^{-1} \mapsto gxA(gx)^{-1}$.

$\ker f = \cap_{x \in G} xN_G(A)x^{-1}$为包含$A$正规化子之最大正规子群.

轨道公式

G作用于Ω, 称$Gx := \{gx: x \in \Omega\}$为$x$的$G-$轨道. 称轨道可迁, 若且仅若$\Omega$轨道唯一, 即$\forall x \in \Omega, Gx = \Omega$.

G_x为G在Ω下的稳定化子, 即$G_x: \{g \in G: gx = x\} \leq G$.

$|Gx| = [G: G_x] = \dfrac{|G|}{|G_x|}$, Gx可迁当且仅当$|\Omega| = \dfrac{|G|}{|G_x|}$对任意$x \in G$均成立.

Burnside引理与Polya计数定理

置$F(g) \subset \Omega$为$\{x: gx = x\}$. 则轨道条数

$$t = \frac{1}{|G|} \sum_{g \in G} F(g)$$

证明: 考虑$\Gamma: \{(g, x): gx = x\}$, 则$|\Gamma| = \sum_{g \in G} |F(g)|$. 另一方面

$$|\Gamma| = \sum_{x\in\Omega}|G_x| = \sum_{x\in\Omega}\frac{|G|}{|Gx|} = \sum_{i=1}^{t}\sum_{x\in Gx_i}\frac{|G|}{|Gx|}$$
$$= \sum_{i=1}^{t}|Gx_i|\frac{|G|}{|Gx_i|} = t|G|$$

明所欲证.

Polya计数定理可视作Burnside引理之一般推广. 对于含n个对象的置换群G，用t种颜色着色的不同方案数为：

$$l = \frac{1}{|G|}\sum_{g\in G}t^{c(a_g)}$$

其中$c(a_g)$为置换a_g型之指数和.

Polya计数定理之母函数形式另有高用, 兹不予赘述. 下以两则计数问题结尾:

1. 以氟, 氯, 溴, 碘四种卤素取代苯环, 试问卤代苯总数?

   解: 考虑二面体群D_6. 旋转σ^i之型为$\frac{n}{\gcd(i,6)}^{\gcd(i,6)}$, $n/2$个奇数翻转$\sigma^{2k+1}\tau$之型为$2^{n/2}$, $n/2$个偶数翻转$\sigma^{2k}\tau$之型为$1^2 2^{n/2-1}$. 今视氢, 氟, 氯, 溴, 碘为五色, 则由Polya计数定理知

   $$l = \frac{1}{12}\left(\sum_{i=1}^{6}5^{\gcd(i,6)} + \frac{6}{2}(5^3+5^4)\right) = 1505$$

   故卤代苯总数为1504.

2. n颗珠子与r中颜色串为项链, 则不同项链之数量为

   $$t = \frac{1}{2n}\sum_{i=1}^{n}r^{\gcd(n,i)} + \begin{cases}\frac{1}{2}r^{\frac{n+1}{2}}, & n\text{为奇数},\\ \frac{1}{4}r^{\frac{n}{2}}(1+r), & n\text{为偶数}.\end{cases}$$

Sylow定理

叙述

注: 统一记$N(q)$为q阶子群之数量. Sylow定理证法纷呈, 今以篇幅故从略.

Sylow I定理

若有限群G之阶数含有p^r因子, p为素数, r为正整数, 则$N(p^r) \equiv 1 \mod p$.

> *Remark: G有素数阶子群. Sylow I定理实则Cauchy定理之加强.*

Sylow II定理

给定有限群阶数之因子分解$n = |G| = \prod_i p_i^{r_i}$, 诸$p_i^{r_i}$阶群称作$G$的Sylow p_i-子群. G的Sylow p_i-子群两两共轭.

今考虑某一Sylow p_i-子群N_i, 则N_i之共轭群数目为$[G : N_G(N_i)]$. 因此$N(N_i) \mid n$. 结合Sylow I定理可知

$$N(p_i^{r_i}) \equiv 1 \mod p_i, \quad N(p_i^{r^i}) \mid \prod_{k \neq i} p_k^{r_k}$$

Sylow III定理

有限群之任一p^r阶群均含于某一Sylow p-子群.

p群与类p群

p群

记一切阶数为p^r之群为p群, 其中p为素数, r为正整数.

p群之中心与正规子群

p群无非平凡中心. 由类数公式

$$|G| = \sum_{a \in R} \frac{|G|}{|C_G(a)|} = |C(G)| + \sum_{a \in R \setminus C(G)} \frac{|G|}{|C_G(a)|}$$

知$|C(G)| \equiv 0 \mod p$.

p^r阶群G有唯一 (因此正规) 的p^{r-1}阶子群G. 考虑G在R上的左诱导作用即知$\dfrac{|G|}{|\ker \pi|} \mid |S_p|$.

因此$\ker \pi = p^{r-1}$. 结合Sylow II定理, 明所欲证.

以另一角度视之, 可先断言p群G之真子群H满足$H < N_G(H)$, 因而$|G|/p$阶群正规.

证明: 若$H \lhd G$则显然. 当$H \not\lhd G$时考虑H在$[H]$上的共轭作用, 这里$|[H]| = [G : N_G(H)]$为p的倍数. 由于$\{H\}$为其中一条长度为1的轨道, 因此至少另有$p-1$条长度为1的轨道方可使得$p \mid |[H]|$. 不妨设$\{gHg^{-1}\}$为另一条长度为1之轨道, 因此对任意$a \in H$均有$agHg^{-1}a^{-1} = gHg^{-1}$, 从而$g^{-1}ag \in N_G(H)$, 进而$g^{-1}Hg \subset N_G(H)$. 由此可得$H < N_G(H)$.

类p群

类p群即阶数为$p^k q^m r^l$等简单形式之群. 下分析几类特殊的类p群.

pq阶群结构

pq阶群非单群. 不妨设$p > q$, $N(p) = kp + 1 \mid q$, 因此p群唯一 (故正规). 下讨论pq阶群之结构.

1. $q \nmid p-1$时, 由$N(q) = kq + 1 \mid p$知$N(q) = N(p) = 1$. 显然$G \cong \mathbb{Z}_p \oplus \mathbb{Z}_q$是循环群.
2. $q \mid p-1$时, $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_q$, 即对任意$\mathbb{Z}_p$与$\mathbb{Z}_q$中的一组生成元$(a, b)$, 总有$b^{-1}ab = a^k$. 同时容易推得$b^{-l}ab^l = a^{k^l}$.

p^2q阶群及非单群

先证明p^2q阶群非单群.

1. $p > q$时, $N(p) = kp^2 + 1 \mid q$, 因此p^2阶群唯一 (故正规).
2. $p < q$时, $N(q) = kq + 1 \mid p^2$. 若$k = 0$则显然q阶群正规. 若$k \neq 0$, 则必有$kq + 1 = p^2$. 注意到p^2个q阶群占用了$p^2(q-1)$个非平凡元, 剩下的p^2个元组成唯一的p群, 因此正规.

再证明p^2q^2阶群非单群, 其中$pq = 6$之情形另考虑.

1. 不妨设$p < q$, 则$N(q^2) = kq + 1 \mid p^2$, 即$kq \mid (p-1)(p+1)$. 显然在$p \geq 3$时$k = 0$, 即q^2阶群为单群.
2. $n = 36$时有$N(9) = 3k + 1 \mod 4$. 下仅需考虑$k = 1$之情形. 考虑Ω为所有9阶子群之集合, 共轭作用$\rho : G \to S(\Omega)$满足$\dfrac{|G|}{|\ker \rho|} \mid 4!$. 若$G$为单群则$\ker \rho$平凡, 显然$|\ker \rho| = 1$或$36$都是不可能的.

> *Remark: 通过如是群作用之方法可解决若干$p^a q^b$型类p群之单群问题。*

Burnside定理阐明了$p^a q^b$阶群非单群.

pqr阶群非单群

下仅需讨论p, q, r两两不等之情形, 不妨设$p \le q \le r$. 反之设群为单群，记其Sylow p, q, r子群之数量分别为l, m, n, 则

$$\begin{gathered} n \mid pq, \quad m \mid pr, \quad l \mid qr \\ n \equiv 1 \mod r, \qquad m \equiv 1 \mod q, \qquad l \equiv 1 \mod p \end{gathered}$$

最小可能的非1解为$n = pq$, $m = r$, $l = q$. 因此

$$\begin{aligned} |G| &\ge pq(r-1) + r(q-1) + q(p-1) + 1 \\ &= pqr + (r-1)(q-1) > |G| \end{aligned}$$

矛盾. 故pqr阶群非单群.

Mersenne素数与群

Mersenne素数即形如$p = 2^n - 1$之素数, 此时$p(p+1)$阶群有非平凡的正规Sylow子群, 即存在p阶或2^n阶子群正规.

证明: $N(p) = kp + 1 \mid 2^n$, 若$k = 0$则显然, $k = 1$即存在2^n个Sylow p-子群. 注意到这2^n个p阶群占用了$2^n(p-1)$个非平凡元, 剩余的2^n个元一定组成Sylow 2-子群.

阶数最小的非Abel单群

已知A_5为阶为60的非Abel单群, 下通过逐一排除法证明所欲求者必为60阶. 由Burnside定理知仅30阶与42阶群可能非单; 我们已知阶数为$2(2n+1)$之群含$2n+1$阶之正规子群, 因此最小之非Abel单群必不可能小于60阶.

若无Burnside定理之结论, 既证阶为$2(2k+1)$, p^m, pq, p^2q, p^2q^2, pqr之群非单群, 下仅需考虑阶数为24, 48, 40, 56之群.

1. 56阶群非单群. 注意到$N(7) = 7k + 1 \mid 8$. 若$k = 0$则含正规子群; $k = 1$时, 则8个7阶群共计占据48个非平凡元, 剩余8个元构成唯一的8阶群, 从而为正规子群.
2. 40阶群必含唯一的5阶子群, 因为$N(5) = 5k + 1 \mid 8$, 从而$k = 0$.
3. 24阶群非单. 注意到$N(3) = 3k + 1 \mid 8$, $k = 0$显然, $k = 1$时$N(3) = 4$. 记Ω为三阶子群之集合, 考虑$\rho : G \to S(\Omega)$为共轭作用. 由于$\ker \rho \ne G$, G为单群时必有$\ker \rho = \{e\}$, 此时$G \cong S_4$非单, 矛盾.
4. 48阶群非单. 同样考虑$N(3) = 3k + 1 \mid 8$即可.

60阶非Abel单群一定为A_5形式. 暂时不给出证明.

群作用与单群分析习题

120阶群非单群

证明: 不妨设G为120阶单群, 考虑$N(5)=5k+1\mid 24$. 当$k=0$时显然非单群. $k=1$时$N(5)=6$, 记所有Sylow 5-子群组成集合Ω. 考虑G在Ω上的共轭作用

$$\rho: G\to S(\Omega), g\mapsto f_g; f_g:\Omega\to\Omega, \omega\to g\omega g^{-1}$$

因此$\dfrac{|G|}{|\ker\rho|}\mid 6!$. 由于$G$为单群且$\ker\rho\neq G$, 因此$G\leq S_6$. 下考虑$G\cap A_6$. 记$H:=G\cap A_6\subset G$.

1. 若G不含于A_6, 则G中偶置换构成指数为2的正规子群, 矛盾.
2. 若G含于A_6, 则考虑A_6在陪集A_6/G上的左诱导作用. 因此存在同态

   $$\pi: A_6\to S_3$$

   $\ker\pi\lhd A_6$矛盾.

于是有如下定理:

单群真子群的阶数规律

$n\geq 5$时, 单群G存在子群H满足$[G:H]=n$. 则考虑G在陪集G/H上的左诱导作用, 有满同态

$$\rho: G\to S_n$$

若G不包含于A_n, 则G中有奇置换, 因此偶置换构成指数为2的子群, 故正规, 矛盾.

因此G可嵌入A_n, 即G同构于A_n中一子群. 不妨设$G\leq A_n$.

考虑陪集划分A_n/G, 及A_n在A_n/G上的左诱导作用

$$\varphi: A_n\to S_{[A_n:G]}$$

由于$\ker\varphi\neq A_n$, 故$\ker\varphi=1$. 因此$[A_n:G]\geq n$.

$GL(n,\mathbb{C})$不含指数有限的真子群

证明: 若含有, 则不妨设$\exists H\leq GL(n,\mathbb{C}):=G$使得$[G:H]=m$. 考虑$G$在陪集$G/H$上的左诱导作用$\rho: G\to S_m$. 显然$[G:\ker\rho]$有限, 记$[G:\ker\rho]=s$. 注意到$\forall B\in G, B^s\in\ker\rho$. 若证明$\forall A\in GL(n,\mathbb{C}), \exists B\in GL(n,\mathbb{C})$使得$B^s=A$, 即有$G=\ker\rho$矛盾. 证明如下:

考虑$A=PJP^{-1}$为相似分解, 其中J为Jordan型. 由于$J=D+N$ (D为J之对角元素)及$DN=ND$, 故

$$K:=\sum_{t=0}^{\infty}\binom{-s}{t}N^tD^{-s-t}=\sum_{t=0}^{n}\binom{-s}{t}N^tD^{-s-t}$$

满足$K^s=J$. 从而$B=PKP^{-1}$即所欲求.

确定有3个共轭类的有限群

证明: 由共轭类公式知$|G|=|C(G)|+\sum_{a\in R\setminus C(G)}\dfrac{|G|}{|C_G(a)|}$. 由于$|[e]|=1$, 下设每一共轭等价类所含元素为$a,b$ 因此$\dfrac{1}{|G|}+\dfrac{1}{|G|/a}+\dfrac{1}{|G|/b}=1$. 分母整数解: $(2,3,6),(2,4,4),(3,3,3)$.

1. 3阶群仅$\mathbb{Z}_3$者, 据Abel性知其共轭类有三.
2. 4阶群皆Abel, 共轭类有四, 舍去.
3. 6阶群仅$\mathbb{Z}_6$与S_3, 显然设去前者. 后者共轭类为$\{e\}$, 对换, 三轮换三者.

455阶群为循环群

证明: 首先有$455=5\cdot 7\cdot 13$. $N(7)=7k+1\mid 65$, 故$N(7)=1$. 同理$N(13)=1$. 不妨设$\langle x\rangle$生成某一Sylow -5群, $\langle y\rangle$生成某一Sylow -7群, $\langle z\rangle$生成某一Sylow -13群, 则$|\langle x\rangle\langle y\rangle|=\dfrac{|\langle x\rangle|\cdot|\langle y\rangle|}{|\langle x\rangle\cap\langle y\rangle|}=35$, 同理$|\langle x\rangle\langle z\rangle|=65$, $|\langle y\rangle\langle z\rangle|=91$. 注意到35阶群, 65阶群, 91阶群皆为Abel群 (因为$p\nmid q-1$), 故x,y,z可交换, 从而455阶群循环.

计算$\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^2}$中$p^2$阶子群个数.

证明: 下分别考虑$\mathbb{Z}_p\oplus\mathbb{Z}_p$, $\mathbb{Z}_{p^2}$型子群数量. 下记$\mathbb{Z}_{p^3}\oplus\mathbb{Z}_{p^2}=\langle x\rangle\langle y\rangle$. 由于所有$p$阶元数量为$p^2-1$, 因此$\mathbb{Z}_p\oplus\mathbb{Z}_p$型子群数量为1. 由于$p^2$阶元数量为$p^2(p^2-1)$, 故$\mathbb{Z}_{p^2}$阶循环群数量为$\dfrac{p^2(p^2-1)}{p^2-p}=p^2+p$. 故$p^2$阶子群之数量为$p^2+p+1$.

特别地, 可以计算$\oplus_{k=1}^n\mathbb{Z}_p$上$p^r$阶子群数量. 首先需明确

$$\mathrm{aut}(\oplus_{k=1}^n\mathbb{Z}_p)=|GL(n,\mathbb{F}_p)|=\prod_{i=1}^{n}(p^n-p^{i-1})$$

即所有满秩线性变换之数量. 因此$\oplus_{k=1}^n\mathbb{Z}_p$上$p^r$阶子群数量即$r$维子空间之数量, 亦即

$$\frac{|GL(n,\mathbb{F}_p)/M_n^r(\mathbb{F}_p)|}{|GL(r,\mathbb{F}_p)|},\quad M_n^r(\mathbb{F}_p):=\left\{\begin{pmatrix}A&0\\*&0\end{pmatrix}:A\in GL(n,\mathbb{F}_p)\right\}$$

经计算得

$$\frac{|GL(n,\mathbb{F}_p)/M_n^r(\mathbb{F}_p)|}{|GL(r,\mathbb{F}_p)|}=\frac{\prod_{i=1}^{n}(p^n-p^{i-1})}{\prod_{i=1}^{r}(p^n-p^{i-1})\cdot\prod_{i=1}^{r}(p^r-p^{i-1})}=\frac{(p^n-1)\cdots(p^{n-r+1}-1)}{(p^r-1)\cdots(p-1)}$$

上式又可视作$\binom{n}{r}_p=\frac{(p^n-1)\cdots(p^{n-r+1}-1)}{(p^r-1)\cdots(p-1)}$. 此类组合数称作Gauss组合数.

有限Abel群一瞥

结构与同构关系

同构定理

可验证, 有限Abel群是其Sylow子群之直和. 下给出一般有限阶Abel群之直和分解, 其自同构群亦然, i.e.

$$\mathrm{aut}(\oplus G_{p_i})\cong\oplus\mathrm{aut}(G_{p_i})$$

一般p群之自同构群结构复杂, 在此考虑特殊的一类: $\oplus_{i=1}^{n}\mathbb{Z}_p$.

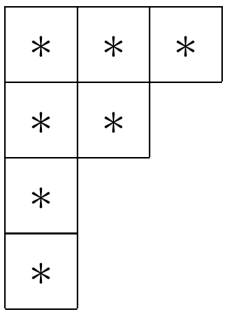
$\mathrm{aut}(\oplus_{i=1}^{n}\mathbb{Z}_p)\cong GL_n(\mathbb{F}_p)$, 是因为自同构等价于线性无关基之变换.

> *Remark:* $|GL_n(\mathbb{F}_p)|=\prod_{k=0}^{n-1}(p^n-p^k)$.

分划与Young图

若存在正整数n及正整数组$(n_1,\cdots,n_k)$使得$n=\sum_{i=1}^{k}n_i$, 则称此划分方式为n的一个分划. 称两个分划相等, 若且仅若其对应数组在计入重数而不计次序之情形下相等.

表示论或物理学中常用Young图分析划分. 正则Young图 (英式, 区别于反序的法式) 为一列左对齐的对应分划所称单元数量递减的矩形串. 如划分$[\lambda]=[3,2,1,1]$对应如下Young图, 直接记作$[\lambda]$. 不同的正则Young图数即$p(n)$.



若将1至n填入Young图使得两两不同, 则得Young表. 若Young表是向下及向右严格递减的, 则称为正则Young表, 而钩形Young表可导出正则Young表的数$d_{[\lambda]}$. 将每单元及其下与其右方格数总和填入, 得钩形Young表, 记作$Y_h^{[\lambda]}$.

6	3	1
4	1	
2		
1		

可以证明: $\frac{n!}{d_{[\lambda]}}$为$Y_h^{[\lambda]}$中左右数之乘积. 此外, Boerner证明了$\sum_{[\lambda]} d_{[\lambda]}^2 = (n!)^2$.

Young之运算与应用甚广, 此处不拟细述.

有限Abel依同构分类

考虑划分Ω与p^n阶群之同构类Γ. 由于$G \cong \mathbb{Z}_p \times G/\mathbb{Z}_p$, 据循环分解知有同构

$$\psi : \Omega \to \Gamma, \{n_i\}_{i=1}^k \mapsto \oplus_{i=1}^k \mathbb{Z}_{n_i}$$

取$p(n)$为n之划分数量, 则$\prod_{i=1}^k p_k^{m_k}$阶Abel群同构类之数量为$\prod_{i=1}^k p(m)$.

一般地, 考虑n的标准素分解$n = \prod_{i=1}^t p_i^{m_i}$, 则对每个$m_i$均有划分$[r_{i1}, \dots, r_{il_1}]$使得

$$G \cong \oplus_{i=1}^t \oplus_{j=1}^{l_i} \mathbb{Z}_{p_i^{r_{ij}}}$$

记所有的$p_i^{r_ij}$构成初等因子组. 视$\{d_{ij}\}_{j=1}^{l_i}$为$\{r_{ij}\}_{j=1}^{l_i}$的降序排列. 记$d_i = \prod_i d_{ij}$, 这里i取遍所有有定义之值, 则称$\{d_k\}_{k=1}^{\sup_i l_i}$为一组不变因子组. 特别地, $\prod_k d_k = n$, 且$d_{i+1} \mid d_i$. 两个Abel群同构若且仅若其不变因子组相同.

如$G \cong (\mathbb{Z}_2 \oplus \mathbb{Z}_8) \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9)$中, 初等因子组为$(2, 8, 3, 3, 9)$, 不变因子组为$(72, 6, 3)$.

Lagrange逆定理

Lagrange定理表述了子群阶数应整除原群阶数, 其逆定理则说明相应子群之存在性, 即$\forall h, h \mid |G|$, 存在$H \leq G$使得$|H| \mid |G|$. 考虑Abel群之结构定理, 及p^n阶群存在p^r阶子群($r \leq n$), 不难作出所有的h阶子群.

周期性与挠子群

对任意选定的n, 对Abel群定义$t_n(G):\{a\in G:a^n=1\}$, $t_n(G)$即挠子群. 素挠子群可视为挠子群之延拓, 定义如下:

$$G_{(p)}:=\{a\in G:a^{p^n}=1\}$$

可见$G_{(p)}$与$t_n(G)$均为正规子群. 对有限阶循环群, $t_m(\mathbb{Z}_n)\times\mathbb{Z}_{n/\gcd(m,n)}\cong\mathbb{Z}_n$. 挠子群给出了一类提取$\mathbb{Q}$子群之方式, 如下所示

$$(\mathbb{Q}/\mathbb{Z})_{(p)}=(\cup_{k=0}^{\infty}\mathbb{Z}_{1/p^k})/\mathbb{Z}$$

Abel群是无挠的若且仅若每一非平凡元素有无穷阶数.

先引入exponent. 群的exponent指所含元素阶数之最小公倍数, 即

$$\exp(G):=\mathrm{lcm}(\{o(a):a\in G\})$$

对Abel群即$\min(\{n\in\mathbb{N}:a^n=1,\forall a\in G\})$.

$\exp(G)=|G|$若且仅若G为循环群.

> *Remark: 素数定理*$\exp(n)\sim\mathrm{lcm}(1,\cdots,n)$*与公式类似, 因而*
>
> $$|(\langle k^{-1}:k=1,2,\cdots,n\rangle,+)/\mathbb{Z}|\approx e^n$$

群之分合

群之分解与扩张

直积分解

若群G能同构于若干子群之直积, i.e. $G\cong G_1\times G_2\times\cdots\times G_k$, 其中乘法运算是自然继承的. 由定义, 我们首先要求$G_i\lhd G$. 以下给出直积分解之等价叙述:

1. G中任意元可唯一地写作$g_1\cdots g_k$之形式, 其中$g_i\in G_i$.
2. $G=G_1\cdots G_k$, 且1之表示方法唯一.
3. $G=G_1\cdots G_k$, $(G_1\cdots G_i)\cap G_{i+1}\equiv\{1\}$.

> *Remark: 其中蕴含了*$G_i\cap G_j=\{1\}$, G_i*与*G_j*间元素可对易等诸多性质.*

$G \cong G_1 \times \cdots G_k$蕴含了同构于$G_i$的诸$H_i \lhd G$之存在性.

> *Remark.* $G \cong G_1 \times \cdots \times G_k$未必蕴含$G = \prod_{i=1}^k G_i$. 例如$K_4$同构于某二阶正规子群与自身之直积.

> *Remark.* $G \cong G_1 \times \cdots \times G_k$未必说明$G$之子群(或正规子群)可由诸$G_i$之子群(或正规子群)之直积表示. 同样以$K_4$为例即可导出矛盾.

G可交换若且仅若诸G_i可交换, 此时直积又作直和, i.e. $G = \oplus_{i=1}^k G_i$.

正合列

考虑同态

$$\cdots \overset{f_0}{\to} G_1 \overset{f_1}{\to} G_2 \overset{f_2}{\to} \cdots \overset{f_i}{\to} G_{i+1} \cdots$$

长度有限或无限. 若对任意i皆有$\ker f_{i+1} = \operatorname{im} f_i$, 则称链正合. 有常用之恒同整合列

$$1 \longhookrightarrow \ker \varphi \overset{\text{嵌入}}{\longhookrightarrow} G \overset{\varphi}{\twoheadrightarrow} \varphi(G) \twoheadrightarrow 1$$

群扩张

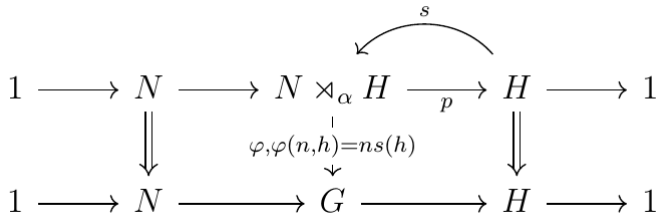
群扩张之一般形式为

$$1 \longrightarrow N \longrightarrow G \xrightarrow{p} H \longrightarrow 1$$

称群扩张(上下两行)等价若且仅若φ为同构. 同态$s \in \hom(H, G)$若满足$ps|_H$为恒同映射, 则称s为扩张之分裂.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \xrightarrow{p} & H & \longrightarrow & 1 \\ & & \Vert & & \downarrow{\scriptstyle \varphi} & & \Vert & & \\ 1 & \longrightarrow & N & \longrightarrow & G' & \xrightarrow{p'} & H & \longrightarrow & 1 \end{array}$$

若$G = N \rtimes_\alpha H$, 则有可裂扩张



其中$\alpha : h \mapsto f_h; f_h(n) = hnh^{-1}$. 易验证$\varphi$为同构.

群之列

正规列

称群的递降子群列为正规列, 若且仅若每一递降为取正规子群之操作, i.e.

$$G = G_0 \rhd G_1 \rhd G_2 \cdots \rhd G_n = \{1\}$$

其中G_i/G_{i+1}为商群.

若能于相邻之两项间安插新者, 则称之加细. 加细为真加细若且仅若新安插群较左右者真包含.

合成列

称正规列为合成列, 若且仅若商群均为非平凡单群.

细观单群定义可见合成列恰无冗余, 亦无再 (真) 加细之余地. 有限群总有合成列, 一般的群则未必. 同一群可以有多条合成链, 类比第二同构定理中"商即子之商"之定论, 可定义两条正规列相同若且仅若其商群在计入重数而不记顺序之情形下同构. 以相同关系对正规列进行划分可知其偏序关系, 极小(大)元即$G \rhd \{1\}$. Jordan–Hölder阐明了同一群之所有合成列等价, 即真加细之极致将正规列划分为若干可对易之单元.

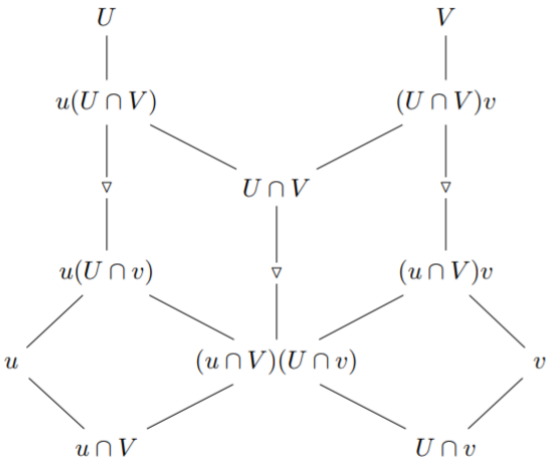
欲明Jordan–Hölder所言, 下引入Zassenhaus引理.

Zassenhaus引理(蝴蝶定理)

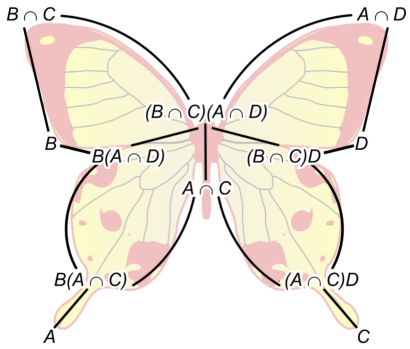
若对G之子群U, V取相应之正规子群$u \lhd U, v \lhd V$, 则有

$$\frac{u(U \cap V)}{u(U \cap v)} \cong \frac{U \cap V}{(u \cap V)(U \cap v)} \cong \frac{(U \cap V)v}{(u \cap V)v}$$

如下图中三组包含正规关系之平行列所示.



称之蝴蝶定理是因为



证明: 可验证交关系

$$u(U\cap v)\cap(U\cap V)=(u\cap V)(U\cap v)=(U\cap V)(u\cap V)v$$

$$u\cap(u\cap V)(V\cap u)=u\cap V$$
$$U\cap v=(u\cap V)(V\cap u)\cap v$$

由$v\lhd V$知$(U\cap v)\lhd(U\cap V)$, 从而$u(U\cap v)\lhd u(U\cap V)$. 由第一同构定理知

$$\frac{u(U\cap V)}{u(U\cap v)}\cong\frac{U\cap V}{(u\cap V)(U\cap v)}$$

同理可得另一侧蝶翼上之对应式子.

Schreier加细定理

两个正规列一定能在能在某种加细方式下等价, 即有等价的加细. 下证明

$$G=G_0\rhd\cdots\rhd G_r\rhd G_{r+1}=\{1\}$$
$$G=H_0\rhd\cdots\rhd H_s\rhd H_{s+1}=\{1\}$$

有等价之加细.

证明: 对$0 \leq i \leq r$与$0 \leq j \leq s$定义

$$G_{i,j} := G_{i+1}(H_j \cap G_i), \quad H_{j,i} := (G_i \cap H_j)H_{j+1}$$

遂有加细

$$\cdots \rhd G_i = G_{i,0} \rhd \cdots G_{i,s+1} = G_{i+1} \rhd \cdots$$

及

$$\cdots \rhd H_j = H_{j,0} \rhd \cdots H_{j,r+1} = H_{j+1} \rhd \cdots$$

由

$$\frac{G_{i,j}}{G_{i,j+1}} = \frac{G_{i+1}(H_j \cap G_i)}{G_{i+1}(H_{j+1} \cap G_i)} \cong \frac{(H_j \cap G_i)H_{j+1}}{(H_j \cap G_{i+1})H_{j+1}} \cong \frac{H_{j,i}}{H_{j,i+1}}$$

明所欲证.

Jordan–Hölder定理

任意两个合成列均等价. 这是Schreier加细定理的显然推论.

合成因子

合成因子为合成列中全体商群之无交并, 及计入重数而不记顺序之并, 记为$JH(G)$.

对正合列$1 \to N \to G \xrightarrow{\varphi} Q \to 1$, 假设$N$与$Q$有合成列$(N_j)_{j=1}^r$与$(Q_i)_{i=1}^s$, 则$G$亦有合成列

$$G = \varphi^{-1}(Q) \rhd \varphi^{-1}(Q_1) \rhd \cdots \rhd \varphi^{-1}(Q_s) = N \rhd N_1 \rhd \cdots \rhd N_r = \{1\}$$

由$\dfrac{\varphi^{-1}(Q_i)}{\varphi^{-1}(Q_{i+1})} \cong \dfrac{Q_i}{Q_{i+1}}$, 故$JH(G) = JH(N) \cup JH(Q)$.

对有限Abel群G而言, $JG(G)$中元素均为素数阶群(循环群). 这是因为Cauchy定理与对易性保证了

$$1 \to \langle t : t^{p_i} = 1 \rangle \to G_i \xrightarrow{\varphi} G_i / \langle t \rangle \to 1$$

其中$G_i \leq G$, 质数$p_i \mid G_i$.

中心列

称正规列为中心列, 若正规列

$$G = G_0 \rhd G_1 \rhd G_2 \cdots \rhd G_n = \{1\}$$

中诸$G_i \lhd G$, 且$G_i/G_{i+1} \subset C(G/G_{i+1})$.

可解与幂零

定义

称群G可解, 若存在使各商群均交换之正规列. (后叙述诸等价定义.)

称群G超可解, 若诸$G_i \lhd G$, 且G_i/G_{i+1}为素数阶(循环)群.

称G幂零, 若存在对应的中心列.

换位子

导出子群

换位子$[a,b] := aba^{-1}b^{-1}$满足如下性质

1. $ab = [a,b]\cdot ba$. 换位子之名称来源于此.
2. $ab = ba$若且仅若$[a,b] = 1$, 是故Abel群之换位子恒为1.
3. $[a,b]^{-1} = [b,a]$, 但换位子之积不尽封闭.
4. 对$\varphi \in \hom(G,G)$与$(a,b) \in G\times G$, $\varphi([a,b]) = [\varphi(a),\varphi(b)]$. 特别地, $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}]$.

导出子群G'为G中所有换位子生成之子群, 亦即包含所有换位子之最小正规子群: 可由共轭不变性验证$G' \lhd G$.

> *Remark: 导出子群G'愈大则G之Abel性愈弱. $G' = \{1\}$若且仅若G为Abel群.*

导出子群G'为使得商群可交换之最小子群. 换言之, 对$N \lhd G$, 商群G/N可交换若且仅若$G' \le N$.

多次导群

记$G^{(0)} := G, G^{(1)} := G', G^{(i+1)} := (G^{(i)})'$. 可得导出列 (一类合成列)

$$G = G^{(0)} \rhd G^{(1)} \rhd \cdots \rhd G^{(n)} = \{1\}$$

若记$[A, B]$为一切$[a, b]$式换位子之集合, 其中$(a, b) \in A \times B$. 由是可定义$G^{(i+1)} = [G^{(i)}, G^{(i)}]$. 我们将导出子群与与降中心列比较研究.

降中心列

定义

多次导群定义$G^{(i+1)} := [G^{(i)}, G^{(i)}]$, 降中心列定义$G^{[i+1]} := [G^{[i]}, G]$. 易知$G^{(i)} \leq G^{[i]}$.

交换化与中心化

由于对$\varphi \in \hom(G, G)$与$(a, b) \in G \times G$, 总有$\varphi([a, b]) = [\varphi(a), \varphi(b)]$. 因此$G^{(i)}$与$G^{[i]}$关于$\varphi \in \hom(G, G)$不变. 考虑共轭作用知$G^{(i)} \lhd G$, $G^{[i]} \lhd G$.

Prop. 对每一i, $G^{(i)}/G^{(i+1)}$为Abel群, 而$G^{[i]}/G^{[i+1]}$包含于$C(G/G^{[i+1]})$.

证明:

1. $G/G^{(1)}$实为极大交换商, 即最大的Abel商群. 对任一将G映知某Abel群A之映射φ, 存在唯一的$\tilde{\varphi}$使得存在交换图表

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/G^{(1)} \\ & \searrow^{\varphi} & \swarrow_{\exists!\tilde{\varphi}} \\ & A & \end{array}$$

2. 由于$[G^{[i]}, G] = [G^{[i+1]}]$, 故$[G^{[i]}/G^{[i+1]}, G/G^{[i+1]}] = \{1\}$. 因此$G^{[i]}/G^{[i+1]}$包含于$C(G/G^{[i+1]})$.

可解群与幂零群

先下论断: G可解若且仅若$G^{(n)}$在n足够大时等于$\{1\}$. G幂零若且仅若$G^{[n]}$在n充分大时等于$\{1\}$.

下分别证明两句论断:

1. 充分性是显然的. 必要性亦是显然的, 因为总有$G^{(i)} \subset G_i \to \{1\}$.

2. 大体同上.

> *Remark: 幂零群之"幂零"指映射*$[x,\cdot]:G\to G, g\mapsto [x,g]$*幂零, 亦即*
>
> $$[x,[x,\cdots,[x,\cdot]]]:G\to\{1\}$$

可解群性质

1. 可解群的子群与商群皆可解.

   > *Remark: 此处"可解"可全部换做"超可解"或幂零.*

2. 设$N\lhd G$, 则G可解等价于N与G/N可解.
3. 若群存在满足如下性质之正规列, 则可解:

   a. 收缩于$\{1\}$, 且每一商群可交换.
   b. 收缩于$\{1\}$, 且每一商群为素数阶群换群.

   证明: 考虑$G^{(1)}\subset G_i$及Abel群于Cauchy定理下导出的正合列

   $$1\to\langle x:x^p=1\rangle\to A\to A/\langle x\rangle\to 1$$

   即可
4. pq阶群, p^aq^b阶群, pqr阶群, 二面体群, p群, S_4等均可解.

   > *Remark: 实际上p群, 上三角矩阵群等幂零. 在此不做过多探讨.*

5. (Feit&Thompson) 奇数阶群可解

对有限群, 有

$$\text{幂零}\implies\text{超可解}\implies\text{可解}$$

常见导出列 (换位子群导出)

- $S_3\rhd A_3\rhd\{1\}$.
- $S_4\rhd A_4\rhd K_4\rhd\{1\}$.
- $S_5\rhd A_5\rhd A_5\rhd\cdots$.
- (Abel群A) $A\rhd\{1\}$.
- $D_n\rhd\langle\sigma^2\rangle\rhd\{1\}$.
- $Q_8\rhd\mathbb{Z}_2\rhd\{1\}$.
