arXiv:2305.01987v1 [math.GR] 3 May 2023

有限阿贝尔群的算术

路易·马莱-布尔盖

2023年5月4日

目录

1 引言 **2**

2 有限阿贝尔群概述 **2**
2.1 对偶性.2 2.2 子群与商群之间的对应关系.4 2.3 同构于某个固定群的子群.4

3 阿贝尔函数 5
3.1 阿贝尔函数代数.5 3.2 乘法函数.6 3.3 与狄利克雷卷积的联系.8 3.4 示例.9 3.5 μ 的计算.10 3.6 应用.12

4 通过群作用计数 15
4.1 自由作用.15 4.2 正则作用.15 4.3 对于 G 阿贝尔时计算 $L_t(G)$.17

5 对称群的生成 **18**
5.1 等距变换与间隙.18 5.2 应用.20 5.3 等距变换的描述.21

6 展望 **22**

1 引言

本文旨在介绍多种处理有限阿贝尔群的技巧。我们引入狄利克雷卷积的一种类似运算，用以获得关于有限阿贝尔群的组合结果。

原来，*Delsarte* 已经引入了这一工具 [1], ；我是在与一位同事讨论时才意识到这一点的。

接下来，我们利用正则作用的概念得到一个令人惊讶的事实：有限阿贝尔群的生成子集数量 G 可被 G 的基数整除。

最后，我们证明一个关于有限阿贝尔群的对称群的生成定理：利用对换以及由群 G 中的元素所诱导的平移来生成该对称群G 。

2 有限阿贝尔群概述

首先，我们回顾有限阿贝尔群的一些有用事实。关于记号，我们用 $|X|$ 表示有限集合 X 的基数，有时也用 $\mathbb{Z}_n$ 表示 $\mathbb{Z}/n\mathbb{Z}$。最后，若 G 是一个群，我们用 $H \leq G$ 表示 H 是 G 的子群，并用 $H < G$ 表示 H 是 G 的真子群。

2.1 对偶性

设 G 为一个有限阿贝尔群。记 $\widehat{G}$ 为 G的对偶群，即从 G 到 $\mathbb{C}^\times$ （复数域的乘法群）的态射所构成的群，这些态射也称为特征。回顾一下， G 同构于若干循环群的乘积$\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$，其中 $d_1 > 1$和 $d_1 \mid d_2 \mid \cdots \mid d_n$，且这些系数（称为不变因子）是唯一确定的。有限阿贝尔群乘积的对偶群等于各对偶群的乘积，而 $\mathbb{Z}_n$ 的对偶群同构于 $\mathbb{Z}_n$，其中选取一个本原 n次单位根。由此可得：

$$G \cong \widehat{G}$$

然而，一般而言，这两个群之间不存在典范同构。注意，态射 $f\colon G \longrightarrow H$ 会诱导出一个态射 $f^*\colon H \longrightarrow G$，其定义为 $f^*(\chi) = \chi \circ f$。这定义了一个从有限阿贝尔群范畴到其自身的反变函子。

命题。（双对偶性）设 G 为一个有限阿贝尔群。存在一个同构：

$$G \xrightarrow{\alpha_G} \widehat{\widehat{G}}$$

将 x 映射为特征 $\chi \mapsto \chi(x)$。这个同构关于 G 是自然的，也就是说，对于任意有限阿贝尔群之间的态射 $f : G \longrightarrow H$，下图可交换：

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle \alpha_G}\downarrow & & \downarrow{\scriptstyle \alpha_H} \\ \widehat{\widehat{G}} & \xrightarrow[f^{**}]{} & \widehat{\widehat{H}} \end{array}$$

因此，**有限阿贝尔群范畴与其对偶范畴等价**。这尤其导出了子群与商群之间的对应关系。

$\widehat{\ }$**证明。** α_G 显然是一个定义良好的态射，从 G到 G。图表 $\widehat{\ }$可交换：设 $x \in G$ 且 $\chi \in H$：

$$f^{**}(\alpha_G(x))(\chi) = (\alpha_G(x) \circ f^*)(\chi) = f^*(\chi)(x) = \chi \circ f(x)$$

et：

$$\alpha_H(f(x))(\chi) = \chi(f(x))$$

□

定义。 *(湮灭子与核)* 对于 $H \leq G$，记 $H^\perp$ 为 H的湮灭子，也就是说，它是 $\widehat{G}$ 中在 H上取值为零的特征所组成的子群。对于 $K \leq \widehat{G}$，记 $K^\top$ 为 K的核，也就是说，它是 $\chi \in K$的核的交集。

$\widehat{\ }$**命题。** 设 $H \leq G$ 和 $K \leq G$。有如下典范同构：

$$\boxed{\widehat{G/H} \cong H^\perp}$$

et：

$$\boxed{K^\top \cong \widehat{\widehat{G}/K}}$$

特别地：$|G| = |H| \times \left|H^\perp\right| = |K| \times \left|K^\top\right|$。此外还有如下相容性：$\widehat{\ }(H^\perp)^\top = H$ 和 $(K^\top)^\perp = K$。最后，若将 $(H^\perp)^\perp$ 视为 $\widehat{G}$的一个子群，则：

$$\alpha_G(H) = H^{\perp\perp}$$

关于 $\top$也有类似的关系。注意，$\perp$ 和 $\top$ 在 G的子-$\widehat{\ }$群与 G的子群之间定义了一个双射。

$\widehat{\ }$**证明。**首先，$G/H = \mathrm{Hom}(G/H, \mathbb{C}^\times) \cong \{f \in \mathrm{Hom}(G, \mathbb{C}^\times) \mid H \subseteq \mathrm{Ker}\ f\} = H^\perp$，根据商的泛性质。其次：$\widehat{G/K} = \mathrm{Hom}(G/K, \mathbb{C}^\times) \cong \{f \in G \mid K \subseteq \mathrm{Ker}\, f\} \cong \{x \in G \mid \forall \chi \in K\ \chi(x) = 0\} = K^\top$。基数相等可直接推出，因为有限阿贝尔群与其对偶群同构。接下来显然有：

$$H^{\perp\top} \supseteq H$$

而另一包含关系根据基数理由成立。第二个等式也可用同样的方法证明。最后，显然有 $\alpha_G(H) \subseteq H^{\perp\perp}$，而另一包含关系也同样根据基数理由成立。

□

2.2 子群与商群之间的对应

命题。 设 G 是一个有限阿贝尔群。记 $\mathcal{S}(G)$为G的子群集合。存在一个从 $\mathcal{S}(G)$到 $\mathcal{S}(G)$的递减双射，其逆映射也递减（关于包含关系），使得对任意 $H \leq G$：

$$\Gamma(H) \cong G/H$$

et

$$\Gamma^{-1}(H) \cong G/H$$

我们将这样的双射称为**分划** Γ。因此，分划给出了 G 的子群与 G的商群之间的一一对应。

$\widehat{\ }$证明。 取一个从 G 到 G的同构 θ 。显然，这样的同构诱导出一个双射 Θ ，将 G 的子群对应到 G的子群。于是令Γ复合映射为:

$$\mathcal{S}(G) \xrightarrow{\Theta} \mathcal{S}(\widehat{G}) \xrightarrow{\bullet^{\top}} \mathcal{S}(G)$$

这是两个双射的复合，其中一个递增，另一个递减，因此它是一个递减双射（其逆映射也同样如此）。接下来只需验证:

$$\Gamma(H) = \Theta(H)^{\top} \cong \widehat{\widehat{G}/\Theta(H)} \cong \widehat{G}/\Theta(H) = \theta(G)/\theta(H) \cong G/H$$

et

$$\Gamma^{-1}(H) = \Theta^{-1}(H^{\perp}) \cong H^{\perp} \cong \widehat{G/H} \cong G/H$$

原则上，这些同构并非典范的，即使已经固定了 Γ 也是如此。 □

一个有趣的推论是以下事实:

命题。 设 G 为一个有限阿贝尔群。记 $\min G$ 为 G的一个生成集的最小基数。回顾一下，$\min G/H \leq \min G$（如果 x_1，...，x_n 生成 G，那么它们的像生成 G/H）。因此，根据子群与商群之间的对应关系，我们可以直接得到，对于任意 $H \leq G$：

$$\min H \leq \min G$$

2.3 与某个固定群同构的子群

我们将多次使用以下引理:

引理。 设 A 和 B 是两个有限阿贝尔群。记 $\mathrm{Sub}_B(A)$ 为与 B 同构的 A 的子群集合，$\mathrm{Mono}(B, A)$ 为从 B 到 A的单射态射（或单态射）集合。那么:

$$\boxed{|\mathrm{Sub}_B(A)| = \frac{|\mathrm{Mono}(B, A)|}{|\mathrm{Aut}\, B|}}$$

证明。要证明这一点，只需注意到 Aut B 在 Mono(B, A) 上自由作用，并且该作用的轨道对应于从 B 到 A的单态射的同构类，也就是与 B同构的 A的子群。

更准确地说，如果 $g \in \mathrm{Aut}\, B$ 且 $f \in \mathrm{Mono}(B, A)$，则 g 在 f 上的作用由 $f \cdot g = f \circ g$ 给出（右作用）。 □

3 阿贝尔函数

3.1 阿贝尔函数代数

我们考虑有限阿贝尔群的一个按同构分类的代表元系，$\mathbb{G}$。为了遵循集合论，可以取对称群的阿贝尔子群，但我们不打算关注这类问题。记 $\mathbb{A}$ 为从 $\mathbb{G}$ 到 $\mathbb{C}$ 的 $\mathbb{C}$ 向量空间。这些应用称为**阿贝尔函数**。在 $\mathbb{A}$ 上定义卷积乘积如下：设 f、$g \in \mathbb{A}$，定义：

$$\boxed{f * g(G) = \sum_{H \leq G} f(H) g(G/H)}$$

对于 $G \in \mathbb{G}$（求和遍历 G 的所有子群，而不仅仅是按同构分类的代表元）。这里，应将 $f(G)$ 理解为 $f(G_0)$，其中 G_0 是 G 的同构类的代表元。此外，还可以将 $\mathbb{A}$ 的元素视为一些“应用”，它们将一个有限阿贝尔群 G 映射为一个与 G 的同构类无关的数值。我们还定义一种逐项乘积：

$$f \cdot g(G) = f(G) g(G)$$

另外，注意到 fg 和 $f * g$ 是良定义的，因为它们在 G 处的取值不依赖于 G 的选择（在同构意义下）。我们注意到，δ 是一个在平凡群上取值为 1、在其他所有群上取值为 0 的阿贝尔函数，它是 $*$ 的单位元。

定义。（代数 $\mathbb{A}$）
$(\mathbb{A}, *)$ 是一个交换的、结合的且含幺的 $\mathbb{C}$-代数。**在下文中，$\mathbb{A}$ 将表示 $\mathbb{C}$-代数 $\mathbb{A}$，其运算为 $*$。**

其可逆元恰好是满足 $f(1) \neq 0$ 的函数 f。因此，$\mathbb{A}$ 是一个局部环。

证明。固定 $G \in \mathbb{G}$。选取 G 上的一个分划 $\mathcal{S}(G) \xrightarrow{\Gamma} \mathcal{S}(G)$。考察其交换性：

$$f * g(G) = \sum_{H \leq G} f(H) g(G/H) = \sum_{K \leq G} f(\Gamma^{-1}(K)) g(K) = \sum_{K \leq G} f(G/K) g(K) = g * f(G)$$

令 $K = \Gamma(H)$（双射变量替换）。
现在来看结合律:

$$\begin{aligned} f * (g * h)(G) &= \sum_{H \le G} f(H)(g * h)(G/H) \\ &= \sum_{H \le G} \sum_{K \le G/H} f(H) g(K) h(G/H/K) \\ &= \sum_{H \le G} \sum_{H \le L \le G} f(H) g(L/H) h\left(\frac{G/H}{L/H}\right) \\ &= \sum_{H \le G} \sum_{H \le L \le G} f(H) g(L/H) h(G/L) \end{aligned}$$

et :

$$\begin{aligned} (f * g) * h(G) &= \sum_{L \le G} (f * g)(L) h(G/L) \\ &= \sum_{L \le G} \sum_{H \le L} f(H) g(L/H) h(G/L) \end{aligned}$$

δ 是单位元　　对于 $*$：根据交换律，只需验证 $f * \delta = f$，这显然成立　　:

$$f * \delta(G) = \sum_{H \le G} f(H) \delta(G/H) = f(G)$$

接下来，若 $f(1) \neq 0$，我们可以对 G 的阶进行归纳，构造一个数 $g(G)$，它在同构意义下仅取决于 G：令 $g(1) = 1/f(1)$，对于任意非平凡群 G:

$$\boxed{g(G) = -\frac{1}{f(1)} \sum_{H < G} g(H) f(G/H)}$$

由强归纳法可知其定义良好（右边的项在同构意义下不依赖于 G，因为对于 $H < G$，$g(H)$ 的情形确实如此）。因此，g 定义了一个阿贝尔函数，并且容易验证（用强归纳法）:

$$f * g = g * f = \delta$$

因此，不可逆元素的集合是由在 1 处取值为零的 f 构成的极大理想，所以它是 $\mathbb{A}$的唯一极大理想。

□

3.2 乘法函数

引理。（互素阶群的乘积的子群）
设 G和 H 是两个有限群，其基数函数分别为 m 和 n，且二者互素。那么，$G \times H$ 的子群恰好是形如 $A \times B$ 的乘积，其中 $A \le G$ 且 $B \le H$，因此存在一个双射:

$$\boxed{\mathcal{S}(G) \times \mathcal{S}(H) \xrightarrow{\sim} \mathcal{S}(G \times H)}$$

证明。设 $K \leq G \times H$。令 $A = \pi_G(K)$ 和 $B = \pi_H(K)$。取一个贝祖等式 $1 = mu + nv$。设 $(a, b) \in A \times B$。存在 $c \in H$ 和 $d \in G$ 使得：$(a, c) \in K$ 且 $(d, b) \in K$。因此：

$$(a, c)^{nv}(d, b)^{mu} = (a, b)$$

根据拉格朗日定理，因此 $(a, b) \in K$。此外，K 显然包含于 $A \times B$，因此：

$$K = A \times B$$

因此，将 (A, B) 映射到 $A \times B$ 的应用 $\mathcal{S}(G) \times \mathcal{S}(H) \longrightarrow \mathcal{S}(G \times H)$ 是满射，并且是单射，因为 $A = \pi_G(A \times B)$ 且 $B = \pi_H(A \times B)$。 □

定义。 *(*乘法函数*)* 阿贝尔函数 f 称为**乘法的**，如果对任意阶互素的 $G, H \in \mathbb{G}$，都有：$f(G \times H) = f(G)f(H)$，并且 $f(1) = 1$。记 $\mathbb{M}$ 为乘法阿贝尔函数的集合，它是 $\mathbb{A}^\times$的一个子群。若对任意 G 和 H，该关系均成立，则称 f为**完全乘法的**。

证明。首先，根据前一个命题，$\mathbb{M} \subseteq \mathbb{A}^\times$。其次，两个乘法阿贝尔函数的乘积仍是乘法的：若 f 和 g 是乘法的，则有 $f * g(1) = f(1)g(1) = 1$，并且对于 $|G| \wedge |H| = 1$：

$$f * g(G \times H) = \sum_{K \leq G \times H} f(K)g((G \times H)/K) = \sum_{A \leq G,\ B \leq H} f(A \times B)g(G/A \times H/B)$$

由前一个引理可知。又由于 A和 B 的阶互素（根据拉格朗日定理），G/A和 H/B也同样如此，因此，根据 f 和 g 的积性：

$$f * g(G \times H) = \sum_{A \leq G,\ B \leq H} f(A)f(B)g(G/A)g(H/B) = (f * g(G))(f * g(H))$$

因此，$f * g$ 具有积性。现在证明 f^{-1} 具有积性。为此，我们对 $|G| \times |H|$ 使用强归纳法，证明当 $|G| \wedge |H| = 1$ 时：$f^{-1}(G \times H) = f^{-1}(G)f^{-1}(H)$。如果 G是平凡的，或者 H是平凡的，这是显然的。假设 G和 H都不是平凡的。

根据归纳假设，我们可以写成：

$$\begin{aligned}
0 &= \delta(G \times H) \\
&= \sum_{\substack{A \leq G \\ B \leq H}} f^{-1}(A) f^{-1}(B) f(G/A) f(H/B) \\
&= \sum_{\substack{A < G \\ B < H}} f^{-1}(A) f^{-1}(B) f(G/A) f(H/B) + f^{-1}(G \times H) \\
&\quad + \sum_{A<G} f^{-1}(A) f^{-1}(H) f(G/A) + \sum_{B<H} f^{-1}(B) f^{-1}(G) f(H/B) \\
&= \sum_{A<G} f^{-1}(A) f(G/A) \sum_{B<H} f^{-1}(B) f(H/B) + f^{-1}(G \times H) \\
&\quad - f^{-1}(H) f^{-1}(G) - f^{-1}(G) f^{-1}(H) \\
&= (-1)^2 f^{-1}(G) f^{-1}(H) - 2 f^{-1}(G) f^{-1}(H) + f^{-1}(G \times H)
\end{aligned}$$

因此 $f^{-1}(G \times H) = f^{-1}(G) f^{-1}(H)$，由此完成归纳证明。$\mathbb{M}$因此是 $\mathbb{A}^\times$ 的一个子群（δ 显然是乘法的）。 □

3.3 与狄利克雷卷积的联系

定义。 *(*定义在 $\mathbb{N}^*$上的算术函数*)* 也可以将 $\mathbb{A}_{\mathbb{N}^*}$ 定义为从 $\mathbb{N}^*$ 到 $\mathbb{C}$ 的函数构成的 $\mathbb{C}$-代数，其卷积乘积为 $f * g(n) = \sum_{d|n} f(d) g(n/d)$。类似地定义乘法函数 $\mathbb{M}_{\mathbb{N}^*}$（它们是满足 $f(1) = 1$且只要 $a \wedge b = 1$就有 $f(ab) = f(a) f(b)$ 的算术函数）。注意，$\mathbb{A}_{\mathbb{N}^*}$是一个局部整环。

命题。 我们有一个 $\mathbb{C}$-代数的满射态射：

$$\mathbb{A} \longrightarrow \mathbb{A}_{\mathbb{N}^*}$$

将 f 映射到 $n \mapsto f(\mathbb{Z}/n\mathbb{Z})$。
核是由在循环群上取值为零的阿贝尔函数构成的素理想。该态射诱导出一个满射的阿贝尔群态射：

$$\mathbb{M} \longrightarrow \mathbb{M}_{\mathbb{N}^*}$$

证明。 容易验证，这是一个代数态射，因为 $\mathbb{Z}/n\mathbb{Z}$ 的子群（及其商群）与 n的因子一一对应。满射性显而易见，而核是一个素理想，因为 $\mathbb{A}_{\mathbb{N}^*}$ 是整环。

接下来，如果 $f \in \mathbb{M}$，那么它在 $\mathbb{A}_{\mathbb{N}^*}$ 中的像是乘法性的，因为如果 $m \wedge n = 1$，$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(mn)\mathbb{Z}$。
这个态射的满射性仍然成立：设 $f \in \mathbb{M}_{\mathbb{N}^*}$。我们只需定义，对于$G \in \mathbb{G}$： $g(G) = f(n)$，如果 G 是阶为 n的循环群，则取该值；如果 G 不是循环群，则取 0。容易验证，g 是乘法性的。 □

3.4 示例

现在给出几个重要的阿贝尔函数示例。 .

定义。 恒等函数 1（恒为 1）是乘法函数，因此存在乘法逆函数。**记 μ 为这个逆函数（阿贝尔莫比乌斯函数）**。根据前面关于狄利克雷卷积的命题，对于任意$n \in \mathbb{N}^*$，有 $\mu(\mathbb{Z}/n\mathbb{Z}) = \mu(n)$。下一部分将给出有限阿贝尔群 G 的 $\mu(G)$ 的显式公式。

我们也用 $\varphi(G)$ 表示 G 的生成元数。同样，有 $\varphi(\mathbb{Z}/n\mathbb{Z}) = \varphi(n)$。基数函数显然是乘法函数，并诱导出从 $\mathbb{N}^*$ 到 $\mathbb{M}_{\mathbb{N}^*}$的恒等函数。**子群数** 函数就是 $1*1$（它也是**商群数**函数）。

命题。 φ 是乘法函数，且 $\varphi * 1 =$ 基数函数，即 $\varphi = \mu *$ 基数函数。

证明。设 $G \in \mathbb{G}$。我们按元素所生成的子群对 G 中的元素进行分组：

$$|G| = \sum_{H \leq G} \varphi(H)$$

因此 $\varphi*1 =$ 基数函数和 $\varphi = \mu*$基数函数 $\in \mathbb{M}$，因为 $\mathbb{M}$ 是一个群。注意，借助前面定义的态射，我们也可以由此推出欧拉函数的积性。 □

通过相同的方法，可以证明生成 G 的 t 元组（$a_1, \ldots, a_t$）的数量给出了乘法函数 $\mu * (G \mapsto |G|^t)$。因此，函数 μ 在许多计算中都会发挥作用。我们还可以研究由 d 个元素组成、能够生成 G 的子集数量，并由此得到 $\mu * \binom{|\bullet|}{d}$。

最后，函数 $N_t = \mu * t^{|\bullet|}$ 对于 $t \geq 1$ 在下一节中会用到，我们将看到 $|G| \mid N_t(G)$。

命题 。 N_1 是函数 δ，而 N_2 是生成子集数量 $G.$

证明。有 $N_1 = \mu * 1 = \delta$。下面记 P 为“生成子集数量”函数。对于任意群 $G \in \mathbb{G}$，可以按照这些子集所生成的子群 $H \leq G$ 对 G 的子集进行分组计数：

$$2^{|G|} = \sum_{H \leq G} P(H)$$

因此 $2^{|\bullet|} = P * 1$ 所以 $P = N_2$。 □

3.5 μ 的计算

本部分给出一个显式公式，用不变因子表示 $\mu(G)$（其中 $\mu * 1 = \delta$）。为此，由于 μ 是乘法性的，显然只需计算 p-群的情形。

命题。（在 $\mathbb{F}_p$ 上的向量空间情形）设 p 为素数且 $n \in \mathbb{N}$。有：

$$\boxed{\mu\left(\mathbb{Z}_p^n\right) = (-1)^n p^{\frac{n(n-1)}{2}}}$$

特别地，这个例子表明 μ 不是有界的（不同于通常的 Möbius 函数 μ ）。

证明。 $\mathbb{Z}_p^n$ 的子群恰好是 $\mathbb{Z}_p^n$ 的 $\mathbb{F}_p$-子向量空间，因此它们（在同构意义下）具有 $\mathbb{Z}_p^d$ 的形式，其中 d 为其维数。对于 $0 \le d \le n$ ，与 $\mathbb{Z}_p^d$ 同构的 $\mathbb{Z}_p^n$ 的子群数为：

$$\frac{\left|\mathrm{Mono}(\mathbb{Z}_p^d, \mathbb{Z}_p^n)\right|}{\left|\mathrm{Aut}\,\mathbb{Z}_p^d\right|} = \frac{(p^n-1)\dots(p^n-p^{d-1})}{(p^d-1)\dots(p^d-p^{d-1})}$$

（见第 2 节）。
话虽如此，显然只需证明对于任意 n ：

$$\sum_{d=0}^{n}(-1)^d p^{d(d-1)/2}\frac{(p^n-1)\dots(p^n-p^{d-1})}{(p^d-1)\dots(p^d-p^{d-1})} = \delta(n)$$

（通过强归纳法，该等式得出所需结果）
记左边为 A_n。显然 $A_0 = 1$ （乘积为空）。对于 $n \ge 1$ ，有：

$$\begin{aligned}
A_n &= \sum_{d=0}^{n}(-1)^d p^0 p^1 \dots p^{d-1}\frac{(p^n-1)\dots(p^n-p^{d-1})}{(p^d-1)\dots(p^d-p^{d-1})} \\
&= \sum_{d=0}^{n}(-1)^d \frac{(p^n-1)\dots(p^n-p^{d-1})}{(p^d-1)\dots(p-1)} \\
&= \frac{1}{D}\sum_{d=0}^{n}(-1)^d (p^{d+1}-1)\dots(p^n-1)\times(p^n-1)\dots(p^n-p^{d-1}) \\
&= \frac{1}{D}\sum_{d=0}^{n}\prod_{i=0}^{d-1}(p^i-p^n)\prod_{i=d+1}^{n}(p^i-1)
\end{aligned}$$

其中， D 是公分母（$p-1$）.....（p^n-1）。现在，我们通过归纳法证明，对于介于 0 和 n 之间的任意 k：

$$\sum_{d=0}^{k}\prod_{i=0}^{d-1}(p^i-p^n)\prod_{i=d+1}^{n}(p^i-1) = \prod_{i=1}^{k}(p^i-p^n)\prod_{i=k+1}^{n}(p^i-1)$$

对于 $k=0$，结论显然成立。假设命题在 $k<n$ 处成立，并证明它在 $k+1$ 处仍然成立：

$$\begin{aligned}\sum_{d=0}^{k+1}\prod_{i=0}^{d-1}(p^i-p^n)\prod_{i=d+1}^{n}(p^i-1) &= \prod_{i=1}^{k}(p^i-p^n)\prod_{i=k+1}^{n}(p^i-1)+\prod_{i=0}^{k}(p^i-p^n)\prod_{i=k+2}^{n}(p^i-1)\\ &= \prod_{i=1}^{k}(p^i-p^n)\prod_{i=k+2}^{n}(p^i-1)\times\left(p^{k+1}-1+1-p^n\right)\\ &= \prod_{i=1}^{k}(p^i-p^n)\prod_{i=k+2}^{n}(p^i-1)\times\left(p^{k+1}-p^n\right)\\ &= \prod_{i=1}^{k+1}(p^i-p^n)\prod_{i=k+2}^{n}(p^i-1)\end{aligned}$$

这就完成了递推。在第 $k=n$ 步我们得到：

$$A_n=\frac{1}{D}\prod_{i=1}^{n}(p^i-p^n)=0=\delta(n)$$

因为 $n\geq 1$。 □

原则上，前面的计算通常不足以得到 $\mu(G)$。幸运的是，对于所有其他 p-群，μ 结果为零。

命题。设 G 是一个非初等阿贝尔 p群（这意味着存在一个阶为 p^k 且满足 $k\geq 2$的元素）。则有：

$$\mu(G)=0$$

证明。我们通过对 $|G|$ 进行强归纳法来证明。假设对于所有阶严格小于 $|G|$ 的非初等 p-阿贝尔群，该命题都成立（无需初始化）。于是有：

$$\mu(G)=-\sum_{H<G}\mu(H)$$

根据归纳假设，只有初等子群对这个和有贡献。记 G 的 p-挠子群为 $G(p)$，因此有：

$$\mu(G)=-\sum_{H\leq G(p)}\mu(H)$$

因为 $G(p)<G$，因为 G 不是初等的。总计：

$$\mu(G)=-\mu*1(G(p))=-\delta(G(p))=0$$

因为 $G(p)\neq 0$。 □

这两个观察可以概括如下：

定理。 如果 G 是初等 p-群的乘积，则记 $\dim_p G$ 为 $\mathbb{Z}_p$ 在将 G 分解为初等 p-群乘积时出现的幂次，并且有：

$$\boxed{\mu(G) = \prod_{p\in\mathbb{P}} (-1)^{\dim_p G} p^{\frac{\dim_p G(\dim_p G-1)}{2}}}$$

其中 $\mathbb{P}$是素数集合。
反之， $\mu(G) = 0$。

证明。 由 μ 的积性和 p-Sylow 分解可直接得到： $G \cong \bigoplus_{p\in\mathbb{P}} \bigoplus_{k\geq 1} \left(\mathbb{Z}_p^k\right)^{n_{p,\,k}}$。 □

定义。 如果 G 是 p-初等群的（有限）乘积，就称其为**初等的** 。初等群恰好是 μ 值非零的群。于是， $\mathbb{G}$ 中初等群构成的子集自然地与 $\mathbb{N}^*$之间存在一个双射，通过 $G \mapsto |G|$建立（两个初等群同构，当且仅当它们的基数相同）。这个集合在乘积、子群和商群运算下也保持不变（ $\mathbb{G}$ 中由循环群构成的子集也具有这一性质，因为循环群也完全由其基数决定）。因此，对于一个初等群 G， $\mu(G)$仅取决于 G的基数。

3.6 应用

给定两个有限阿贝尔群 A 和 B，记 $\mathrm{Mono}(A,B)$ 为从 A 到 B 的单射态射集合，记 $\mathrm{Epi}(A,B)$ 为从 A到 B 的满射态射集合（这些概念分别与有限阿贝尔群范畴中的单态射和满态射概念一致）。由于有限阿贝尔群范畴与其对偶范畴等价，从 A 到 B 的态射数量与从 B 到 A的态射数量相同，因此 $|\mathrm{Mono}(A,B)|$ 和 $|\mathrm{Epi}(B,A)|$ 相等。

命题。 我们有以下关系：

$$|\mathrm{Hom}(A,B)| = |\mathrm{Hom}(B,A)| = \sum_{H\leq A} \left|\mathrm{Mono}\left(\frac{A}{H}, B\right)\right| = \sum_{H\leq B} |\mathrm{Epi}(A,H)|$$

由 $*$的交换性，也可以将其写作 $\sum_{H\leq A} |\mathrm{Mono}\,(H,B)|$。由公式 $\mu * 1 = \delta$ 可立即推出：

$$|\mathrm{Mono}(A,B)| = |\mathrm{Epi}(B,A)| = \sum_{H\leq A} \mu(A/H)\,|\mathrm{Hom}(H,B)| = \sum_{H\leq B} \mu(B/H)\,|\mathrm{Hom}(A,H)|$$

证明。 我们按照核对从 A 到 B 的态射进行分类并计数，其中核可以是 A 的任意（正规）子群：

$$|\mathrm{Hom}(A,B)| = \sum_{H\le A} |\{f \in \mathrm{Hom}(A,B) \mid \mathrm{Ker}\, f = H\}| = \sum_{H\le A} |\mathrm{Mono}(A/H,B)|$$

根据商的泛性质。对于满态射的公式，这次需要按照像（或余核）对从 A 到 B 的态射进行分类并计数。

□

由此可得给定类型子群的子群数公式（如果子群 H de A 的类型为 B，即它同构于 B，则称之为该类型子群）。

命题。 设 A, B 为两个有限阿贝尔群。与 B 同构的 A的子群数为:

$$\boxed{|\mathrm{Sub}_B(A)| = \frac{\sum_{H\le B} \mu(B)\,|\mathrm{Hom}(B/H,A)|}{\sum_{H\le B} \mu(B)\,|\mathrm{Hom}(B/H,B)|}}$$

证明。 使用一般公式:

$$|\mathrm{Sub_B(A)}| = \frac{|\mathrm{Mono}(B,A)|}{|\mathrm{Aut}\, B|}$$

而且， B是有限的，因此自然有 Aut $B =$ Mono(B, B)。接下来只需应用前面的公式。

□

注记。 根据 μ 的计算，如果 B 是一个 p-群，可以将求和限制在 $B(p)$ 的向量子空间上（ B 的 p-扭元）。如果群 B 足够小，以至于可以对 B 的所有向量子空间 H 计算公式中出现的商群 B/H，那么该公式相当有效。Hom 的基数计算很容易，因为 |Hom| 在每个变量上都是可乘的。

现在给出有限群消去定理的一个证明（**仅适用于阿贝尔情形**），该证明改编自 [4]。

引理。 (数值 Yoneda)
设 A、 B 是两个有限阿贝尔群，且对于任意有限阿贝尔群 X，都有:

$$|\mathrm{Hom}(A,X)| = |\mathrm{Hom}(B,X)|$$

那么 A 和 B 同构。对于不一定交换的有限群，这个引理仍然成立，但卷积已不足以证明它（参见 [3]，了解该情形下的证明）。

此外，只需对任意**循环群** X （或者对任意 p群，对任意 p 素数）验证这一等式即可。

证明。 首先注意，对于任意有限阿贝尔群 X，有 $|\mathrm{Mono}(A,X)| = |\mathrm{Mono}(B,X)|$。为此，只需使用公式：

$$|\mathrm{Mono}(A,X)| = \sum_{H \leq X} \mu(X/H)\,|\mathrm{Hom}(A,H)|$$

并利用引理的假设将公式中的 A 替换为 B。与 Yoneda 引理类似，将此关系应用于 A 和 B：$\mathrm{Mono}(A,A)$ 非空，因此 $\mathrm{Mono}(B,A)$ 非空，反之亦然，$\mathrm{Mono}(A,B)$ 非空。由于它们都是有限群，我们依次推出 $|B| \leq |A|$ 和 $|A| \leq |B|$，因此 A 和 B具有相同的基数函数。又因为存在一个与 B同构的 A 的子群，按基数函数可知该子群就是 A。因此，A 和 B 同构。只需对每个循环群或每个 p-群验证这一点，因为有限阿贝尔群是这类群的乘积（并利用乘积的泛性质）。

□

定理。（有限阿贝尔群的化简）
若 A、B、C 是满足 $A \times B \cong A \times C$ 的三个有限阿贝尔群，则 B 和 C 同构。

证明。 我们使用阿贝尔群（有限阿贝尔群）范畴中余积的泛性质：

设 X 是任意一个有限阿贝尔群，则有：

$$|\text{同态集}(A,X)| \times |\text{同态集}(B,X)| = |\text{同态集}(A \times B, X)| = |\text{同态集}(A \times C, X)| = |\text{同态集}(A,X)| \times |\text{同态集}(C,X)|$$

这些因子都不为零，因此得到：

$$|\mathrm{Hom}(B,X)| = |\mathrm{Hom}(C,X)|$$

由数值 Yoneda 引理可得：B 和 C 同构。 □

以下是另一个有趣的推论：

定理。 设 A 和 B 是两个有限阿贝尔群。若对任意 $d \in \mathbb{N}^*$，A 和 B 中阶为 d的元素个数相同，则二者同构。

证明。 假设可表示为：

$$\forall d \in \mathbb{N}^* \ \ |\mathrm{Mono}(\mathbb{Z}/d\mathbb{Z}, A)| = |\mathrm{Mono}(\mathbb{Z}/d\mathbb{Z}, B)|$$

通过卷积（并且由于循环群的子群仍是循环群），可得：

$$\forall d \in \mathbb{N}^* \ \ |\mathrm{Hom}(\mathbb{Z}/d\mathbb{Z}, A)| = |\mathrm{Hom}(\mathbb{Z}/d\mathbb{Z}, B)|$$

于是由数值 Yoneda 引理得证。 □

猜想。 设 A 和 B 为两个有限阿贝尔群。若对于每个 $d \in \mathbb{N}^*$，A 和 B 都具有相同数量的阶为 d的子群，则它们同构。

4 群作用的计数

在本节中，我们将证明关于阿贝尔函数$N_t = \mu * t^{|\bullet|}$的以下定理。

定理。 对于任意 $G \in \mathbb{G}$， $N_t(G)$ 可被 G 的基数整除。特别地， **的生成子集数量**可被 $|G|$ 整除，因为它就是 N_2。

注意，对于循环群，我们得到 $\sum_{d|n} \mu(d) t^{n/d}$ 可被 n 整除；当 t 是 p 的幂时，这一结果也可以通过计数 $\mathbb{F}_t$ 中次数为 d 的首一不可约多项式得出。

4.1 自由作用

设 G 是一个群， X 是一个 G-集合。若 X 的一个元素的稳定子平凡，则称该元素为**自由元素**。记 $L(X)$ 为 X 的自由元素集合。若 X 的所有元素都是自由元素，则称 X 是**自由的**。

注意到 $L(X)$ 在 G 的作用下保持不变，因此自然是一个自由的 G-集合。我们有如下算术性质：

命题。 如果 X 是一个有限的 G-自由集合，那么 G 是有限的，并且 G的基数整除 X的基数。商 $|X| / |G|$ 是 X的轨道数。

推论。 若 X 是有限的 G-集合，且 G 有限，则 $L(X)$ 的基数函数可被 $|G|$ 整除。

证明。 取 $x \in X$，由于 x 的稳定子是平凡的， G 与 $G \cdot x$之间存在一个双射，因此 G 是有限的，并将 X 划分为轨道（每个轨道的大小均为 $|G|$），即可得到 $|G| \mid |X|$。 □

4.2 正则作用

我们希望研究群 G 的一种非常特殊的作用：固定 X 一个集合，并让 G 作用于 $\mathcal{F}(G, X)$（从 G 到 X的应用集合），方式如下：

$$g \cdot \alpha(x) = \alpha(xg)$$

对于所有 $\alpha \in \mathcal{F}(G, X)$、所有 $g \in G$ 以及所有 $x \in X$。容易验证这是一种群作用，称为**作用 X-正则**。

注记。 情形 $X = \{0, 1\}$ 对应于 G 在其幂集上的平移作用（方向相反）。

正则作用在某种意义上具有普遍性：

命题。*(*正则嵌入*)* 设 X 是一个 G-集合。存在一个从 X 到 $\mathcal{F}(G,X)$ 的 G-集合单射态射。换言之，任何 G-集合都可以嵌入一个正则 G集合中。

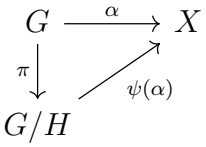
证明。设 $x \in X$。记 $\varphi(x)$ 为函数 $G \longrightarrow X$，它将 g 映射到 gx。显然，这定义了一个单射 $X \hookrightarrow \mathcal{F}(G,X)$，因为 $\varphi(x)(1) = x$。这是一个G-集合的态射：$\varphi(g \cdot x)(h) = hg \cdot x$ 且 $(g \cdot \varphi(x))(h) = \varphi(x)(hg) = hg \cdot x$。 □

定理。设 $H \trianglelefteq G$ 是 G的正规子群。考虑 G/H 上的 X-正则作用以及 $\pi\colon\ G \longrightarrow G/H$ 为商态射。记 $\mathcal{F}(G,X)^H$为由 H的所有元素固定的 $\alpha \in \mathcal{F}(G,X)$的集合（换言之，即稳定子包含$H$的 α）。于是有一个自然双射：

$$\boxed{\mathcal{F}(G,X)^H \cong \mathcal{F}(G/H,X)}$$

此外，将 $\mathcal{F}(G/H,X)$ 自然地视为一个 G 集合时，该双射是一个**同构 G-集合**。

证明。存在自然态射 $\mathcal{F}(G/H,X) \xrightarrow{\varphi} \mathcal{F}(G,X)^H$，定义为 $\beta \mapsto \beta\circ\pi$。$\beta \circ \pi$ 确实由 H 固定：对于任意 $h \in H$ 和 $x \in X$，有 $h \cdot \beta\pi(x) = \beta\pi(xh) = \beta\pi(x)$。反过来，任意元素 $\alpha \in \mathcal{F}(G,X)^H$ 都可经由 π 分解，因为对于任意 $h \in H$和$x \in X$，$\alpha(xh) = h \cdot \alpha(x) = \alpha(x)$，由此可以将 $\psi(\alpha)$ 定义为使图表交换的唯一映射：



因此该图表交换，所以 $\varphi \circ \psi(\alpha) = \alpha$，并且显然对于任意$\beta \in \mathcal{F}(G/H,X)$，由分解的唯一性可知 $\psi \circ \varphi(\beta) = \beta$。

最后，显然，φ 是一个 G-集合态射，由此得出结论。 □

下面记 $\bar{\alpha}$ 为 $\psi(\alpha)$。

推论。对于任意 $\alpha \in \mathcal{F}(G,X)^H$，有（记 Stab 为稳定子）：

$$\boxed{\mathrm{Stab}_{G/H}(\bar{\alpha}) = \mathrm{Stab}_G(\alpha)/H}$$

证明。由于存在这样一个从 G-集合 $\mathcal{F}(G,X)^H$到 $\mathcal{F}(G/H,X)$ 的同构，因此稳定子之间具有相容性。换言之，对于任意 $\alpha \in \mathcal{F}(G,X)^H$，$\alpha$ 的稳定子也是 $\bar{\alpha}$ 的稳定子，其中将 $\mathcal{F}(G/H,X)$ 看作一个 G-集合。因此有：

$$\mathrm{Stab}_G(\alpha) = \mathrm{Stab}_G(\bar{\alpha})$$

因此，$\mathrm{Stab}^{G/H}(\bar{\alpha}) = \mathrm{Stab}_G(\bar{\alpha})/H$(清楚)。由此可得所需公式。 □

由上述内容可知，对于 $H \trianglelefteq G$，自由元素与 $\mathcal{F}(G/H,\ X)$ **中稳定子为**H 的元素之间存在一一对应关系。

定义。当 G 和 X 有限时，记 $L_{|X|}(G)$ 为 $\mathcal{F}(G,X)$的自由元素个数（这只取决于 $|X|$ 和 G，且在同构意义下确定）。注意，根据前文所述，这个数**能被** $|G|$ 整除。

采用这一记法，有：

$$\boxed{L_{|X|}(G/H) = |\{\alpha \in \mathcal{F}(G,X) \mid \operatorname{Stab}\alpha = H\}|}$$

4.3 计算 $L_t(G)$ 在 G 阿贝尔时的情形

我们可以将 L_t （前面定义的函数）视为一个阿贝尔函数。于是可以得到这个数的一个简洁公式：

命题。设 $t \geq 1$。有如下阿贝尔函数等式：

$$\boxed{L_t = N_t}$$

其中 $N_t = \mu * t^{|\bullet|}$,

证明。取一个含有 t 个元素的 X，并按照各元素的稳定子对其进行分组，从而计算 $\mathcal{F}(G,X)$：

$$t^{|G|} = \sum_{H \leq G} |\{\alpha \in G \mid \operatorname{Stab}(\alpha) = H\}| = \sum_{H \leq G} L_t(G/H)$$

因此我们有 $t^{|\bullet|} = 1 * L_t$。对 μ 进行卷积可得：

$$L_t = \mu * t^{|\bullet|} = N_t$$

□

推论。本节开头引入的定理可直接由此推出，因为$L_t(|G|)$能被 $|G|$整除：**的生成子集数量能被**$|G|$整除。此外，我们还有如下算术结果（将上述结论特化到群$\mathbb{Z}/n\mathbb{Z}$即可得到）：

$$\boxed{\sum_{d|n} \mu(d) t^{n/d} \equiv 0 \ [n]}$$

5 对称群的生成

5.1 等距变换与间隙

考虑一个阿贝尔群（不一定是有限群） G，**其元素至少有 3 个**，以及它的凯莱嵌入 $G \longrightarrow \mathfrak{S}_G$。下文中，我们将 G与其在凯莱嵌入下的像视为相同，因此记作 $G \subseteq \mathfrak{S}_G$。我们提出如下问题（例如在伽罗瓦理论中经常会遇到）：要生成 $\mathfrak{S}_G$，还需要在 G 中加入什么?

我们先从一个一般性结果开始:

引理。设 X 是一个集合。X 的有限支撑置换全体 $\mathfrak{S}_X^f$，是由对换生成的 $\mathfrak{S}_X$ 的子群。

证明。显然，$\mathfrak{S}_X^f$ 是包含对换的 $\mathfrak{S}_X$ 的子群。接下来，若 $\sigma \in \mathfrak{S}_X^f$，考虑其有限支撑 S 以及 σ的自然限制 $\eta \in \mathfrak{S}_S$。由于 S 是有限的，$\mathfrak{S}_S$ 由对换生成，因此可以将 η 写成对换的乘积，进而 σ也可以写成对换的乘积。 □

定义。（模 H等距变换）设 H 是 G的一个子群。元素 $\sigma \in \mathfrak{S}_G$ 称为**模等距映射** H，如果对任意 x、$y \in G$，都有:

$$\sigma(x) - \sigma(y) \equiv x - y \ [H]$$

模 H 的等距变换构成 $\mathfrak{S}_G$ 的一个子群，包含 G，记作 $O(H)$。

定义。（K 的间隙）现在设 K 是 $\mathfrak{S}_G$ 的一个子群，包含 G（这样的群称为 Cayley 群）。若满足以下等价条件之一，则称元素 $\delta \in G$ 是 K 的一个**间隙**:

— $(0\ \delta) \in K$
— $\exists g \in G\ (g\ g+\delta) \in K$
— $\forall g \in G\ (g\ g+\delta) \in K$

K 的间隙构成 G 的一个子群，记作 $\Delta(K)$.

证明。**这三个条件等价:** 第三个条件显然推出第一个条件，第一个条件推出第二个条件；若第二个条件成立，取一个满足 $(g\ g+\delta) \in K$ 的 g；设 $h \in G$，则有:

$$(h\ h+\delta) = (h-g) \circ (g\ g+\delta) \circ (g-h) \in K$$

因为 K 是 Cayley 群。

$\Delta(K)$ **是** G **的一个子群:** 显然有 $0 \in \Delta(K)$。设 $x, y \in \Delta(K)$，则 $(0\ x) \in K$，因此 $(x\ 0) \in K$，故 $-x \in \Delta(K)$。接下来 $(x\ x+y) \in K$，所以在 x 和 $x+y$ 均非零时，对其进行共轭可得:

$$(0\ x+y) = (x\ x+y)(0\ x)(x\ x+y) \in K$$

因此 $x+y \in \Delta(K)$。反之则显而易见。 □

由此定义了一个保序映射 $O:\ \mathcal{S}(G)\ \longrightarrow\ \mathcal{S}_c(\mathfrak{S}_G)$（Cayley子群），以及一个保序映射 $\Delta:\mathcal{S}_c(\mathfrak{S}_G)\ \longrightarrow \mathcal{S}(G)$。一般而言，它们并非彼此互逆，但仍有：

定理。 Δ是满射， O 是单射，并且：

$$\boxed{\Delta \circ O = \mathrm{id}}$$

此外， O 具有一个左伴随， L 由下式给出：

$$L(K) = \langle \sigma(x) - \sigma(y) - x + y \mid \sigma \in K, x, y \in G \rangle$$

证明。 只需证明 $\Delta \circ O = \mathrm{id}$。设 H 是 G的一个子群，则有 $H \subseteq \Delta \circ O(H)$，因为给定一个 $h \in H$，$(0\ h)$ 确实是一个模等距映射。接下来，如果$\delta \in \Delta \circ O(H)$，那么 $(0\ \delta) \in O(H)$。由于 G 至少有 3 个元素，因此存在 $x \in G \setminus \{0, \delta\}$，使得：

$$(0\ \delta)(x) - (0\ \delta)(0) \equiv x - 0\ [H]$$

Autr也就是说， $x - \delta - x \in H$ 因此 $\delta \in H$。 L 与 O 之间的伴随关系显而易见。 . □

定义。 (由子集生成的Cayley子群)
如果 $S \subseteq \mathfrak{S}_G$，记包含 S 的最小凯莱子群为 $(\!(S)\!)$。显然，$(\!(S)\!) = \langle G \cup S \rangle$。

命题。 对于 $\tau = (x\ y)$，有如下关系：

$$\boxed{\Delta((\tau)) = \langle y - x \rangle}$$

更一般地，对于 $\tau_i = (x_i\ y_i)$，若 $1 \le i \le n$，则有：

$$\boxed{\Delta((\tau_1, \ldots, \tau_n)) = \langle \delta_1, \ldots, \delta_n \rangle}$$

其中 $\delta_i = y_i - x_i$。

证明。 显然 $\Delta((\tau_1, \ldots, \tau_n)) \supseteq \langle \delta_1 \ldots, \delta_n \rangle$，因为 $\tau_i \in (\!(\tau_1, \ldots, \tau_n)\!)$。接下来奇妙之处出现了：$\tau_i \in O(\langle \delta_1, \ldots, \delta_n \rangle)$，因此 $(\!(\tau_1, \ldots, \tau_n)\!) \subseteq O(\langle \delta_1 \ldots \delta_n \rangle)$（因为这是一个凯莱子群），并且由 Δ 的单调性可得：

$$\Delta((\tau_1, \ldots, \tau_n)) \subseteq \Delta \circ O(\langle \delta_1, \ldots, \delta_n \rangle) = \langle \delta_1, \ldots, \delta_n \rangle$$

由此得证。 □

以下命题充分说明了本节的动机：我们将生成（有限支撑的）对称群的问题归结为一个更简单的问题，即生成 G。

命题。 设 K 是一个凯莱群。则:

$$\boxed{K \supseteq \mathfrak{S}_G^f \iff \Delta(K) = G}$$

若 G有限，则有:

$$\boxed{K = \mathfrak{S}_G \iff \Delta(K) = G}$$

证明。 以下等价关系显而易见（由前面证明过的引理可得）:

$$K \supseteq \mathfrak{S}_G^f \iff K \text{ contient toutes les transpositions} \iff \Delta(K) = G$$

□

从这些一般性结论中得出的重要事实如下:

定理。 沿用前面的记号，有:

$$\boxed{((\tau_1, \ldots, \tau_n)) \supseteq \mathfrak{S}_G^f \iff \langle \delta_1, \ldots, \delta_n \rangle = G}$$

而当 G 有限时:

$$\boxed{((\tau_1, \ldots, \tau_n)) = \mathfrak{S}_G \iff \langle \delta_1, \ldots, \delta_n \rangle = G}$$

5.2 应用

来看一个直接的应用:

定理。 （用一个 n-轮换和一个对换生成 $\mathfrak{S}_n$ ）设 $n \geq 3$ 且 $\tau = (i\ j) \in \mathfrak{S}_n$。轮换（1 2 ... n）和对换 τ 当且仅当 $n \wedge (j - i) = 1$ 时生成 $\mathfrak{S}_n$。特别地，如果 $p \geq 3$ 是素数，则一个 p- 轮换和一个对换总能生成 $\mathfrak{S}_p$。

证明。 将前面的结果应用于 $G = \mathbb{Z}_n$。 □

另一个应用是， $x \mapsto x + 1$、对换（0 2）和对换（0 3）生成 $\mathbb{Z}$ 的所有有限支集置换。

注记。 这一切对一个阶为 2 的群都不成立，因为 $\mathfrak{S}_2$ 等于 ((id))，而记 id $=$(1 1) 时，我们发现 $1 - 1$ 与 2 不互素。

5.3 等距变换的描述

沿用对称群部分中的记号。设 H 是 G 的一个子群，且 $f \in O(H)$。根据定义：

$$f(x) - f(y) \equiv x - y \ [H]$$

对所有 $x, y \in G$，可以将其改写为：

$$f(x) - x \equiv f(y) - y \ [H]$$

换句话说，$f(x) - x$ 是一个模 H 常数，将其记为 $c(f) \in G/H$。此外，一个置换是模 H 等距映射，当且仅当存在这样一个模 H 常数。

命题。这定义了一个群同态：

$$O(H) \xrightarrow{c} G/H$$

证明。需要证明，对于 f、$g \in O(H)$，有 $c(f \circ g) = c(f) + c(g)$。事实上，对于 $x \in G$，我们观察到：

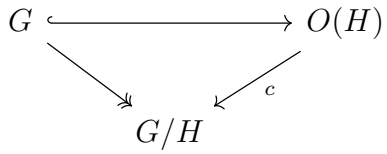
$$f \circ g(x) - x \equiv f \circ g(x) - g(x) + g(x) - x \equiv c(f) + c(g) \ [H]$$

不严谨地将 $c(f)$ 记作 $c(f)$ 的一个代表元。 □

命题。c 的核由保持模 H 等价类不变的态射构成。因此有以下正合列（必要时可对模 H 的等价类重新排序）：

$$1 \longrightarrow (\mathfrak{S}_H)^{[G:H]} \longrightarrow O(H) \longrightarrow G/H \longrightarrow 1$$

证明。映射 $(\mathfrak{S}_H)^{[G:H]} \longrightarrow O(H)$ 对应于 $(\mathfrak{S}_H)^{[G:H]}$ 在 G 上对每个等价类的作用，该作用是忠实的，并且确实通过模 H 的等距变换实现，因为该态射像中的每个元素都存在一个模 H (0) 的常数。接着，态射 c 是满射，因为下面的图表可交换：



□

推论。因此，当 G 为有限时，记 g 为 G 的基数函数，h 为 H 的基数函数，可直接得到：

$$\boxed{|O(H)| = \frac{(h!)^{\frac{g}{h}} g}{h}}$$

6 展望

一个自然的问题是，能否将卷积推广到非交换群，只对正规子群求和。遗憾的是，这样会失去交换性和结合性（结合性方面的问题在于，可能出现 H 是 K 的正规子群，且 K 是 G 的正规子群，但 H 并非G的正规子群）。一种可能的推广思路是将其应用于主环上的模，且这些模的商群具有有限基数（例如 $k[X]$，其中 k 是有限域）。

同样，当原群是非交换群时，关于对称群的讨论便不再适用（因此需要改变等距的定义）。

在与我的同事 Rafik SOUANEF 讨论时，我们意识到，函数μ 似乎与具有固定结构的子群数有关——也就是说，给定一个有限阿贝尔群 A，其同构于一个固定群 B 的子群 A 的数量。事实上，我们成功给出了这个数量的一个公式，该公式由 A 和 B 的不变因子决定，参见 [2]。我们甚至还找到了第二种不使用卷积的证明方法。再一次，这个公式早已在 [1] 中通过另一种不同的方法被发现，只是我们后来才意识到这一点。

参考文献

[1] S. Delsarte. 有限阿贝尔群上的莫比乌斯函数。《数学年刊》，*1948*年*7*月，第二辑，第*49*卷，第*3*期（*1948*年*7*月），第*600-609*页。[2] Souanef 和 Mallet-Burgues。具有给定结构的子群数。[3] Lovasz。对结构的运算。[4]N. Marquis。TD 3 代数 1（巴黎高师）。网址：https://www.math.ens.psl.eu/~nmarquis/TD_3.pdf。