抽象代数笔记
群论: 初见

EndlieDownAHell

2023 年 3 月 31 日

幺半群与群

半群: 群胚 G 上有一代数运算 $\cdot : G \times G \to G$ 具有结合性.
附加关键词:

(i) 幺: 存在 $e \in G$ 使得 $\forall a \in G, ae = ea = a$

(ii) 交换 (communitative, Abelian): $\forall a, b \in G, ab = ba$

定理 1 半群 G 成一群当且仅当左 (右) 逆元与左 (右) 恒等元同时存在.

Proof. 假定左恒等元 e 非右恒等元, 将知道

$$ae \neq ea$$

考虑到 $e = aa^{-1}$, 这也即

$$aaa^{-1} \neq aa^{-1}a$$

同时右乘 a^{-1}, 这也即 $aaa^{-1}a^{-1} = aa^{-1}aa^{-1}$, 然而考虑到

$$aaa^{-1}a^{-1} = a(aa^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

$$aa^{-1}aa^{-1} = (aa^{-1})(aa^{-1}) = ee = e$$

这导致了矛盾, 于是只能 $ae = ea = a$.

假定右逆 a^{-1} 非 a 的左逆元, 则 $a^{-1}a \neq e$, 左乘 a, 右乘 a^{-1}, 将得到

$$aa^{-1}aa^{-1} \neq aa^{-1}$$

这显然导致了矛盾, 于是 $a^{-1}a = aa^{-1} = a$. □

命题 2 若群 G 满足 $\forall a \in G, a^2 = e$, 则 G 是 Abel 群.

Proof. 不难知道

$$xyxy = e$$

考虑到 $x^2 = e, y^2 = e$, 左乘 yx 即得

$$e^2xy = yxe$$

这也即 $xy = yx$. □

定理 3 半群 G 成群当且仅当方程 $ax = b, ya = b$ 在群内有解.

Proof. 群中方程的成立显然, 对于反向的命题, 我们通过找出满足条件的恒等元与逆元完成证明:

取定 $a, b \in G$, 假定 x_1, x_1', x_2, x_2' 分别是如下四个方程的解:

$$ax_1 = a, x_1'a = a$$

$$bx_2 = b, x_2'b = b$$

我们来证明 $x_1 = x_2 = x_1' = x_2'$, 假定 $x_1 \neq x_1'$, 则知道

$$ax_1a \neq ax_1'a$$

这将使得 $a^2 \neq a^2$, 显然是矛盾的, 同理我们能够证明 $x_2 = x_2'$, 从而我们不再区分 x_1, x_1' 及 x_2, x_2'.

假定 $x_1 \neq x_2$, 则知道

$$ax_1b \neq ax_2b$$

这便是 $ab \neq ab$, 同样导致着矛盾, 于是 $x_1 = x_2$.

至此我们完成了恒等元存在性的证明.

针对 $a \in G$, 我们取定 y, y' 满足

$$ay = e, y'a = e$$

假若 $y \neq y'$, 则

$$aya \neq ay'a$$

于是 $a \neq a$, 矛盾, 则 $y = y'$, 我们从而确定了逆元的存在.

现在, G 显然成一群. □

子群, 陪集, 正规子群

子群

定理 4 取定集合 $H \subset G$, 其中 G 为一群, 则 H 为 G 的子群当且仅当 $\forall a, b \in H, ab^{-1} \in H$.

Proof. 正向命题显然, 对于反向的命题, 令 $a = b = x$, 则 $xx^{-1} = e \in H$, 于是恒等元在 H 中, 令 $a = e, b = x$, 则 $ex^{-1} = x^{-1} \in H$, 于是逆元在 H 中, 令 $a = x, b = y^{-1}$, 则 $xy \in H$, 则 H 对运算封闭, 于是 H 成一群. □

针对 $S \subset G$ 取定 $S^- = \{x^{-1} \mid x \in S\}$, 于是

$$\langle S \rangle = \left\{ \prod_{i=1}^{n} x_i \mid x_i \in S \cup S^-, n \in N \right\}$$

构成一个群, 被称为 S 生成的群.

取定 G 的子群 H, 针对元素 a, 称 $aH = \{ah \mid h \in H\}, Ha = \{ha \mid h \in H\}$ 为 H 的左, 右陪集, 定义群上集合乘法 $AB = \{an \mid a \in A, b \in B\}$ 后这也即 $\{a\}H, H\{a\}$, 关于子群的陪集, 我们有如下景观 (这些命题针对右陪集的情况同样成立):

定理 5 (i) 存在等价关系 $a\sim b: aH=bH$, 且 $G/\sim$ 恰为全体陪集的集合.

(ii) $|aH|=|bH|$, 针对有限集记 $|G|/|aH|=[G:H]$, 则当 H 为 G 子群, K 为 H 子群时

$$[G:K]=[G:H][H:K]$$

Proof. $aH=bH$ 成等价关系显然, 假若 $aH=bH$, 取定 $e\in H$, 于是不难察觉 $b\in aH, a\in bH$, 从而 a,b 在同一陪集中, 同样的, 假若 a,b 在同一陪集 cH 中, 则可取定 h_1,h_2 使得

$$a=ch_1, b=ch_2$$

取定 $h_1^{-1}, h_2^{-1}\in H$, 则 $ah_1^{-1}=bh_2^{-1}=c$, 从而 $c\in aH, bH$, 故而若 a,b 在同一陪集中, 则 $aH=bH$, 于是 $G/\sim$ 确实为陪集的全体.

显然可以建立如下的 $1-1$ 映射, 从而知道 aK, bH 是等势的:

$$f: aH\to bH, ah\to bh$$

假定 $G=\bigcup_{i=1}^{n} x_iH$, $H=\bigcup_{j=1}^{m} y_jK$, 现在通过证明 $\{x_iy_jK\}$ 是一组无交的集合来完成证明.

假若 $x_iy_jK=x_{i'}y_{j'}K$, 将知道

$$x_iy_jKH=x_{i'}y_{j'}K$$

由于 $y_jK, y_{j'}K\subset H$, 将有 $y_jKH=y_{j'}KH=H$, 也即

$$x_iH=x_{i'}H$$

于是 $x_i=x_{i'}$, 从而又能推出 $y_jK=y_{j'}K$, 于是有 $y_j=y_{j'}$, 至此我们证明了 $\{x_iy_jK\}$ 的互异性.

假定 $g\in G$, 必然 $g\in x_iH$, 于是存在 h 使得 $g=x_ih$, 又考虑到 $h\in y_jK$, 于是

$$g\in x_iy_jK$$

这便证明了 $\{x_iy_jK\}$ 将 G 覆盖, 至此命题证完. □

命题的公式中, 假若令 $K=\{e\}$, 即得大名鼎鼎的 Lagrange 定理:

$$[G:H]=|G|/|H|$$

正规子群

若 $\forall x\in G, xH=Hx$, 则称 H 为 G 的正规子群, 记作 $H\lhd G$.

察看 $G/H=G/\sim$, 不难发现集合乘法已经为我们找到了一个自然的运算:

$$(xH)(yH)=(Hx)(yH)=(Hxy)(H)=xy(HH)=xyH$$

不难验证这运算使得 G/H 形成一个群, 称为商群.

命题 6 $H<G, [G:H]=2\Rightarrow H\lhd G$

Proof. $[G:H]$, 则 $G/H=\{H, aH\}$, 考虑 Ha, 由于 $|aH|=|Ha|$, H 的右陪集的全体只能是 $\{H, Ha\}$, 考虑到 $H\cup aH=G, H\cup Ha=G$, 只能 $Ha=aH$, 于是 $H\lhd G$. □

我们最后以如下一条命题的证明结束本小节:

定理 7 $H < G, K < G$, 则 $HK < G$ 当且仅当 $KH < G$, 且此时自然地将有 $HK = KH$.

Proof. 当 KH 为群时, 我们知道下面的命题出现:

$$k_1h_1k_2h_2 \in KH, (kh)^{-1} \in KH$$

现在, 我们来验证 HK 成群:

若 $h_1k_1, h_2k_2 \in HK$, 为了证明 $h_1k_1h_2k_2 \in HK$, 考虑到求逆元的映射 $a \to a^{-1}, hk \to k^{-1}h^{-1}$ 是一个 $1-1$ 映射, 我们只需要证明

$$h_2^{-1}k_2^{-1}h_1^{-1}k_1^{-1} \in HK$$

考虑到 H, K 成群, 自然 $h^{-1} \in H, k^{-1} \in K$, 以 h', k' 代替之, 将得到

$$h_1'k_1', h_2'k_2' \in HK$$

于是欲证的式子从 KH 成群便已经十分清晰了.

假若 $hk \in HK$, 我们来证明 $(hk)^{-1} \in HK$, 为此我们考虑证明

$$hk \in KH$$

考虑到 HK 成群, $(hk)^{-1} = k'h' \in KH$, 自然 $hk \in KH$. 反向命题的证明与此类似, 对于 $KH = HK$, 只需要看到下面的式子一切便是十分清晰的了:

$$(hk)^{-1} = k'h'$$

□

循环群

定义自行查阅, 本节只证明一些结论.

定理 8 无限循环群有且仅有两个生成元.

Proof. 察看无限循环群的结构, 其中自然存在如下元素:

$$a, a^2, \cdots, a_n, \cdots$$

考虑到这群的无限性, 显然 $a^n = e$ 绝无可能实现, 故而只能另立恒等元 e, 假若 a^k 的元素即在序列 $\{a_n\}$ 将知道

$$a^{k+n} = e$$

从前, 这绝无可能, 因而只能另立逆元于群中, 不难观察到一下事实:

$$(a^n)^{-1} = (a^{-1})^n$$

应用结合律便能知道这事实的成立, 为此我们能够从 a 的逆元 a^{-1} 生成全体 a^n 的逆元, 则现在我们确定了无限循环群的结构如下:

$$\cdots, a^{-n}, \cdots, a^{-1}, e, a, \cdots, a^n, \cdots$$

□

定理 9 假定 $\langle a\rangle$ 是 n 阶循环群, 则 $\langle a^r\rangle = \langle a\rangle$ 当且仅当 $\gcd(r,n) = 1$.

Proof. a^r 为 $\langle a\rangle$ 的生成元便要求着 $a^r, \cdots, a^{nr}$ 是互异的, 这实际上便意味着

$$r, \cdots, nr$$

构成模 n 的一组完全剩余系, 这便要求着 $(n,r) = 1$, 否则取定 $k = \dfrac{n}{\gcd(n,r)} < n$, 将有

$$kr = \frac{nr}{\gcd(n,r)} = \operatorname{lcm}(n,r)$$

这便导致了所列数列不成完全剩余系.

反向命题的证明只是模算数的平凡结果. □

定理 10 取定 $\langle a\rangle$ 阶为 n, 针对 $d \mid n$, 存在唯一阶为 d 的子群 $\langle g^{\frac{n}{d}}\rangle$

Proof. 察看 a^r 的阶, 这便要求我们找到最小的正数 k 使得

$$kr \mod n = 0$$

当 $(n,r) = 1$ 时, 阶显然为 n, 当 $(n,r) \neq 1$ 时, 满足条件的 k 自然便是 $\dfrac{n}{(n,r)}$, 因此, $\langle a^r\rangle$ 的阶为 d, 当且仅当

$$\frac{n}{(n,r)} = d$$

这便是 $r = \dfrac{tn}{d}, t \perp n$, 从而所求子群便是 $\langle a^{\frac{n}{d}}\rangle$. □

定理 11 取定阶为 n 的循环群, 取定其阶分别为 $d, l (d, l \mid n)$ 的子群 G_1, G_2, 则 $G_1 \cap G_2$ 阶为 $\gcd(d,l)$, G_1G_2 的阶为 $\operatorname{lcm}(d,l)$.

Proof. 知道 $G_1 = \langle a^{\frac{n}{d}}\rangle, G_1 = \langle a^{\frac{n}{l}}\rangle$, 于是 $G_1 \cap G_2$ 中元素的指数必然同时被 $\dfrac{n}{d}, \dfrac{n}{l}$ 整除, 其中最小元便是:

$$a^L, L = \operatorname{lcm}\left(\frac{n}{d}, \frac{n}{l}\right)$$

计算这最小元的阶, 即得

$$\begin{aligned}
|G_1 \cap G_2| &= \frac{n}{\gcd(L,n)} = \frac{dln}{\gcd(dlL, dln)} \\
&= \frac{dln}{\gcd\left[\operatorname{lcm}\left(ln, dn\right), dln\right]} \\
&= \frac{dln}{\gcd\left[n\operatorname{lcm}\left(l,d\right), dln\right]} = \frac{dl}{\gcd[\operatorname{lcm}(l,d), dl]} \\
&= \frac{dl}{\operatorname{lcm}(d,l)} = \gcd(d,l)
\end{aligned}$$

我们同样来计算 G_1G_2 中最小元的阶, 得到

$$|G_1G_2| = \frac{n}{\gcd\left(\dfrac{n^2}{dl}, n\right)} = \frac{ndl}{\gcd(n^2, ndl)} = \frac{dl}{\gcd(n, dl)} = \operatorname{lcm}(d,l)$$

□

定理 12 针对群 G 中的元素 a, b, c, 有

$$|a| = |a^{-1}|, |ab| = |ba|, |a| = |cac^{-1}|$$

Proof. 察看 $(a^{-1})^k$ 的结果, 将知道

$$(a^{-1})^k = (a^k)^{-1}$$

考虑到 e 的逆元只能是 e, 便知道, 使得 $(a^{-1})^k = e$ 的最小的 k 便是 $|a|$.

ba 的阶为 k, 当且仅当其是满足 $(ba)^{k+1} = ba$ 的最小整数, 考虑到如下改写

$$(ba)^{k+1} = b(ab)^k a$$

自然 $k = |ab|$.

对于 cac^{-1}, 我们采取同样的做法, 得到

$$(cac^{-1})^{|a|} = ca^{|a|}c^{-1}$$

若上式非 e, 将有

$$a^{|a|} = e \neq c^{-1}c$$

这不可能, 于是命题成立. □

命题 13 假若 $a, b \in G$ 交换, 也即 $ab = ba$, 存在 $q \in G, |q| = \mathrm{lcm}(|a|, |b|)$

Proof. 令 $q = ab$, 从交换性, 知道

$$q^k = a^k b^k$$

于是命题自然成立. □

命题 14 有限交换群中存在元素 a, 其阶被所有元素的阶整除.

Proof. 构造如下元素, 其余与前一命题类似:

$$q = \bigcup_{a_i \in G} a_i$$

□

群同态, 群同构

考虑映射 $\det : \mathrm{GL}_n(F) \to (F - \{0\}, *), M \to \det M$, 这显然是一般线性群到 F 上生成的乘法群的同态.

命题 15 假定群 G 的一个生成元集合为 S, 则群同态 f 由其在 S 上的限制 $f\mid_S$ 唯一决定.

Proof. 注意到 G 中元素可以被表为如下形式:

$$g = \prod_{a_i \in S} a_i^{k_i}, k_i \in \mathbb{Z}$$

考虑到 $f(ab) = f(a)f(b), f(a^{-1}) = f(a)^{-1}$, 命题的成立便已经十分清晰了. □

命题 16 $f : G \to G'$ 为单射当且仅当 $\mathrm{Ker} f = \{e\}$, 此时 $G \cong \mathrm{im} f$, 称 f 为 G 到 G' 的嵌入.

Proof. 假若 $f(a)=f(a')$ 自然知道

$$f(a^{-1}a')=f(e)$$

则 $\mathrm{Ker}f=\{e\}$ 时只能 $a^{-1}a'=e$, 于是 $a=a'$, 从而 f 为单射, 否则假定非恒等元的 $k\in\mathrm{Ker}f$, 于是可以且必然有 $a^{-1}a'=k$, 从而 $a\neq a'$, 则 f 非单射. □

定理 17 $\mathrm{Ker}f\lhd G$

Proof. 若 $a,b\in\mathrm{Ker}f$, 则

$$f(ab^{-1})=f(a)f(b)^{-1}=e$$

于是 $\mathrm{Ker}f<G$, 另外的, 假若 $x\in\mathrm{Ker}f,g\in G$, 自然有

$$f(gxg^{-1})=f(g)f(x)f(g)^{-1}=e\Rightarrow gxg^{-1}\in\mathrm{Ker}f$$

从而自然 $\mathrm{Ker}f\lhd G$. □

定理 18 若 $f:G\to G'$ 是满的, 则 $f^{-1}(p),p\in G'$ 恰是 $G/\mathrm{Ker}f$ 中的一个陪集, 考虑到 $f:g\to\in f$ 必然是满射, 实际上有

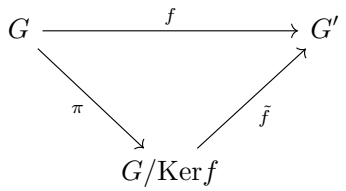
$$\mathrm{im}f\cong G/\mathrm{Ker}f$$

Proof. 从 f 为满射, 可假定 $f(q)=p$, 不难发现 $q\mathrm{Ker}f\subset f^{-1}(a)$, 另外的, 假若 $f(q')=p$, 将有

$$f(q^{-1}q')=e$$

于是 $q^{-1}q'\in\mathrm{Ker}f$, 从而 $q'=q(q^{-1}q')\in q\mathrm{Ker}f$, 故 $f^{-1}(p)\subset q\mathrm{Ker}f$. □

这启示我们在 G' 与 $G/\mathrm{Ker}f$ 间建立自然同态 $\pi:x\to x\mathrm{Ker}f$, 考虑到商集所具有泛性质, 我们实际知道使得下图表交换的 $\tilde{f}$ 唯一:



定理 19 取定满同态 $f:G\to\mathrm{im}f$, 针对着任意 $K<G,\mathrm{Ker}f\subset G$ 有

$$f^{-1}[f(K)]=K$$

且 $K\lhd G$ 当且仅当 $f(K)\lhd\mathrm{im}f$.

对于 $K_1<K_2$ 还有

$$[K_2:K_1]=[f(K_2):f(K_1)]$$

Proof. 若 $x\in f^{-1}[f(K)]$, 将有

$$f(x)=f(k),k\in K$$

则 $f(xk^{-1})=e$, 于是 $xk^{-1}\in\mathrm{Ker}f$, 从而

$$x=(xk^{-1})k\in\mathrm{Ker}fK=K$$

于是 $f^{-1}[f(K)] \subset K$ 对于反向的 $K \subset f^{-1}[f(K)]$, 这是十分自然的事情.

$gkg^{-1} \in K$ 当且仅当 $f(g)g(k)f(g)^{-1} \in f(K)$, 于是 $K \lhd G$ 当且仅当 $f(K) \lhd \mathrm{im}f$.

假定 $[K_2 : K_1] = r$, 则可将 K_2 分解为

$$K_2 = \bigcup_{i=1}^{r} x_i K_1$$

假若 $f(x_i)f(K_1) \cap f(x_j)f(K_1) \neq \varnothing$, 取定 $k_1, k_2 \in K$ 使得

$$x_i k_1 = x_j k_2$$

于是 $x_i = x_j k_2 k_1^{-1}$, 这便意味着 $x_i \in x_j K_1$, 这是不可能的.

另外的, 取定 $f(x_i k) \in f(K_2)$, 即得

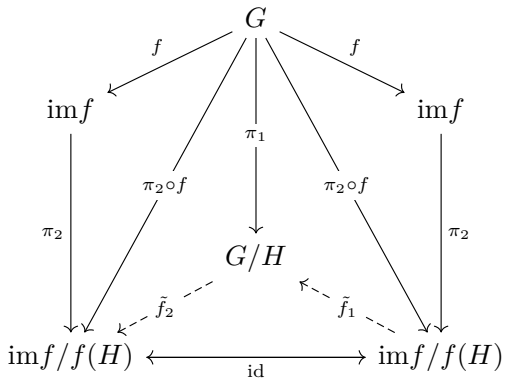
$$f(x_i k) \in f(x_i)f(K_1)$$

于是自然 $[f(K_2) : f(K_1)] = r$. □

定理 20 取定同态 $f : G \to G'$, 假若 $H \lhd G, \mathrm{Ker}f \subset H$, 则

$$\mathrm{im}f/f(H) \cong G/H$$

Proof. 察看如下交换图,



其中 $\tilde{f}_1, \tilde{f}_2$ 的存在性与唯一性由 G/H 的泛性质决定. □

定理 21 若 $N \lhd G$, 取定 $H < G$, 则

$$HN/N \cong H/H \cap N$$

Proof. $gng^{-1} \in N$, 考虑到 $hn' \in G$, 于是

$$(hn')n(hn')^{-1} \in N$$

而对于 $n_0 \in H \cap N$, 从 $N \lhd G$ 与 H 的封闭性, 知道

$$hn_0h^{-1} \in N, hn_0h \in H \Rightarrow hn_0h \in H \cap N$$

现在便证明了商群 $HN/N, H/H \cap N$ 的存在性.

对于同构, 考虑建立同态 $f : H \to HN/N, h \to hN$, 则 $f(h) = N$ 当且仅当 $h \in H$, 故而

$$\mathrm{Ker}f = H \cap N$$

应用 $\mathrm{im}f \cong G/\mathrm{Ker}f$, 得到

$$HN/N \cong H/N \cap H$$

□

群塔: 正规列, 可解列, 合成列

如下的序列被称为群塔:

$$G_0 > G_1 > \cdots > G_n$$

如下的序列被称为正规群塔:

$$G_0 \rhd G_1 \rhd \cdots \rhd G_n$$

若这正规群塔的商群 G_i/G_{i+1} 均是 Abel 群/循环群, 便称其为 Abel 塔或循环塔.

若群 G 存在结尾为 $\{e\}$ 的 Abel 塔, 称 G 是可解群.

定理 22 取定同态 $f : G \to G'$, 再取定如下群塔:

$$T_1 : G = G_0 > G_1 \cdots G_n$$

$$T_2 : f^{-1}(G_0) > f^{-1}(G_1) > \cdots > f^{-1}(G_n)$$

则 T_1 为正规塔/Abel 塔/循环塔时 T_2 同样为正规塔/Abel 塔/循环塔.

Proof. 取定 $g_i \in f^{-1}(G_i), g_{i+1} \in f^{-1}(G_{i+1})$, 为证明 $g_i g_{i+1} g_i^{-1} \in f^{-1}(G_{i+1})$, 只需验证:

$$f(g_i g_{i+1} g_i^{-1}) \in G_{i+1}$$

考虑到 $G_i \rhd G_{i+1}$ 时命题自动成立, 故而 T_1 是正规塔时 T_2 同样是正规塔.

对于商群, 不难注意到, 总有 $f^{-1}(G_i) \supset \mathrm{Ker} f$ 成立, 于是根据第一同构定理, 自然成立

$$G_i/G_{i+1} \simeq f^{-1}(G_i)/f^{-1}(G_{i+1})$$

于是 T_1 为 Abel 塔/循环塔时 T_2 自然为 Abel 塔/循环塔. □

向群塔 $T : G_0 > G_1 > \cdots > G_n$ 中添加有限个子群得到的新群塔被称为原群塔 T 的一个加细.

定理 23 有限群的 Abel 塔总可加细为循环塔.

Proof. 先来察看交换群的情况, 针对交换群 G, 取定 Abel 群塔如下:

$$T : G = G_0 \rhd G_1 \rhd \cdots \rhd G_n$$

当 $|G| = 2$ 时, 情况只能是

$$T : G \rhd \{e\}$$

当我们假设 $|G| < r$ 时命题成立, 而来勘看 $|G| = r$ 时 G 的 Abel 群塔 T, 我们取定这群塔中最后一个非平凡的群 $G_k \neq \{e\}$, 再取定 $x \in G_k, x \neq e$, 由于 G 为一交换群, 便可生成群同态:

$$f : G \to G/\langle x \rangle$$

利用同构定理, 依这群同态生成如下 Abel 群塔:

$$f(G) \rhd f(G_1) \rhd \cdots \rhd f(G_k)$$

这群塔中 $|f(G)| = |G/\langle x \rangle| < r$ 是自然的, 于是依照归纳假设我们可将这群塔加细为如下循环群塔:

$$f(\mathfrak{G}) \rhd f(\mathfrak{G}_1) \rhd f(\mathfrak{G}_2) \rhd \cdots \rhd f(\mathfrak{G}_l) = f(\mathrm{Ker} f)$$

于是新的群塔:

$$\mathfrak{G} \rhd \mathfrak{G}_1 \rhd \cdots \rhd \mathfrak{G}_\mathfrak{l}$$

便是 T 的满足要求的加细.

针对非交换群的群 G, 我们对每一个子链 $G_i \rhd G_{i+1}$ 进行加细, 考虑到 G_i/G_{i+1} 成一 Abel 群, 于是存在如下极简的 Abel 塔:

$$G_i/G_{i+1} \rhd \{e\}$$

建立同态 $f : G_i \to G_i/G_{i+1}$, 这塔可加细为循环塔:

$$f(G_i) \rhd f(G_{i,1}) \rhd \cdots \rhd f(G_{i,k}) \rhd \{f(\mathrm{Ker}f)\} = f(G_{i+1})$$

回看原像, 我们已经将 $G_i \rhd G_{i+1}$ 加细为:

$$G_i \rhd G_{i,1} \rhd \cdots \rhd G_{i,k} \rhd G_{i+1}$$

针对全部的 $G_i \rhd G_{i+1}$ 完成这样的加细, 工作便已经完成. □

定理 24 (黄油飞蝇引理) 取定 $U, V < G$, $u \lhd U, v \lhd V$, 则

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

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

且有

$$u(U \cap V)/u(U \cap v) \simeq (U \cap V)v/(u \cap V)v$$

Proof. 取定 $xy \in u(U \cap V)$, 其中 $x \in u, y \in U \cap V$, 从 $u \lhd U$ 有

$$\begin{aligned} xy[u(U \cap v)]y^{-1}x^{-1} &= (xu)[y(U \cap v)]y^{-1}x^{-1} \\ &= u(U \cap v)y^{-1}x^{-1} \\ &= u(U \cap v)x^{-1} = (U \cap v)ux^{-1} = (U \cap V)u \\ &= u(U \cap V) \end{aligned}$$

于是 $u(U \cap v) \lhd u(U \cap V)$, 同样的我们能够证明 $(u \cap V)v \lhd (U \cap V)v$.

现在来证明定理的另一部分, 从 $u \lhd U, u(U \cap v) \lhd u(U \cap V)$ 知道, 对于任意 $x \in U \cap V$, 有

$$xu(U \cap v)x^{-1} = ux(U \cap V)x^{-1} = u(U \cap V)$$

于是 $u(U \cap v) \lhd U \cap V$, 从第二同构定理, 即得

$$(U \cap V)u(U \cap v)/u(U \cap v) \simeq U \cap V/(u \cap V) \cap u(U \cap V)$$

对于等式左边, 应用

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

这式子的证明如下:
一方面我们有

$$\text{RHS}\subset u(U\cap v)\cap V(U\cap v)$$

考虑到 $U\cap v\subset v\subset V$, 得到

$$\text{RHS}\subset u(U\cap v)\cap V$$

从 $u\subset U, U\cap v\subset U$, 知道 $u(U\cap v)=[u(U\cap V)]\cap V$, 将这式子加在上式, 得到

$$\text{RHS}\subset u(U\cap v)\cap(U\cap V)=\text{LHS}$$

对于反向的包含式, 取定 $z\in u(U\cap v)\cap(U\cap V)\subset V$, 其自然可以表为 $z=xy, x\in u, y\in U\cap v\subset V$, 这式子, 从 $y^{-1}\in V$ 将知道

$$x=zy^{-1}\subset V\Rightarrow x\in u\cap V$$

于是 $z=xy\subset(u\cap V)(U\cap v)$, 从而 LHS $\subset$ RHS, 于是等式成立.

我们将得到:

$$U\cap V/(u\cap V)(U\cap v)\simeq u(U\cap V)/u(U\cap v)$$

从对称性, 同样有下面的式子成立:

$$V\cap U/(v\cap U)(u\cap V)\simeq v(V\cap U)/v(V\cap u)$$

从 $v\lhd V$, 也即

$$U\cap V/(v\cap U)(u\cap V)\simeq(V\cap U)v/(V\cap u)v$$

再应用等式 $(u\cap V)(U\cap v)=(U\cap v)(u\cap V)$, 于是已经成立:

$$u(U\cap V)/u(U\cap v)\simeq v(U\cap V)/v(u\cap V)$$

□

对于正规塔 $T: G_0\rhd\cdots\rhd G_n$, 称序列 $\{G_i/G_{i+1}\}$ 为 T 的商群列, 对于长度一致的正规塔 T_1, T_2, 假若能为 T_1, T_2 的商群列确定一个指派法则, 使得被指派的两个商群同构, 则称 T_1, T_2 是等价的.

定理 25 群 G 的两个末端为 $\{e\}$ 的正规塔总可加细到彼此等价.

Proof. 取定 G 的如下两个正规塔:

$$T_1: G=G_0\rhd\cdots\rhd G_n=\{e\}$$

$$T_1: G=H_0\rhd\cdots\rhd H_m=\{e\}$$

针对 $G_i\rhd G_{i+1}$, 生成如下序列:

$$G_{i,k}=G_{i+1}(H_k\cap G_i)$$

于是 $G_i\rhd G_{i+1}$ 存在如下加细:

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

针对 T_1 中全体 $G_i\rhd G_{I+1}$ 进行同样的操作, 得到加细 T_1', 针对 T_2 进行类似的操作, 得到加细 T_2', 两者的长度均为 $(m-1)(n-1)+1$.

我们构造的加细塔的商群列具有如下的形式:

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

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

注意到 $G_{i+1} \lhd G_i, H_{j+1} \lhd H_j$, 应用蝴蝶引理, 即得

$$H_{j+1}(G_i \cap H_j)/H_{j+1}(G_{i+1} \cap H_j) \simeq H_{j+1}(G_i \cap H_j)/H_{j+1}(G_{i+1} \cap H_j)$$

这便为我们建立了证明加细等价所需的指派. □

定理 26 (Jordan-Hölder) 取定 G 中正规塔 $T : G \rhd G_1 \rhd \cdots \rhd G_n = \{e\}(G_i \neq G_{i+1})$, 使得其商群列的全体均为单群, 假若再有同样的正规塔 T', 必然与 T 等价.

Proof. 将 T, T' 一齐加细至等价, 于是命题的成立只需要我们证明 T 与 T 的加细等价, 察看 $G_i \rhd G_{i+1}$ 及相应的加细

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

考虑到 G_i/G_{i+1} 成一单群, 我们通过说明 $G_i \rhd G_{i+1}$ 无法被真加细来完成论证, 取定 $G_{i,j} \rhd G_{i+1}$ 满足

$$G_i \rhd G_{i,j} \rhd G_{i+1}$$

显然 $G_{i,j}/G_{i+1} \lhd G_i/G_{i+1}$, 于是只能 $G_{i,j}/G_{i+1} = \{e\}, G_i/G_{i+1}$, 也即 $G_{i,j} = G_i, G_{i+1}$.

$G_{i,j}$ 如此, 针对 $G_{i,j-1}$ 重复这一步骤, 便知道插入 $G_i \rhd G_{i+1}$ 的群永无可能与 G_i, G_{i+1} 互异, 于是这加细的结果去除重复部分得到的仍然是 T, 这便说明加细与 T 的等价性, 再应用等价关系的传递性, 命题得证. □

群作用

若能针对群 G 与集合 S 进行如下指派:

$$G \times S \to S, (x, s) \to x \cdot s$$

且满足着:

$$(xy) \cdot s = x \cdot (y \cdot ys), e \cdot s = s$$

则称 G 在 S 上有一个作用, S 是一个 G 集.

针对 G 集 S, 我们可以定义其上一个变换:

$$\sigma_x : S \to S, s \to x \cdot s$$

这变换同时又满足着:

$$\sigma_{xy} = \sigma_x \circ \sigma_y$$

特殊的, 有

$$\sigma_x \sigma_{x^{-1}} = \sigma_e = \mathrm{id}_S = \sigma_{x^{-1}} \sigma_x$$

于是 $\{\sigma_x \mid x \in G\}$ 组成了 S 上的一个变换群, 自然, 我们能够建立 G 到 S 的对称群的一个同态, 此时我们也说 G 被表为一个变换群:

$$G \to S_S, x \to \sigma_x$$

两个被 G 作用的 G 集 S, S' 间若能建立如下映射, 这映射将被称为一个 G 映射:

$$f(x \cdot s) = f(x) \cdot s$$

另外的, 对于 G 集, 我们定义 $s \in S$ 在 G 的轨道为 $G_s = \{x \cdot s \mid x \in G\}$.

假若针对 $a, b \in S$, 总能找到 $x \in G$ 使得 $a = x \cdot b$, 则称 G 在 S 上是可迁的, 可迁的一个典型例子便是 GL_n 在 $\mathbb{R}^n - \{0\}$ 上是可迁的.

现在, 针对 G 集 S 中的元素 s, 可以定义

$$\mathrm{St}_G(s) = \{x \in G \mid x \cdot s = s\}$$

不难证明 $\mathrm{St} < G$, 其被称为 s 在 G 中的稳定化子.

定理 27 若 X 是 G 的可迁集, 针对 $x \in X$, 将能给定 G 同构:

$$X \simeq G/\mathrm{St}(x)$$

Proof. 预备着按照如下方案给出所需的同构映射:

$$\varphi : G/\mathrm{St}(x) \to X, g\mathrm{St}(x) \to g \cdot x, g \in G$$

这映射的存在性需要我们证明这指派法则是良定义的, 为此我们察看 g, g' 使得 $g\mathrm{St}(x) = g'\mathrm{St}(x)$, 得到:

$$\begin{aligned} g\mathrm{St}(x) = g'\mathrm{St}(x) &\Leftrightarrow g^{-1}g\mathrm{St}(x) = g^{-1}g'\mathrm{St}(x) \Leftrightarrow e\mathrm{St}(x) = g^{-1}g'\mathrm{St}(x) \\ &\Leftrightarrow g^{-1}g'\mathrm{St}(x) = \mathrm{St}(x) \Leftrightarrow g^{-1}g' \in \mathrm{St}(x) \\ &\Leftrightarrow g^{-1}g'x = x \Leftrightarrow g'x = gx \end{aligned}$$

于是我们确定了 φ 的良定性, 顺带确定了 φ 是单射.

对于满射, 察看 X 的可迁性

$$\forall y \in X, \exists g \in G, y = g \cdot x = \varphi[\mathrm{St}(x)]$$

现在只需要证明 φ 确为一 G 映射, 为此查看 $u \in G$, 得到

$$u\varphi[g\mathrm{St}(x)] = u \cdot (g \cdot x) = (ug) \cdot x = \varphi[u(g\mathrm{St}(x))]$$

□

注 1 考虑到 Gx 正是 G 的一个可迁集, 我们能够针对全体 $x \in X$ 宣称:

$$Gx \simeq G/\mathrm{St}(x)$$

另外的, 针对有限群 G, 这便意味着 $|Gx| = [G/\mathrm{St}(x)]$.

我们假定 $Gs_1 \cap Gs_2 \neq \varnothing$, 取定 $s \in Gs_1 \cap Gs_2$, 便将有 $x_1, x_2 \in G$ 使得

$$s = x_1 s_1 \Rightarrow Gs = G(x_1 \cdot s_1) = Gs_1$$

$$s = x_1 s_1 \Rightarrow Gs = G(x_2 \cdot s_2) = Gs_2$$

于是必然 $Gs_1 = Gs_2$, 这只能指向一个结果, 即全体轨道构成了 G 集 S 的一个分划. 于是我们自然有如下的轨道分解公式:

定理 28 若 $|S|$ 为有限集, 则

$$|S| = \sum_{i\in I}[G/\mathrm{St}(s_i)]$$

定理 29 取定有限群 G, 以及 $H, K < G$, 则

$$|HK| = \frac{|H|\cdot|K|}{|H\cap K|}$$

Proof. 取定 G/K, 在其上指定 H 的作用:

$$G/K \to G/K, gK \to hgK$$

于是自然 HK 在视作 K 在这作用下的轨道时可以被改写为:

$$HK = \bigcap_{i=1}^{n} h_i K$$

从而 $|HK| = n|K|$, 这式子中 n 表征着 $h \in H$ 可以将 K 指向多少个不同的集合, 自然, 这指引我们得到如下等式:

$$n = [H/\mathrm{St}(K)]$$

不难发觉 $\mathrm{St}(K) = H \cap K$, 于是我们有

$$|HK| = n|H| = \frac{|K|}{|K\cap H|}\cdot|H| = \frac{|H|\cdot|K|}{|H\cap K|}$$

□

从这式子我们即得群 G 中与子群 H 共轭的子群个数为 $[G/\mathrm{St}(H)]$.

下面我们察看几个典型的变换群:

共轭

按照如下方法建立 G 到 G 自身的一个作用:

$$\sigma_x : G \to G, s \to xsx^{-1}$$

不难验证 σ_x 总是 G 的一个自同构, 且 $\overline{G} = \{\sigma_x \mid x \in G\}$ 构成 $\mathrm{Aut}G$ 的一个子群, 如下交换图为我们给出了一个群同态:

这同态的核可计算如下:

$$\mathrm{Ker}\sigma = \{x \in G \mid \sigma_x(y) = y, y \in G\} = \{x \in G \mid \forall y \in G, xy = yx\}$$

最后一项被称为 G 的中心 C_G, 自然, $C_G = \{e\}$ 时, σ 构成一个单同态.

这作用也可衍生至 G 的幂集上, 具体而言, 则是依照集合乘法定义:

$$\sigma_x : \mathcal{P}(G) \to \mathcal{P}(G), A \to xAx^{-1}$$

这作用被称为共轭作用, 特殊的, 假若能为 $A, B < G$ 寻得 $x \in G$ 使得 $A = \sigma_x(B)$, 称 A, B 是共轭的.

不难察觉共轭变换的稳定子为:

$$\mathrm{St}(H) = \{x \mid xHx^{-1} = H\}$$

后一项, 当 $H < G$ 时也称为 H 的正规化子, 记作 $N_G(H)$.

共轭作用的轨道 Gs 被称为 G 的一个共轭类, 这时候的轨道分解公式便改写为

$$|G| = \sum_{s \in C} [G/\mathrm{St}(s)]$$

称为类公式, 另外的, 将轨道中的 $G_s(s \in C_G \Leftrightarrow Gs = \{s\})$ 剥离出来, 即得

$$|G| = |C_G| + \sum_{s \in C - C_G} [G/\mathrm{St}(s)]$$

平移

针对全体 $x \in G$, 定义相应的平移变换

$$L_x : G \to G, y \to xy$$

同样的, 针对 $A \subset G$, 可定义:

$$L_x : \mathcal{P}(G) \to \mathcal{P}(G), A \to L_x(A)$$

这变换实际上为我们指定了 $G/H, H < G$ 上的一个映射:

$$L_x : G/H \to G/H, aH \to xaH$$

这是 G 在 $\mathcal{P}(G), G/H$ 上的另一种作用.

平移作用的轨道与稳定子均是平凡的, 列举如下以待读者核验:

$$\mathrm{St}(s) = e, Gs = G$$

$$\forall H < G, \mathrm{St}(H) = H, GH = G$$

对称群

取定 $\sigma \in S_n$, 生成子群 $G = \langle \sigma \rangle$, 定义群作用 $\sigma^m \cdot i = \sigma^m(i)$, 自然可以取定最小的 r 使得 $\sigma^r(i) = i$, 于是我们要有 i_k 的轨道

$$Gi_k = \{i_k, \sigma(i_k), \cdots, \sigma^{r-1}(i_k)\}$$

取定 $\tau \in S_n$, 若 τ 对字符集 $I = \{i_1, \cdots, i_r\}$, 满足

$$\tau(i_k) = i_{k+1}, 1 \le k \le r-1, \tau(i_r) = i_1$$

$$\forall j \notin I, \tau(j) = j$$

则称 τ 是一个 r-轮换, 自然, 任意置换在其轨道上均是一个轮换, 而轮换又可被分解为 2-轮换, 也即对换, 从而我们能将置换分解为对换.

对换导致的逆序直接将置换其结果的逆序数相联系, 于是我们能够确信置换分解为对换的方式尽管不唯一, 得到的对换个数的奇偶性却是确定的, 从而我们能够产生基置换与偶置换的原则.

本着偶数与偶数之和仍然为偶数的原则, 我们能够声明全体偶置换构成一个群, 这群被称为交错群, 记作 A_n, 另外的, 应用高等代数中的方法, 我们能够确信:

$$|A_n| = \frac{1}{2}|S_n|$$

(有小朋友要问了, 阿这你写一堆文字说明糊弄证明算什么东西啊? 我非常讨厌组合学的东西, 看你不知道和你说一声)

定理 30 $A_n, n \geq 5$ 是单群.

Proof. 全 NM 一堆组合学, 自己找资料吧, 顺达一提拿这个结论还能说明 $S_n, n \geq 5$ 的非平凡正规子群只有 A_n. □

p 群与 Sylow 群

取素数 p, p 群是 $|G| = p^n$ 的群 G.

命题 31 p 群的非平凡子群为 p 群, p 群的中心为 p 群.

Proof. 命题的前一半根据 Lagrange 定理自然是成立的, 对于后一半, 证明 p 群的中心不是 $\{e\}$ 即可, 假若是, 察看类公式:

$$|G| = C_G + \sum_{s \in C - C_G} [G/\mathrm{St}(s)]$$

考虑到 $[G/\mathrm{St}(s)]$ 是 $|G|$ 的约数, 即得

$$p^n = 1 + \sum_{d | p^n} d$$

这显然是导致矛盾的. □

命题 32 取定有限 n 阶 Abel 群 G, 若 $p \mid n$, 则 G 中有 p 阶子群.

Proof. 采用归纳法证明, 对于 $n = 2$ 的情形, 命题是自然成立的, 假定命题对于 n 之前的数成立, 现在来察看 n 的情形.

取定 $a \in G$, $|a| = k$, 若 $p \mid k$, 则可取定 $b = a^{\frac{p}{k}}$, 自然 $\langle b \rangle$ 是 G 的一个 p 阶子群, 从而命题成立, 非如此, 从 G 是交换群, 至少有 $\langle a \rangle \lhd G$, 于是可生成群 $G/\langle a \rangle$, 其阶为 m, 一方面 $m < n$, 另外的

$$p \mid mk$$

之前假定了 $p \perp k$, 只能 $p \mid m$, 据归纳假设, 便能在 $G/\langle a \rangle$ 中取定元素 $g\langle a \rangle$, 其阶为 p, 这便说明着 p 是使得 $g^p \in \langle a \rangle$ 的最小整数, 这也便意味着

$$g^{kp} = e$$

此时, g^k 的阶, 要么为 1, 要么为 p, 其若为 1, 便知道着 g 的阶 p 将整除 k, 这是不可能的, 于是我们便找到了所需要的阶为 p 的元素 g^k, 这已经宣告着证明的结束. □

推论 33 阶为 p^n 的 p 群 G 总有 Abel 塔

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$$

特殊的, $|G_i/G_{i+1}| = p$, 因而这塔同时又是一个循环塔.

Proof. 前已证明 C_G 同样是 p 群, 这群又是交换的, 于是能找到其一阶为 p 的子群, 从而我们能够针对 $n = 1, 2$ 的情形证明这命题, 现在假定命题在 n 以下的情形成立, 察看 n 的情况:

同样的在 C_G 中取定了 G 的 p 阶子群 G_{n-1}, 由于 C_G 中的元素在 G 中是交换的, 故而 G_{n-1} 针对 G 中全体元素交换, 于是 $G \rhd G_{n-1}$, 这商群的阶为 p^{n-1}, 据归纳假设即可构造如下 Abel 塔:

$$G_0/G_{n-1} \rhd G_1/G_{n-1} \rhd \cdots \rhd G_{n-2}/G_{n-1} \rhd G_{n-1}$$

且满足着 $(G_i/G_{n-1})/(G_{i+1}/G_{n-1})$.

构造同态 $f : G_0 \to G_0/G_{n-1}$, 从上述群塔中我们便能得到同样为 Abel 塔的

$$G_0 \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd \{e\}$$

另外的, 从第一同构定理,

$$(G_i/G_{n-1})/(G_{i+1}/G_{n-1}) \simeq G_{i+1}/G_i$$

于是自然也有 $G_{i+1}/G_i = p$, 这便完成了我们的证明. □

命题 34 p 群 G 的真子群 K 严格包含于 $N_G(K)$ 中.

Proof. 针对 $n = \log_p |G|$ 进行数学归纳法, $n = 1$ 时 G 的真子群仅有 $\{e\}$, 其正规化子为 G 本身, 于是命题自然成立. 假定命题对 n 以下的情形成立, 现在来察看 n 的情况:

取定 G 的中心 C_G, 再取定真子群 H, 若 $H \subsetneq C_G \subset C_H \subset N_G(H)$, 则命题已经成立, 否则我们将要断言 $C_G \subset H$, 于是便能建立如下一个商群间的关系:

$$H/C_G < G/C_G$$

C_G 是 p 群, 故而 G/C_G 亦是 p 群, 依照归纳假设, 也便知道

$$H/C_G \subsetneq N_{G/c_G}(h/C_G)$$

这使得我们能够从 $G - H$ 中取定 g, 满足

$$gC_G(H/C_G) = (H/C_G)C_G g$$

即 $\{gh_iC_G\} = g(H/C_G) = (H/C_G)g = \{C_G h_i g\}$, 从中便知晓了 gH 与 Hg 的同一性.

这便宣告着证明的结束. □

将 $|G|$ 作质因分解如下:

$$|G| = \prod_{i=1}^{n} p_i^{\varepsilon_i}$$

假若能为 G 寻得子群 P, 使得 $|P| = p_i^{\varepsilon_i}$, 称 P 是 G 的一个 Sylow p 群.

定理 35 对 $|G|$ 的素因数 p, 总有 Sylow p 群存在.

Proof. 同样针对 $|G|$ 应用归纳法, $|G| = 2$ 时命题是自然成立的, 假定了命题在 n 以下的情况成立, 现在便来察看 n 的情形:

假若 $\forall H < G$, $p \mid [G : H]$, 考虑到类公式:

$$|G| = |C_G| + \sum_{x \in C - Z} [G : \mathrm{St}(x)]$$

于是必然 $p \mid |C_G|$, 而 C_G 作为一个交换群, 将能在其中取得 p 阶子群 H, 查看商群 G/H 及对应的自然同态 $f : G \to G/H$, 从归纳假设知道到存在 Sylow-p 群 K 于 $|G/H|$ 中, 满足

$$|K| = p^{\varepsilon - 1}, K = \{g_i H\}_{1 \le i \le |K|}$$

于是 $f^{-1}(K)$ 必然是 G 的子群, 与此同时同时, 按照下述的表法, 其阶必然为 p^{ε}:

$$f^{-1}(K)=\bigcup_{i=1}^{n}g_iH$$

至此我们完成了命题的证明. □

定理 36 (i) G 的 p 群总是 G 的某个 Sylow p 群的子群.

(ii) G 的 Sylow p 子群总是彼此共轭的.

(iii) G 的 Sylow p 子群的个数 n_p 总满足 $n_p\equiv 1 \pmod p$.

Proof. 取定 sylow p 群 u, 则自然

$$p\nmid [G:u]$$

而 $[G:u]=[G:N_G(u)][N_G(u):u]$, 后者与 G 上共轭作用的轨道 Gu 的阶是一致的, 于是我们知道

$$p\nmid |Gu|$$

另一方面, 取定一个 p 群 H, 我们能在 Gu 上指定共轭映射, 使得 Gu 成一 H 集, 以此再对 $|Gu|$ 作轨道分解, 即得

$$|Gu|=\sum_{\mathfrak{u}\in R_u}[H:\mathrm{St}(\mathfrak{u})]=\sum_{\mathfrak{u}\in R_u}[H:N_H(\mathfrak{u})]$$

一方面, $[H:N_H(\mathfrak{u})]$ 将 $|H|=p^k$ 整除, 于是 $[H:N_H(\mathfrak{u})]$ 要么为 1, 要么为 p 的幂, 另一方面, $p\nmid |Gu|$, 故而必然有 $\mathfrak{u}$ 使得

$$[H:N_H(\mathfrak{u})]=1\Rightarrow H=N_H(\mathfrak{u})$$

这便声明了 $\mathfrak{u}$ 中元素关于 u 均是交换的, 从而 $H<N_G(\mathfrak{u})$, 依照正规化子的性质, 将有

$$H\mathfrak{u}\lhd G,\mathfrak{u}\lhd H\mathfrak{u}$$

从第二同构定理, 这也即

$$H\mathfrak{u}/\mathfrak{u}\simeq H/H\cap\mathfrak{u}$$

式子右边自然是一个 p 群, 于是式子左边同样是一个 p 群, 这便说明着 $H\mathfrak{u}$ 同样是是一个 p 群 ($|H\mathfrak{u}|=|H\mathfrak{u}/\mathfrak{u}||\mathfrak{u}|$), 先天成立着 $\mathfrak{u}\subset H\mathfrak{u}$, 然而反向包含式的成立将使得 $\mathfrak{u}$Sylow p 群的性质破缺, 于是只能是 $\mathfrak{u}=H\mathfrak{u}$, 此刻, Sylow p 群 $\mathfrak{u}$ 将 p 群 H 包含了起来.

> 嗯嗯嗯?$\mathfrak{u}$ 什么时候变成 Sylow p 群了? 不难发现一个基本事实, $\mathfrak{u}$ 所属的 $R_u\subset Gu$ 成一 G 集, 而 Sylow p 群 u 经共轭作用后得到的仍然是 Sylow p 群, 所需证明的只是:
>
> (i) gug^{-1} 仍然成一群, 只需注意到下式:
>
> $$\forall gxg^{-1},gyg^{-1},gxg^{-1}gy^{-1}g^{-1}=gxy^{-1}g^{-1}\in gug^{-1}$$
>
> (ii) gug^{-1} 成一 Sylow p 群, 这只是
>
> $$x=y\Leftrightarrow gxg^{-1}=gyg^{-1}$$
>
> 的直接结果.
>
> 另外一个被遗漏的内容是对正规化子性质的唐突使用, 下面对这性质证明之:
>
> 若 $K<N_G(H)$, 则 $KH<G$, $H\lhd KH$
>
> **Proof.** 取 $k_1h_1,k_2h_2\in KH$, 自然
>
> $$k_1h_1(k_2h_2)^{-1}=k_1h_1h_2^{-1}k_2^{-1}=(k_1h_1)k_2^{-1}(k_2h_2^{-1}k_2^{-1})\in KH$$
>
> 于是 $KH<G$, 另外的,
>
> $$khHh^{-1}k^{-1}=kHk^{-1}=H$$
>
> 于是 $H\lhd K$. □

取定 Sylow p 群 u, v, u 作为 p 群, 自然在 Gv 的某个成员 $\mathfrak{v}$ 中, 然而 u 是 Sylow p 群, 故而只能 $u = \mathfrak{v}$, 从而 $u \in Gv$, 从而 u, v 共轭.

所有 Sylow p 子群间彼此共轭的事实向我们揭示了 Gu 遍历了全体 G 的 Sylow p 子群, 将其视为 u 集, 进行轨道分解, 得到

$$|Gu| = \sum_{\mathfrak{u} \in R_u} [u : N_u(\mathfrak{u})]$$

$[u : N_u(\mathfrak{u})]$ 要么为 1(且是唯一的), 要么为 p 的幂, 于是自然 $n_p = |G_u| \equiv 1 \pmod{p}$. □

> 你问我为什么? 考虑到 $N_u(v) = \mathrm{St}_u(v), v \in Gu$, 使得 $\mathrm{St}_u(v) = u$ 的集合 $v = gug^{-1}$ 必然针对全体 $u_0 \in u$ 满足
> $$u_0 gug^{-1}u_0^{-1} = gug^{-1}$$
> 这也便是
> $$u = (g^{-1}u_0 g)u(g^{-1}u_0^{-1}g)$$
> 从而 $g^{-1}u_0 g \in \mathrm{St}_u(u) = u$, 由于 u_0 任取, 这也便是 $g^{-1}ug = u$.
> 没啦, 已经证完了, 你没发现上面那个式子就是 $v = u$ 么?
>
> 所以我为什么特地注释这个小框框呢? 因为我卡了好几天, Silly Enough.

定理 37 取定有限集 G 以及 $N \lhd G$, 若 P 是 G 的一个 Sylow p 子群, 则 PN/N 是 G/H 的一个 Sylow p 子群, $P \cap N$ 是 N 的一个 Sylow p 子群.

Proof. 对于 PN/H, 依据第二同构定理知道

$$PN/N \simeq P/P \cap N$$

后者显然为一个 p 群, 从而 PN/P 同样是一个 p 群, 我们再来证明这群是 Sylow p 群:

取定自然同态 $f : G \to G/N$, 从定理 19 得到

$$[G/N : PN/N] = [G : PN]$$

注意到 $[G : PN]$ 自然是 $[G : P]$ 的因数, 然而从 P 的 Sylow p 群属性知道 $p \nmid [G : P]$, 于是

$$p \nmid [G : PN] = [G/N : PN/N]$$

从而 PN/N 的确是 G/N 的 Sylow p 子群.

$P \cap N$ 自然是 N 的 p 子群, 而我们可依照定理 29 将 $[N : P \cap N] = |N|/|P \cap N|$ 表出如下:

$$|PN| = \frac{|P||N|}{|P \cap N|} \Rightarrow \frac{|N|}{|P \cap N|} = \frac{|PN|}{|P|}$$

后一项作为 $[G : P]$ 的因子, 自然是不能被 p 整除的, 于是我们完成了命题的证明. □

有限生成的 Albel 群

以下给出群直积的三种等价定义: 取定群 G 的有限个子群 $\{A_i\}$, 若其满足条件 I/II/III, 称 G 是 $\{A_i\}$ 的直积, 记作

$$G = \prod_{i=1}^{n} A_i = A_1 \times \cdots \times A_n$$

Definition I:

(i) $G=\prod_{i=1}^{n}A_i=A_1\cdots A_n$

(ii) $\forall g\in G$, 表法 $g=\prod_{i=1}^{n}a_i$ 是唯一的.

(iii) $i\neq j$ 时, $a_ia_j=a_ja_i, a_i\in A_i, a_j\in A_j$

Definition 2:

(1) $G=\prod_{i=1}^{n}A_i=A_1\cdots A_n$

(2) G 中恒等元 e 表法唯一.

(3) $i\neq j$ 时, $a_ia_j=a_ja_i, a_i\in A_i, a_j\in A_j$

Definition C:

(a) $G=\prod_{i=1}^{n}A_i=A_1\cdots A_n$

(b) $\forall i, A_i\lhd G$

(c) $\left(\prod_{k=1}^{i}A_k\right)\cap A_{i+1}=\{e\}$

我们分别证明 Definition 2 与 Definition I, Definition C 与 Definition I 的等价性, 以此说明这三种定义等价.

I=2: 只需从 I 中推出 (2), 从 2 中推出 (ii), 前者是显然的, 对于后者, 取定 $g\in G$ 的如下两种表出:

$$g=\prod_{i=1}^{n}a_i, g=\prod_{i=1}^{n}a_i'$$

于是依据 A_i, A_j 间的交换性, 知道

$$e=gg^{-1}=\prod_{i}^{n}a_ia_i'^{-1}$$

考虑到 e 实际上只有唯一的一种如下表出:

$$e=\prod_{i=1}^{n}e_i$$

于是对应相等即得 $a_ia_i'^{-1}=e_i$, 也即 $a_i=a_i'$ 这便说明了 g 的表法的唯一性.

2=C: 只需从 (b), (c) 中推出 (2),(3), 从 (2),(3) 中推出 (b), (c) 即可.

对于前者, 依据 (3) 容易知道 $a_jA_i=A_ia_j$ 的成立, 这便说明了 $A_i\lhd G$, 也即 (b), 另外的, A_{i+1} 的元素 a_{i+1}, 若在 $\prod_{k=1}^{i}A_k$ 之中, 便立即可被如下的式子表出:

$$a_{i+1}=\prod_{k=1}^{i}a_k$$

也即

$$e = a_{i+1}^{-1} \prod_{k=1}^{i} a_k$$

考虑到 (2) 的成立, 即得 $a_{i+1}^{-1} = e$, 也即 $a_{i+1} = e$.

对于后者, 取定 e 的一个表法

$$e = \prod_{i=1}^{n} a_i$$

即得

$$a_n^{-1} = \prod_{i=1}^{n-1} a_i$$

考虑到 (c) 的意蕴, 便只能是 $a_n^{-1} = e$, 归纳之, 即知道 (2) 的成立. 至于 (3) 的成立, 期望证明如下等式:

$$a_i a_j a_i^{-1} a_j^{-1} = e$$

注意到如下改写以及 $A_i \lhd G$:

$$a_i a_j a_i^{-1} a_j^{-1} = (a_i a_j a_i^{-1}) a_j^{-1} = a_i (a_j a_i^{-1} a_j^{-1})$$

我们将能够知道 $a_i a_j a_i^{-1} a_j^{-1} \in A_i \cap A_j$, 再思 (c) 之涵义, 即能确信这乘积的结果是 e, 这便宣告了整个证明的结束.

现在在 Abel 群中改换符号, 我们将幺元记作 0, 运算记作 $+$.

取定 Abel 群 A, 若 $a \in A$ 的阶是有限的, 称 a 是挠元, 全体挠元组成 A 的一个子群 A_τ, 称为 A 的挠子群.

若 $A = A_\tau$, 称 A 是一个挠群, 自然, 有限生成的挠 Abel 群都是有限的, 只需注意到下面一个简单事实即可:

$$A = \langle S \rangle \Rightarrow A = \sum_{x_i \in S} k x_i$$

其中 k 的取值由于 x_i 均是挠元将是有限的, 于是自然得知 A 是有限的.

取定素数 p, 则对应的有 A 中如下子挠群:

$$A(p) = \{x \in A \mid |x| = p^m\}$$

从素数 p 的原子性, $A(p)$ 的一个生成群自然是 S 的如下子集:

$$S(p) = \{x \in S \mid |x| = p^k\}$$

从而 $|A(p)| = \prod_{x \in S(p)} |x|$ 自然是 p 的幂数, 因而 $A(p)$ 成一 p 群.

定理 38 有限 Abel 群 A 可被表为如下形式:

$$A = \bigoplus_{p, A(p) \neq \{e\}} A(p)$$

Proof. 将 $|A|$ 分解如下:

$$|A| = \prod_{i=1}^{n} p_i^{\varepsilon_i}$$

$n=1$ 的时候命题的成立正如张京华 ◯ 很大一样显然, 现在假定命题对 n 以下的情况成立, 现在来查看 n 的情形, 为此我们取:

$$m=p_n^{\varepsilon_n}, m'=\frac{|A|}{m}$$

自然 $m\perp m'$, 于是据 Bezout 定理可取定 $r,s\in\mathbb{Z}$ 使得

$$rm+sm'=1$$

从而有[1]

$$A=1\cdot A=(rm+sm')A\subset mA+m'A$$

现在我们再来证明 $A=mA\oplus m'A$, 为此只需要验证 $mA\cap m'A=0$, 取定 $\mathfrak{a}\in mA\cap m'A$, 于是

$$\mathfrak{a}=ma, \mathfrak{a}=m'a', a,a'\in A$$

从而有[2]

$$m'\mathfrak{a}=m'ma=|A|a=0$$

$$m\mathfrak{a}=mm'a'=|A|a=0$$

于是 $a=1\cdot a=(rm+sm')a=0$, 从而 $A=mA\oplus m'A$.

取定 $A_m=\{x\in A\mid mx=0\}$, 若 $m'a\in m'A$, 自然 $m(m'a)=|A|a=0$, 于是 $m'A\subset A_m$, 而若 $x\in A_m$, 则 $x=1\cdot x=(rm+sm')x=m'sx\in m'A$, 从而 $A_m\subset m'A$, 综上

$$A_m=m'A$$

自然有 $A_m=A(p_n)$, 于是

$$A=mA\oplus A(p_n)$$

对于剩余的 mA, 一方面其阶自然为 m', 另一方面从归纳假设其已可按定理所述的方式分解, 于是我们确定了命题针对 n 的情形成立, 至此全部的证明工作已完成. □

引理 39 取定非循环的有限 Abel p 群 A 中的元素 a, 要求这元素的阶在 A 中是极大的, 取定 $\bar{b}=b\langle a\rangle\in A/\langle a\rangle$, 若 $|\bar{b}|=p^r$, 则 $\bar{b}$ 中所有元素的阶均不小于 p^r, 且确有 $\mathfrak{b}\in\bar{b}$, $|\mathfrak{b}|=p^r$.

Proof. 假若存在 $b'\in\bar{b}$ 满足 $|b'|<p^r$, 立即有 $|b'|\bar{b}=|b'|b'\langle a\rangle=0\langle a\rangle=\bar{0}$, 这与我们假定的 $\bar{b}$ 的阶为 p^r 相矛盾, 于是 $\forall b\in\bar{b}, |b|\geq p^r$. 这同时也意味着我们若要证明 b 中确有阶为 p^r 的元素存在, 只需要找到 $\mathfrak{b}\in\bar{b}$, 使得 $p^r\mathfrak{b}=0$.

假若取定 $b\in\bar{b}$, 这样的 $\mathfrak{b}$ 应当可以被表为

$$\mathfrak{b}=b-ka$$

此刻 $p^r\mathfrak{b}=0$ 也便是 $p^rb=p^rka$, 故而只要能有合适的 $ka\in\langle a\rangle$, $\mathfrak{b}$ 的存在性便得到了证明.

根据我们的假设, $p^rb\in p^r\bar{b}=\langle a\rangle$ 也便意味着 $p^rb=na$, 再将 n 改写为 $n=p^\varepsilon\mu, \mu\perp p$, 于是式子变成了

$$p^\varepsilon\mu a=p^rka$$

[1] $x>y\Rightarrow yA\subset xA$ 这种比张京华 ◯ 很大还显然的事情不用我多说了吧?

[2] Huh? YOu ASk mE whY?oH, jUsT BEcauSe JinGhuA ZhAnG's bALls aRe sO bIG!

从 $\mu \perp p$, 自然 $|\mu a| = |a| = p^\alpha$, 这便意味着 $|p^r ka| = |p^\varepsilon \mu a| = p^{\alpha-\varepsilon}$, 从而 $\mathfrak{b}$ 的存在性最终只要求我们能够在 $\langle a\rangle$ 中找到阶为 $p^{\alpha-\varepsilon+r}$ 的 ka, 这样的 ka 的存在性只要求如下一个简单的不等式的成立:

$$0 \leq \alpha - \varepsilon + r \leq \alpha$$

左边的不等式, 从 $p^\alpha \geq \mu p^\varepsilon$ 便得到了证明, 对于右边的不等式, 注意到 $p^r b = p^\varepsilon \mu a$, 于是能够计算得到 $|b| = p^{\alpha-\varepsilon+r}$, 然而 $|a|$ 既已在 A 中极大, 便只能是

$$\alpha - \varepsilon + r \leq \alpha$$

这便是不等式的后半部分.

至此, $\mathfrak{b}$ 的存在性便是颠扑不破的了. □

若能将有限 Abel p 群 A 分解为如下阶为 p^{r_i} 的循环群 $\{A_i\}$, 称 $(p^{r_1}, \cdots, p^{r_n})$ 为 A 的类型.

$$A \simeq \bigoplus_{i=1}^{n} A_i$$

定理 40 有限 Abel p 群总可分解为有限个循环 p 群 A_i 的直和, 且生成的相应类型 $(p^{r_1}, \cdots, p^{r_n})$ 在不考虑顺序的前提下是唯一确定的.

Proof. 分解的存在性: A 循环的情况下命题是显然成立的, 其余情形则针对 $|A|$ 做归纳, 取定 A 中阶极大元素 a, 查看商群 $A/\langle a\rangle$, 其中的陪集从前一条引理总可取出一个与陪集本身同阶的元素作为代表元, 现在由于 $A/\langle a\rangle$ 的阶自然是小于 $|A|$ 的, 于是我们可做如下直积分解:

$$A/\langle a\rangle = \bigoplus_{i=1}^{n-1} A_i$$

其中, 针对各循环群 A_i 我们假定其生成元是 $\bar{a}_i$, 代表元的取法正如前所述, 于是, 当我们考虑 $x \in A$ 所生成的陪集 $\bar{x} = x\langle a\rangle$ 时, 有下述的式子成立:

$$\bar{x} = \sum_{i=1}^{n-1} k_i \bar{a}_i, k_i \in \mathbb{N}$$

从而我们知道

$$\overline{x - \sum_{i=1}^{n-1} k_i \bar{a}_i} = \bar{0} \Leftrightarrow x - \sum_{i=1}^{n-1} k_1 a_i \in \langle a\rangle = A_n$$

从而我们能够针对任意 $x \in A$ 声称 $x = \sum_{i=1}^{n} k_i a_i$, 也即

$$A = \sum_{i=1}^{n} A_i, A_i = \langle a_i\rangle$$

接下来我们再证明这是一个直和, 为此验证 0 的表法唯一, 查看式子:

$$\sum_{i=1}^{n} k_i a_i = 0 \Rightarrow \sum_{i=1}^{n-1} k_i \bar{a}_i = \bar{0}$$

而从 $\bar{A}_i$ 的直和属性来看, 自然得到 $\forall i \leq n-1, k_i \bar{a}_i = \bar{0}$ 从而 $|a_i| \mid k_i$, 即是 $k_i a_i = 0$, 于是上式也即

$$k_n a_n = 0$$

至此我们证明了所有的 $k_i a_i$ 均是 0, 这便说明了 0 的表法的唯一性, 因而 $\{A_i\}$ 确实构成一直和.

分解的唯一性: 同样对 $|A|$ 进行归纳, 假定 A 被按照如下两种形式分解:

$$A = \bigoplus_{i=1}^{n} A_i = \bigoplus_{j=1}^{m} B_j$$

相应的类型为 $(p^{r_1}, \cdots, p^{r_n}), (p^{s_1}, \cdots, p^{s_m})$, 不难验证 $pA < A$, 且有

$$pA = \bigoplus_{i=1}^{n} pA_i = \bigoplus_{j=1}^{m} pB_j$$

相应的类型指数变为 $(p^{r_1-1}, \cdots, p^{r_n-1}), (p^{s_1-1}, \cdots, p^{s_m-1})$.

此刻依照归纳假设, 序列 $\{r_1 - 1, \cdots, r_n - 1\}, \{s_1 - 1, \cdots, s_m - 1\}$ 中的非零部分是一致的, 这便意味着 $(p^{r_1}, \cdots, p^{r_n})$, $(p^{s_1}, \cdots, p^{s_m})$ 中大于 p 的部分是一致的, 而对于等于 p 的部分, 考虑到

$$|A| = \prod_{i=1}^{n} p^{r_i} = \prod_{j=1}^{m} p^{s_i}$$

其自然也是全同的. □

群 A 中若是只有 $\{e\}$ 是有限阶的, 称 A 是无挠或挠自由的.

定理 41 无挠的有限生成 Abel 群必然可以被唯一分解为有限个无限循环群的直和.

Proof. 取定 A 的生成元集 S, 将其视为一个 $\mathbb{Z}$-模, 取定其中极大整系数线性无关向量组 $\{x_1, \cdots, x_n\}$, 挪用我们在线性空间上的结论, 能够确信这些极大整系数线性无关组的向量个数是一致的, 且通过整系数线性组合将能把 S, 进而 A 中的元素表出, 这便声明了

$$A = \sum_{i=1}^{n} \langle x_i \rangle$$

另外的, 考虑到 $\{x_1, \cdots, x_n\}$ 的线性无关属性, 任何的表法

$$\sum_{i=1}^{n} k_i x_i = 0$$

将唯一地指向 $k_i = 0$, 于是 $k_i x_i$ 为 0, 于是 0 的表法唯一, 也即

$$A = \bigoplus_{i=1}^{n} \langle x_i \rangle$$

□

定理 42 取定有限生成的 Abel 群 A, $A_{\mathcal{T}}$ 是 A 的挠子群, 则挠自由群 $A/A_{\mathcal{T}}$ 在同构意义上唯一确定了一个使得

$$A = A_{\mathcal{T}} \oplus A/A_{\mathcal{T}}$$

成立的挠自由群 B.

Proof. 取定 $\bar{x} \in A/A_{\mathcal{T}}$, 若 $m\bar{x} = \bar{0}$, 自然 $mx \in A_{\mathcal{T}}$, 后者的元素全是挠元, 故而可取定 q 使得 $qmx = 0$, 这便说明了 x 是 A 的挠元, 从而只能 $\bar{x} = \bar{0}$, 故 $A/A_{\mathcal{T}}$ 是无挠的, 则据上一条定理我们将能把 $A/A_{\mathcal{T}}$ 分解为直和:

$$A/A_{\mathcal{T}} = \bigoplus_{i=1}^{n} \langle \bar{a_i} \rangle$$

取定

$$B = \bigoplus_{i=1}^{n} \langle a_i \rangle$$

$\bar{a_i}$ 无限阶, a_i 便也是无限阶的, 故 B 是挠自由的, 下面验证 $A = A_{\mathcal{T}} \oplus B$:

取定 $a \in A$, 自然 $\bar{a}$ 可被表为:

$$\bar{a} = \sum_{i=1}^{n} k_i \bar{a}_i$$

这也便是

$$a = a_0 + \sum_{i=1}^{n} k_i a_i, a_0 \in A_{\mathcal{T}}$$

故而 $a = a_0 + b, a_0 \in A_{\mathcal{T}}, b \in B$, 又 $A_{\mathcal{T}}$ 中元素阶数有限, B 是无挠的, 两者交集只能是 $\{0\}$, 于是直和成立.

对于唯一性, 对于满足 $A = A_{\mathcal{T}} \oplus B'$ 的无挠子群 B', 容易证明 $B \simeq A/A_{\mathcal{T}}$, 于是各个 B 在同构意义上是唯一的. □

现在, 我们便得到了本节的顶点:

推论 43

有限生成的 Abel 群可唯一地分解为循环 p 群与无限循环群的直和.