抽象代数-群论 整理

子群，陪集，Lagrange定理

正规子群，商群，正规化子，中心化子，换位子子群，导群

循环群总结

1. 循环群的分类

2. 有限阶循环群的子群

无限阶循环群$\mathbb{Z}$的子群是$l\mathbb{Z}$（$l \geq 0$）

有限阶有如下性质：设$G = \langle a \rangle$是n阶循环群，则有：

- 阶数公式：$\mathrm{ord}(a^k) = \frac{\mathrm{ord}(a)}{(n,k)}$，证明是Bezout等式.
- 生成元：a^k是生成元，当且仅当$(n,k) = 1$（由阶数公式立刻得到）
- 生成元的个数：$\varphi(n)$
- d阶元的个数：d是n的因子，则G有$\varphi(d)$个d阶元（$ord(a^k) = d$当且仅当$(n,k) = \frac{n}{d}$也就是$k = \frac{ln}{d}$且$(l,d) = 1$，这样的l有$\varphi(d)$个.
- d阶子群存在唯一：d是n的因子，则G有唯一d阶子群. $\langle a^{n/d} \rangle$是d阶子群，而任何d阶子群中的元素必然形如$a^{ln/d}$.

同态基本定理

1. 群同态的性质

- 保幺，保逆
- 核是正规子群，像是子群
- $f : G_1 \to G_2$同态，有如下对应：
  - $H_1 \leq G_1 \Rightarrow f(H_1) \leq G_2$
  - $H_2 \leq G_2 \Rightarrow f^{-1}(H_2) \leq G_1$.
  - $N_2 \lhd G_2 \Rightarrow f^{-1}(N_2) \lhd G_1$.
  - $N_1 \lhd G_1$，一般没有$f(N_1) \lhd G_1$，若f是满同态，则此事成立.
  - $f^{-1}f(H_1) = H_1 \ker f$，$f(f^{-1}(H_2)) = H_2 \cap \mathrm{Im} f$.
  - 同构保所有的结构，保阶，保正规子群结构，等等.

2. 同态基本定理

- 同态基本定理$G/\ker f \cong \mathrm{Im} f$.
- 商群的商群：考虑同态$f : G/N \to G/K$，则$(G/N)/(K/N) \cong G/K$（用同态基本定理）
- $H \leq G$，$N \lhd G$，考虑同态：H嵌入G，再商同态到G/N.

  则$\ker f = H \cap N$，$\mathrm{Im} f = \{\overline{h} \in G/N : h \in H\} = HN/N \leq G/N$.

  同态基本定理$H/(H \cap N) \cong HN/N$.
- 商同态的泛性质：G是群，$N \lhd G$，$f : G \to H$是群同态，满足$f(N) = 1$.

  则存在唯一的g是群同态：$G/N \to H$，使得$f = g \circ \pi$.

  （意思就是，所有满足$f(N) = 1$的同态都是从π上长出来的）

  泛性质的抽象语言：$\mathrm{Hom}_{\mathrm{Grp}}(G/N, H) = \{f \in \mathrm{Hom}_{\mathrm{Grp}}(G, H) : f(N) = 1\}$.

  此同构是典则的.

3. 自同构群，内自同构群

- 考虑$\mathrm{Hom}_{\mathrm{Grp}}(G_1, G_2)$.
  - 若G_2Abel，则它具有Abel群结构，其幺元为平凡同态，乘法由逐点乘给出.
  - 若$G_1 = G_2$，则$\mathrm{Hom}_{\mathrm{Grp}}(G, G)$在复合下构成含幺半群$(\mathrm{Hom}_{\mathrm{Grp}}(\mathrm{G}, \mathrm{G}), \circ)$，其乘法可逆元组成的集合是该含幺半群中的自同构群$\mathrm{Aut}(G)$.
- **命题** $\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}, G) = G$，其中典则双射为$f \mapsto f(1)$，由1是生成元可知单射，通过构造可知映满.

  若G是Abel群，则$\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}, G)$在逐点乘运算下具有Abel群结构，此时上面的**典则双射是一个Abel群同构**.

  特别地，取$G = \mathbb{Z}$，$\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}, \mathbb{Z}) = \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}) = \mathbb{Z}$.

  对于加法，$\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}) = \mathbb{Z}$是Abel群同构.

不仅如此，还可以考虑复合，对于复合，$\mathrm{End}_{\mathbb{Z}}(\mathbb{Z})=\mathbb{Z}$也保乘，即左边的复合对应右边的整数乘法.（保含幺半群结构）

总结来说，$\mathrm{End}_{\mathbb{Z}}(\mathbb{Z})=\mathbb{Z}$一个作为环的同构.

特别地，左边的自同构群对应右边乘法可逆元组成的集合，所以有：

$$\mathrm{Aut}(\mathbb{Z})=\{\pm 1\}.$$

- **命题** 前面：用商同态的泛性质，$\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}/n\mathbb{Z},G)=\{f\in\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}/n\mathbb{Z},G),f(n\mathbb{Z})=1\}$.

  这里还有：$\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}/n\mathbb{Z},G)=\{G\text{中的}n\text{阶元}\}$

  典则双射为$f\mapsto f(\bar{1})$.

  若G为Abel群，则左边是Abel群，而右边：G中的n阶元在G的乘法下成为了G的一个子群，所以，这是一个Abel群同构.

  取$G=\mathbb{Z}/n\mathbb{Z}$得到的一个**重要结果**：

  $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z})$和$\mathbb{Z}/n\mathbb{Z}$作为环相等.

  所以

  $$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})=(\mathbb{Z}/n\mathbb{Z})^{\times}$$

  【例，结合后面的群作用】G是奇数阶群，有5阶正规子群N，则N必然在$Z(G)$内.

  【证明】考虑G在子群N上的共轭作用，因为N是正规子群，所以G作为$\mathrm{Aut}(N)$中的元素作用在N上，这给出了群同态$f:G\to\mathrm{Aut}(N)$. 因为5阶群必为循环群，所以$\mathrm{Aut}(N)=\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$，而$\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})=(\mathbb{Z}/5\mathbb{Z})^{\times}\cong\mathbb{Z}/4\mathbb{Z}$，所以$|\mathrm{Aut}(N)|=4$. 根据同态基本定理以及Lagrange定理，从奇数阶群到4阶群的群同态只有平凡同态，所以G在N上的作用平凡，即$\forall g\in G,n\in N$，$gng^{-1}=n$，所以$N\subset Z(G)$.

- 内自同构群. 乘法由复合给出. $\mathrm{Inn}(G)\lhd\mathrm{Aut}(G)$

  命题：考虑$\varphi:G\to\mathrm{Aut}(G),a\mapsto\varphi_a$.

  则$\mathrm{Im}\varphi=\mathrm{Inn}(G)$，$\ker\varphi=Z(G)$.

  所以：$G/Z(G)\cong\mathrm{Inn}(G)$.

对称群

1. Cayley定理

任何群G，G同构于其底集上的一个置换群（即对称群的一个子群）

证明是构造著名的Cayley同态$G\to S_G$，$a\mapsto L_a$. 则$G\cong\mathrm{Im}L$.

【例】G是$2k$阶群，k为奇数，则G必然含有k阶正规子群.

【证明】考虑Cayley同态，$G\cong\mathrm{Im}\rho$. 因为G是偶数阶群，所以必然有二阶元a，由此可以构造一个L_a是k个不交对换之积，从而L_a是一个奇置换. 从而$L_a\notin A_{2k}$，根据指数为2的正规子群的性质可知$\mathrm{Im}\rho\cap A_{2k}$是$\mathrm{Im}\rho$中的指数为2的正规子群，群同态拉回得到$G$的$k$阶正规子群.□

2. 一些简单性质

- k-循环的不同表示，k-循环的逆
- 不交的循环彼此交换
- S_n中的任何元素可以写成**不交循环的复合**. 且分解方法（不计次序）唯一. 其具体的操作方法为：追踪一个元素的变化.
- **用循环分解读出阶**：用循环分解表示S_n中的元素后，假设是m个不交循环的复合，其长度从大到小为$k_1\geq\cdots\geq k_m$，$k_1+\cdots+k_m=n$，则其ord可以直接读出来是$lcm(k_1,\cdots,k_m)$.

  由其循环分解唯一确定出的 partition of n称为是该置换的型.

3. S_n中元素的共轭

- 观察：$\sigma\tau\sigma^{-1}(\sigma(i)) = \sigma(\tau(i))$.
- 若τ为$k-$循环$(i_1\cdots i_k)$，则$\tau(i_1)=i_2$，所以$\sigma\tau\sigma^{-1}(\sigma(i_1))=\sigma(i_2)$，以此类推可得$\sigma\tau\sigma^{-1}=(\sigma(i_1)\cdots\sigma(i_k))$，于是$\sigma\tau\sigma^{-1}$也是$k-$循环.
- 因为任何一个置换可唯一（不计次序，即型的唯一）地写成不交循环的乘积：

  $$\tau=\tau_1\cdots\tau_m.$$

  所以$\sigma\tau\sigma^{-1}=(\sigma\tau_1\sigma^{-1})\cdots(\sigma\tau_m\sigma^{-1})$.

  注意到$\sigma\in S_n$是双射，所以不交循环做共轭后仍然是不交循环，因此$\sigma\tau\sigma^{-1}$和τ具有相同的型.

  反之，具有相同的型的两个置换必然是共轭的.
- **定理** 型是S_n中元素的共轭不变量，事实上，S_n中的两个置换共轭当且仅当它们的型相同.
- **定理（S_n中的元素按型划分）**
  - S_n中元素的型就是其共轭类. 所以$\{S_n$ 中的共轭类$\}$与$\mathcal{P}(n)$之间是一个一一对应.
  - S_n中的类方程：按型划分. 例如S_4元素的型有$(4),(3,1),(2,2),(2,1,1)(1,1,1,1)$，个数分别为$3!=4$，$4\times 2!=8$，$3$，$C_4^2=6$，$1$.

    $24=4+8+3+6+1.$

    S_n的类方程可以显式写下，注意到正规子群一定是一些共轭类的不交并. S_4正规子群的阶一定是类方程中一些数字的和，且有限制：①要含有1，②要整除24.

    观察可知非平凡的情况只可能有$8+3+1=12$和$3+1=4$，所以，S_4至多两个非平凡的正规子群，事实上的确如此（分别是A_4和K_4）.

4. S_n的生成元和奇偶性

- 生成元组可以是：
  1. 所有的对换（因为k循环显然可以一步步写成对换的积）
  2. $(12),(23),(34),\cdots(n-1,n)$（因为所有的对换可以写成它们的积，对$j-i$用数学归纳法）
  3. $(12),(13),(14),\cdots,(1,n)$（注意$(13)=(23)(12)$）.
  4. $(12\cdots n),(12)$
- **命题** $N\lhd S$包含一个对换，则$N=S$.【证明】所有的对换型相同从而都共轭，因为$N\lhd S$，所以N包含所有对换，而所有对换生成S，所以$N=S$.
- 置换的奇偶性定义：$\sigma\in S_n$诱导了$P\in GL_n(\mathbb{Q})$，P是只在$(\sigma(i),i)$这n个位置是1，其他位置都是0的置换矩阵. 则显然有$(x_1\cdots x_n)P(\sigma)=(x_{\sigma(1)}\cdots x_{\sigma(n)})$（将它形式上看成一个线性变换），还有$(x_1\cdots x_n)P(\sigma)P(\tau)=(x_1\cdots x_n)P(\sigma\tau)$.

  将置换的符号定义成$\det P(\sigma)\in\{\pm1\}$. 有一个同态$sgn: S_n\to\{\pm1\}$，$sgn(\sigma):=\det P(\sigma)$.
- 交错群A_n：$\ker sgn=A_n$，即所有偶置换组成的集合.
- 一些性质：
  - $A_n\lhd S_n$且$[S_n:A_n]=2$.
  - 对换是奇置换.
  - k循环的奇偶性和k的奇偶性相反.
  - 乘法与奇偶性规律.
  - A_n是S_n中唯一的指数为2的正规子群.【证明】假设N也是，去证明$A_n\subseteq N$. 置换总能写成对换之积，因为对换是奇置换，所以偶置换总是可以写成偶数个对换之积. 注意到N是指数为2的正规子群，所以它不含任何对换，根据指数为2正规子群的性质，任何两个对换的乘积在N中，从而任何偶数个对换之积在N中，从而所有的偶置换在N中，从而A_n在N中.
- 另一些性质：
  - $n\geq 3$时$Z(S_n)=1$.

- A_n为单群（$n \geq 5$）
- $n \geq 2$时$[S_n, S_n] = A_n$.
- 当$n \geq 5$时，S_n的正规子群只有$S_n, A_n, 1$.
- 把S_n中的对换送到对换的自同构必为S_n的一个内自同构.（考虑自同构在生成元上的取值，结合它是同构得到$\sigma(1i) = (ab_i)$，其中$a, b_2, \cdots, b_n$是$\{1, \cdots, n\}$的一个排列. 注意内自同构必将对换送到对换，以及内自同构群同构于$\mathrm{Inn}(S_n) \cong S_n/Z(S_n) = S_n (n \geq 3)$，而这里得到把对换送到对换的自同构至多有$n!$个，比较阶数可得结论.

- 一些例子
  - 例1 素数阶循环群是单群，**Abel单群只能是素数阶群**.
  - 例2 若G是非Abel 单群，则$Z(G) = 1$且$[G, G] = G$，特别地，G不可解.（由单群可知$Z(G) = G$或1，而G的情况由非Abel 排除. 类似地$[G, G] = 1$的情况也被非Abel排除）

群作用（本次课程没有涉及组合数学计数问题）

1. 两种定义和一些基本的例子

- $*$定义：G是群，X是集合，定义一个映射$* : G \times X \to X$，$(a, x) \mapsto a * x$，满足两个条件：
  - 1. $1 * x = x$ for all $x \in X$.
  - 2. $g_1 * (g_2 * x) = (g_1 g_2) * x$.

  则称映射$*$是群G对集合X的一个作用.
- 同态版本定义：G是群，X是集合，S_X是X的对称群（全体$X \to X$的双射构成的群）.

  若映射$\rho : G \to S_X$是一个群同态，则说ρ定义了G在X上的一个作用.
- 两种定义是等价的.
- 一些自然的例子：
  - $* : S_n \times \{1, 2, \cdots, n\} \to \{1, 2, \cdots, n\}$，$\sigma * i = \sigma(i)$.（自然的作用）

    同态版本：$\rho : S_n \to S_n$，$\sigma \mapsto \sigma$，这是个恒等自同构.
  - $* : D_n \times V(n) \to V(n)$. 其中$D_n$的群元素作为保正$n$边形的正交变换作用在正$n$边形的顶点集$V(n)$.

    同态版本：$\rho : D_4 \to S_4$，将D_4的群元素送到由它实现的顶点集V_4上的置换.

    计算可得$\mathrm{Im}\rho$是S_4中的一个八阶子群.（计算方法：考虑ρ在D_4生成元a, b上的取值即可）
  - 线性代数里的例子：设V是F-线性空间，$* : \mathrm{GL}_F(V) \times V \to V$，$\varphi * v := \varphi(v)$，其中$\varphi$是线性映射.这个例子是群元素作为线性映射作用在$V$中的向量上.

    同态版本：$\rho : \mathrm{GL}_F(V) \to S_V, \varphi \mapsto \varphi$，其中左边的$\varphi$是群元素（是一个可逆线性变换），而右边的$\varphi$是$\varphi$作为集合$V$上的双射出现的. 也就是右边的$\varphi$忘记了$V$上的线性空间结构.

    所以，这里的ρ是一个单同态.

- 一些用的很多的例子：
  - **群G对自身的左作用**（或：Cayley同态）：

    $* : G \times G : a * x \mapsto ax$.

    同态版本即Cayley同态：$\rho : G \to S_G$，$a \mapsto (x \mapsto ax)$，或者$a \mapsto L_a$.

    Cayley同态是忠实作用. 这是因为$L_a = id \Rightarrow a = 1$. $\ker \rho = \{a \in G, L_a = id\} = 1$.

    Cayley同态是传递的，其轨道为整个G.

    G中任何元素g的稳定化子都是G的平凡子群1.

    【例】（回忆：Cayley定理）：G同构于其底集G上的一个置换群（即对称群的一个子群）

    证明方法是构造Cayley同态：$\rho : G \to S_G$，$a \mapsto L_a$，则由$\ker \rho = 1$可知ρ是单同态，根据同态基本定理可得$G \cong \mathrm{Im}\rho \leq S_G$.
  - **群G对自身的共轭作用**：

$*: G\times G: a*x\mapsto axa^{-1}$.

同态版本：$\rho: G\to S_G, a\mapsto \varphi_a$.

这里的φ_a是一个G的自同构，事实上是G的内自同构.

所以$\mathrm{Im}\rho=\mathrm{Inn}(G)$.（这就是内自同构群的定义）

【注】群G对自身的共轭作用是一个"保群结构"的作用，φ_a是一个群同构. 类似的情况还有$\mathrm{GL}_F(V)$作用在V上，则对应的$\mathrm{Im}\rho\subset \mathrm{GL}_F(V)$，即该作用是以可逆线性变换作用在$V$上的.

轨道：这个群作用非传递，其轨道为$\mathrm{Conj}_G(x)$，即x所在的$G-$共轭类.

（注意："同轨道关系"是一个等价关系，共轭也是等价关系）

稳定化子： 因为$axa^{-1}=x$当且仅当$a\in Z_G(x)$，所以$\mathrm{Stab}_G(x)=Z_G(x)$.

轨道-稳定化子公式： $|\mathrm{Conj}(x)|=[G:Z_G(x)]$.

【注】在做题时，群对自身的共轭作用的O-S公式常和类方程一起使用：

$$|G|=|Z(G)|+\sum_{x\in\Sigma'}|\mathrm{Conj}(x)|=|Z(G)|+\sum_{x\in\Sigma'}[G:Z_G(x)]$$

这里Σ'表示的是$\Sigma-Z(G)$，Σ为共轭类的代表元集，Σ'是除了中心元以外的共轭类代表元集.

- **群G对自己子群的共轭作用**：

  星作用：$*: G\times\{H: H\le G\}$，$g*H=gHg^{-1}$.

  轨道：以H的共轭子群为元素的集合$\mathrm{Conj}(H)$.

  稳定化子：$N_G(H)$.

  轨-稳公式：$|\mathrm{Conj}(H)|=[G:N_G(H)]$.

  【例】特别地：

  1.H的共轭子群的个数：$|\mathrm{Conj}(H)|=[G:N_G(H)]$.

  2.H是G的正规子群$\Leftrightarrow$ H的共轭子群只有本身$\Leftrightarrow|\mathrm{Conj}(H)|=1\Leftrightarrow G=N_G(H)$.

- **群G在商集上的作用**：

  $*: G\times(G/H)$，$a*[bH]=[abH]$.

  形式上：很像左作用.

  由这个作用也给出G到G/H的对称群S_X的同态$\rho: G\to S_X$.

  【例1】

  $\ker\rho=\{x\in G,[xaH]=[aH],\forall a\in G\}=\{x\in G,a^{-1}xa\in H,\forall a\in G\}=\bigcap_{a\in G}aHa^{-1}\lhd G$

  【例2】$[G:H]=m$，令$\ker\rho=N$，则有：

  1. $N\le H$.（事实上，N是含在H内的G的最大正规子群）
  2. $G/N\cong\mathrm{Im}\rho$，所以$[G:N]=|\mathrm{Im}\rho|$整除$|S_X|=m!$.

  【例3】$n\ge 5$，H是S_n的子群且$H\ne A_n$，$H\ne S_n$，则$[S_n:H]\ge n$.

  【证明】由例2，存在$N\lhd S_n$，使得$N\le H$，所以$N=1,A_n$或S_n，又因为$H\ne A_n$且$H\ne S_n$，所以$N\ne A_n$且$N\ne S_n$，所以$N=1$，所以$[S_n:N]=|S_n|$，所以$|S_n|$整除$[S_n:H]!$，所以$n!|[S_n:H]!$，所以$[S_n:H]\ge n$.□

  轨道：此作用传递，轨道都是G/H.

  G/H**中元素**$[H]$**的稳定化子**为H.其他点的稳定化子是H的一个共轭子群.

2.轨道和稳定化子的概念

- **轨道**：G作用在X上，定义X上二元关系$x_1 \sim_G x_2 \Leftrightarrow$存在$g \in G$使得$g * x_1 = x_2$.
  - 容易验证是等价关系.
  - 等价类称为轨道，记作O_x，x为代表元.
  - 称群作用是**传递的**，如果只有一个轨道.
  - 例如，$\mathrm{Isom}^+(C)$作用在$V(C)$上传递.这是因为“上面”的四个顶点可用旋转轴彼此送到，而“侧面”和“下面”的也可以彼此送到，所以8个顶点位于同一个轨道.
- **稳定化子**：G作用在X上，G中元素g称为G的稳定化子，如果$g * x = x$对任何$x \in X$成立.
  - 稳定化子$\mathrm{Stab}_G(x)$是G的子群.
  - 轨道-稳定化子公式，$H := \mathrm{Stab}_G(x)$，则H-陪集合的个数$[G:H]$和轨道中元素的个数$|O_x|$是相等的.（证明：考虑映射$f: G \to O_x, g \mapsto g * x$的纤维）.
  - 例如，$\mathrm{Isom}^+(C)$作用在$V(C)$上，任取一个顶点$x \in V(C)$，则其稳定化子是穿过x的那条旋转轴对应的三个旋转变换，即$|\mathrm{Stab}_G(x)| = 3$，所以x所在轨道$|O_x| = [\mathrm{Isom}^+(C) : \mathrm{Stab}_G(x)] = 8$. 即8个顶点在同一个轨道上.

3.群作用例题

【例1】$g \in G$，$g * x$的稳定化子$\mathrm{Stab}_G(g * x) = g\mathrm{Stab}_G(x)g^{-1}$.

注：在轨道-稳定化子公式中，$|O_x| = [G : \mathrm{Stab}_G(x)]$，而同轨道关系是等价关系，而我们知道一个子群和他的共轭子群元素个数一样，所以，选取不同的代表元用轨道-稳定化子公式来数轨道中的元素结果是一样的.

【例2】G作用在X上，$x \in X$.

设$H = \mathrm{Stab}_G(x)$，$H' = aHa^{-1}$为H的一个共轭子群，则：

$$\#\{x' \in O_x : \mathrm{Stab}_G(x') = H'\} = [N_G(H) : H].$$

即：O_x中恰好有$[N_G(H) : H]$中个元素的稳定化子等于某个共轭子群.

【提示】关键要用到$\mathrm{Stab}(g * x) = gHg^{-1}$.

【例3】N在$\mathrm{Conj}_G(n)$上的共轭作用.

$N \lhd G$，$n \in N$，$\mathrm{Conj}_G(n)$在N中未必还是共轭类，一般地，它将恰好分裂为$\frac{|Conj_G(n)|}{|Conj_N(n)|}$个$N-$共轭类，且每个共轭类的元素个数都相等，都等于$|\mathrm{Conj}_N(n)|$.

【提示】对$\mathrm{Conj}_G(n)$中的任何元素，其$N-$共轭类就是该作用的轨道，其稳定化子为$Z_N(n)$的一个共轭子群.由轨道-稳定化子公式可以数出$N-$共轭类中元素个数是$|\mathrm{Conj}_N(n)|$.

【例4】G作用在X上，给出$\rho : G \to S_X$同态，若为单同态，则每个置换都对应G中的一个唯一元素（由G中的唯一元素实现）. 这称为G作用在X上是忠实的.

可以造出一个忠实作用：$\overline{\rho} : G/\ker\rho \to S_X$，则这是单同态.

一个很好的例子如下：

$\mathrm{GL}_F(V)$作用在V上，这诱导了它在V的全体一维线性子空间构成的集合$\mathbb{P}(V)$上的一个作用.具体而言后者是

$$\mathbb{P}(V) = \{\ell \subset V, \dim\ell = 1\}.$$

称为V的“射影空间”.

$$\begin{aligned}\ker\rho &= \{\varphi \in GL_F(V) : \varphi(l) = l, \forall l \in V, \dim l = 1\} \\ &= \{\varphi \in GL_F(V) : \forall\alpha \in V, \alpha \neq 0, \exists\lambda \in F, \varphi(\alpha) = \lambda\alpha\} \\ &= \{\lambda id_V : \lambda \in F^\times\}.\end{aligned}$$

（第二个等号是因为：l是φ的一维不变子空间当且仅当是φ的特征子空间当且仅当是φ的特征向量张成的一维子空间，第三个等号是因为：任何非零向量都是φ的特征向量，当且仅当φ是纯量阵.）

所以$GL_F(V)/\ker\rho=PGL_F(V)$忠实地作用在$\mathbb{P}(V)$上.

Sylow 定理

1.$p-$群相关整理

- **p群的中心非平凡.**

  【证明】考虑$p-$群按共轭类划分的类方程：

  $$|G|=|Z(G)|+\sum_{x\in\Sigma'}|Conj_G(x)|=|Z(G)|+\sum_{x\in\Sigma'}[G:Z_G(x)].$$

  $x\in\Sigma'\Rightarrow x$非中心元$\Rightarrow[G:Z_G(x)]>1$.

  因为G是$p-$群，由拉格朗日定理可知存在$l\geq 1$使得$[G:Z_G(x)]=p^l$.

  所以p整除$\sum_{x\in\Sigma'}[G:Z_G(x)]$，又因为$p$整除$|G|$，所以$p$整除$|Z(G)|$，故$|Z(G)|$非平凡，事实上$Z(G)$必是$p$的一个幂次$p^i(i\geq 1)$.

  【remark】承认p群的中心非平凡后，再根据Lagrange定理即可看出$Z(G)$的阶必然是p的一个幂次.

- p^2阶群必然是Abel群.

- p群作用的性质.

  - 群作用的不动点集X^G：

    $x\in X^G$ 当且仅当 $g*x=x,\forall x\in G$ 当且仅当$Stab_G(x)=G$ 当且仅当 O_x是单点集x.

  - 若G是$p-$群，作用在集合X上，则有：

    1. $|X|$**与**$|X^G|$**模**p**同余.**
    2. 特别地，若p不整除$|X|$，则群作用必有不动点即$X^G\neq\varnothing$
    3. 特别低，若群作用有唯一不动点，则必有$|X|$模p余1.

    【证】按同轨道划分的类方程为：

    $$|X|=\sum_{x\in\Sigma}|O_x|=|X^G|+\sum_{x\in\Sigma'}[G:Stab_G(x)].$$

    因为G是$p-$群，所以$[G:Stab_G(x)]=p^l\ (l\geq 1)$（由Lagrange定理），所以$p$整除右边的一项，所以$|X|$和$|X^G|$模$p$同余.

    【remark】这个证明是$p-$群中心非平凡的拓展，即把类方程推广到了一般的$p-$群作用情形.

- p群的一些不常用性质（都使用p群的中心非平凡推出）

  【例1】G是$p-$群，N是G的非平凡正规子群，则$N\cap Z(G)$非平凡.

  注：N也是p群，所以N的中心$Z(N)$非平凡，注意到$N\cap Z(G)$包含$Z(N)$，所以非平凡.

  【例2】若H是G的真子群，则H是$N_G(H)$的真子群.

  注：**降阶+数学归纳法.** 对$|G|=p^m$中的幂次m用数学归纳法，假设对$1\leq n\leq m-1$的任何n，命题都已经成立.

  ①若G的中心不含在H内，则存在中心元x但是不在H内，此时$xHx^{-1}=H$，所以$x\in N_G(H)$，所以H是$N_G(H)$的真子群.

  ②若G的中心在H内，因为$Z(G)$在G中正规，所以在H中也正规，考虑$H/Z(G)$，则比较阶数可知，$H/Z(G)$是$G/Z(G)$的真子群.因为$G/Z(G)$也是$p-$群且阶严格小于G，所以可以用归纳假设得到$H/Z(G)$是$N_{G/Z(G)}(H/Z(G))$的真子群，用第6周作业题4可得$N_{G/Z(G)}(H/Z(G))=N_G(H)/Z(G)$. 所以$H/Z(G)$是$N_G(H)/Z(G)$的真子群，再比较阶数可得$|H|<|N_G(H)|$即$H$是$N_G(H)$的真子群.

  【例3】$|G|=p^m$，则G的$m-1$阶子群必正规.

注：考虑指数传递性即得$[G:N_G(H)]=1$也就是$G=N_G(H)$.

【例4】$|G|=p^m$，则对任何$1\le k\le m$，存在G的p^k阶**正规**子群.

注：**降阶+数学归纳法.**

对m用数学归纳法，假设对$m-1$，命题已经成立.

考虑G的中心$Z(G)$，则$Z(G)=p^i(i\ge 1)$. 由Cauchy引理可知$Z(G)$有p阶元，记为a，记$N=\langle a\rangle$，则$N\lhd G$. 考虑$\overline{G}=G/N$，对任何$1\le k\le m$，由归纳假设可知$\overline{G}$有$k-1$阶正规子群$\overline{H}$，注意到$\overline{H}\lhd\overline{G}$当且仅当$H\lhd G$，且$H$形如$H/N$，所以$|H|=|H/N||N|=p^{k-1}p=p^k$，故$H$就是$G$的$p^k$阶正规子群.

2.Sylow定理

- Cauchy引理：G是有限Abel群，p是$|G|$的素因子，则G有p阶子群.

  【证明】降阶+数学归纳法.

  任取$a\in G$.

  ①若$p|ord(a)$，则$ord(a^{\frac{ord(a)}{p}})=p$，则已经找到了$G$的$p$阶子群.

  ②若$p\nmid ord(a)$，则对$|G|$用数学归纳法，假设对任何$1\le m\le|G|-1$命题都已经成立.

  令$N=\langle a\rangle$，因为G是Abel群，所以$N\lhd G$，可考虑$\overline{G}=G/N$，故$|\overline{G}|=|G|/|N|$，故$|G|=|\overline{G}||N|$. 因为$p\nmid|N|$，$p\mid|G|$，所以$p\mid|\overline{G}|$.

  又因为$|\overline{G}|<|G|$，根据归纳假设，$|\overline{G}|$有p阶子群，记为$\overline{H}$. 故$\overline{H}$中有p阶元$\overline{b}$. 记$ord(b)=u$，则$b^u=1$，所以$\overline{b}^u=1$，所以$ord_{\overline{G}}(\overline{b})\mid ord_G(b)$，所以$p|ord_G(b)$，从而$ord(b^{\frac{ord(b)}{p}})=p$，故$G$有$p$阶子群.

- Sylow第一定理：G是有限群，$|G|$有分解$|G|=p^mk$，其中p是素数，$m\ge 1$，$p\nmid k$.则对任何$1\le l\le m$，G有p^l阶子群.特别地，G的Sylow-p子群存在.

  【证明】降阶+类方程+数学归纳法.

  考虑G的类方程

  $$|G|=|Z(G)|+\sum_{x\in\Sigma'}[G:Z_G(x)].$$

  对m使用归纳法.假设对$m-1$命题已经成立. 考虑中心$Z(G)$的阶：

  ①$p\mid|Z(G)|$，因为$Z(G)$是Abel群，由Cauchy引理，存在p阶元$a\in Z(G)$，令$N=\langle a\rangle$.因为N中的元素均为G的中心元，所以$N\lhd G$，可以考虑$\overline{G}=G/N$，则$|\overline{G}|=p^{m-1}$. 因为$p^l\mid|G|$，所以$p^{l-1}\mid|\overline{G}|$，根据归纳假设，$\overline{G}$中有$p^{l-1}$阶子群$\overline{H}$. $\overline{H}$形如H/N，其中$N\le H\le G$，所以$|H|=|\overline{H}||N|=p^{l-1}p=p^l$.即$G$有$p^l$阶子群$H$.

  ②$p\nmid|Z(G)|$，因为$p\mid|G|$，根据类方程可知存在$x\in\Sigma'$使得$p\nmid[G:Z_G(x)]$. 因为$|G|=|G:Z_G(x)||Z_G(x)|$，所以$p^l\mid|Z_G(x)|$. 另一方面，因为$x\in\Sigma'$，所以$x\notin Z(G)$，所以$Z_G(x)\lneq G$. 因此根据归纳假设可知$Z_G(x)$有p^l阶子群H，则H也是G的p^l阶子群.

- Sylow第二和第三定理（关于G的Sylow p-子群的命题）G是有限群，$|G|$有分解$|G|=p^mk$，其中p是素数，$m\ge 1$，$p\nmid k$. 考虑G的Sylow p-子群（p^m阶子群），有：

  - 1.G的任何p-子群都含在G的某个Sylow p-子群内.
  - 2.（常用）G的Sylow p-子群彼此共轭. 特别地，设H是G的Sylow p-子群，则$H\lhd G$当且仅当$|\mathrm{Syl}_p(G)|=1$即G的Sylow p子群唯一.
  - 3.（常用）设G的Sylow p-子群个数为r，则$r\mid k$且$r\equiv 1\mod p$.

  【证明】**考虑p-群作用.** 设K是G的任何一个p子群，H是G的某个Sylow p-子群（存在性已经证明），则我们要证明的是：K一定包含在H的某个共轭子群中. 一旦证明了这一点，立刻得到：

  1. 因为H的共轭子群也是一个Sylow p-子群，所以K包含在G的某个Sylow p-子群中.

2. 取K是任何一个Sylow p-子群H'，则H'在H的某个Sylow p-子群中，比较阶数可得H'就是H的共轭子群.即所有Sylow p-子群都与H共轭.

为了说明K一定包含在H的某个共轭子群内，我们考虑K在$Conj(H)$上的共轭作用. 则这是一个p-群作用，我们断言，$H' \in Conj(H)$是该群作用的不动点，当且仅当$K \subseteq H'$.

充分性是显然的，下证明必要性，即H'是不动点给出K含在H'内. 这将用到p-群作用的重要性质：因为H'是不动点，所以$kH'k^{-1} = H', \forall k \in K$，所以$kH' = H'k, \forall k \in K$，所以$KH' = H'K$，所以$KH'$是$G$的子群.比较阶数：

$$|KH'| = \frac{|K||H'|}{|K \cap H'|} \geq |H| = p^m.$$

因为$|K|$和$|H'|$都是p-子群，所以看上式第一个等号可知KH'也是p-子群，所以其可能的最大阶数就是p^m，所以$KH' = p^m$，$|K \cap H'| = |K|$，所以$K \subseteq H'$.

这就证明了断言. 取$K = H$可知H'是$H \curvearrowright Conj(H)$的不动点当且仅当$H \subseteq H'$，再比较阶数可得$H' = H$，所以，$H \curvearrowright Conj(H)$的不动点只有$H$，根据$p$-群作用的重要性质可得$|Conj(H)| \equiv 1 \mod p$.所以，$p \nmid |Conj(H)|$.再考虑$K \curvearrowright Conj(H)$，则该作用必然有不动点$H' \in Conj(H)$，再根据断言可得$K \subseteq H'$，这就证明了$K$含在$H$的共轭子群$H'$内.

最后证明3. 这已经很容易了，设H是某个Sylow p-子群，注意到Sylow p-子群的个数就等于H共轭类的元素个数，根据轨道稳定化子公式：

$$r = |\mathrm{Syl}_p(G)| = |Conj(H)| = [G : N_G(H)] \mid [G : H] = \frac{p^m k}{p^m} = k.$$

而根据$|Conj(H)| \equiv 1 \mod p$立刻看出$r \equiv 1 \mod p$.

【注】证明1,2得到的重要结果$|Conj(H)| \equiv 1 \mod p$已经在3中体现出来.

- **有关pq阶群**：p, q是互异素数，$p < q$.
  - 观察：Sylow p-子群的个数满足$n_p | q$且$n_p \equiv 1 \mod p$，所以$n_p = 1$或$n_p = q$都有可能，且$n_q = q$只有当$q \equiv 1 \mod p$时才有可能.

    Sylow q-子群的个数满足$n_q | p$且$n_q \equiv 1 \mod q$，所以$n_q = 1$，所以G有唯一Sylow q-子群.
  - 若$q \not\equiv 1 \mod p$，则$n_p = 1$且$n_q = 1$. 此时考虑Sylow p-子群N_p和Sylow q-子群N_q，则有：$N_p = \langle a \rangle$，$N_q = \langle b \rangle$，其中a, b分别是p阶和q阶元. 由唯一性可知N_p和N_q都是正规子群. 我们注意两个事实：

    ① 若$ab = ba$且$ord(a)$与$ord(b)$互素，则$ord(ab) = ord(a)ord(b)$.（证明是硬算）

    ② N_1和N_2均为正规子群，且$N_1 \cap N_2 = 1$，则N_1中任一元素和N_2中任一元素交换.（证明是考虑N_1和N_2的换位子，看出它一定等于1）

    根据Lagrange定理算阶数可知$N_p \cap N_q = 1$，所以N_p中元和N_q中元交换，特别地$ab = ba$，所以$ord(ab) = pq$. 所以$G = \langle ab \rangle \cong C_{pq}$.
  - 若$q \equiv 1 \mod p$. 则pq阶元有两种

    在$n_p = 1, n_q = 1$情形下，pq阶元为C_{pq}.

    在$n_p = q, n_q = 1$情形下，pq阶元为$C_p \rtimes C_q$.（C_p和C_q的半直积，其表达式为：$\langle a, b | a^p = b^q = 1, aba^{-1} = b^i \rangle$，其中$i$是$(\mathbb{Z}/q\mathbb{Z})^\times$中的$p$阶元

3.一些例题

- 【例1】p, q是两个不同素数，则p^2q阶群必然有一个正规的Sylow-子群.
- 【例2】63阶、108阶、**72阶群不是单群**，15阶、91阶群必是循环群，231阶群有唯一的11阶子群、唯一的7阶子群、**唯一的21阶子群**，30阶群有唯一的5阶子群、唯一的3阶子群和**唯一的15阶子群**.
- 【例3】H是G的Sylow p-子群，K是G的子群而且$N_G(H) \leq K$，则$N_G(K) = K$.

【证明】对任何$x \in N_G(K)$，xHx^{-1}也是GSylow p-子群. 因为$xKx^{-1} = K$，所以$xHx^{-1} \subset xKx^{-1} = K$，所以$xHx^{-1}$也是$K$的Sylow p-子群，又因为H是G的从而是K的Sylow p-子群，所以存在$y \in K$使得$yxHx^{-1}y^{-1} = H$，所以$yx \in N_G(x) \leq K$，又因为$y \in K$，所以$x \in K$，所以$N_G(K) \subseteq K$从而$N_G(K) = K$.

- 【例4】k为奇数且$k > 1$，则$D_{2k} \cong D_k \times C_2$.

直积

1. 直积的重要性质

- $G_1' = \{(a_1, 1) : a_1 \in G\} \subset G_1 \times G_2$

  $G_2' = \{(1, a_2) : a_2 \in G\} \subset G_1 \times G_2$

  则：

  - $G_1' \lhd G_1 \times G_2, G_2' \lhd G_1 \times G_2$
  - $G_1' \cap G_2' = 1$
  - G_1'中元与G_2'中元交换
  - $G_1'G_2' = G$
  - $G_1' \cong G_1$，$G_2' \cong G_2$，$G/G_1' \cong G_2$，$G/G_2' \cong G_1$.（后两个：考虑投影同态P_2和P_1的同态基本定理）
  - 若$N_1 \lhd G_1, N_2 \lhd G_2$，则有$N_1 \times N_2 \lhd G_1 \times G_2$，且$(G_1 \times G_2)/(N_1 \times N_2) \cong G_1/N_1 \times G_2/N_2$.

2. 内直积

内直积关系是如下的等价命题：

- G是群，H_1, H_2是两个子群，则TFAE：

  - $H_1 \lhd G, H_2 \lhd G, H_1 \cap H_2 = 1$，$G = H_1H_2$.
  - H_1中元和H_2中元交换，$H_1 \cap H_2 = 1$，$G = H_1H_2$.
  - H_1中元和H_2中元交换，且有“唯一分解”性质，也就是，$\forall g \in G$，存在唯一的$h_1 \in H_1, h_2 \in H_2$使得$g = h_1h_2$.

  并且，以上条件之一成立时，称H_1和H_2为内直积关系. 内直积关系成立后，$G = H_1H_2 \cong H_1 \overset{external}{\times} H_2$.

  以后可以不区分内直积和外直积.

- M_1, M_2是加法群，若$M_1, M_2 \leq M$（自动正规），且成立：$M_1 \cap M_2 = 0$，$M_1 + M_2 = G$（或等价地，$\forall m \in M$，存在唯一的$m_1 \in M_1, m_2 \in M_2$使得$m = m_1 + m_2$）

  那么就说，M_1和M_2是内直和关系，$M = M_1 \oplus M_2$.

- G是群，$H_1, \cdots, H_n$是n个子群，则TFAE：

  - $H_i \lhd G$，$H_i \cap (H_1 \cdots H_{i-1}H_{i+1} \cdots H_n) = 1$，$G = H_1 \cdots H_n$.
  - $H_i \lhd G$，$H_i \cap (H_1 \cdots H_{i-1}) = 1$，$G = H_1 \cdots H_n$.（不能减弱为：两两交为1，参见线性代数）
  - H_i中元与H_j中元交换（$i \neq j$），$H_i \cap (H_1 \cdots H_{i-1}H_{i+1} \cdots H_n) = 1$，$G = H_1 \cdots H_n$.
  - H_i中元与H_j中元交换（$i \neq j$），$H_i \cap (H_1 \cdots H_{i-1}) = 1$，$G = H_1 \cdots H_n$.
  - H_i中元和H_j中元交换$(i \neq j)$，且有“唯一分解”性质，也就是，$\forall g \in G$，存在唯一的$h_i \in H_i$使得$g = h_1h_2 \cdots h_n$.

- 重要命题：若$m_1, \cdots, m_n$两两互素，则：

  $$C_{m_1} \times \cdots \times C_{m_n} \cong C_{m_1 \cdots m_n}.$$

  逆过程：循环群准素分解

  一般过程：**有限Abel群准素分解**（类似于：线性代数中根子空间分解）

  $|G| = p_1^{e_1} \cdots p_r^{e_r}$.（类似：线性代数中的特征多项式）

  GAbel，所以G的Sylow子群正规从而唯一. G的唯一Sylow-p_i子群记为H_i.

则有：$H_i=\{a\in G, a^{p_i^{e_i}}=1\}$，按照定义来看类似于线性代数中的根子空间$\ker(\mathscr{A}-\lambda_i Id)^{e_i}$

根据线性代数中根子空间的等价定义，H_i也有等价定义$\bigcup_{l=0}^{\infty}\{a\in G: a^{p_i^{l_i}}=1\}$.

我们的结论是，G是这些Sylow子群的直积，即$G=H_1\times\cdots\times H_n$.

证明：和线性代数完全一样.

对于循环群因为循环群的因子和其子群是一一对应，所以可以直接写出这些Sylow子群H_i.

更一般的大定理是**有限生成(f.g.)Abel群的结构定理**（不在期中范围内）

有限（有限生成）Abel群的结构定理

1. 有限Abel群准素分解

$|G|=m=p_1^{e_1}\cdots p_r^{e_r}$，$G$是Abel群，$p_1,\cdots,p_r$是不同的素数.

观察：G是Abel群，所以G的一切子群在共轭下封闭（均为正规子群），回忆Sylow第一和第二定理（G的Sylow p-子群存在，G的任何一个$p-$子群含在某个Sylow p-子群中，且G的任何两个Sylow p-子群都共轭）可知：

G有唯一的Sylow-p_i子群，记为H_i，特别地，若G是循环群，则为循环群直积的逆过程.（循环群准素分解）

断言：

①有限Abel群准素分解：$G=H_1\times\cdots\times H_r$.

- 【证明】较容易，对r用数学归纳法，去证明内直积关系$H_1\cap H_1\cdots H_{r-1}=1$且$|H_1\cdots H_r|=|H_1|\cdots|H_r|$.

  $r=2$的情形：$|H_1|=p_1^{e_1}$，$|H_2|=p_2^{e_2}$. 因为$|H_1\cap H_2|\mid|H_1|$且$|H_1\cap H_2|\mid|H_2|$，所以$H_1\cap H_2=1$，所以$|H_1H_2|=\frac{|H_1||H_2|}{|H_1\cap H_2|}=|H_1||H_2|$.

  若已知对r成立，则$|H_1\cdots H_r|=p_1^{e_1}\cdots p_r^{e_r}$，$H_1,\cdots,H_r\le G$，则$|H_{r+1}|=p_{r+1}^{e_{r+1}}$，根据阶数分析可知$H_{r+1}\cap(H_1\cdots H_r)=1$，所以$|H_1\cdots H_{r+1}|=p_1^{e_1}\cdots p_{r+1}^{e_{r+1}}$.

②H_i不仅仅扮演着G的唯一Sylow p_i-子群的角色，还是：被p_i的某个幂次干掉的元素

$$H_i=\{a\in G, a^{p_i^{e_i}}=1\}=\{a\in G, \exists l\ge 0, \text{使得} a^{p_i^l}=1\}=\bigcup_{l=0}^{\infty}\ker p_i^l.$$

最后一个记号是模仿线性代数的准素分解. 下面简要说明为什么H_i是这样的集合.

- 第一个等号：若H_i是Sylow p_i-子群，则其群阶数为$p_i^{e_i}$. 由拉格朗日定理可知$ord(a)|p_i^{e_i}$，所以自然有$a^{p_i^{e_i}}=1$，$\forall a\in H_i$，因此$H_i\subset$右边. 反过来，如果$a^{p_i^{e_i}}=1$，考虑商群G/H_i，则$\overline{a}^{p_i^{e_i}}=\overline{1}$，由拉格朗日定理可知$ord(\overline{a})|p_i^{e_i}$且$ord(\overline{a})\mid|G/H_i|$. 因为$\gcd(|G/H_i|,p_i^{e_i})=1$，所以$\overline{a}=\overline{1}$也就是$a\in H_i$. 这就证明了第一个等号.
- 第二个等号：右边包含左边是显然的，只需要证明左边包含右边. 若存在$l\ge 0$使得$a^{p_i^l}=1$，分情况讨论. 若$l\le e_i$，则$a^{p_i^{e_i}}=(a^{p_i^l})^{p_i^{e_i-l}}=1$. 若$l>e_i$，由拉格朗日定理可知$ord(a)\mid|G|=p_1^{e_1}\cdots p_i^{e_i}\cdots p_r^{e_r}$，另一方面，$ord(a)|p_i^l$. 由$l>e_i$可知$(p_1^{e_1}\cdots p_r^{e_r},p_i^l)=p_i^{e_i}$，所以$ord(a)|p_i^{e_i}$，所以$a^{p_i^{e_i}}=1$，这就证明了第二个等号.

【例】循环群准素分解（这个可以直接显式地写下）

$G=\langle a\rangle\cong C_n$，$n=p_1^{e_1}\cdots p_r^{e_r}$，$H_i=\langle a^{n/p_i^{e_i}}\rangle$，$\langle a\rangle=\langle a^{n/p_1^{e_1}}\rangle\times\cdots\times\langle a^{n/p_r^{e_r}}\rangle$.

（这是因为，循环群的子群和其因子d一一对应，且就是a^d生成的子群.）

【例】 Lagrange定理的逆定理对有限Abel群成立.

【证明】对有限Abel群（加法群）$|G|=p_1^{e_1}\cdots p_s^{e_s}$，其中$p_1,\cdots,p_s$是互不相同素数，$e_i\ge 1$. 则有准素分解：

$$G=H_1\oplus\cdots\oplus H_s$$

其中H_i是G的$p_i^{e_i}$阶唯一Sylow p_i-子群. 若$d\mid|G|$，所以$d=p_1^{l_1}\cdots p_s^{l_s}$，其中$0\le l_i\le e_i$. 我们要证明$G$的确有$d$阶子群.

对每个H_i用Sylow定理可知存在$p_i^{l_i}$阶子群$\hat{H}_i$，根据直和的性质可知

$$\hat{H}_1 \oplus \cdots \oplus \hat{H}_s \leq H_1 \oplus \cdots \oplus H_s.$$

且$|\hat{H}_1 \oplus \cdots \oplus \hat{H}_s| = p_1^{l_1} \cdots p_s^{l_s} = d$

所以，G有d阶子群□

2. 有限生成Abel群的结构定理

- 【定理】有限生成Abel群的结构定理

  M是$f.g.$Abel群，则存在唯一的$m_1, \cdots, m_k$是正整数，$1 < m_1 \mid m_2 \mid \cdots \mid m_k$，以及$r \geq 0$，使得

  $$M \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_k\mathbb{Z} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r个}.$$

  其中$m_1, \cdots, m_k$称为是M的不变因子组，上述分解也被称为有限Abel群不变因子分解.

  对每个直和项再做循环群的准素分解，又可以得到

  $$M \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{e_s}\underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r个}$$

  其中$p_1^{e_1}, \cdots, p_s^{e_s}$称为$M$的初等因子，它们是由$M$唯一确定下来的，且$p_1, \cdots, p_s$允许重复，$e_i \geq 1$.

  【例】决定72阶Abel群由哪些同构类.

  $72 = 2^3 \times 3^2$，先求其不变因子组可能有哪些：

  $$2, 2, 18; \quad 2, 6, 6; \quad 2, 36; \quad 3, 24; \quad 6, 12; \quad 72.$$

  共6种，每个直和项再做循环群准素分解可得其初等因子表示：

  $$\begin{aligned}
  &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \\
  &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \\
  &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \\
  &\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \\
  &\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \\
  &\mathbb{Z}/72\mathbb{Z} = \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}.
  \end{aligned}$$

3. 有限生成Abel群结构定理的证明

- 【定义】（自由Abel群） F是Abel群，若$\exists n \geq 1$，使得$F \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$，则称$F$是有限生成自由Abel群. 例如，$\mathbb{Z}$的一组生成元为$\underbrace{\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}, \begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix}, \cdots, \begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}}_{n个}$.
- 【引理1】$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^n, \mathbb{Z}^m) = M_{m \times n}(\mathbb{Z})$.
  - 回忆$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) = \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}) \cong \mathbb{Z}$. 这是上面结论的一个特殊情形.
  - 其典范双射由$\pi : A \mapsto \begin{bmatrix} \mathcal{A} \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^n, \mathbb{Z}^m) \\ \mathcal{A} : \mathbb{Z}^n \to \mathbb{Z}^m, x \mapsto Ax \end{bmatrix}$给出.

  【证明】

  - 先验证$\mathcal{A}$是一个群同态，这是显然的.
  - 再证明这时单射. 若$A \neq B$，则存在i使得A的第i列不等于B的第i列，所以$Ae_i \neq Be_j$，所以$\mathcal{A} \neq \mathcal{B}$，所以$\pi$是单射.

- 再证明这是满射.注意，同态是由在生成元处的取值唯一确定的，设$f:\mathbb{Z}^n\to\mathbb{Z}^m$是同态，记$f(e_i)=\alpha_i\in\mathbb{Z}^m$，$1\le i\le n$，令$A=(\alpha_1,\cdots\alpha_n)\in M_{m\times n}(\mathbb{Z})$，则断言$\pi(A)=f$，这只需要注意同态在生成元处的取值即可验证：

$$\begin{aligned}f(k_1,\cdots,k_n)&=f(k_1e_1+\cdots+k_ne_n)=k_1f(e_1)+\cdots+k_nf(e_n)\\&=k_1\alpha_1+\cdots+k_n\alpha_n=A\begin{pmatrix}k_1\\k_2\\\vdots\\k_n\end{pmatrix}.\end{aligned}$$

- 【引理2】采用引理1的自然等同，复合运算：

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^n,\mathbb{Z}^m)\times\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^k,\mathbb{Z}^n)\to\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^k,\mathbb{Z}^m),\quad(f,g)\mapsto f\circ g$$

  对应矩阵乘法：

$$M_{m\times n}(\mathbb{Z})\times M_{n\times k}(\mathbb{Z}),\quad(A,B)\mapsto AB.$$

  【证明】这是显然的. 将A等同于$\mathcal{A}\in\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^n,\mathbb{Z}^m)$，$B$等同于$\mathcal{B}\in\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^k,\mathbb{Z}^n)$，则：

$$\mathcal{A}\circ\mathcal{B}(x)=\mathcal{A}(\mathcal{B}(x))=\mathcal{A}(Bx)=ABx=(AB)x.$$

  所以$\mathcal{A}\circ\mathcal{B}$对应$AB$.

- 【引理3】$M_n(\mathbb{Z})=\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^n)$作为环，对应法则为$(A\mapsto\mathcal{A}:\mathbb{Z}^n\to\mathbb{Z}^n,\quad x\mapsto Ax)$.

  【证明】双射在引理1中已经证明，保加来自Abel群同构（引理1），保乘来自引理2的对应.□

  【remark】特别地，考虑$\mathrm{Aut}(\mathbb{Z}^n)$，它是自同态环$\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^n)$的单位群，这对应于环$M_n(\mathbb{Z})$的单位群，后者记为$\mathrm{GL}_n(\mathbb{Z})$.

- 【命题】$\mathrm{GL}_n(\mathbb{Z})=M_n(\mathbb{Z})^\times=\{A\in M_n(\mathbb{Z}),\det A=\pm1\}$.

  【证明】（用伴随矩阵的概念）

  可逆⇒行列式：$AB=BA=I_n$给出$\det A\det B=1$，根据定义$\det A,\det B\in\mathbb{Z}$，所以$\det A=\pm1$.

  可逆⇐行列式：$\det A=\pm1$，则$A^*A=AA^*=\det AI_n$，而且根据伴随矩阵的定义可知$A^*\in M_n(\mathbb{Z})$（暂时将$M_n(\mathbb{Z})$看成$M_n(\mathbb{Q})$的子环），所以取$B=\det AA^*$可知A是可逆的.

  □

- 【引理4】$\mathbb{Z}^m\cong\mathbb{Z}^n$当且仅当$m=n$，即有限生成自由Abel群的同构类由其秩确定.

  【证明】$\mathbb{Z}^m\cong\mathbb{Z}^n$，故存在环同态$f:\mathbb{Z}^m\to\mathbb{Z}^n$，$g:\mathbb{Z}^n\to\mathbb{Z}^m$，两者互为逆映射，即$f\circ g=id_{\mathbb{Z}^n}$，$g\circ f=id_{\mathbb{Z}^m}$，即根据前面的等同，存在$A\in M_{n\times m}(\mathbb{Z})$，$B\in M_{m\times n}(\mathbb{Z})$使得$AB=I_n,BA=I_m$. 考虑$\mathbb{Q}$上的线性代数可知$m=n$，所以$A,B$作为$M_{n\times m}(\mathbb{Z})$和$M_{m\times n}(\mathbb{Z})$中的元素时也有$m=n$.

  □

- 【引理5】M是有限生成（不必自由）Abel群，则存在$n\ge1$，以及$N\le\mathbb{Z}^n$（$\mathbb{Z}^n$的子群），使得$M\cong\mathbb{Z}^n/N$.

  【证明】设$S=\{a_1,\cdots,a_n\}$是M的一个生成元组，考虑同态：

$$\varphi:\mathbb{Z}^n\to M,\quad(k_1,\cdots,k_n)\mapsto\sum_{i=1}^n k_ia_i.$$

  因为S生成M，所以这是一个满同态，因此$\mathbb{Z}^n/\ker\varphi\cong M$.□

- 【例】$\mathbb{Z}\oplus\mathbb{Z}$是2秩自由Abel群，则：

  $\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus2\mathbb{Z}\cong\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. 事实上，$2\mathbb{Z}\oplus2\mathbb{Z}=(2k,2l)=k(2,0)+l(0,2)=\begin{pmatrix}2&0\\0&2\end{pmatrix}\begin{pmatrix}k\\l\end{pmatrix}$.

  $N=\{(3k+2l,2k+4l),k,l\in\mathbb{Z}\}\subseteq\mathbb{Z}\oplus\mathbb{Z}$，$N=k(3,2)+l(2,4)$，如何计算$\mathbb{Z}^2/N$的同构类?

  可以硬算，$\mathbb{Z}^2$为平面整点，考察N陪集的结构，可以分析出商群是8阶循环群.

  问：有没有一般的计算方法?

- 【命题】设$A \in M_{m\times n}(\mathbb{Z})$，则存在$P \in \mathrm{GL}_n(\mathbb{Z})$（定义如前），$Q \in \mathrm{GL}_n(\mathbb{Z})$，使得：

$$PAQ = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \end{pmatrix}.$$

其中$d_1 \mid \cdots \mid d_r$，$d_i \geq 1$，实际上这是矩阵环$M_{m\times n}(\mathbb{Z})$中的“相抵标准形”. 上面矩阵未必是方阵，而是$m \times n$的矩阵. 其中$d_i = \frac{D_i}{D_{i-1}}$，其中$D_i = \gcd(A\text{的}i\text{阶子式})$.（$D_i$称为$A$的行列式因子，$d_i$称为$A$的不变因子）

【证明】照抄线性代数中$\lambda-$矩阵 Smith Form（法式）的证明□

【例】计算上面两个矩阵的不变因子和Smith标准形.

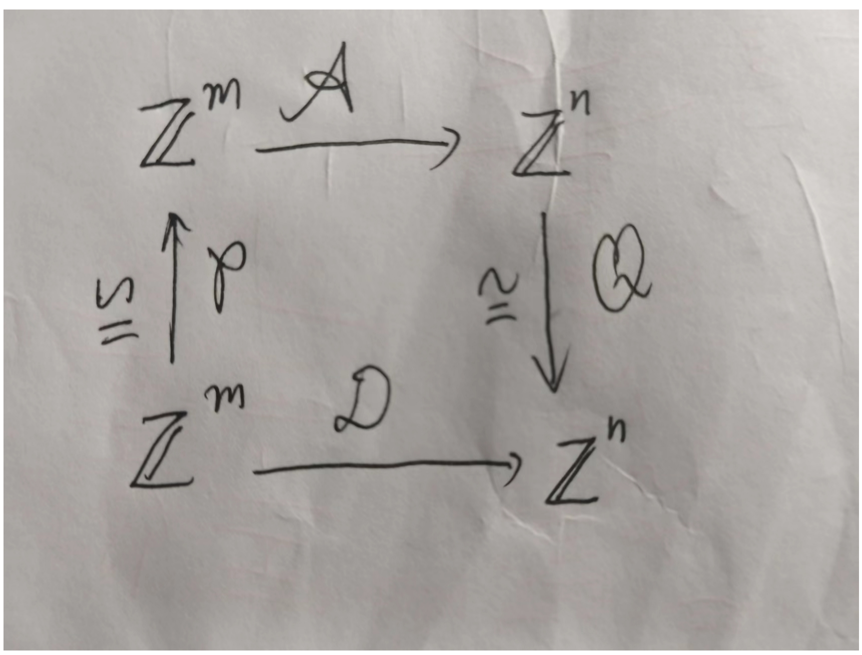
$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$，$D_1 = 2$，$D_2 = 4$，$d_1 = 2$，$d_2 = 2$，所以Smith Form就是本身.

$\begin{pmatrix} 3 & 2 \\ 2 & 4 \end{pmatrix}$，$D_1 = 1$，$D_2 = 8$，$d_1 = 1$，$d_2 = 8$，所以Smith Form就是$\begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}$.

- 【命题】$A \in M_{n\times m}(\mathbb{Z})$，$A = (\alpha_1, \cdots, \alpha_m)$，$\alpha_i \in \mathbb{Z}$. $N = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m \subset \mathbb{Z}^n$（类似于列空间），则$N = \mathrm{Im}\mathcal{A}$，其中$\mathcal{A}$是由矩阵$A$诱导的$\mathbb{Z}^m$到$\mathbb{Z}^n$的同态.

考虑Smith Form，存在$\begin{cases} Q \in \mathrm{GL}_n(\mathbb{Z}), \\ P \in \mathrm{GL}_m(\mathbb{Z}), \end{cases}$ 使得$QAP = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \end{pmatrix}$.

根据前面的引理2，设P, Q诱导的同构为$\mathcal{P}$和$\mathcal{Q}$，则有如下的交换图：



注意$\mathcal{P}, \mathcal{Q}$是同构，$\mathrm{Im}\mathcal{A} = \mathrm{Im}\mathcal{D}$，所以$\mathbb{Z}^n/\mathrm{Im}\mathcal{A} \cong \mathbb{Z}^n/\mathrm{Im}\mathcal{D}$. 注意$D$的形式可知其Im容易直接计算：

$$\mathrm{Im}\mathcal{D} = d_1\mathbb{Z} \oplus \cdots \oplus d_s\mathbb{Z} \oplus \underbrace{0 \oplus \cdots \oplus 0}_{n-s\text{个}}$$

所以$\mathbb{Z}^n/\mathrm{Im}\mathcal{D} \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-s\text{个}}$,

□

【remark】还差最后一步，因为这里将N实现为了m个$\mathbb{Z}^n$中元素的有限生成，我们将要说明对$\mathbb{Z}^n$的任何子　群都可以这么做.

- 【引理6】$\mathbb{Z}^n$的子群必然同构于秩$\leq n$的有限生成自由Abel群.

【remark】这件事情对有限生成Abel群也对，即n秩有限生成Abel群必然是秩$\le n$的有限生成Abel群.

但是这件事情对有限生成群不对，即有限生成群的子群一般未必有限生成.

- 【证明】对n用数学归纳法.

  $n=1$，$\mathbb{Z}$的子群有0和$k\mathbb{Z}$，注意$k\mathbb{Z}\cong\mathbb{Z}$，因此结论成立.

  一般地，设$N\le\mathbb{Z}^n$，假设结论对$n-1$已经成立，为了使用假设，令$F=\{(0,x_2,\cdots,x_n),x_2,\cdots,x_n\in\mathbb{Z}\}$（类似于取出了一个$n-1$维子空间（超平面））.

  则$F\cong\mathbb{Z}^{n-1}$.

  令$N_1=\{k_1,\exists(k_1,*,\cdots,*)\in N\}\subset\mathbb{Z}$（所有$N$中可能出现的第一个分量的取值），则$N_1$是投影群同态$P_1:\mathbb{Z}^n\to\mathbb{Z},(x_1,\cdots,x_n)\mapsto x_1$在$N$中的像，因为$N\le\mathbb{Z}^n$，所以$N_1=\mathrm{Im}P_1\le\mathbb{Z}$.

  以上通过N_1某个子群在群同态下的像说明了N_1是$\mathbb{Z}$的子群，从而$N_1=0$或者$N_1=d\mathbb{Z}$.

  ①$N_1=0$，则观察F的形式可知，$N\le F\cong\mathbb{Z}^{n-1}$，由归纳假设可知$N$是秩$\le n-1$的自由Abel群.

  ②$N_1=d\mathbb{Z}$，则存在$\alpha=(d,*,\cdots,*)\in N$.

  断言$N=\langle\alpha\rangle\oplus(N\cap F)$. 首先显然两者的交是$0$，另一方面$\langle\alpha\rangle+(N\cap F)=N$，这是因为，考虑$N$中任何元素$(x_1,\cdots,x_n)$，因为$x_1\in N_1$，所以$x_1=qd$，其中$q\in\mathbb{Z}$，因此，记$\alpha=(d,k_2,\cdots,k_n)$，则有：

  $$(0,x_2-qk_2,\cdots,x_n-qk_n)+q(d,k_2,\cdots,k_n)=(x_1,\cdots,x_n).$$

  其中第一项在$N\cap F$中，第二项在α生成的子群.

  显然$ord(\alpha)=\infty$，所以$\langle\alpha\rangle\cong\mathbb{Z}$，而$N\cap F\subseteq F\cong\mathbb{Z}^{n-1}$.

  所以，根据归纳假设可知$N\cap F$是秩l自由Abel群，其中$l\le n-1$.

  所以

  $$N\cap F\oplus\langle a\rangle\cong\mathbb{Z}\oplus\mathbb{Z}^l\cong\mathbb{Z}^{l+1}.$$

  所以$N\cong\mathbb{Z}^{l+1}$，其中$l+1\le n$，即N是一个秩$\le n$的自由Abel群.□

【remark】以上通过将任何一个f.g.Abel群M实现为$\mathbb{Z}^n/N$（n秩自由Abel群商掉其某个子群），再利用环中　　的线性代数说明了任何有限生成自由Abel群N是某个$\mathrm{Im}\mathcal{A}$，以及$\mathrm{Im}\mathcal{A}$可以化成$\mathrm{Im}\mathcal{D}$从而变得可以直接计算.　　最后，我们说明了n秩自由Abel群的所有子群都是有限生成Abel群，从而证明了有限Abel群结构定理的存在性　　（不变因子分解）.

【remark】这是一种内部攻破的证明方法，也就是将f.g.Abel群实现成自由Abel群的商群，再转化为环线性　　代数的语言.

- 证明唯一性. 也就是：

  若M既同构于$\mathbb{Z}/m_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_k\mathbb{Z}\oplus\mathbb{Z}^r$，又同构于$\mathbb{Z}/m_1'\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_l'\mathbb{Z}\oplus\mathbb{Z}^s$，且满足：

  $$2\le m_1\mid\cdots\mid m_k,\quad 2\le m_1'\mid\cdots\mid m_l'.$$

  则有$k=l,r=s$，$m_i=m_i'$.

  【证明】设$f:\mathbb{Z}/m_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_k\mathbb{Z}\oplus\mathbb{Z}^r\to\mathbb{Z}/m_1'\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_l'\mathbb{Z}\oplus\mathbb{Z}^s$是同构，则断言：

  $$f(\mathbb{Z}/m_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_k\mathbb{Z}\oplus0)=\mathbb{Z}/m_1'\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_l'\mathbb{Z}\oplus0,$$

  这是因为，同构是保扭子群的.（参见后面的定义）

  且f诱导了同构：

  $$\widetilde{f}:\mathbb{Z}/m_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_k\mathbb{Z}\to\mathbb{Z}/m_1'\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_l'\mathbb{Z}$$

  还诱导了

$$\begin{aligned}&\overline{f}:(\mathbb{Z}/m_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_k\mathbb{Z}\oplus\mathbb{Z}^r)/(\mathbb{Z}/m_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_k\mathbb{Z}\oplus 0)\\&\to(\mathbb{Z}/m_1'\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_l'\mathbb{Z}\oplus\mathbb{Z}^s)/(\mathbb{Z}/m_1'\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_l'\mathbb{Z}\oplus 0).\end{aligned}$$

- 【命题】$f:G_1\to G_2$是同构，$H_1\leq G_1$，则f诱导了同构:$f:H_1\to f(H_1)$，$f(H_1)\leq G_1$. 且若$H_1=N_1\lhd G$，则f也诱导了同构：

  $$f:G_1/N_1\to G_2/f(N_1),\quad f(N_1)\lhd G_2.$$

  【证明】这是因为群同构会保子群结构，也保正规子群结构□

有了以上命题，则第一个同构$\widetilde{f}$是成立的. 另一方面，注意$\overline{f}$左边同构于$\mathbb{Z}^r$，右边同构于$\mathbb{Z}^s$，根据引理4，$\mathbb{Z}^r\cong\mathbb{Z}^s\to r=s$.不变因子的唯一性根据同构也可以推出（参见去年抽象代数课程笔记）

【remark】不变因子组和秩都是f.g. Abel群的同构不变量，由此可以给出f.g. Abel群的同构类划分.

- 【定理】（有限生成Abel群的结构定理）

  M为$f.g.$ Abel群，则存在唯一的不变因子组$m_1,\cdots,m_k$，以及$r\geq 0$，使得

  $$M\cong\mathbb{Z}/m_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_k\mathbb{Z}\oplus\mathbb{Z}^r.$$

  或者写成内直和的形式（将外直和对应的同构拉回）

  $$M\cong\langle a_1\rangle\oplus\cdots\oplus\langle a_k\rangle\oplus\langle a_{k+1}\rangle\oplus\cdots\oplus\langle a_{k+r}\rangle.$$

  其中前k个a_i的阶数是m_i，后r个阶数为∞.

  写成初等因子的形式：

  $$M\cong\langle b_1\rangle\oplus\cdots\oplus\langle b_s\rangle\oplus\langle b_{s+1}\rangle\oplus\cdots\oplus\langle b_{s+r}\rangle.$$

  前s个b_j的阶数为$p_j^{e_j}$，最后r个为∞.

  且这些分解的扭部分唯一，p-扭部分也唯一，也就是$\bigoplus_{ord(b_j)=p\text{的幂次}}\langle b_j\rangle$唯一.
- 扭子群：M是加法群，$\mathrm{Tor}(M)=\{x\in M,\exists n\geq 1,\text{使得}nx=0\}$.称为$M$的扭子群
- p-扭子群：$\mathrm{Tor}_p(M)=\{x\in M,\exists n\geq 0,\text{使得}p^lx=0.\}$.

容易看出，扭子群和p-扭子群都是由M确定的（唯一的），因此有了以上有限Abel群结构定理的唯一性.

4. 有限（有限生成）Abel群结构定理的例题

【例】$M=\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$，这是一个1秩有限生成Abel群的同构类，且其扭部分为$\mathbb{Z}/2\mathbb{Z}$. 将相应的同构拉回，写成内直和形式，有$M=\langle a\rangle\oplus\langle b\rangle$，其中$b=(0,\overline{1})$是2阶元，$a=(1,\overline{0})$是无限阶元.

我们要说明的事情是，**虽然扭部分唯一，但这不代表直和项中循环群是唯一的.** 为此，考虑$\widetilde{a}=a+b=(1,\overline{1})$，则显然$\widetilde{a}$也是无限阶元.

考虑$\langle\widetilde{a}\rangle$：

$$\langle\widetilde{a}\rangle=\{n\widetilde{a}:n\in\mathbb{Z}\}=\{(2k,\overline{0}):k\in\mathbb{Z}\}\cup\{(2k+1,\overline{1}),k\in\mathbb{Z}\}$$

这时显然有$\langle\widetilde{a}\rangle\neq\langle a\rangle$（自由部分同构但不相同），但是此时仍有$M=\langle\widetilde{a}\rangle\oplus\langle b\rangle$. 这是因为，首先可以验证$\langle\widetilde{a}\rangle\cap\langle b\rangle=0$，而且$(n,\overline{m})=na+mb=n(a+b)+(m-n)b=n\widetilde{a}+(m-1)b.$

【remark】在考虑有限生成Abel群M的循环群内直和分解时，扭部分是不能改变的（扭部分由M唯一确定），但是，**自由部分可以改变**，所以，直和项是不唯一的.

【例】计算M的自同构群.

【分析】若f是自同构，则对于分解$M=\langle a\rangle\oplus\langle b\rangle$，用$f$作用可得到

$$M=f(M)=\langle f(a)\rangle\oplus\langle f(b)\rangle.$$

注意f是同构，所以$ord(f(a)) = ord(a) = \infty, ord(f(b)) = ord(b) = 2$.

反之，如果能找到$\widetilde{a}, \tilde{b} \in M$，满足$ord(\widetilde{a}) = \infty$，$ord(\tilde{b}) = 2$，且$M = \langle \widetilde{a} \rangle \oplus \langle \tilde{b} \rangle$，那么就存在唯一的$f \in Aut(M)$，使得$f(a) = \widetilde{a}$，$f(b) = \tilde{b}$，注意群同构（一般地，群同态）由生成元处的取值唯一确定.

事实上，以上我们将$Aut(M)$与以下集合做了1-1对应：

$$\{(\widetilde{a}, \tilde{b}) : \widetilde{a}, \tilde{b} \in M, ord(\widetilde{a}) = \infty, ord(\tilde{b}) = 2, \text{且有直和分解} M = \langle \widetilde{a} \rangle \oplus \langle \tilde{b} \rangle\}$$

所以实际上只需要算这个集合.

设$\widetilde{a} = (n, \overline{m}), n \neq 0$，$\overline{b} = b = (0, \overline{1})$.（二阶元只有一个）

阶数的不同已经保证了无交，下面要根据$M = \langle a \rangle + \langle b \rangle$的条件进行求解.

注意如果$n \neq \pm 1$，则一定有元素无法生成，而当$n = \pm 1$时，确能生成所有的元素，所以求出了集合：

$$\{(\widetilde{a}, \tilde{b}) : \tilde{b} = b = (0, 1), \widetilde{a} = (1, \overline{0}), (1, \overline{1}), (-1, \overline{1}), (-1, \overline{0})\}.$$

于是$Aut(\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$是4阶群. 4阶群只有$K_4$和$C_4$. 为此需要计算一下$f$作为群元素的阶数来推断群结构. 当$a = (1, \overline{1})$时，$(f \circ f)(1, 0) = f(1, 1) = f(1, 0) + f(0, 1) = (1, 1) + (0, 1) = (1, 0)$，同理$(f \circ f)(0, 0) = (0, 0)$；当$a = (-1, \overline{0})$时，$(g \circ g)(1, 0) = g(-1, 0) = -g(1, 0) = (1, 0)$，同理$(g \circ g)(0, 0) = (0, 0)$，所以$f, g$都是二阶元，有两个2阶元，这一定是$K_4$.

$\square$

【例】计算一个全是扭的有限Abel群$M = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$的自同构群$Aut(M)$的同构类.

【remark】注意，根据上面的等同，这时可以直接算出来$Aut(M)$的阶数：

$$|\langle \widetilde{a} \rangle \oplus \langle \tilde{b} \rangle| = |\langle \widetilde{a} \rangle||\langle \tilde{b} \rangle| = 8.$$

所以$|Aut(M)| = 8$，同构类有C_8, D_4和Q_8.

下面为了算群结构，需要具体找出满足条件的那些“元素对”. 条件是满足阶数+生成+无交. 无交当且仅当$\langle \widetilde{a} \rangle$和$\langle \tilde{b} \rangle$中的2阶元不同（因为由阶数的不同就可以排除其他那些元素相等的可能性），也就是$\tilde{b} \neq 2\widetilde{a}$. 写下8种情况后，考虑由它们确定的群同构的阶数来判断群结构. 最终算出是D_4.$\square$

合成列，可解群，幂零群

1. 合成列

- 次正规列：G是群，若有子群列：

  $$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_i \triangleleft G_{i+1} \triangleleft \cdots \triangleleft G_{r-1} \triangleleft G_r = G. (*)$$

  其中$G_i \leq G$且每个$\triangleleft$表示$G_i \triangleleft G_{i+1}$.

  称这个子群列是G的一个次正规列.
- 正规列：若次正规列还有$G_i \triangleleft G$对每个i成立，则称这是正规列.
- 商因子：设G有$(*)$形状的次正规列，称每相邻两项给出的商群$G_0, G_1/G_0, \cdots, G_r/G_{r-1}$为次正规列的商因子.
- 次正规列的长度：将$(*)$中真包含关系的个数为次正规列的**长度**
- 合成列，合成因子：若每个商因子都是单群，则称次正规列是一个合成列， 合成列的商因子称为合成因子.
- 【例】对一般的群G，G不总是有合成列，若有，也未必唯一.
  - $\mathbb{Z}$没有合成列.

    【证明】若有合成列$1 \leq A_0 \leq \cdots \leq A_{r-1} \leq A_r = \mathbb{Z}$，则商因子$A_i/A_{i-1}$是Abel单群给出存在素数$p_i$使得$A_i/A_{i-1} \cong C_{p_i}$，又因为$|\mathbb{Z}| = |A_{r-1}||\mathbb{Z}/A_{r-1}| = |A_{r-2}||A_{r-1}/A_{r-2}||\mathbb{Z}/A_{r-1}| = \cdots$

$= |A_0||A_1/A_0|\cdots|\mathbb{Z}/A_{r-1}| = p_1\cdots p_r < \infty$，这与$|\mathbb{Z}| = \infty$矛盾.□

【remark】从证明过程可以看出，**无限Abel群必然都没有合成列**，因为以上过程只用到了$\mathbb{Z}$是无限Abel群，而这是由事实：**Abel单群$\Leftrightarrow$素数阶循环群**决定的.

- D_4有不同的合成群列：

$$1 \lhd \langle a^2\rangle \lhd \langle a\rangle \lhd D_4;\quad 1 \lhd \{1,a^2\} \lhd \{1,a^2,b,ab\} \lhd D_4.$$

- 【命题】若G是群，$N \lhd G$，若正规子群N和商群G/N都有合成列，则G必有合成列.

  【证明】证明是把这两个合成列用某种方式拼起来

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_r = N$$
$$1 = \overline{G_0} \lhd \overline{G_1} \lhd \cdots \lhd \overline{G_s} = \overline{G}$$

  其中记号$\overline{G_i}$表示G_i/N.

  后面的这些为商群的子群，根据群同态只是可知，商群的子群一一为对应于G中含有N的子群（对应法则为商同态拉回），即$G_i = \pi^{-1}(\overline{G_i})$.

  考虑列：

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_r = N = G_0 \lhd G_1 \lhd \cdots \lhd G_s = G$$

  首先验证这的确是次正规列，因为$G_i/G_{i-1} \cong \overline{G_i}/\overline{G_{i-1}}$，根据商群的合成列可知右边是单群，所以左边也是单群，所以这是G的合成列.□

- 【定理】有限群一定有合成列

  【证明】对G的阶用数学归纳法，若G是单群，则其合成列为$1 \lhd G$，不用证明. 若G不是单群，则存在$1 \lhd N \lhd G$，其中N是非平凡的正规子群，从而$|N|, |G/N| < G$，根据归纳假设可知N和G/N都有合成列，根据前面命题可知G有合成列.

- 【例】有限阶循环群有合成列. 设$n = p_1\cdots p_r$，p_i素允许重复，令$C_{p_1\cdots p_i}$是G的唯一$p_1\cdots p_i$阶子群（循环群与其阶数的因子一一对应），则有子群列：

$$1 \le C_{p_1} \le C_{p_1p_2} \le \cdots \le C_{p_1\cdots p_{r-1}} \le C_n.$$

  合成因子为$C_{p_1},\cdots,C_{p_r}$.

  【remark】事实上素因子分解的不同顺序会给出C_n的不同合成列，这又反映出有限群的合成列不唯一. 但是，合成因子$C_{p_1},\cdots,C_{p_r}$在不计次序下是唯一的.

- 【例】有限Abel群的合成列.

  有限Abel 群G的结构为：

$$G \cong C_{m_1} \times \cdots \times C_{m_k},\quad 2 \le m_1 \mid \cdots \mid m_k$$

  其中$m_1,\cdots,m_k$是不变因子组.

  考虑子群列：

$$1 \le C_{m_1} \times 1 \times \cdots \times 1 \le C_{m_1} \times C_{m-2} \times 1 \times \cdots \times 1 \le \cdots \le C_{m_1} \times \cdots \times C_{m_{k-1}} \times 1 \le G.$$

  则：这是G的一个正规列，商因子是$C_{m_1},\cdots,C_{m_{k-1}},C_{m_k}$.

  根据前面的例子，循环群有合成列，再用前面的命题可以一步一步地将商因子合成列塞到原来的子群列中，此时合成因子被继承，这样一步一步就可以拼出G的合成列，且G的合成因子一一对应于$|G|$的素因子（允许重复）

  【remark】G的合成因子是Abel单群即素数阶群，所以，如果从阶的角度考量，$|G|$等于合成因子阶的乘积，因此其合成列一定是上面构造出来的形式.

- 【例】计算S_n的合成因子.

$$S_3 : 1 \lhd A_3 \lhd C_3$$

合成因子为C_3和C_2.

$$S_4 : 1 \lhd \begin{matrix}\langle(12)(34)\rangle \\ \langle(13)(24)\rangle \\ \langle(14)(23)\rangle\end{matrix} \lhd K_4(\text{幺元}+\text{所有的}(2,2)\text{置换}) \lhd A_4 \lhd S_4$$

注意S_4下面必须放A_4，若放K_4，因为$S_4/K_4 \cong S_3$，这不是单群.

合成因子为C_2, C_2, C_3, C_2.

$S_n(n \geq 5)$的合成列就只有$1 \lhd A_n \lhd S_n$，注意事实：A_n是S_n的唯一非平凡正规子群，而且A_n是单群$(n \geq 5)$.

2. Jordan-Holder定理

Jordan-Holder定理是描述有限群合成因子唯一性的定理.

【定理】（Jordan-Holder）G有限群，若有两个合成列：

$$\begin{aligned} 1 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{r-1} \lhd G \\ 1 \lhd G_1' \lhd G_2' \lhd \cdots \lhd G_{s-1}' \lhd G \end{aligned}$$

则有：$r = s$，且存在$\sigma \in S_r$使得$G_i/G_{i-1} \cong G'_{\sigma(i)}/G'_{\sigma(i-1)}$.

【引理】设$1 \lhd G_1 \lhd \cdots \lhd G_{r-1} \lhd G$是合成列，$N \lhd G$，则在允许重复的意义下，可以构造另一个列：

$$1 \lhd G_1 \cap N \lhd G_2 \cap N \lhd \cdots \lhd G_{r-1} \cap N \lhd N \lhd G_1 N \lhd G_2 N \lhd \cdots \lhd G_{r-1} N \lhd G.$$

这个疑似的“合成列”目前只是一个次正规列，但是：如果去掉以上的重复项，就变成合成列，而且长度就是r.

事实上，具体来说，对任何i以下两种情况有且仅有一种发生：

① $G_{i-1} \cap N = G_i \cap N$，且$G_{i-1}N \lhd G_i N$非平凡；且$G_i N/G_{i-1}N \cong G_i/G_{i-1}$；

② $G_{i-1} \cap N \lhd G_i \cap N$非平凡，且$G_{i-1}N = G_i N$；且$G_i \cap N/G_{i-1} \cap N \cong G_i/G_{i-1}$.

【证明】考虑$f : G_i \cap N \xrightarrow{i} G_i \xrightarrow{\pi} G_i/G_{i-1}$

$\ker f = G_{i-1} \cap N$，这建议了单同态$\overline{f} : (G_i \cap N)/(G_{i-1} \cap N) \to G_i/G_{i-1}$.

且$\mathrm{Im}\overline{f} = (G_i \cap N)G_{i-1}/G_{i-1}$.

根据wk8hw-10知$(G_i \cap N)G_{i-1} = G_i \cap (G_{i-1}N)$，由$(G_i \cap G_{i-1}N)/G_{i-1} \lhd G_i/G_{i-1}$可知$\mathrm{Im}\overline{f} \lhd G_i/G_{i-1}$

$$\begin{aligned} (G_i/G_{i-1})/\mathrm{Im}\overline{f} = (G_i/G_{i-1})/(G_i \cap (G_{i-1}N)/G_{i-1}) \cong G_i/(G_i \cap (G_{i-1}N)) \cong G_i N/G_{i-1}N; \\ \mathrm{Im}\overline{f} = (G_i \cap N)G_{i-1}/G_{i-1} = (G_i \cap N)/(G_i \cap N) \cap G_{i-1} = (G_i \cap N)/(G_{i-1} \cap N). \end{aligned}$$

一旦得到了这两个同构，注意G_i/G_{i-1}是单群，所以：

①$\mathrm{Im}\overline{f} = 1$，则$G_i/G_{i-1} \cong G_i N/G_{i-1}N$，而$G_i \cap N \cong G_{i-1} \cap N$.

②$\mathrm{Im}\overline{f} = G_i/G_{i-1}$，则$G_i N \cong G_{i-1}N$，而$G_i \cap N/G_{i-1} \cap N \cong G_i/G_{i-1}$.

□

【Jordan-Holder定理的证明】

对第个列以及$G'_{s-1} \lhd G$用引理，得到一个允许重复的合成列：

$$1 \lhd (G_1 \cap G'_{s-1}) \lhd \cdots \lhd (G_r \cap G'_{s-1}) \lhd G'_{s-1} \lhd G_1 G'_{s-1} \lhd \cdots \lhd G_{r-1} G'_{s-1} \lhd G.$$

而G/G'_{s-1}是单群，所以G'_{s-1}是G的极大正规子群，也就是G'_{s-1}和G之间无法再非平凡地插入其他正规子群，所以存在唯一的i，使得

$$G'_{s-1} = G_1 G'_{s-1} = \cdots = G_{i-1} G'_{s-1} \lhd G_i G'_{s-1} = \cdots = G$$

中间的$\lhd$非平凡.也可以直接用G/G'_{s-1}是单群来考虑，总之以上不难推出.

与此同时根据引理可知，后半链与前半链的商因子具有对应关系，也就是有以下严格关系：

$$1 \lhd (G_1 \cap G'_{s-1}) \lhd \cdots \lhd (G_{i-1} \cap G'_{s-1}) = (G_i \cap G'_{s-1}) \lhd \cdots \lhd G'_{s-1}(*)$$

上面的$\lhd$都是非平凡的.

根据引理后半段：

$$\begin{cases} G/G'_{s-1} = G_iG'_{s-1}/G_{i-1}G'_{s-1} \cong G_i/G_{i-1}; \\ (G_j \cap G'_{s-1})/(G_{j-1} \cap G'_{s-1}) \cong G_j/G_{j-1} \quad \text{for all } j \neq i. \end{cases}$$

从而，$(*)$是一个G'_{s-1}的长度为$r-1$的合成列，合成因子就是$G_1, \cdots, G/G_{r-1}$.

与条件中所给的合成列的前一段作比较：

$$1 \lhd G'_1 \lhd G'_2 \lhd \cdots \lhd G'_{s-1}(\square)$$

$(\square)$长度是$s-1$，$(*)$长度是$r-1$，对r用数学归纳法，由归纳假设可知$r-1=s-1$，所以$r=s$，且由归纳假设，比较$(*)$和$(\square)$的合成因子可知合成因子在不计次序下唯一. $\square$

3. 可解群

- 可解群的定义，若存在$i \geq 1$使得$G^{(i)} = 1$，则称G可解.

  观察：这会给出一个次正规列：

  $$1 = G^{(i)} \lhd \cdots \lhd G^{(2)} \lhd G^{(1)} \lhd G.$$

  这是因为若$[N_1, N_2]$中N_1, N_2都是正规子群，则$[N_1, N_2]$也是正规的.

  以上的次正规列称为可解群的导列.（事实上，这是正规列）

- 可解列：商因子为Abel群的次正规列

- 【命题】G可解当且仅当G有可解列，这可以当成是G可解的另一种定义.

  【证明】$\Rightarrow$显然，取导列，导列的商因子是Abel群.

  $\Leftarrow$ 根据导群的泛性质，如果有可解列

  $$1 \lhd G_1 \lhd \cdots \lhd G_{r-1} \lhd G$$

  因为商因子均为Abel群，所以根据导群的泛性质可知$G^{(1)} \subset G_{r-1}$，
  $G^{(2)} = [G^{(1)}, G^{(1)}] \subset [G_{r-1}, G_{r-1}] \subset G_{r-2}$.（最后一个包含又用到导群的泛性质），这样依次归纳下去得到$G^{(k)} \subset G_{r-k}$，所以$G^{(r)} \subset 1 \Rightarrow G^{(r)} = 1$，故$G$可解.$\square$

- 【命题】若G可解，则G的任何子群和商群可解

  若$N \lhd G$，N与G/N均可解，则G可解（与合成列相关结论是类似的）

  【证明】注意两个事实：

  - $H \leq G$给出$H^{(i)} \leq G^{(i)}$
  - $N \lhd G$，$G/N = \overline{G}$，则$\overline{G^{(i)}} = \overline{G}^{(i)}$，前者是$G^{(i)}$在商同态下的像.

  第二个事实是用wk8hw-11. $i=0$时不用证明，若对$i-1$成立则：

  $$\overline{G^{(i)}} = \overline{[G^{(i-1)}, G^{(i-1)}]} = [\overline{G^{(i-1)}}, \overline{G^{(i-1)}}] = [\overline{G}^{(i-1)}, \overline{G}^{(i-1)}] = \overline{G}^{(i)}$$

  第一个等号是定义，第二个是作业，第三个是归纳假设，第四个是定义.

  有了这两个事实，命题是显然的.$\square$

  【remark】也可以用可解列版本的定义来证明. 将商群可解列提升为从N开始的终止于G的次正规列，其商因子得到继承，所以得到G的一个商因子都Abel的次正规列.

- 【命题】G有限，则G可解当且仅当G的合成列（由Jordan-Holder，不计次序下唯一）的合成因子都是素数阶循环群.

  $\Leftarrow$显然

  $\Rightarrow$ G可解，所以G有可解列，因为G是有限群，所以商因子是有限Abel群，而有限Abel群的合成因子和其阶数的素因子一一对应，所以每个商因子有合成列且合成因子为素数阶循环群，一步一步地将商群提升并塞入G的可解列之间，根据合成因子得到继承可知G的合成列的合成因子都是素数阶循环群，这些合成因子就是每个有限Abel群的商因子的合集$\square$

- 【例】有限Abel群一定可解

  非Abel单群总是不可解，因为$G^{(1)} = G$.

  $A_n(n \geq 5)$非Abel单，不可解，$S_n(n \geq 5)$也不可解，因为$S_n^{(1)} = A_n$，而可解性是会被子群继承的，所以$A_n(n \geq 5)$不可解$\Rightarrow$ $S_n(n \geq 5)$不可解.

- 【例】小于60阶的群都可解（A_5是最小阶的非Abel单群，事实上也是最小阶的不可解群，这是因为若$|G| < 60$，则其合成因子的阶必然< 60，从而G的合成因子是小于60阶单群所以都是Abel单群即素数阶循环群，所以G的合成列都是可解列，所以G可解）

- 【引理】p群可解.

  【证明】$Z(G) \neq 1$，对$|G|$数学归纳法，因为$|G/Z(G)|$也是p群且阶数严格小于$|G|$，所以根据归纳假设可知$G/Z(G)$可解，而$Z(G)$是Abel群必然可解，根据前面的命题知G可解.$\square$

- 【定理】Burnside定理，p, q素，则$p^a q^b$阶群都可解

  【推论】不可解群有至少3个不同素因子

- 【定理】奇阶定理，奇数阶群都可解

4. 幂零群

- G是群，$G_1 := G$，$G_2 := [G, G]$，$G_3 := [G, G_2]$，$\cdots$.

  幂零群：若存在$k \geq 1$使得$G_k = 1$，则称G是幂零群

  注意$G^{(i-1)} \subset [G, G_{i-1}] = G_i$，所以：

- 【命题】幂零$\Rightarrow$可解

- 【命题】若G幂零，则其商群和子群都幂零

  若$N \lhd G$，N和G/N都幂零，一般没有G幂零.

  但是，如果$N \leq Z(G)$且G/N幂零，则G幂零.

  【证明】可证明$\overline{G_k} = (\overline{G})_k$，所以：商群幂零$\Rightarrow$存在$k$使得$G_k \subset N$，而$N \leq Z(G)$，所以$G_k \leq Z(G)$，所以$G_{k+1} = [G, G_k] \leq [G, Z(G)] = 1$, 所以$G$幂零.$\square$

- 【命题】Abel群幂零.

- 【命题】p群幂零

  【证明】（降阶+数学归纳法），$|G/Z(G)| < |G|$且$G/Z(G)$是p群，对$|G|$用数学归纳法，根据归纳假设$G/Z(G)$幂零，根据以上命题（取$N = Z(G)$）得G幂零.$\square$

- 【命题】有限群幂零当且仅当其Sylow子群都正规.

- 【例】$C_7 \rtimes C_3$，其Sylow 3-子群不正规，所以不幂零. 但是取N_7则N_7幂零且G/N_7也幂零，这说明若$N \lhd G$，N和G/N都幂零，一般没有G幂零.