arXiv:2301.09993v1 [math.CO] 24 Jan 2023

学士论文

同构类

of

顶点传递

竞赛图

作者：Stefan Zetzsche 编号：导师：Matthias Hamann 博士 院系：自然科学、计算机科学与数学 学位课程：数学理学学士 提交年份：2016

汉堡大学，Bundesstr. 55，20146 汉堡

摘要

竞赛图是通过为无向完全图的每条边指定一个方向而得到的图。我们给出了素数阶点传递竞赛图的同构类数量公式。为此，我们引入了凯莱竞赛图，它是一类特殊的凯莱有向图，并证明素数阶点传递竞赛图的同构类与素数阶凯莱竞赛图的同构类之间存在一一对应关系。

目录

1 引言 7

2 代数工具 9
2.1 置换群.9 2.2 计数.10

3 Cayley 图 13
3.1 顶点传递图.13 3.2 Rectracts.15 3.3 识别.16 3.4 同构.17

4 竞赛图 21
4.1 点传递竞赛图. 21

5 结论 29
5.1 推广.29 5.2 非 Cayley 顶点传递锦标赛.30 5.3 定义在非同构群上的凯莱图.31

1 引言

在他1967年的论文 [**13**] 中，Turner 枚举了素数阶顶点传递图的同构类。事实上，每个素数阶顶点传递图都同构于一个凯莱图。Turner 证明，两个凯莱图 Cay($\mathbb{Z}_p, S$) 和 Cay($\mathbb{Z}_p, S'$) 同构，当且仅当 $S' = aS$ 对某个 $a \in \mathbb{Z}_p^\times$成立。因此，同构类的数量就是关系“$S$ 等价于 S'”的等价类数量，其中 S 等价于 S'，当且仅当 $S' = aS$ 对某个 $a \in \mathbb{Z}_p^\times$成立。为枚举这些等价类，他以如下方式使用了 P´olya 枚举定理。连接集 S 可与特征函数集合$X = \{\varphi\colon \mathbb{Z}_p \setminus \{0\} \to \{0,1\}\}$对应。我们知道，每个 $a \in \mathbb{Z}_p^\times$都会置换 $\mathbb{Z}_p \setminus \{0\}$，并且可以通过定义 $a\varphi(d) = \varphi(a^{-1}d)$，将其扩展为 X 的一个置换。于是，P´olya 枚举定理给出了 X 在 $\mathbb{Z}_p \setminus \{0\}$ 作用下的轨道数量，这等于等价类的数量。

Alspach 和 Mishna [**1**] 于 2002年推广了这一方法。为此，如果 Cay(Γ, S) 与 Cay(Γ, S') 同构当且仅当 $S' = aS$ 对某个群自同构 $a \in$ Aut(Γ) 成立，则称特定的凯莱（有向）图 Cay(Γ, S) 为（D）CI（有向）图。此外，如果对于任意S、S'，Cay(Γ, S) 与 Cay(Γ, S') 同构当且仅当 $S' = aS$对某个群自同构 $a \in$ Aut(Γ) 成立，则称 Γ 为（D）CI群。借助这些定义，Alspach 和 Mishna 得以将 Turner 的结果推广到定义在无平方因子阶循环群上的凯莱（有向）图、任意阶的循环（有向）图，以及定义在初等阿贝尔群上的凯莱（有向）图。遗憾的是，他们的方法无法用于枚举素数阶点传递竞赛图的同构类。不过，沿着 Turner 的思路，我们能够证明每个这样的图都同构于一种特殊的凯莱有向图，即凯莱竞赛图。更进一步，我们指出，$\mathbb{Z}_p$ 的凯莱竞赛图是 DCI 有向图。因此，我们也尝试枚举相关的等价类，不过采用的思路略有不同。在第二章和第三章中，我们介绍所有必要的概念，即群作用、点传递性和凯莱图。具体而言，我们证明，任意无向、连通且顶点传递的图都是某个凯莱图的收缩。此外，我们还试图理解图在什么情况下同构于凯莱图。主要结果由定理 4.1.3 给出。最后一章探讨一种

将我们的方法可能推广到任意阶群的情形。具体来说，我们考察 Mansilla [7] 关于点传递竞赛图无限族的构造，这些竞赛图并非凯莱竞赛图；并研究 Joy Morris [9],的一篇论文，该文探讨两个定义在非同构群上的凯莱图在什么情况下同构。

2 代数工具

首先，我们先明确一下记号。图记作 G, H，其顶点集和边集分别记作 $V(G)$ 和 $E(G)$。顶点记作 v, w，从 v 到 w 的边记作 $v \sim w$。为避免误解，我们会直接写明两个元素等价，而不再使用 $\sim$。群记作 Γ，子集通常记作 S，其元素记作 ρ, σ, g, h, a, b。不过，由于凯莱图的顶点集本身也是群，有时我们不得不在这些记号之间切换。集合也一样，我们将其记作 V, W 或 X, Y，其中 V 表示该集合还将作为顶点集使用。集合 X 的阶记作 $|X|$；若写作 $|G|$，则表示 $|V(G)|$。此外，$\Gamma' < \Gamma$ 表示 Γ' 是 Γ 的子群。我们将写作 $\mathbb{Z}_n$，而不写作 $\mathbb{Z}/n\mathbb{Z}$。乘法单位群记作 $\mathbb{Z}_n^\times$。若存在映射 $\varphi\colon V(G) \to V(H)$，使得只要 $v \sim w$，就有 $\varphi(v) \sim \varphi(w)$，则称两个图 G, H 同态。此时映射 φ 称为（图）同态。若还存在同态 $\varphi^{-1}\colon V(H) \to V(G)$，使得 $\varphi \circ \varphi^{-1} = \mathrm{id}_{V(H)}$ 且 $\varphi^{-1} \circ \varphi = \mathrm{id}_{V(G)}$，则称 G 和 H 同构，并记作 $G \cong H$。此时，φ 和 φ^{-1} 称为（图）同构。进一步，若 $G = H$，则称它们为（图）自同构。自同构群记作 $\mathrm{Aut}(G)$。$\bigcup$ 上的点表示不交并。我们大多采用乘法记号表示群，尽管主要应用对象是加法群 $\mathbb{Z}_n$。除非另有说明，我们使用的所有群都是有限群。$\mathbb{F}_n$ 是阶为 n 的唯一域。$\deg^+(v)$ 和 $\deg^-(v)$ 分别表示某个顶点 v 的出度和入度。第 i 个坐标上的投影记作 pr_i。

2.1 置换群

本节基本上将遵循 [4]。设 V 是一个集合。V 上的所有置换构成的群，也就是 V 上的所有双射构成的群，记作 $\mathrm{Sym}(V)$；如果 $|V| = n \in \mathbb{N}$，则简记为 $\mathrm{Sym}(n)$。$\mathrm{Sym}(V)$ 的任意子群都称为 V 上的置换群。因此，如果 V 是图 G 的顶点集，那么 G 的自同构群就是 V 上的一个置换群。

首先，我们将回顾代数中的一些基本构造。设 Γ 是一个

群，且 V是一个集合。如果存在一个映射 φ: $\Gamma \times V \to V$，使得

$$\varphi(1, v) = v \text{ for all } v \in V$$

and

$$\varphi(g, \varphi(h, v)) = \varphi(gh, v) \text{ for all } g, h \in \Gamma, v \in V,$$

我们称 Γ 作用在 V上。 φ 诱导出一个群同态，即所谓的置换表示 $\rho: \Gamma \to \mathrm{Sym}(V)$，其定义为

$$\rho(g)(v) := \varphi(g, v)$$

反之亦然。对于 $v \in V$、 $g \in \Gamma$，我们将记号简写为

$$v^g := \rho(g)(v).$$

于是，对于每个子集 $W \subseteq V$， W^g是一个子集，且每个 $g \in \Gamma$ 都会在 $\mathcal{P}(V)$ 上诱导一个置换。若对于所有 $g \in \Gamma$，都有 $H^g = H$，则称 $H \subseteq V$是 Γ-不变的。这类子集使我们能够引入 $g \downharpoonright H$，即将 g 诱导的置换限制到 H上。再次， $\Gamma \to \mathrm{Sym}(H)$ $g \mapsto g \downharpoonright H$ 的像是作用在 H上的一个置换群。若对于任意 v、 $w \in V$，都存在 $g \in \Gamma$使得 $v^g = w$，则称置换群 Γ 是传递的。

对于 $v \in V$，考虑轨道 $v^\Gamma := \{v^g \mid g \in \Gamma\} \subseteq V$。显然，它是$\Gamma$-不变的。此外，我们有

$$(v^g)^{hg^{-1}} = v^{hg^{-1}g} = v^h,$$

因此， Γ 在 v^Γ上传递作用。令 $w \in v^\Gamma$，则 $w = v^g$、 $g \in \Gamma$，因此$w^h = (v^g)^h = v^{hg} \in v^\Gamma$，对于 $h \in \Gamma$成立。另一方面， $v^h = v^{hg^{-1}g} = (v^g)^{hg^{-1}} = w^{hg^{-1}} \in w^\Gamma$。因此， $w^\Gamma = v^\Gamma$ 成立，对于 $w \notin v^\Gamma$ 也有。$w^\Gamma \cap v^\Gamma = \emptyset$。由此可得 $V = \bigcup_v v^\Gamma$，进而得出，任何 Γ-不变子集都是 Γ的轨道之并。这等同于承认

$$v \text{ equivalent to } w \text{ if and only if } \exists g \in \Gamma : v^g = w$$

在 V上定义了一个等价关系。因此， Γ 在 V上传递作用，当且仅当只有一个轨道。

2.2 计数

若 Γ 是作用在 V上的置换群，对于任意 $v \in V$，我们定义稳定子$\Gamma_v := \{g \in \Gamma \mid v^g = v\}$. 我们通过 $\Gamma_{v_1,\ldots,v_k} := \bigcap_i \Gamma_{v_i}$ 推广这一概念，并借助集合稳定子 $\Gamma_W := \{g \in \Gamma \mid W^g = W\}$这一概念，将其弱化到任意 $W \subseteq V$。若 G 是一个群，且 $H \subseteq$ 是一个子群，则关系

$$a \text{ equivalent to } b \text{ if and only if } \exists h \in H : a = bh$$

在 G上定义了一个等价关系。元素 b 的等价类记作 bH，称为 H 在 G 中的左陪集，其对应的子群为 b。由于稳定子 Γ_v 是 Γ的子群，因此我们得到 Γ 的一个划分，其中各部分是 Γ_v的左陪集。

LEMMA 2.2.1. 设 Γ 是作用在 V 上的置换群，且 $W \subseteq V$是 Γ的一个轨道。那么对于任意 v、$w \in W$，存在 $h \in \Gamma$，使得 $\{g \in \Gamma \mid v^g = w\} = h\Gamma_v$。反过来，对于任意 $h \in \Gamma$、$v \in W$，存在 $w \in W$，使得对所有 $g \in h\Gamma_v$：$v^g = w$。

PROOF. 设 v、$w \in W$。由于 W是 Γ的一个轨道，Γ在 W上是传递的。因此，存在 $h \in \Gamma$，使得 $v^h = w$。假设还存在另一个 $g \in \Gamma$，使得 $v^g = w$。那么 $v^h = v^g$，因此 $v^{h^{-1}g} = (v^g)^{h^{-1}} = (v^h)^{h^{-1}} = v^{h^{-1}h} = v$。所以 $h^{-1}g \in \Gamma_v$ 且 $g \in h\Gamma_v$。反过来，设 $g \in h\Gamma_v$。那么 $v^g = v^h =: w$。 □

LEMMA 2.2.2（轨道-稳定子定理）。设 Γ 是作用于 V 的置换群，且 $v \in V$。那么

$$|\Gamma_v||v^\Gamma| = |\Gamma|.$$

PROOF. 对于固定的 $v \in V$ 集合 $W := v^\Gamma$。由前面的引理 2.2.1 可知，W 与 Γ_v 的左陪集之间存在一个双射。由于 $\Gamma = \dot\cup_h h\Gamma_v$，我们知道 Γ 可以划分为 $|W| = |v^\Gamma|$ 个 Γ_v 的左陪集，每个左陪集都包含 $|\Gamma_v|$ 个元素。 □

两个不同点 v、$w \in V$ 的稳定子之间有什么关系？下面的引理针对 v、w 位于同一轨道的情形给出了答案。

LEMMA 2.2.3. 设 Γ 是作用于 V 的置换群，且 $v \in V$。若$g \in \Gamma$，则 $g\Gamma_v g^{-1} = \Gamma_{v^g}$。

PROOF. 设 $ghg^{-1} \in g\Gamma_v g^{-1}$。则 $(v^g)^{ghg^{-1}} = v^{ghg^{-1}g} = v^{gh} = (v^h)^g = v^g$。反之，若 $h \in \Gamma_{v^g}$，则有 $v^g = (v^g)^h = v^{hg}$，因此 $v = (v^g)^{g^{-1}} = (v^{hg})^{g^{-1}} = v^{g^{-1}hg}$。所以 $g^{-1}hg \in \Gamma_v$ 或 $h \in g\Gamma_v g^{-1}$。 □

现在我们将引入稳定子的一个对偶概念。对于 $g \in \Gamma$，由 g 固定的不动点为 $\mathrm{fix}(g) := \{v \in V \mid v^g = v\}$。Burnside 的下述引理指出，$\Gamma$ 在 V 上的轨道数等于任意元素 $g \in \Gamma$ 的不动点平均数。

LEMMA 2.2.4（Burnside）。设 Γ 是作用于 V 上的置换群。那么

$$|\{v^\Gamma \mid v \in V\}||\Gamma| = \sum_{g \in \Gamma} |\mathrm{fix}(g)|.$$

PROOF. 计数 g 得到 $|\{(g, v) \mid g \in \Gamma, v \in V, v^g = v\}| = \sum_{g\in\Gamma} |固定(g)|$。另一方面，计数 v 得到 $|\{(g, v) \mid g \in \Gamma, v \in V, v^g = v\}| = \sum_{v\in V} |\Gamma_v|$。根据 $h \mapsto ghg^{-1}$，对于任意 $g \in \Gamma$，我们有 $|\Gamma_v| = |\Gamma_{v^g}|$。因此

$\sum_{v\in v^\Gamma}|\Gamma_v| = |v^\Gamma||\Gamma_v| = |\Gamma|$，其中最后一个等式用到了轨道-稳定子引理 2.2.2。因此 $\sum_{g\in\Gamma}|\text{固定}(g)| = \sum_{v\in V}|\Gamma_v| = |\{v^\Gamma \mid v\in V\}||\Gamma|$，从而证明了该结论。

□

3 凯莱图

3.1 顶点传递图

如果自同构群 Aut(G) 在 $V(G)$ 上传递地作用，我们就称图 G 是顶点传递的；也就是说，对于任意 $v, w \in V(G)$，都存在 $\rho \in \mathrm{Aut}(G)$，使得 $v^\rho = w$。本节将从一些简单的例子开始。

对于 $k \in \mathbb{N}$，令 k维超立方体 Q_k 为顶点集 $\mathbb{Z}_2^k$ 的图，并且当且仅当存在某个 i, $1 \leq i \leq k$ 满足 $v_i \neq w_i$ 时，$v \sim w$；但对于所有 $j, 1 \leq j \leq k, j \neq i$，$v_j = w_j$。

LEMMA 3.1.1. k维超立方体 Q_k 是顶点传递的。

PROOF. 对于 $v \in \mathbb{Z}_2^k$，考虑 $V(Q_k)$ 的置换 ρ_v：$w \mapsto w + v$。由于 $w, u \in V(Q_k)$ 恰好在一个位置上不同时，当且仅当 $w + v$ 和 $u + v$ 恰好在一个位置上不同时，ρ 也是一个自同构。集合 $\Gamma = \{\rho_v \mid v \in G\}$ 构成 Aut(Q_k) 的一个子群。它的作用是传递的，因为对于任意 $v, w \in V$，映射 ρ_{-v+w} 将 v 映射到 w。

□

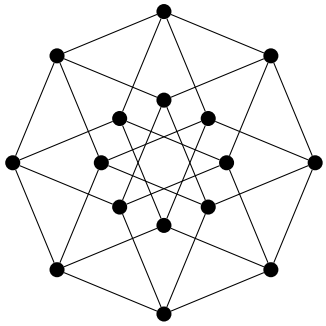

图3.1：四维超立方体 Q_4

顶点数为 n 的圈是图 C_n，其顶点集为 $\mathbb{Z}_n$，且当且仅当 $v - w \equiv \pm 1$ 取模 n时有 $v \sim w$。若 $\rho \in$ 属于对称群 Sym(n)，且满足 $\rho(v) \equiv v + 1$ 取模 n，则可得 $\rho \in$ 属于自同构群 Aut(C_n)。因此，自同构群 Aut(C_n) 必须包含循环子群$H := \{\rho^k \mid 0 \leq k \leq n-1\}$.。对于任意两个 v、$w \in V$（C_n），都可以找到一个 $\rho^k \in H$，使得 $\rho^k(v) = w$，也就是说，H 在 C_n上具有传递性。

DEFINITION 3.1.2. 设 Γ 是一个群，且令 $S \subset \Gamma$ 满足 $1 \notin S$。凯莱有向图 $\overrightarrow{\text{Cay}}(\Gamma, S)$ 是一个图，其顶点集为 Γ，边集为 $\{(g, gs) \mid g, s \in \Gamma\}$。此外，若 $S = S^{-1}$，则定义凯莱图 $\text{Cay}(\Gamma, S)$。另一方面，若 $S \cap S^{-1} = \emptyset$ 且 $S \cup S^{-1} = \Gamma \backslash \{1\}$，则定义凯莱竞赛图 $\overrightarrow{\text{Cay}}_{\text{tourn}}(\Gamma, S)$。无论哪种情况，集合 S 都称为连接集。

由此可得，$g \sim h$ 当且仅当 $g^{-1}h \in S$。如果 $1 \in S$，由于$g \sim g$，对于所有 $g \in \Gamma$，我们就会得到环。

DEFINITION 3.1.3. 竞赛图是通过为无向完全图中的每条边指定一个方向而得到的有向图。

REMARK 3.1.4. Cayley竞赛图是一个竞赛图。

PROOF. 设 Γ 是一个群。设 $S \subset \Gamma$ 满足 $1 \notin S$、 $S \cap S^{-1} = \emptyset$、 $S \cup S^{-1} = \Gamma \setminus \{1\}$。设 g、 $h \in \Gamma$、 $g \neq h$。后者推出 $g^{-1}h \neq 1$，因此 $g^{-1}h \in S$ 或 $g^{-1}h \in S^{-1}$。由于 $S \cap S^{-1} = \emptyset$，两者中只有一个成立。前者推出$g \sim h$。另一方面，若 $g^{-1}h \in S^{-1}$，则有$(g^{-1}h)^{-1} = h^{-1}g \in S$，即 $h \sim g$。因此，相应的凯莱竞赛图 $\overrightarrow{\text{Cay}}_{\text{tourn}}(\Gamma, S)$是一个竞赛图。

□

回顾前面的例子，我们现在可以写出

$$Q_k = \text{Cay}(\mathbb{Z}_2^k, S),\ S = \{e_i \mid 1 \leq i \leq k\}$$

and

$$C_n = \text{Cay}(\mathbb{Z}_n, S),\ S = \{\pm 1\}.$$

LEMMA 3.1.5. Cayley 有向图 $\overrightarrow{\text{Cay}}(\Gamma, S)$ 是顶点传递的。

PROOF. 固定一个 $w \in \Gamma$，考虑映射 $\rho_w : v \mapsto wv$。它有逆映射 $\rho_{w^{-1}}$，因此是一个置换。由于 $(\rho_w(v))^{-1}\rho_w(u) = (wv)^{-1}(wu) = v^{-1}w^{-1}wu = v^{-1}u$，可知 $\rho_w(v) \sim \rho_w(u)$ 当且仅当 $v \sim u$。因此，$\{\rho_w \mid w \in \Gamma\}$ 构成 $\text{Aut}(\overrightarrow{\text{Cay}}(\Gamma, S))$ 的一个子群。对于任意 $v, w \in \Gamma$, $\rho_{wv^{-1}}(v) = wv^{-1}v = w$，这证明了传递性。

□

注意，这对 Cayley 图和 Cayley 竞赛图也成立，因为它们也是凯莱有向图。

是否存在不是凯莱（有向）图的顶点传递（有向）图？答案是肯定的。我们将在稍后拥有更强有力的工具时证明这一点。接下来还可以探讨：对于哪些 $n \in \mathbb{N}$，存在阶为 n 的顶点传递图，但它不是凯莱图。

首先，我们来证明：每个连通的顶点传递图都是某个凯莱图的收缩。

3.2 Rectracts

Definition 3.2.1. 设 G 为一个图， $H \subseteq G$ 为其子图。若存在一个同态 $\varphi\colon G \to H$，使得 $\varphi \restriction H = \mathrm{id}_H$，则称 H 为一个收缩。

任意无向、连通且顶点传递的图都是某个凯莱图的收缩。

Proof. 设 G 是一个连通顶点传递图。固定 $v \in V(G)$，考虑

$$S := \{g \in \mathrm{Aut}(G) \mid v \sim v^g\}.$$

由于我们不允许出现圈， $id \notin S$。若 $g \in S$，则 $v \sim v^g$，因此还有$v^{g^{-1}} \sim (v^g)^{g^{-1}} = v$。由于 G 是无向图，同样有 $v \sim v^{g^{-1}}$，从而 $g^{-1} \in S$。令

$$\Gamma := \langle S \rangle$$

为由 S生成的群。利用归纳法证明， Γ 在$V(G)$上作用传递。于是由引理 2.2.1 可得一个双射 ϕ，它将Γ 中 Γ_v 的左陪集映射到 $V(G)$。我们定义映射

$$\varphi\colon \mathrm{Cay}(\Gamma, S) \to G,\ g \mapsto \phi(g\Gamma_v).$$

有 $S = \Gamma_v S \Gamma_v$。为此，考虑 $g \in S$、 h、$h' \in \Gamma_v$。于是 $v = v^h \sim (v^g)^h = v^{hg} = (v^{h'})^{hg} = v^{hgh'}$，因此 $hgh' \in S$。另一方面， $S \subset \Gamma_v S \Gamma_v$，因为 $\mathrm{id} \in \Gamma_v$。为验证 φ是一个同态，考虑 $ag \in a\Gamma_v$和 $bh \in b\Gamma_v$。于是 $ag \sim bh$ 当且仅当（ag）$^{-1}bh = g^{-1}a^{-1}bh \in S$ 当且仅当 $a^{-1}b \in S$。最后一个等价关系来自以下事实： $g \in \Gamma_v$ 当且仅当 $g^{-1} \in \Gamma_v$ 和 $S = \Gamma_v S \Gamma_v$。因此，两个不同的左陪集之间要么完全没有边，要么不同陪集中的任意两个元素之间都有边。此外，同一个左陪集中的元素之间没有边，因为 $id \notin S$。我们还需验证 ϕ 是一个同态，即若两个左陪集 $g\Gamma_v$ 和 $h\Gamma_v$ （属于 Γ_v ）完全相邻，则 $w \sim w'$也成立，其中$w = \phi(g\Gamma_v)$ $w' = \phi(h\Gamma_v) \in V(G)$。由于 Γ 在 V上传递作用，我们可以找到a、 $b \in \Gamma$，使得 $w = v^a$ 且 $w' = v^b$。因此， $w \sim w'$ 当且仅当 $v^a \sim v^b$当且仅当 $v \sim v^{a^{-1}b}$ 当且仅当 $a^{-1}b \in S$。现在利用这一事实： $g\Gamma_v$恰好由那些 $a \in \Gamma$组成，使得 $v^a = w$ ； 而 $h\Gamma_v$ 恰好由那些 $b \in \Gamma$组成，使得 $v^b = w'$。

如果我们将 φ 限制为左陪集的代表元，就得到 id_G，这证明了该结论。 □

Definition 3.2.3. 设 Γ 为一个群， $\Gamma_0 \subseteq \Gamma$ 为一个子群，且 $S \subseteq \Gamma$，使得 $1 \notin S$和 $S = S^{-1}$。凯莱陪集图 $\mathrm{Ccg}(\Gamma, S, \Gamma_0)$ 定义为$V(\mathrm{Ccg}(\Gamma, S, \Gamma_0))$ $= \{a\Gamma_0 \mid a \in \Gamma\}$，并且 $a\Gamma_0 \sim b\Gamma_0$当且仅当 $(ag)^{-1}bh \in S$对某些 $g, h \in \Gamma_0$成立。

在前述证明的条件下，令 $\Gamma_0 := \Gamma_v$，得到以下推论。

COROLLARY 3.2.4（Sabidussi [**12**]）。每个无向连通顶点传递图都同构于一个凯莱陪集图。 □

3.3 识别

作用于集合 V 上的置换群 Γ 称为半正则的，如果对每个 $v \in V$，其稳定子群都是平凡的。若它既是半正则的又是传递的，则称为正则的。回顾引理 2.2.2 可知，如果 Γ 是半正则的，那么 $|v^\Gamma| = |\Gamma|$。如果 Γ 也是传递的，则它只有一个轨道，即 V。因此 $|V| = |\Gamma|$。
群同构是一个双射映射 $\varphi\colon \Gamma \to \Gamma'$，区间取值于两个群 Γ, Γ' 之间，并满足对于所有 $g, h \in \Gamma$， $\varphi(gh) = \varphi(g)\varphi(h)$。为表示这样的映射存在，我们写作 $\Gamma \cong \Gamma'$。如果 $\Gamma = \Gamma'$，这样的映射称为群自同构。

LEMMA 3.3.1. 设 $\overrightarrow{\mathsf{Cay}}(\Gamma, S)$ 为凯莱有向图。$\mathsf{Aut}(\overrightarrow{\mathsf{Cay}}(\Gamma, S))$ 中存在一个与 Γ 同构的正则子群。

PROOF. 在引理 3.1.5 的证明中，我们已经看到，映射 $(\rho_w : \Gamma \to \Gamma, v \mapsto wv)_{w\in\Gamma}$ 构成 $\mathsf{Aut}(\overrightarrow{\mathsf{Cay}}(\Gamma, S))$ 的一个子群，并在Γ上传递作用。由 $\rho_w \overset{\varphi}{\mapsto} w$可知，该子群与 Γ 同构，因为我们有 $\varphi(\rho_u\rho_w) = \varphi(\rho_{uw}) = uw = \varphi(\rho_u)\varphi(\rho_w)$，根据定义，核是平凡的，且$\varphi$ 是满射。唯一固定顶点的元素是 $\rho_{\mathbb{1}} = \mathsf{id}_\Gamma$。 □

LEMMA 3.3.2. 设 G 为无向图，且 $\Gamma \subseteq \mathsf{Aut}(G)$ 是作用于 G 的一个正则子群。那么存在一个与 G 同构的凯莱图 $\mathsf{Cay}(\Gamma, S)$。此外，若 G 是竞赛图，且 $\Gamma \subseteq \mathsf{Aut}(G)$ 是作用于 G 的一个正则子群，则存在一个与 G 同构的凯莱竞赛图 $\overrightarrow{\mathsf{Cay}}_{\mathrm{tourn}}(\Gamma, S)$。

PROOF. 设 $v \in V(G)$ 固定。对于任意 $w \in V(G)$，我们找到唯一的 $\rho_w \in \Gamma$，使得 $v^{\rho_w} = w$，因为 Γ 是传递的。考虑 $S := \{\rho_w \mid v \sim v^{\rho_w} = w\}$。我们有 $\mathsf{id}_G \notin S$，因为这会得到 $v \sim v$。此外，若 $S = S^{-1}$ 是无向的，则 G，因为 $v \sim v^{\rho_w}$ 当且仅当 $v^{\rho_w^{-1}} \sim (v^{\rho_w})^{\rho_w^{-1}} = v$。另一方面，若 G 是竞赛图，则 $v^{\rho_w^{-1}} \sim v$ 当且仅当 $v \not\sim v^{\rho_w^{-1}}$ 也成立。因此 $S \cap S^{-1} = \emptyset$ 且 $S \cup S^{-1} = \Gamma \setminus \{1\}$。现在设 $w, u \in V(G)$。由于 $\rho_w^{-1} \in \mathsf{Aut}(G)$，有

$$\begin{aligned} w \sim u \text{ if and only if } v = (v^{\rho_w})^{\rho_w^{-1}} = w^{\rho_w^{-1}} \sim u^{\rho_w^{-1}} = (v^{\rho_u})^{\rho_w^{-1}} = v^{\rho_w^{-1}\rho_u} \\ \text{if and only if } \rho_w^{-1}\rho_u \in S. \end{aligned}$$

因此，通过将每个 $w \in V(G)$ 与 $\rho_w \in \Gamma$ 相对应，我们分别得到 G 与 $\mathsf{Cay}(\Gamma, S)$ 之间或 $\overrightarrow{\mathsf{Cay}}_{\mathrm{tourn}}(\Gamma, S)$ 的同构。 □

由此得到 Sabidussi 的结果，这是识别凯莱图的一项基础工具。

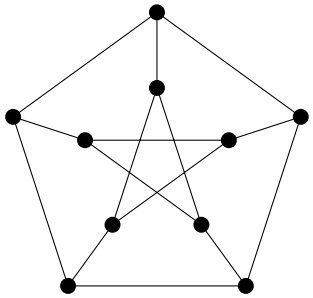

图 3.2：彼得森图 $J(5, 2, 0)$。

COROLLARY 3.3.3 (Sabidussi [11])。无向图 G 同构于凯莱图，当且仅当 $\mathrm{Aut}(G)$ 含有一个正则子群。此外，竞赛图 G 同构于凯莱竞赛图，当且仅当 $\mathrm{Aut}(G)$ 含有一个正则子群。

□

现在我们可以证明这一论断：存在一个不是 Cayley 图的顶点传递图。为此，设 $v, k, i \in \mathbb{N}$，使得 $v \geq k \geq i$，并令 Ω 为一个大小为 v 的固定集合。图 $J(v, k, i)$ 定义为顶点集 $V := \{M \in \mathcal{P}(\Omega) \mid |M| = k\}$ 和边集 $E := \{\{M, N\} \mid |M \cap N| = i\}$。图 $J(5, 2, 0)$ 称为彼得森图。它的顶点是 $\{1, ..., 5\}$ 的二元素子集。每个 $\rho \in S_5$ 都在 $V(J(5, 2, 0))$ 上诱导一个置换 ρ'。此外，每个 ρ' 都是一个自同构，因为 $\{a, a'\}, \{b, b'\} \subseteq V(J(5, 2, 0))$ 不同，当且仅当 $\rho'(\{a, a'\}) = \{\rho(a)\ \rho(a')\}$ 且 $\rho'(\{b, b'\}) = \{\rho(b)\ \rho(b')\}$ 不同。这一点成立，因为否则 ρ 就不是单射。因此，令 $\varphi\colon S_5 \mapsto \mathrm{Aut}(J(5, 2, 0))\ \ \rho \mapsto \rho'$，可得 $\varphi(S_5) < \mathrm{Aut}(J(5, 2, 0))$。由此可知该图是顶点传递的，因为对于任意两两不同的 $a, a', b, b' \in \{1, ..., 5\}$，我们都能找到唯一的 $\rho \in S_5$，使得 $\rho(a) = b$，$\rho(a') = b'$，即 $\rho' \in \varphi(S_5)$，使得$\rho'(\{a, a'\}) = \{b, b'\}$。

假设彼得森图是凯莱图。由于彼得森图的阶为 10，根据引理 3.3.1，我们可以找到一个阶为 10 的正则子群 Γ，它是 $\mathrm{Aut}(J(5, 2, 0)) = S_5$ 的子群。但是，$\Gamma \subseteq S_5$ 中的每个对合（即阶为 2 的元素）都会固定一个顶点。这与 Γ 的正则性矛盾。因此，彼得森图是一个顶点传递但不是凯莱图的图。

3.4 同构

一个相关的问题是确定两个凯莱图何时同构。本节将把讨论范围限定在定义于同一个群上的凯莱图。

LEMMA 3.4.1. 设 Γ 为一个群，φ 为 Γ的群自同构。那么 $\overrightarrow{\mathrm{Cay}}(\Gamma, S) \cong \overrightarrow{\mathrm{Cay}}(\Gamma, \varphi(S))$。此外，$\mathrm{Cay}(\Gamma, S) \cong \mathrm{Cay}(\Gamma, \varphi(S))$，并且

$\overrightarrow{\mathrm{Cay}}_{tourn}(\Gamma, S) \cong \overrightarrow{\mathrm{Cay}}_{tourn}(\Gamma, \varphi(S))$.

PROOF. 首先，我们验证 $\overrightarrow{\mathrm{Cay}}(\Gamma, \varphi(S))$ 定义良好。由于 φ 是一个自同构，若 $1 = \varphi(s) \in \varphi(S)$，则可推出 $S \ni s = 1$，这与假设矛盾。对于另外两种情况，注意到当且仅当 $\varphi(g) \in \varphi(S)$ 时，我们也有 $g \in S$；而当且仅当 $\varphi(S) \ni \varphi(g^{-1}) = \varphi(g)^{-1}$ 时，我们有 $g^{-1} \in S$。现在，分别利用这一点以及当且仅当 $g^{-1} \in S$ 时有 $g \in S$、当且仅当 $g^{-1} \notin S$ 时有 $g \in S$。最后，设 $g, h \in \Gamma$。我们得到，当且仅当 $g^{-1}h \in S$ 时有 $g \sim h$，而当且仅当 $\varphi(S) \ni \varphi(g^{-1}h) = \varphi(g)^{-1}\varphi(h)$ 时有 $g \sim h$；这又当且仅当 $\varphi(g) \sim \varphi(h)$。因此，$\varphi$ 在这三种情况下都是同构。

□

若群 Γ 在集合 V 上的群作用满足：对于任意的 $v, v', w, w' \in V$，$v \neq v'$，$w \neq w'$，都存在 $\rho \in \Gamma$，使得 $v^\rho = w$ 且 $v'^\rho = w'$，则称该作用是二重传递的或 2-传递的。

LEMMA 3.4.2（Burnside [3]）。设 $p \in \mathbb{P}$ 和 Γ 是 $\mathrm{Sym}(p)$ 的传递子群。则，要么 Γ是二重传递的，要么 Γ 包含一个阶为 p 的正规 Sylow p-子群。

我们的第一个重要结果是 Turner 提出的以下引理。

LEMMA 3.4.3（Turner [14]）。设 $p \in \mathbb{P}$。那么，$\mathrm{Cay}(\mathbb{Z}_p, S) \cong \overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S')$，当且仅当对于某个 $a \in \mathbb{Z}_p^\times$，$S' = aS$。此外，该表述对于凯莱图和凯莱竞赛图也定义良好。

PROOF. 令 $S' = aS$对某个 $a \in \mathbb{Z}_p^\times$成立。由于 $\varphi_a \colon \mathbb{Z}_p \to \mathbb{Z}_p, v \mapsto av$是群自同构，引理 3.4.1 得出 $\overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S) \cong \mathrm{Cay}(\mathbb{Z}_p, \varphi_a = (S))$ $\overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S')$，并且根据同一引理，这一定义对凯莱图和凯莱竞赛图也同样良定义。

对于另一个方向，只需考虑凯莱有向图。令 $\overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S) \overset{\varphi}{\cong} \overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S')$。

假设 $\mathrm{Aut}(\overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S))$ 或 $\mathrm{Aut}(\overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S'))$ 是二重传递的。那么 $\overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S)$ 和 $\overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S')$ 相同，二者要么是 K_p，要么是 $\overline{K}_p$。为证明它们各自必为其中之一，不失一般性地取 $\overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S)$，并假设它不是 $\overline{K}_p$。那么对于某个 v，有 $v \sim v', v' \in \mathbb{Z}_p$，$v \neq v'$。对于任意 $w, w' \in \mathbb{Z}_p$，$w \neq w'$，我们可找到 $g \in \mathrm{Aut}(\overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S))$，使得 $v^g = w$ 且 $v'^g = w'$。因此，$w \sim w'$，由此得到 K_p。由于 K_p 和 $\overline{K}_p$ 不同构，结论得证。因此，我们分别得到 $S = S' = \emptyset$ 或 $S = S' = \{1, \ldots, p-1\}$。于是取集合 $a := 1 \in (\mathbb{Z}_p)^\times$。

现在假设 $\Gamma = \mathrm{Aut}(\overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S))$ 和 $\Gamma' = \mathrm{Aut}(\overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S'))$ 都不是二重传递的。我们知道 Calyey 有向图是顶点传递的，因此引理 3.4.2 意味着存在由 $g = (x_0\ x_1\ \ldots\ x_{p-1})$ 和 $g' = (y_0\ y_1\ \ldots\ y_{p-1})$ 生成的、阶为 p 的唯一正规 Sylow p-子群。通过重新命名顶点，不失一般性地假设 $g = (0\ 1\ \ldots\ p-1) = g'$。

由于

$$\begin{aligned}\varphi(i) \sim \varphi(j) &\text{ if and only if } i \sim j\\ &\text{if and only if } i^g \sim j^g\\ &\text{if and only if } i+1 \sim j+1\\ &\text{if and only if } \varphi(i+1) \sim \varphi(j+1),\end{aligned}$$

由此可得 $(\varphi(0)\ \varphi(1)\ \ldots\ \varphi(p-1)) \in \mathrm{Aut}(\overrightarrow{\mathrm{Cay}}(\mathbb{Z}_p, S'))$。因此,

$$(\varphi(0)\ \varphi(1)\ \ldots\ \varphi(p-1)) = g'^a = (0\ a\ \ldots\ a(p-1))$$

对于某个 $a \in \mathbb{Z}_p^\times$，我们将其视为 $\{1,\ldots,p-1\} \subset \mathbb{N}$ ing'^a 中的一个元素。定义 $k := a^{-1}\varphi(0) \in \mathbb{Z}_p$，则 $\varphi(0) = ak$，由此对所有 i，有 $\varphi(i) = \varphi(0) + ai = ak + ai = a(k+i)$。由此可得

$$\begin{aligned}s \in S &\text{ if and only if } i \sim i+s \text{ for all } i\\ &\text{if and only if } \varphi(i) \sim \varphi(i+s) \text{ for all } i\\ &\text{if and only if } a(k+i) \sim a(k+(i+s)) = a(k+i) + as \text{ for all } i\\ &\text{if and only if } as \in S'.\end{aligned}$$

□

THEOREM 3.4.4. 一个带有 $|G| = p \in \mathbb{P}$ 的无向图 G 是顶点传递的，当且仅当 G 同构于一个凯莱图。此外，一个带有 $|G| = p \in \mathbb{P}$ 的竞赛图 G 是顶点传递的，当且仅当 G 同构于一个凯莱竞赛图。

PROOF. 如果 G 是凯莱图或凯莱竞赛图，那么根据引理 3.1.5，它是顶点传递的。

另一方面，设 G 是阶为 p 的任意无向顶点传递图。如果 Aut(G) 是二重传递的，我们已经在引理 3.4.3 的证明中看到，G 要么是 K_p，要么是 $\overline{K}_p$。它们分别是连接集为 $S = \{1,\ldots,p-1\}$ 和 $S = \emptyset$ 的 Cayley 凯莱图。竞赛图的自同构群不可能是二重传递的，因为这会产生一个无向图。

如果 Aut(G)不是二重传递的，那么根据引理 3.4.2，它必定包含一个阶为 p 的唯一正规 Sylow$p$-子群 Γ。请注意，这里必须要求 Aut(G)在 G上传递，也就是说，G 是顶点传递的。Γ 必须由形如 $g = (x_0\ x_1\ \ldots\ x_{p-1})$、且满足 $\bigcup_i x_i = \{0,\ldots,p-1\}$ 的置换生成。不失一般性，设 x_0 是一个从它出发存在一条边的顶点。将 x_i 重命名为 i后，可假设 $g = (0\ 1\ \ldots\ p-1)$。于是，对于任意 $v \in G$，v 的稳定子都是平凡群，因此 Γ 是一个正则子群。现在由引理 3.3.3 可得结论。具体而言，固定 $v \in G$，则 G

同构于凯莱图 Cay(Γ, S)，其中 $S := \{\rho_w \mid v \sim v^{\rho_w} = w\}$，由 $w \mapsto \rho_w$ 给出。如果 G 是竞赛图，那么 Γ 仍是一个正则子群；由引理 3.3.3 还可推出，G 同构于一个凯莱竞赛图。 □

在证明的最后，举例来说，取 $v := 0$。然后令 $i \in \{1, ..., p-1\}$，使得 $v = 0 \sim i = v^{g_i}$，其中此时 $g_i = g^i$。现在，若 $k - l = i$ 取模 p，则 $g_k g_l^{-1} = g^k g^{p-l} = g^{k-l} = g_{k-l} = g_i \in S$。因此，$g_k \sim g_l$，从而得到$k \sim l$。因此，对于所有 $w \in \{0, ..., p-1\}$，$w \sim w + i$ 取模 p。我们得到了一种所谓的循环图。这已经表明，循环图可以用几种等价的方式来描述。一种刻画方式是，图的自同构群包含一个循环子群，该子群在图的顶点上具有传递作用。另一种刻画方式是，若两个顶点 v和 $v + i$ 相邻，则任意两个顶点 w 和 $w + i$ 也相邻。第三种刻画方式是，该图是一个循环群的凯莱图。

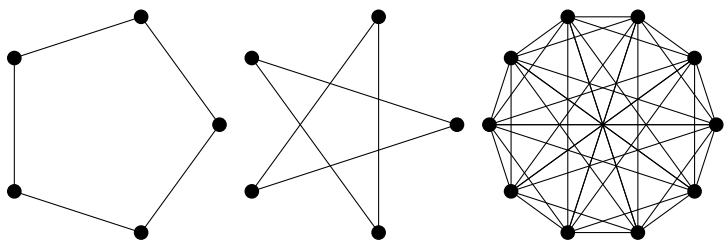

图 3.3：三个循环图

请注意，Cay($\mathbb{Z}_n, S$) $\cong$ Cay($\mathbb{Z}_n, S'$) 当且仅当 $S' = aS$ 对于某些$a \in \mathbb{Z}_n^\times$ 成立，这并非对每个 $n \in \mathbb{N}$ 都成立。例如，考虑 $n = 25$，其中

$$S = \{1, 4, 5, 6, 9, 11, 14, 16, 19, 20, 21, 24\}$$

and

$$S' = \{1, 4, 6, 9, 10, 11, 14, 15, 16, 19, 21, 24\}.$$

两个对应的凯莱图都是 5-圈的花环积，这个术语我们将在最后一章定义，因此二者同构。不过，不存在$a \in \mathbb{Z}_{25}^\times$，使得 $S' = aS$。为此，注意到必有 $a = a*1 \in S' \cap \mathbb{Z}_{25}^\times$；因此 $a \in \{1, 4, 6, 9, 11, 14, 16, 19, 21, 24\}$。由此可得 $a \neq 1$和 $a \neq 4$，因为$a * 5 = 4 * 5 = 20 \notin S'$。同理，其他所有可能性都会导致矛盾。

4 竞赛图

在本 本章将给出 t 的主要结果 论文中。

4.1 点传递竞赛图

我们先从一条简短的注开始。

REMARK 4.1.1. 每个点传递竞赛图的阶都是奇数。

PROOF. 设 G 是一个点传递竞赛图。点传递性意味着 $\deg^+(v) = \deg^+(w) = k$ 且 $\deg^-(v) = \deg^-(w) = \ell$ 对所有 $v, w \in V(G)$ 均成立。因此，我们有

$$|G|k = \sum_v \deg^+(v) = \sum_v \deg^-(v) = |G|\ell,$$

由此可得 $k = \ell$。由于竞赛图是完全的，我们还有 $2k = k + \ell = |G| - 1$；若 $|G|$ 为偶数，则会导出矛盾。 □

DEFINITION 4.1.2. 设 $p \in \mathbb{P} \setminus \{2\}$ 和 $p - 1 = 2^k r,\ 2 \nmid r$。递归定义为

$$\begin{aligned}
&S(r) = 0,\\
&S(m) = \sum_{\substack{m|n|r,\\ m<n}} \mathrm{pr}_1(\varphi_p(n))\mathrm{pr}_2(\varphi_p(n)),\ 1 \le m < r,\\
&\varphi_p(m) = (k, \frac{p-1}{m}),\ \text{such that } 2^{\frac{\frac{p-1}{m}}{2}} - S(m) = k\frac{p-1}{m},\ 1 \le m \le r.
\end{aligned}$$

THEOREM 4.1.3. 设 $p \in \mathbb{P} \setminus \{2\}$ 和 $p - 1 = 2^k r,\ 2 \nmid r$。存在

$$\sum_{\substack{m|r,\\ 1\le m\le r}} \mathrm{pr}_1(\varphi_p(m))$$

阶为 p的点传递竞赛图的同构类。

PROOF. 根据引理 3.4.4，以及每个阶为 p 的群都同构于 $\mathbb{Z}_p$ 这一事实可知，在将同构图视为相同之后， p 个顶点上的点传递竞赛图与 $\mathbb{Z}_p$ 上的凯莱竞赛图之间存在一一对应关系。我们可以将任意凯莱竞赛图的连接集 S

与元组 $\frac{p-1}{2}$ （$x_1, ..., x^{\frac{p-1}{2}}$）对应，其中 $x_i \in \{i, -i\}$，因为 $0 \notin S$ 和 $i \in S$ 或 $-i \in S$，但对于所有 $i = 1, ..., \frac{p-1}{2}$，只有其中一个成立。为表示这种对应关系，我们记作 $S \cong_{ident}$ （$x_1, ..., x^{\frac{p-1}{2}}$）。由此可知，除同构外，存在 $2^{\frac{p-1}{2}}$ 个可能的连接集 S 或点传递竞赛图。根据引理 3.4.3 可知

$$\overrightarrow{\mathrm{Cay}}_{tourn}(\mathbb{Z}_p, S) \cong \overrightarrow{\mathrm{Cay}}_{tourn}(\mathbb{Z}_p, S') \text{ if and only if } S' = aS \text{ for some } a \in \mathbb{Z}_p^\times.$$

我们在 $\mathbb{Z}_p$ 上凯莱竞赛图的连接集集合上定义如下等价关系

$$S \text{ equivalent to } S' \text{ if and only if } S' = aS \text{ for some } a \in \mathbb{Z}_p^\times.$$

由此可知，任一等价类的最大大小为$|\mathbb{Z}_p^\times| = p - 1$。假设存在一个等价类 E，其中有 $|E| < p - 1$。令 $S \in E$，那么对于某些a、$b \in \mathbb{Z}_p^\times$，有 $aS = bS$ 或 $S = a^{-1}bS$。我们如何找出所有这样的 S?
设$(x'_1, ..., x'_{\frac{p-1}{2}})$是一个 $\frac{p-1}{2}$-元组，使得 $x'_i \in \mathbb{Z}_p$，$(\bigcup_i x'_i) \cap (\bigcup_i x'_i)^{-1} = \emptyset$且 $x'_i \neq x'_j$，若 $i \neq j$。通过重新排列并在$\{-\frac{p-1}{2}, ..., \frac{p-1}{2}\}$中使用同余值，我们可以将此元组与$(x_1, ..., x^{\frac{p-1}{2}})$ $x_i \in \{i, -i\}$对应起来。我们用写作$(x'_1, ..., x'_{\frac{p-1}{2}})$ $\cong_{rewrite} (x_1, ..., x^{\frac{p-1}{2}})$来表示这种对应。令 $a \in \mathbb{Z}_p^\times$。于是我们得到

$$aS \cong_{ident} a(x_1, ..., x_{\frac{p-1}{2}}) = (ax_1, ..., ax_{\frac{p-1}{2}}) \cong_{rewrite} (x'_1, ..., x'_{\frac{p-1}{2}}).$$

因此，我们可以利用关于 a 对 $\{-\frac{p-1}{2}, ..., \frac{p-1}{2}\}$ 的作用的信息来理解乘法 aS。我们知道， $\mathbb{Z}_p^\times$ 是 $\langle a \rangle$的左陪集的不交并:

$$\mathbb{Z}_p^\times = \dot{\bigcup}_{b \in I \subseteq \mathbb{Z}_p^\times} b\langle a \rangle = \dot{\bigcup}_{i=1,...,k} \{y_1^i, ..., y_\ell^i\},$$

其中， I 是某个代表元集合，且 $\ell = |\langle a \rangle|$、 $k = |\mathbb{Z}_p^\times / \langle a \rangle|$ 和 $y_j^i \in \{-\frac{p-1}{2}, ..., \frac{p-1}{2}\}$。我们马上会看到，如果存在某个 a-不变的 S，那么 $|\langle a \rangle|$ 必为奇数，因此 $k = |\mathbb{Z}_p^\times / \langle a \rangle|$ 必为偶数。因此，左陪集两两成对，且每对中的左陪集仅符号不同。我们从每对中选取一个，记为 $\{y_1'^j, ..., y_\ell'^j\}$，于是得到

$$a(x_1, ..., x_{\frac{p-1}{2}}) \cong_{rewrite} (x_1, ..., x_{\frac{p-1}{2}}) =: x$$

当且仅当

$$x \cong_{ident} \{c_1\{y_1'^1, ..., y_\ell'^1\}, ..., c_\ell\{y_1'^{\frac{k}{2}}, ..., y_\ell'^{\frac{k}{2}}\}\},$$

其中 $c_i \in \{-1, 1\}$、 $i = 1$、 ....、 ℓ。因此， a-不变的 S 有 $2^{\frac{k}{2}}$ 种可能。

为了更好地理解，我们以 $p = 11, a = 5$ 为例进行简要说明。要得到下图，我们先从最内侧的两列开始，将它们乘以 $a = 5$，重新排序，然后将它们与相应的

值写在 $\{-5,...,5\}$ 中:

1	2	-3	-4	-5
1	2	8	7	6
6	1	7	2	8
-1	-2	-3	-4	-5
1	2	3	4	5
5	10	4	9	3
10	9	3	4	5
-1	-2	3	4	5

因此，乘以 a 时，会取 $\{-1,1\}$ 中所选值的符号，并在 $\{-5,5\}$ 中得到符号相同的值；会取 $\{-2,2\}$ 中所选值的符号，并在 $\{-1,1\}$ 中得到符号不同的值，依此类推。因此我们有

$$(15),(2-1),(34),(4-2),(53)$$

或者也可以用圈的形式写为

$$(1534-2),$$

因为 (-21) 与 $(2-1)$ 包含相同的信息。注意，我们只需要图表的一半。现在可以看出哪些集合在 a 作用下是不变的。这些集合是 $\{1,5,3,4,-2\} \cong_{ident}$ (1 −2 3 4 5) 和 $\{-1,-5,-3,-4,2\} \cong_{ident}$(−1 2 −3 −4 −5)。通过考察 $\langle a\rangle = \langle 5\rangle = \{1,5,5^2,5^3,5^4,5^5\} = \{1,5,3,4,-2\} \subseteq \mathbb{Z}_p^\times$ 的左陪集，我们可以去掉图表。在这种情况下，只有两个左陪集： $\{1,5,3,4,-2\}$ 和 $\{-1,-5,-3,-4,2\}$。我们总能得到这样的相关成对集合，它们包含相同的信息。一个更复杂的例子是 $p=13, a=3$。这样我们得到 $\frac{p-1}{|\langle a\rangle|} = \frac{12}{3} = 4$ 个左陪集：$\underline{\quad p-1\quad}\{1,3,-4\},\{-1,-3,4\},\{5,2,6\},\{-5-2-6\}$，因此有 $2^{\frac{|\langle a\rangle|}{2}} = 2^2 = 4$ 种可能的 a-不变的 S，因为我们可以从每一对中各选一个集合来构造这样的 S。

让我们回到证明。哪些 a 确实会产生一个 a-不变的 S? 假设$-1 \in \langle a\rangle$，则 $1,-1 \in \langle a\rangle$。如果 S 是 a-不变的，这就意味着所识别的 S 元组在第一个位置的符号，与它在第一个位置的符号相反，这是不可能的。因此，不存在 a-不变的 S。由于 $\langle a\rangle$ 是由 a 生成的循环群，对于任意满足 $|\langle a\rangle| = kd$ （其中某个 $k \in \mathbb{N}$）的 $d \in \mathbb{N}$，$\langle a^k\rangle$ 都是阶为 d 的唯一子群。因此，$\{-1,1\} \subseteq \langle a\rangle \subseteq \mathbb{Z}_p^\times$ 是阶为 2 的唯一子群，故如果存在某个 a-不变的 S，那么 $|\langle a\rangle|$ 不能被 2 整除。

我们已经看到，任意 a-不变的 S 都可以写成 $\langle a\rangle$ 的 $\frac{|\mathbb{Z}_p^\times/\langle a\rangle|}{2}$ 个左陪集的并集。由此可知，所有与 S 等价的集合 S' 都是

a-不变的。为此，注意到由于 $S' = bS$，对于某个 $b \in \mathbb{Z}_p^\times$， b 只是对左陪集进行置换。
遗憾的是，并非所有 a-不变的 S 都必然等价。设 $b\langle a\rangle = c\langle a\rangle$，则

$$\begin{aligned} bd\langle a\rangle &= db\langle a\rangle \\ &= dc\langle a\rangle \\ &= cd\langle a\rangle. \end{aligned}$$

因此， $bS = cS$，所以任意一个 $2^{\frac{|\mathbb{Z}_p^\times/\langle a\rangle|}{2}}$ a-不变的 S 都包含在一个大小为最大值 $|\mathbb{Z}_p^\times/\langle a\rangle|$的等价类中。

再次设 $\langle a\rangle \subseteq \langle b\rangle \subseteq \mathbb{Z}_p^\times$。由于

$$c\langle b\rangle = c\dot{\bigcup}_{d\in I\subseteq\mathbb{Z}_p^\times} d\langle a\rangle = \dot{\bigcup}_{e\in J\subseteq\mathbb{Z}_p^\times} e\langle a\rangle,$$

$\mathbb{Z}_p^\times$ 中的任意一个 $\langle b\rangle$ 左陪集都可以写成 $\langle a\rangle$左陪集的并。这里的关键如下：如果 S 是 b-不变的，就可以将其写成 $\langle b\rangle$左陪集的并，其中每一对仅符号不同的左陪集中选取一个。假设这样的 S 至少有一次同时包含 $\langle a\rangle$中一对仅符号不同的左陪集。那么， S 也会同时包含 $\langle b\rangle$左陪集对中的两个元素，而这对左陪集包含 $\langle a\rangle$左陪集。这显然与 S 是 b-不变的这一阶乘相矛盾。因此可知，如果 S是 b-不变的，那么它也必定是 a-不变的。因此，在 $2^{\frac{|\mathbb{Z}_p^\times/\langle a\rangle|}{2}}$ a-不变的 S 中， $2^{\frac{|\mathbb{Z}_p^\times/\langle b\rangle|}{2}}$ 是 b-不变的，因而包含在大小为最大值 $|\mathbb{Z}_p^\times/\langle b\rangle| < |\mathbb{Z}_p^\times/\langle a\rangle|$的等价类中。

设 E 是集合 S的等价类，且它是 a-不变的，并且$\langle a\rangle$ 是所有由元素生成且保持S 不变的群中的极大群。假设 E 未达到其最大规模 $|\mathbb{Z}_p^\times/\langle a\rangle|$。那么 $bS = cS$，对于某个 b， $c \in \mathbb{Z}_p^\times$，即 S 是 $d = b^{-1}c$-不变的。如果 $\langle d\rangle \subseteq \langle a\rangle$，最大规模不会变小。因此，假设相反的情况 $\langle a\rangle \subsetneq \langle d\rangle$。但根据假设， $\langle a\rangle$ 是极大的，所以这就产生了矛盾。这意味着E 达到了其最大规模 $|\mathbb{Z}_p^\times/\langle a\rangle|$。

为得到公式，令 $1 \le m \le r$, $m|r$ 和 $n > m$，使得 $n|r$, $m|n$。我们找到 a, $b \in \mathbb{Z}_p^\times$，使得 $|\langle a\rangle| = m$, $|\langle b\rangle| = n$ 和 $\langle a\rangle \subseteq \langle b\rangle$。正如我们已经看到的，可以推出，任何 b-不变的 S 也是 a-不变的。因此，在$2^{\frac{|\mathbb{Z}_p^\times/\langle a\rangle|}{2}}$ a-不变的 S中，$2^{\frac{|\mathbb{Z}_p^\times/\langle b\rangle|}{2}}$是 b-不变的。 $S(m)$计算与这些 n对应的集合之和。随后，由 $2^{\frac{|\mathbb{Z}_p^\times/\langle a\rangle|}{2}} - S(m)$计算出那些 a-不变但对任何合适的 b而言并非 b-不变的集合的数量。因此，等价类的数量由 $2^{\frac{|\mathbb{Z}_p^\times/\langle a\rangle|}{2} - S(m)}$ $|\mathbb{Z}_p^\times/\langle a\rangle|$ $= \mathrm{pr}_1(\varphi(m))$给出。故等价类的总数由对 $\mathrm{pr}_1(\varphi(m))$求和得出。

□

Example 4.1.4. 考虑 $p = 331 \in \mathbb{P}$。根据我们的定义，我们将按如下方式计算。我们有 $p-1 = 330 = 2*11*3*5$ 和$\varphi_p(\frac{p-1}{2}) = \varphi_p(11*3*5) = (1,2)$，因为

$$2^{\frac{\frac{p-1}{2}}{\frac{p-1}{2}}} - S(\frac{p-1}{2}) = k*(\frac{p-1}{\frac{p-1}{2}}) \Leftrightarrow 2 = k2 \Leftrightarrow k = 1.$$

因此，我们得到 $S(11*3) = S(11*5) = S(3*5) = \mathrm{pr}_1(\varphi_p(11*3*5))\mathrm{pr}_2(\varphi_p(11*3*5)) = 2$。因此，我们得到 $\varphi_p(11*3) = (3,10)$，因为

$$2^{\frac{\frac{11*3*5*2}{11*3}}{2}} - S(11*3) = k*\frac{11*3*5*2}{11*3} \Leftrightarrow 32-2 = k5*2 \Leftrightarrow k = 3.$$

同理，我们计算 $\varphi_p(11*5) = (1,6)$ 和 $\varphi_p(3*5) = (93,22)$。接下来，我们或许想计算 $\varphi_p(11)$。目前已知的是 $S(11) = 1*2+3*10+1*6 = 38$。因此，我们计算

$$2^{\frac{\frac{11*3*5*2}{11}}{2}} - S(11) = k*\frac{11*3*5*2}{11} \Leftrightarrow 32768-38 = k30 \Leftrightarrow k = 1091,$$

因此 $\varphi_p(11) = (1091,30)$。同理可得

$$\varphi_p(3) = (327534518354199, 110),$$
$$\varphi_p(5) = (130150493, 66).$$

最后一次计算是 $\varphi_p(1)$。我们得到 $S(1) = 1*2+3*10+1*6+93*22+1091*30+327534518354199*110+130150493*66 = 36028805608929242$。此外，

$$2^{\frac{\frac{11*3*5*2}{1}}{2}} - S(1) = k*\frac{11*3*5*2}{1}$$
$$\Leftrightarrow 467680523945888933825179146469210206001842324459 90 = k11*3*5*2$$
$$\Leftrightarrow k = 14172137089269361631066034741491218363692191 6503.$$

因此，

$$\varphi_p(1) = (14172137089269361631066034741491218363692191 6503, 330).$$

求和可得结果

$$14172137089269361631066034741491251117157042 2384$$

同构类。注意，最大规模等价类的数量为 $\mathrm{pr}_1(\varphi_p(1))$。

我们可以使用以下 Prolog 程序进行计算。

```
列表和（[X]，X）。列表和
（[X,Y|T]，R）：－
```

Z 是 X+Y，列表和（[Z |T] , R）。幂运算（X, Y, Z）： –Z 是 X∗∗Y。阶乘（X, 0）： –Y 是 X 取模 2，不是（Y == 0），！。阶乘（X,C）： –Y 是 X/ 2，阶乘（Y,D），C 是 D + 1。除法（X,R）： –Y 是 X–1，阶乘（Y, F），幂运算（2, F,D），R 是 (X–1)/D。s（P,M, 0）： –除法（P,M）。s（P, 0, S）： –除法（P,V），查找全部（E,（区间取值（1,V,N），0 是 V 取模 N，varphi（P,N,K,L），E 是 K∗L），List），列表和（List,S）。s（P, M,S）： –除法（P,V），Mp 是 M+1，查找全部（E, （区间取值（Mp,V,N），0 是 V 取模 N，0 是 N 取模 M，varphi（P,N,K,L），

E 为 K*L），L 为列表），列表和
（列表，S）。变量 phi（P，M，K，
L）：—L 为（P−1）/M，s（P，M，S），
幂运算（2，L/2，E），K 为（E −S）/
L。结果（P，R）：—除法（P，V），
查找所有（K，（区间取值（1，V，
M），0 为 V 取模 M，变量 phi（P，
M，K，））），列表），列表和（列表，
R）。

-

-

程序得出以下结果。

p	同构类的数量	p	同构类的数量
3	1	43	49940
5	1	47	182362
7	2	53	1290556
11	4	59	9256396
13	6	61	17895736
17	16	67	130150588
19	30	71	490853416
23	94	73	954437292
31	1096	79	7048151672
37	7286	83	26817356776
41	26216	...	

对于 $p = 11$, 相应 $2^{\frac{p-1}{2}} = 32$ 生成集的等价类如下所示

$\{\{1,2,3,4,5\},\{2,4,6,8,10\},\{3,6,9,1,4\},\{4,8,1,5,9\},\{5,10,4,9,3\},\{6,1,7,2,8\},$

$\{7,3,10,6,2\},\{8,5,2,10,7\},\{9,7,5,3,1\},\{10,9,8,7,6\}\},$
$\{\{1,2,3,7,5\},\{2,4,6,3,10\},\{3,6,9,10,4\},\{4,8,1,6,9\},\{5,10,4,2,3\},\{6,1,7,9,8\},$

$\{7,3,10,5,2\},\{8,5,2,1,7\},\{9,7,5,8,1\},\{10,9,8,4,6\}\},$
$\{\{1,2,3,4,6\},\{2,4,6,8,1\},\{3,6,9,1,7\},\{4,8,1,5,2\},\{5,10,4,9,8\},\{6,1,7,2,3\},$

$\{7,3,10,6,9\},\{8,5,2,10,4\},\{9,7,5,3,10\},\{10,9,8,7,5\}\},$
$\{\{1,9,3,4,5\},\{2,7,6,8,10\}\}.$

这种结构体现在 $\varphi_{11}(5) = (1, 2)$ 和 $\varphi_{11}(1) = (3, 10)$ 中。

5 结论

5.1 推广

我们如何从先前的结果继续推进？当前最迫切的问题是，能否将定理 4.1.3.推广到任意 $n \in \mathbb{N}$，或者至少推广到带有 $p \in \mathbb{P}, k \in \mathbb{N}$ 的 p^k。遗憾的是，即使是后一种情况也会遇到困难。在证明一开始，我们就用到了这样一个事实：每个素数阶 p 的顶点传递竞赛图，都可以唯一地识别为定义在 $\mathbb{Z}_p$ 上的凯莱竞赛图。这一结论基于引理 3.4.4，而后者最终用到了 Burnside 引理 3.4.2。但对于素数幂，这一结论并没有一般形式。

接下来，我们将采用捷径，只关注凯莱竞赛图，也就是说，不再讨论其与普通锦标赛的关系。第二节将深入说明，这通常会构成一种限制。再次回顾主定理 4.1.3 的证明，我们用到了引理 3.4.3，其内容如下：

$$\overrightarrow{\mathrm{Cay}}_{tourn}(\mathbb{Z}_p, S) \cong \overrightarrow{\mathrm{Cay}}_{tourn}(\mathbb{Z}_p, S') \text{ if and only if } S' = aS \text{ for some } a \in \mathbb{Z}_p^{\times}.$$

推广这一思想，若一个特定的凯莱图 Cay(Γ, S) 满足：Cay(Γ, S) ≅ Cay(Γ, S') 当且仅当 $S' = aS$ 对某个群自同构$a \in$ Aut(Γ)成立，则称其为 CI 图。此外，若对于任意的 S, S'，Cay(Γ, S) ≅Cay(Γ, S') 当且仅当 $S' = aS$ 对某个群自同构 $a \in$ Aut(Γ)成立，则称 Γ 为 CI 群。因此， Γ 是 CI 群，当且仅当其上的每个凯莱图都是 CI 图。类似地，我们定义 DCI 有向图 $\overrightarrow{\text{Cay}}$(Γ, S) 和 DCI 群。换言之，引理 3.4.3 的上述陈述表明，对于适当的 S， $\overrightarrow{\text{Cay}}_{tourn}(\mathbb{Z}_p, S)$ 是 DCI 有向图。尽管如此，仅凭这一点，我们无法推断 $\mathbb{Z}_p$ 是 DCI 群，因为有些集合 S 会生成凯莱有向图，却不会生成凯莱竞赛图。

不过，确定所有循环 CI 群和 DCI 群的任务已由 Muzychuk 完成；其结果如下。

Lemma 5.1.1（Muzychuk [10]）。循环群 $\mathbb{Z}_n$ 是 CI 群，当且仅当 $n = 8$、9、18 或 $n = 2^e m$，其中 m 为奇数且无平方因子，并且 $e \in \{0, 1, 2\}$。

Lemma 5.1.2 (Muzychuk [10]). 循环群 $\mathbb{Z}_n$ 是 DCI 群，当且仅当 $n = 2^e m$，其中 m 为奇数且无平方因子的，并且 $e \in \{0, 1, 2\}$。

按照我们的主要证明，我们可以尝试推导出具有 $n = 2^e \cdot p_1 \cdot \ldots \cdot p_k$ 的 $\mathbb{Z}_n$ 上凯莱竞赛图的同构类数量，其中 $p_i \in \mathbb{P} \setminus \{2\}, p_i \neq p_j$，条件是 $i \neq j$ 且 $e = 0$（每个顶点传递竞赛图的阶都是奇数）。不过，继续沿用证明中的构造，我们发现，为了确保每个给定的合适阶恰好对应一个子群，我们用到了 $\mathbb{Z}_p^\times$ 是循环群这一事实。关于这个问题，可以得到以下结论。

REMARK 5.1.3. $\mathbb{Z}_n^\times$ 当且仅当 $n = 2, 4, p^k, 2p^k$ 时是循环的，其中 $p \in \mathbb{P} \setminus \{2\}, k \in \mathbb{N}$。

因此，我们陷入了困境，因为我们选择的 n 要么导致 $\mathbb{Z}_n$ 成为 DCI-群，要么导致 $\mathbb{Z}_n^\times$ 是循环的，而这两种情况都只在平凡情形下成立，即 $n = p \in \mathbb{P} \setminus \{2\}$。

5.2 非 Cayley 顶点传递锦标赛

如前所述，研究凯莱竞赛图而非顶点传递竞赛图，实际上是一种限制。确切地说，存在一种顶点传递竞赛图，它不是凯莱竞赛图。此外，还可以构造出这类图的无限族。该如何做到这一点？一个重要的组成部分是元循环有向图，它们由 Alspach 和 Parsons [2] 定义如下。设$m \in \mathbb{N}_{\geq 1}, n \in \mathbb{N}_{\geq 2}, a \in \mathbb{Z}_n^\times$和 $S_0, \ldots, S_{m-1} \subseteq \mathbb{Z}_n$，使得

1. $0 \notin S_0$
2. 对于 $0 \leq r \leq m-1$，$a^m S_r = S_r$。

元循环有向图 $G = G(m, n, a, S_0, \ldots, S_{m-1})$ 是一个顶点集为

$$\{v_j^i \mid i \in \mathbb{Z}_m, j \in \mathbb{Z}_n\}$$

且边集为

$$\{[v_j^i, v_h^{i+r}] \mid r \in \mathbb{Z}_m, h \in j + a^i S_r\}.$$

我们在 $V(G)$ 上定义置换 ρ, σ：$(v_j^i)^\rho = v_{j+1}^i$、$(v_j^i)^\sigma = v_{aj}^{i+1}$，并得到如下刻画。

LEMMA 5.2.1（Alspach 和 Parson [2]）。元循环图 $G = G(m, n, a, S_0, \ldots, S_{m-1})$ 是顶点传递的，且 $\langle \rho, \sigma \rangle \leq \mathrm{Aut}(G)$。反之，任何顶点集为 $V(G)$ 且 $\langle \rho, \sigma \rangle \leq \mathrm{Aut}(G)$ 的有向图 G' 都是一个 (m, n)-元循环图。

Maruˇsiˇc [8] 已证明，每个阶为 p^k 且具有$k \leq 3$ 的顶点传递有向图必然是凯莱有向图。另一方面，他还为每个 $k \geq 4$ 构造了一个阶为 p^k的非 Cayley 点传递有向图：

LEMMA 5.2.2（Maruˇsiˇc [8]）。设 $p \in \mathbb{P}, k \geq 3, a \in \mathbb{Z}_{p^k}^\times$ 的阶为 p^2。设$S_0 = \langle a^p \rangle$和 $S_1 = \langle 0 \rangle$。设 $S_i = \emptyset, 2 \leq i \leq p-1, p \neq 2$。则元循环有向图 $G(p^k, p, a) = G(p^k, p, S_0, \ldots, S_{p-1})$ 不是 Cayley 有向图。

基于这些结果，Mansilla [7] 随后构造了一个由阶为 $p^k, p \in \mathbb{P} \setminus \{2\}, k \geq 4$ 的非 Cayley 顶点传递锦标赛组成的无限族。因此，设 $a \in \mathbb{Z}_{p^k}^{\times}$ 的阶为 p^2，并令 $G = G(p^k, p, a)$ 为引理 5.2.2 中对应的元循环有向图。设 Γ 为 Aut(G) 中包含 ρ 和 σ的 Sylow p-子群。现在的主要思路是构造一个竞赛图 $T = T(p^k, p, a)$，使得 $V(T) = V(G)$，且 Aut(T) $= \Gamma$。从引理 5.2.2 的原始证明可以看出，Γ 没有任何正则子群，因此 $T(p^k, p, a)$ 不是 Cayley 图。不过，由于 $\langle \rho, \sigma \rangle \leq \Gamma =$ Aut(T)，根据引理 5.2.1，T 将是一个 (p^k, p)-元循环有向图，因此它是顶点传递的。

我们如何由此得到无穷多个非 Cayley 顶点传递锦标赛？令 $q \in \mathbb{P}, q \equiv 3$ 取模 4。当且仅当 $s - r$ 是非零平方时，Paley 锦标赛 $P(q)$ 的顶点集为 $\mathbb{F}_{p^n}$，且 $r \sim s$。两个有向图 G_1, G_2 的字典积，其顶点集为 $V(G_1) \times V(G_2)$，并且当且仅当 $v \sim v'$ 或 $v = v'$ 且 $w \sim w'$时，$(v, w) \sim (v', w')$。Mansilla 通过将旧的非 Cayley 顶点传递锦标赛与 Paley 锦标赛作字典积，构造新的非 Cayley 顶点传递锦标赛，并证明了以下结果。

LEMMA 5.2.3. 令 $m = p_1^{\ell_1} \cdot \ldots \cdot p_r^{\ell_r}$，$2 < p_1 < \ldots < p_r$，$\ell_1, \ldots, \ell_r \in \mathbb{N}_{\geq 1}$。若存在一个指标 $i, 1 \leq i \leq r$，使得对于每个 $1 \leq j \leq r, i \neq j$，$l_i \geq 4$ 且 $p_j \equiv 3$ 取模 4，则存在一个阶为 m的非 Cayley 顶点传递锦标赛。

因此，如果我们有一个阶为$s = p^k k \geq 4$的非凯莱点传递竞赛图，那么对于任意 r 个模 4 同余于 3 的素数之积，我们都可以得到一个阶为 rs 的新非凯莱点传递竞赛图。

5.3 定义在非同构群上的凯莱图

研究非素数阶凯莱竞赛图时，会遇到一个问题：可能会出现多个阶相同但彼此非同构的群。由此很容易证明，在阶相同但彼此非同构的群上存在非同构的凯莱竞赛图。然而，一个更有趣的问题是：对于某个群，是否存在一个凯莱竞赛图，使其与定义在任何其他同阶非同构群上的凯莱竞赛图都不同构？Anne Joseph [6] 曾对素数平方开展过一些相关研究。这里我们将简要回顾 Joy Morris [9] 扩展版本中的内容。不过在此之前，让我们先验证前面提出的论断。

考虑 $n = 3^2$，那么在同构意义下，唯一的非同构群是$\mathbb{Z}_9$ 和 $\mathbb{Z}_3^2$。我们定义集合

$$S = \{1, 7, 3, 5\} \subseteq \mathbb{Z}_9$$

and

$$S' = \{(0,1),(2,0),(1,1),(2,1)\} \subseteq \mathbb{Z}_3^2.$$

这两个集合都生成了9阶凯莱竞赛图。现在我们将进一步探讨所有边都指向同一方向的三角形数量。记住， $a \sim b$ 当且仅当 $b = a + s$、$s \in S$ 以及（a， b）$\sim$（a'， b'），当且仅当（a'， b'）$=$（a， b）$+ s$、$s \in S'$。

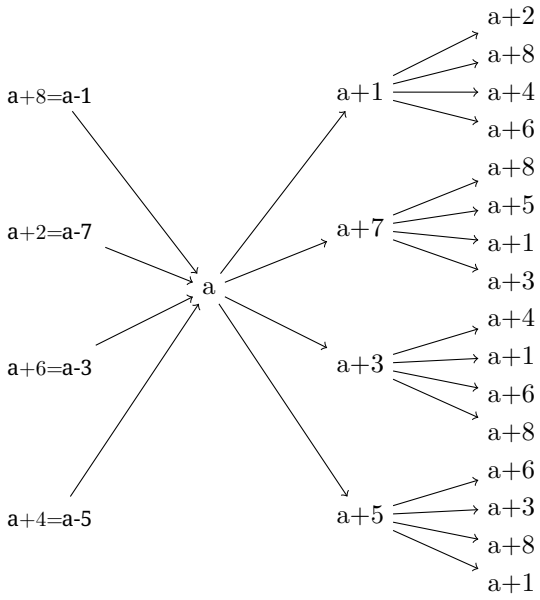

图5.1： $S = \{1,7,3,5\} \subseteq \mathbb{Z}_9$

以图5.1为例， $a = 0$ 和 $a + 1 = 1$。它们共有4个三角形，且每条边的方向都相同。另一方面，在图

$$\overrightarrow{5\ 2,} \qquad {}_{tourn}\ \mathbb{Z}_9\ S\ \ncong \text{中},$$

我们找不到这样的一对顶点。这意味着 $\overrightarrow{\text{Cay}(\ ,\ )}\ \text{Cay}_{tourn}(\mathbb{Z}_3^2, S')$，从而证明了这一断言。现在我们将探讨 Joy Morris [9]的结果。

设 G、H 是有向图。花环积 $G \wr H$ 定义为满足 $V(G \wr H) = V(G) \times V(H)$ 且 $(v,w) \sim (v',w')$ 当且仅当

$$v = v' \text{ and } w \sim w'$$

or

$$v \sim v'.$$

在阶为 $p^k, p \in \mathbb{P}$ 的阿贝尔群集合上定义如下偏序。当且仅当存在一条子群链

$$\Gamma_1 < \Gamma_2 < ... < \Gamma_n = \Gamma,$$

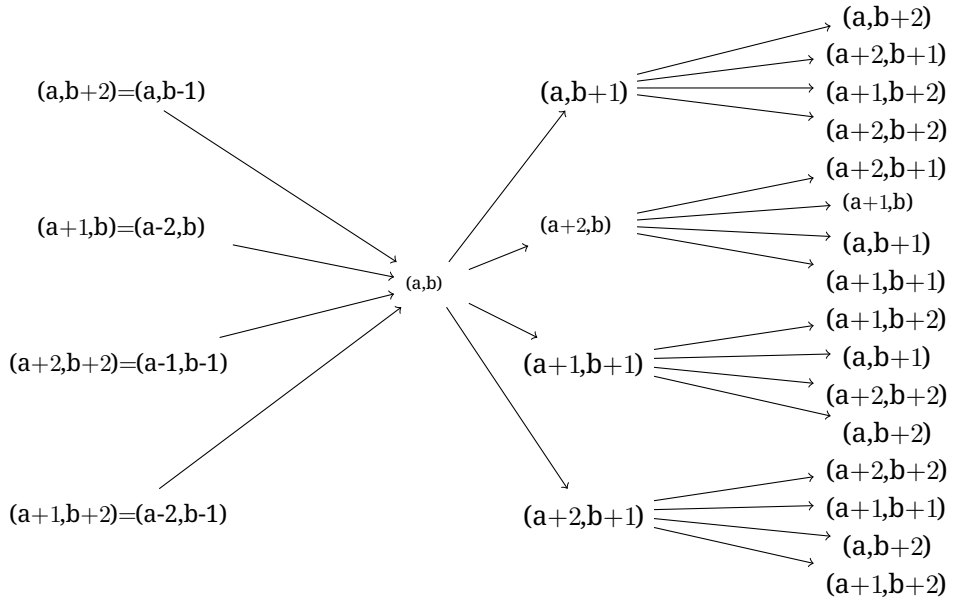

图5.2： $S' = \{(0, 1), (2, 0), (1, 1), (2, 1)\} \subseteq \mathbb{Z}_3^2$

使得 $\Gamma_1, (\Gamma_2/\Gamma_1)$ ...., (Γ_n/Γ_{n-1}) 是循环的，并且

$$\Gamma' \cong \Gamma_1 \times (\Gamma_2/\Gamma_1) \times .... \times (\Gamma_n/\Gamma_{n-1}).$$

我们给出一个关于 $k = 5$ 的简短例子。

EXAMPLE 5.3.1. 根据有限生成阿贝尔群基本定理可知，任何阶为 p^5 的阿贝尔群都同构于形如 $\mathbb{Z}_{p^{k_1}} \times ... \times \mathbb{Z}_{p^{k_6}}, \sum_i k_i = 5$ 的群。对于 $m \geq n$，包含映射 $\mathbb{Z}_{p^m} \overset{\iota}{\hookrightarrow} \mathbb{Z}_{p^n}, [x]_m \mapsto [x]_n$ 是良定义的： $[x]_m = [y]_m$ 等于 $x = y + lp^m = y + (lp^{m-n})p^n, l \in \mathbb{Z}$，而这等于 $[x]_n = [y]_n$。因此，我们有 $\mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^m}/\ker(\iota) \cong \mathbb{Z}_{p^m}/\mathbb{Z}_{p^{m-n}}$。现在考虑 $\Gamma' = \mathbb{Z}_p \times \mathbb{Z}_{p^4}$ 和 $\Gamma = \mathbb{Z}_{p^5}$。由于 Γ 是加法循环的，对于每个 $k = 1, ..., 5$，都存在唯一一个阶为 p^k 的子群，在本例中它是 $\mathbb{Z}_{p^k}$。因此，我们有一条 1-链

$$\Gamma_1 = \mathbb{Z}_p < \mathbb{Z}_{p^5} = \Gamma$$

and

$$\Gamma' = \mathbb{Z}_p \times \mathbb{Z}_{p^4} \cong \mathbb{Z}_p \times (\mathbb{Z}_{p^5}/\mathbb{Z}_p) = \Gamma_1 \times (\Gamma/\Gamma_1),$$

由此得到 $\Gamma' \leq_{po} \Gamma$。接下来考虑 $\Gamma' = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^3}$ 和 $\Gamma = \mathbb{Z}_p \times \mathbb{Z}_{p^4}$。我们再次得到一个 1-链

$$\Gamma_1 = \{0\} \times \mathbb{Z}_p < \mathbb{Z}_p \times \mathbb{Z}_{p^4} = \Gamma,$$

and

$$\begin{aligned}\Gamma' = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^3} &\cong \{0\} \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^3} \\ &\cong \{0\} \times \mathbb{Z}_p \times \big((\mathbb{Z}_p \times \mathbb{Z}_{p^4})/(\{0\} \times \mathbb{Z}_p)\big) = \Gamma_1 \times (\Gamma/\Gamma_1).\end{aligned}$$

继续推导，得到图 5.3。

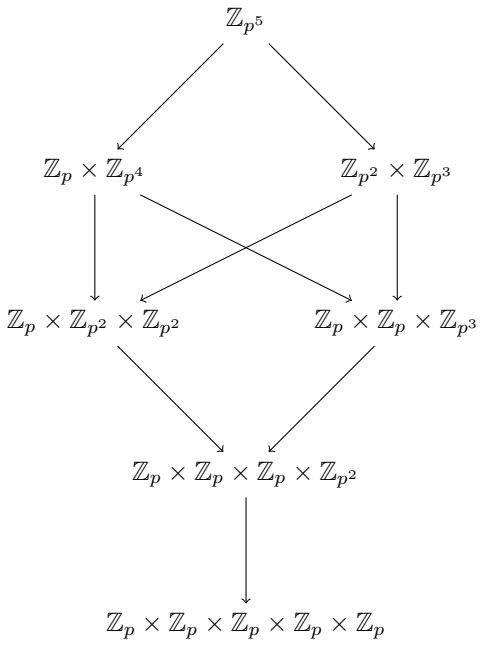

图 5.3：阶为 p^5 的阿贝尔群的偏序。

现在可以给出主要结果。

THEOREM 5.3.2. 设 Γ 是阶为 p^k 的阿贝尔群，$p \in \mathbb{P} \setminus \{2\}$ 且 $G := \overrightarrow{\mathsf{Cay}}(\Gamma, S)$。则以下各项等价：

1. G 同构于同时定义在 $\mathbb{Z}_{p^k}$ 和 Γ' 上的凯莱有向图，其中 Γ' 是阶为 p^k 的任意阿贝尔群。

2. 存在子群链 $\Gamma_1 < \Gamma_2 < ... < \Gamma_n = \Gamma$，使得

   (a) $\Gamma_1, (\Gamma_2/\Gamma_1), ..., (\Gamma_n/\Gamma_{n-1})$ *are cyclic,*

   (b) $\Gamma_1 \times (\Gamma_2/\Gamma_1) \times .... \times (\Gamma_n/\Gamma_{n-1}) \leq_{po} \Gamma'$,

   (c) For all $s \in S \setminus \Gamma_i$*, we have* $s + \Gamma_i \subseteq S$*, for* $i = 1, ..., n-1$

3. 存在定义在循环的 p-群 Γ_1,...,Γ_n 上的凯莱有向图 G_1,...,G_n，使得 $\Gamma_1 \times ... \times \Gamma_n \leq_{po} \Gamma$ 和 $G \cong G_n \wr ... \wr G_1$。

由此又可推出：

4. G 与阶为 p^k、且在偏序中大于 Γ' 的每个阿贝尔群上的凯莱有向图同构。

EXAMPLE 5.3.3. 重新考察 $\overrightarrow{\mathsf{Cay}}_{tourn}(\mathbb{Z}_9, \{1,7,3,5\})$。我们已经看到，它不同构于 $\overrightarrow{\mathsf{Cay}}_{tourn}(\mathbb{Z}_3^2, \{(0,1),(2,0),(1,1),(2,1)\})$。假设存在一个定义在 $\Gamma' = \mathbb{Z}_3^2$ 上的凯莱竞赛图，且它与之同构。那么第一个命题成立，因为每个凯莱竞赛图都是凯莱有向图，因此第二个命题也必然成立。$\Gamma = \mathbb{Z}_9$ 有两个子群，分别是 $\Gamma_1 = \langle 3 \rangle = \{0,3,6\}$ 和 $\{0\}$。不失一般性，我们只需考虑 Γ_1。现在，由 2(c) 可得，对所有 $s \in S \setminus \Gamma_1 = \{1,7,3,5\} \setminus \{0,3,6\} = \{1,7,5\}$:

$$s + \Gamma_1 = s + \{1,7,3,5\} \subseteq S = \{1,7,3,5\}.$$

这对于 $s = 1$ 并不成立，这就产生了矛盾。因此，$\overrightarrow{\mathsf{Cay}}_{tourn}(\mathbb{Z}_9, \{1,7,3,5\})$ 不同构于 $\mathbb{Z}_3^2$ 上的任何凯莱竞赛图。

EXAMPLE 5.3.4. 另一方面，要证明 $\overrightarrow{\mathsf{Cay}}_{tourn}(\mathbb{Z}_3^2, \{(0,1),(2,0),(1,1),(2,1)\})$ 不同构于 $\mathbb{Z}_9$ 上的任何凯莱竞赛图，并不像之前那样顺利。反设结论不成立，则对于 $\Gamma' = \mathbb{Z}_9$，命题 1 成立。同样，不失一般性，只需考察非平凡子群，因为仅由 $\Gamma = \mathbb{Z}_3^2$ 和平凡子群构成的子群链不满足 2(a)。三阶子群共有四个:

1. $\Gamma_1 = \{(0,0),(1,0),(2,0)\}$，2. $\Gamma_2 = \{(0,0),(0,1),(0,2)\}$，3. $\Gamma_3 = \{(0,0),(1,1),(2,2)\}$，4. $\Gamma_4 = \{(0,0),(1,2),(2,1)\}$.

因此，取 $S = \{(0,1)、(2,0)、(1,1)、(2,1)\}$，我们得到:

1. $S \setminus \Gamma_1 = \{(0,1)、(1,1)、(2,1)\}$，2. $S \setminus \Gamma_2 = \{(2,0)、(1,1)、(2,1)\}$，3. $S \setminus \Gamma_3 = \{(0,1)、(2,0)、(2,1)\}$，4. $S \setminus \Gamma_4 = \{(0,1)、(2,0)、(1,1)\}$.

现在，在 2. 中我们有 $(2,0) + (0,2) = (2,2) \notin S$，在 3. 中有 $(0,1) + (1,1) = (1,2) \notin S$，在 4. 中有 $(0,1) + (2,1) = (2,2) \notin S$。但在 1. 中，我们却遗憾地会成功。因此，我们的反证法行不通。更进一步，这个 1-链

$$\Gamma_1 = \{(0,0),(1,0),(2,0)\} < \mathbb{Z}_3^2 = \Gamma$$

实际上满足 2.：一方面，我们有 $\Gamma_1 = \{(0,0),(1,0),(2,0)\}$ 以 (1,0) 为循环的；另一方面，我们有

$$\begin{aligned}\Gamma/\Gamma_1 &= \mathbb{Z}_3^2/\{(0,0),(1,0),(2,0)\} \\ &= \big\{\{(0,0),(1,0),(2,0)\},\{(1,1),(2,1),(0,1)\},\{(2,2),(0,2),(1,2)\}\big\},\end{aligned}$$

它是循环的，生成元为 {(1, 1)、(2, 1)、(0, 1)}。此外，我们有

$$\begin{aligned}\Gamma_1 \times \Gamma/\Gamma_1 &= \{(0,0),(1,0),(2,0)\} \times (\mathbb{Z}_3^2/\{(0,0),(1,0),(2,0)\}) \\ &\cong \mathbb{Z}_3^2 \\ &= \mathbb{Z}_3 \times (\mathbb{Z}_9/\mathbb{Z}_3) \\ &= \Gamma_1' \times (\Gamma'/\Gamma_1')\end{aligned}$$

通过映射 $((i,0),[(j,j)]) \mapsto (i,j)$。因此，$\Gamma_1 \times (\Gamma/\Gamma_1) \leq_{po} \Gamma'$。由此可知，$\longrightarrow$ $\mathsf{Cay}_{tourn}(\mathbb{Z}_3^2, \{(0,1),(2,0),(1,1),(2,1)\})$ 与 $\mathbb{Z}_9$ 上的一个凯莱有向图同构。由于同构关系，该凯莱有向图也是一个竞赛图。因此，它最终必定是一个凯莱竞赛图。

声明

本论文由我独立撰写，未使用除所列辅助资料以外的任何资料，尤其未使用来源目录中未列出的互联网来源。本论文此前未曾提交至其他考试程序。提交的书面版本与电子存储介质上的版本完全一致。

Stefan Zetzsche

参考文献

[1] Brian Alspach 和 Marni Mishna。有向图与凯莱图的枚举。《离散数学》，256(3):527–539，2002年。[2] Brian Alspach 和 TD Parsons。顶点传递图的一种构造。《加拿大数学杂志》，34(2):307–318，1982年。[3] W Burnside。论奇数阶群的若干性质。《伦敦数学会会刊》，1(1):162–184，1900年。[4] Chris Godsil 和 Gordon F Royle。代数图论，第207卷。施普林格科学与商业媒体，2013年。[5] Geˇna Hahn 和 Claude Tardif。图同态：结构与对称性。载于《图对称性》，第107–166页。施普林格，1997年。[6] Anne Joseph。素数平方阶群上凯莱有向图的同构问题。《离散数学》，141(1):173–183，1995年。[7] S`onia P Mansilla。非凯莱顶点传递竞赛图的无限族。《离散数学》，288(1):99–111，2004年。[8] Dragan Maruˇsiˇc。阶为 p^k 的顶点传递图与有向图。北荷兰数学研究，115:115–128，1985年。[9] Joy Morris。非同构群上的同构凯莱图。《图论杂志》，31(4):345–362，1999年。[10] M Muzychuk。高秩初等阿贝尔群不是 CI 群。《离散数学》，264(1):167–185，2003年。[11] Gert Sabidussi。论一类无不动点图。《美国数学会会刊》，9(5):800–804，1958年。[12] Gert Sabidussi。顶点传递图。《数学月刊》，68(5):426–438，1964年。[13] James Turner。具有素数个点的点对称图。《组合理论杂志》，3(2):136–145，1967年。

[14] James Turner。具有素数个点的点对称图。《组合理论杂志》，3(2):136–145，1967年。