Pure Mathematics 理论数学, 2023, 13(12), 3549-3558
Published Online December 2023 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2023.1312369

Hans汉斯

有限群的基本理论与应用

姬凤杰*，李　芸

塔里木大学信息工程学院，新疆 阿拉尔

收稿日期：2023年11月13日；录用日期：2023年12月14日；发布日期：2023年12月27日

摘　要

有限群是群论中一个重要且广泛研究的分支，对于数学、物理学、化学以及密码学等领域都具有重要意义。本论文旨在介绍有限群的定义、性质及分类，Abel群的定义，有限*p*群的定义和结构定理，即Sylow定理。并探讨有限群的相关理论在不同领域中的应用，包括几何学(对称性与立体几何、曲面理论、张量积分与变换、状态空间搜索)、数论、物理学(对称性与粒子物理学、能带理论与固体物理学、场论和粒子物理)和密码学等领域。

关键词

有限群，Abel群，有限*p*群，Sylow定理

The Basic Theory and Applications of Finite Groups

Fengjie Ji*, Yun Li

School of Information Engineering, Tarim University, Alaer Xinjiang

Received: Nov. 13th, 2023; accepted: Dec. 14th, 2023; published: Dec. 27th, 2023

Abstract

Finite group is an important and widely studied branch of group theory, which is of great significance for fields such as mathematics, physics, chemistry, and cryptography. This paper aims to introduce the definition, properties, and classification of finite group, the definition of Abel group, the definition and structure theorem of finite p-groups, namely the Sylow theorem. And explore the application of related theories of finite groups in different fields, including geometry (symmetry and solid geometry, surface theory, tensor integration and transformation, state space search),

*通讯作者。

文章引用: 姬凤杰, 李芸. 有限群的基本理论与应用[J]. 理论数学, 2023, 13(12): 3549-3558.
DOI: 10.12677/pm.2023.1312369

number theory Fields such as physics (symmetry and particle physics, band theory and solid state physics, field theory and particle physics) and cryptography.

Keywords

Finite Groups, Abel Group, Finite *p* Groups, Sylow Theorem

1. 引言

1.1. 研究背景和意义

有限群是抽象代数的一个重要分支，其研究对象是一类具有特定结构的代数系统，也是数学和物理学中最重要的概念之一。有限群的研究背景可以追溯到 19 世纪，群论在那个时候成为数学的一个重要分支，并且被广泛应用于各个领域，如密码学、代数编码、图像处理、物理学、化学、生物学等等。有限群的基本性质和结构不仅具有严谨的数学证明和推理，而且在各个实际问题中也体现出了很强的应用价值。

在现代密码学中[1]，有限群作为一种重要的代数结构，被广泛应用于构造公钥密码学和对称密码学的安全算法。另外，有限群是描述对称性的基本工具，被用于描述物理现象和化学反应中的对称性群和空间群等。在化学中，有限群的研究对于分子的对称性分析和化学反应机理的解析有重要的作用。在生物学中，群论被用来理解蛋白质的结构和功能等等。

在有限群中，通过一些基本定理能够对群进行简单的分类[2]。这对于研究群的性质和特征及其应用有非常重要的作用。例如，有限简单群的分类是群论的一个伟大成就，这种分类的结果被广泛应用于编码理论、代数几何、计算机科学等领域。

群论的一些概念和方法在计算机科学中被广泛应用[3]，比如可重集合、置换、哈希函数、错误纠正码等等。这些应用使群论成为计算机科学的一部分。

因此，有限群的研究不仅是数学的重要分支，而且具有非常重要的实际应用，了解有限群的性质、特征以及应用范围对于深入认识数学和各个学科领域有着重要意义。

1.2. 论文结构

本文将从以下几个方面进行论述：第二节，首先介绍了群的基本概念和有限群的定义，包括群的四个基本公理，群元素的性质和关系，以及有限群的基本概念。其次，探讨有限群的一些基本性质，包括子群、生成元、同态与同构、正规子群和商群等。第三节将讨论有限群的分类问题，包括半单群与简单群、有限 Abel 群的分类和有限 p 群的结构定理等。第四节，本文将介绍有限群在各个领域的应用，包括群论与几何学的关系、有限群在代数数论中的应用、在物理学与化学中的应用(空间群与晶体学、有限群在量子力学中的应用和对称性群与化学反应的研究)以及有限群在密码学中的应用。

2. 有限群的定义与基本性质

2.1. 群与有限群的概念

群是一种代数结构，其定义包括四个基本公理：封闭性、结合律、恒等元素和逆元素。

定义 2.1 [4]称非空集合 G 为一个**群**，若在 G 中定义了一个二元运算，且二元运算满足：

1) 封闭性：对 $\forall a,b\in G$，都有

$$ab\in G;$$

2) 结合律：对 $\forall a,b,c\in G$，都有

$$(ab)c=a(bc);$$

3) 单位元：$\exists e\in G$，$\forall a\in G$，都有

$$ae=ea=a;$$

4) 逆元：对 $\forall a\in G$，都 $\exists a'\in G$，使得

$$aa'=a'a=e.$$

注：当群 G 的二元运算为乘法时，则 G 就是一个乘法群：当群 G 的二元运算为加法时，则 G 就是一个加法群。

定义 2.2 若群 G 满足交换律，即对 $\forall a,b\in G$，都有

$$ab=ba,$$

则称 G 为交换群或 *Abel* 群。

定理 2.1 以下四个命题等价：

1) G 是群；

2) G 有左单位元 l，而且 $\forall a\in G$ 关于这个左单位元 l 都是左可逆的；

3) G 有右单位元 r，而且 $\forall a\in G$ 关于这个右单位元 r 都是右可逆的；

4) $\forall a,b\in G$，方程 $ax=b, ya=b$ 在 G 中都有解。

定理 2.2 设是群，则

1) 若 e 是 G 的左(右)单位元，则 e 也是 G 的右(左)单位元，从而 e 是 G 的单位元；

2) 若 b 是 G 的左(右)逆元，则 b 也是 G 的右(左)逆元，从而 b 是 G 的逆元。

定理 2.3 设 G 是群，$e\in G$，则

e 是 G 的单位元 $\Leftrightarrow e^2=e$。

定义 2.3 如果群 G 的元素个数是有限的，则这个群就被称为有限群。

有限群具有很多重要的性质和结构，依据这些性质和结构，可以对有限群进行分类和描述。

定义 2.4 [4]设 G 是一个群，e 是 G 的单位元，若使

$$a^m=e \tag{1}$$

成立的最小正整数 m 存在，则 m 称为元素 a 的阶，记作 $|a|=m$。若使式(2.1)成立的正整数 m 不存在，则称 a 是无限阶的，记作 $|a|=\infty$。

注意：当是加法群时，其运算是加法，单位元为零元 0，所以式(1)具有以下形式：

$$ma=e.$$

2.2. 子群与生成元

子群是群的一个子集，满足群的四个基本公理，并且对于群运算具有封闭性。

定义 2.5 若群 G 的非空子集 H 满足 $H^2\subseteq H$，$H^{-1}\subseteq H$，则 H 为 G 的子群，记作 $H\le G$。

显然，$H=\{e\}$ 和 $H=G$ 都是群 G 的子群，叫做群 G 的**平凡子群**。如果 $H\neq\{e\}$ 且 $H\neq G$，就称 H 为群 G 的**真子群**。

定理 2.4 若 H 是群 G 的一个非空子集，则 H 为群 G 的子群的充要条件是对 $\forall a,b\in G$，都有

$$ab^{-1}\in G.$$

定理 2.5 (传递性) 设 $H\le K$，$K\le G$，则 $H\le G$。

由于有限群的元素是有限的，因此有限群的子群的元素也是有限的。此外，有限群的子群具有很重要的性质和结构，可以通过它们完整地描述整个有限群。

生成元是群中的一个概念，其意义是通过一个元素反复运算得到的群中的其它元素。对于一个有限群 G，如果有一个元素 a，使得 a 的所有幂都可以表示为 G 的元素，那么我们称 a 为有限群 G 的生成元。生成元的存在对于描述有限群的结构和性质非常重要，可以帮助我们理解有限群的子群、阶数等概念。

定义 2.6 设 G 为群，若存在 G 的一个元素 a，使得 G 中的任意元素均由 a 的幂组成，即

$$G=\left\{a^n\,|\,n\in Z\right\},$$

则称群 G 为**循环群**，元素 a 为循环群 G 的**生成元**，记为 $G=\langle a\rangle$。

定理 2.6 设群 $G=\langle a\rangle$，则

1) 若 $|a|=\infty$，则对 $\forall s,t\in Z$，如果 $s\ne t$，有 $a^s\ne a^t$，即

$$\cdots,a^{-2},a^{-1},e,a^1,a^2,\cdots$$

是 $\langle a\rangle$ 的全体互异的元素。

2) 若 $|a|=n$，则 $\langle a\rangle$ 是 n 阶群，且

$$\langle a\rangle=\left\{e,a,a^2,\cdots,a^{n-1}\right\}.$$

定理 2.7 循环群 G 的任一子群都是循环群，且子群的阶为群 G 的阶的因子。

定理 2.8 (Lagrange) [4]设 G 是有限群，$H\le G$，则 $|G|=|H||G:H|$。

例 2.1 求出模 10 的剩余类加群 Z_{10} 的所有子群。

解 模 10 的剩余类加群

$$Z_{10}=\{0,1,2,3,4,5,6,7,8,9\}$$

是由[1]生成的 10 阶循环群，由定理 2.7 可得，其子群都是循环群且为 12 的正因子，故的子群共有 4 个，分别为：

1 阶子群：$\langle 0\rangle=\{0\}$；

2 阶子群：$\langle 5\rangle=\{0,5\}$；

5 阶子群：$\langle 2\rangle=\langle 8\rangle=\{0,2,4,6,8\}$；

10 阶子群：$\langle 1\rangle=\langle 7\rangle=\langle 3\rangle=\langle 10\rangle=Z_{10}$。

2.3. 同态与同构

同态是群之间的一个映射，它保持了群的运算结构。

定义 2.7 设 G,G' 是两个群，f 是 G 到 G'的一个映射。如果对 $\forall a,b\in G$，都有

$$f(a)f(b)=f(ab),$$

那么，称 f 为 G 到 G'的一个同态。

同态可以帮助我们研究不同群之间的联系和相似性。

定义 2.8 如果对 $\forall a,b\in G$，若 $a\ne b$，有 $f(a)\ne f(b)$，就称映射 f 为单映射。如果同态 f 是单映射，则称 f 是单同态。

如果对 $\forall a' \in G'$，都存在 $a \in G$，使得 $f(a) = a'$，就称映射 f 为满映射。如果同态 f 是满映射，则称 f 是满同态。

如果 f 既是单同态又是满同态(即同态是一一映射)，则称 f 为同构映射。

定义 2.9 设 G, G' 是两个群，如果 f 是 G 到 G'的一个同构映射，则称两个群 G 与 G'同构，记为 $G \cong G'$。

同构的群具有相同的结构和性质，可以通过同构关系将一个群中的问题转化为另一个同构的群中的问题，因此同构在研究有限群的分类和性质时起到了重要的作用。

2.4. 正规子群与商群

正规子群是群中的一个重要概念。在介绍正规子群定义前，先介绍一个等价定理。

定理 2.9 [4]设 N 是 G 的子群，则下面条件等价。

1) 对 $\forall a \in G$，有 $aN = Na$；

2) 对 $\forall a \in G$，有 $aNa^{-1} = N$；

3) 对 $\forall a \in G$，有 $aNa^{-1} \subseteq N$。

定义 2.10 设 N 是 G 的一个子群，如果对都有

$$aN = Na,$$

则称 N 是 G 的正规子群(或不变子群)，记作 $N \lhd G$。

注：任意一个群 G 都有两个正规子群：$\{e\}$ 与 G，这两个正规子群称为 G 的平凡正规子群。

正规子群在群的运算和结构中起到了重要的作用，可以帮助我们研究群的性质和分类。

例 2.2 交换群的子群都是的正规子群。

证 设 $H \leq G$，因为 G 是交换群，所以 $\forall a \in G$，$n \in N$ 都有 $an = na$，从而 $aN = Na$，因此 $N \lhd G$。

商群是群中的另一个重要概念，它是通过对群中的一个正规子群进行等价关系的划分而得到的，它可以帮助我们研究群的结构和性质。

定义 2.11 设 G 是群，$N \lhd G$，令

$$G/N = \{aN \mid a \in G\},$$

规定：

$$(aN)(bN) = (ab)N, \quad \forall aN, bN \in G/N$$

则 G/N 是一个群，G/N 称为商群。

3. 有限群的分类

3.1. 单群与半单群

单群是一类特殊的有限群，它没有非平凡正规子群。单群是有限群中最基本的结构之一，其研究对于理解有限群的结构和性质具有重要的意义。根据研究结果，单群被分为了几个不同的系列，包括素数阶凯莱群、素数阶环状群、素数阶连续不交换群等。

单群的研究可以追溯到 19 世纪末和 20 世纪初，当时数学家开始思考群的结构和分类问题。然而，直到 20 世纪的后半叶，随着大量工作和众多数学家的努力，才得以形成单群的分类定理。

全部的有限单群是[4]：

1) 素数阶循环群；

2) $n \geq 5$ 的交错群 A_n；

3) Lie 型单群(共 16 族)；

4) 26 个散在单群。

单群的分类定理，也称为“喜马拉雅定理”，是群论研究的一个里程碑性发展。这个定理表明，每个有限的单群都可以归类为几个类别之一。具体来说，它提供了 18 个无限家族和 26 个“偶然”的单群。这个分类定理于 1980 年代完成，经过多年的努力和大量的数学证明，被公认为群论中的杰作。

这个分类定理的重要性在于，它为数学家提供了一个强大的工具，可以帮助他们简化和研究各种数学结构的问题，例如代数代数、数论、拓扑等等。此外，单群的研究也对物理学、计算机科学和密码学等领域有着广泛的应用。

值得一提的是，简单群的分类定理仍然是群论中最复杂和艰巨的证明之一，涉及了众多分支和概念的深入研究和精妙运用。因此，单群的发展和研究不仅为群论的发展作出了巨大贡献，而且也推动了数学整体的发展。

半单群(*Semisimple Group*)是一类特殊有限群，具有很强的性质和结构。它没有异于 1 的交换正规子群的有限群，即设 G 是有限群，若 G 是拟单群的中心积或 $G=1$，则称 G 为半单群。

3.2. 有限 Abel 群的分类

在介绍有限 Abel 群的相关概念之前，先介绍一些概念及性质。

定义 3.1 [5]设 p 是素数，称群 G 的元素 a 为 p-元素，如果 $|a|$ 是 p 的方幂；而称 a 为 p'-元素，如果 $(|a|,p)=1$。

特别的，单位元素 1 既是 p-元素，又是 p'-元素。

定义 3.2 称群 G 为 p 群，如果 G 的每个元素皆为 p-元素。

定义 3.3 称 p 群 S 为群 G 的 Sylow p-子群，如果 S 是 G 的极大 p-子群，即不存在 G 的 p-子群 $S_1 > S$。

定理 3.1 [5]设 A 是有限交换群，素数 $p\|A|$，并且 $p^n\|A|$，即 $p^n\|A|$，但 p^{n+1} 不整除 $|A|$，则 A 存在 Sylow p 子群 S_p，且 $|S_p|=p^n$，特别地，有限交换 p 群的阶是 p 的方幂。

定理 3.2 设 M 是有限 p 群 G 的极大子群，则

$$|G:H|=p，且 M \lhd G。$$

定理 3.3 设 G 是有限 p 群，$|G|=p^n>1$，则 G 的中心

$$Z(G)>1.$$

定理 3.4 设 G 是有限 p 群，N 是 G 的 p 阶正规子群，则

$$N \le Z(G).$$

定理 3.5 有限交换群 A 是它的 Sylow p 子群 S_p 的直积，

$$A=\bigtimes_p S_p,$$

这里 p 取遍所有使 $S_p \neq 1$ 的素数集合，而“$\times$”表示直积符号。

定理 3.6 [5]有限交换 p 群可以分解为循环子群的直积，即

$$A=\langle a_1\rangle\times\cdots\times\langle a_s\rangle,$$

并且直因子的个数 s 以及诸直因子的阶 $p^{e_1},p^{e_2},\cdots,p^{e_s}$，由 A 唯一确定，叫做 A 的型不变量。而元素 $\{a_1\},\cdots,\{a_s\}$ 叫做 A 的一组基底。

根据定理 3.5 和定理 3.6，可得任意一个有限 Abel 群都可以分解为若干个循环子群的直积。这个分解形式具有唯一性，可以帮助我们准确地描述和分类有限 Abel 群。

例 3.1 Klein (克莱因) 4 元数群记为 $K_4 = \langle a,b \mid a^2 = b^2 = 1, ab = ba \rangle \cong Z_2 \times Z_2$，即为 4 阶的初等交换 2 群。群 $G_1 = \langle a,b,c \mid a^2 = b^2 = c^2 = 1, ab = ba, ac = ca, bc = cb \rangle \cong Z_2 \times Z_2 \times Z_2$，即为 8 阶的初等交换 2 群。群 $G_2 = \langle a,b \mid a^2 = b^4 = 1, ab = ba \rangle \cong Z_2 \times Z_4$，即为 4 阶循环群和 2 阶循环群的直积。

3.3. 有限 p 群的结构定理

在有限群的分类中，有限 p 群是一类特殊的有限群，其中 p 是一个素数。对于有限 p 群的研究，有一个重要的结构定理，即 p 群的结构定理(也称为 Sylow 定理)。

定理 3.7 (Sylow 定理) 设 G 是有限群，p 是素数，

1) (Sylow 第一定理)设 $p^n \| |G|$，即 $p^n \| |G|$，但 p^{n+1} 不整除 $|G|$，则 G 中必存在 p^n 阶子群，叫做 G 的 Sylow p 子群。

2) (Sylow 第二定理) G 的任意两个 Sylow p 子群皆在 G 中共轭。

3) (Sylow 第二定理) G 中 Sylow p 子群的个数是 $|G|$ 的因子，并且 $n_p \equiv 1 (\mathrm{mod}\ p)$。

利用 p 群的结构定理，我们可以对有限 p 群进行分类和描述。例如，对于阶数为 p^n 的有限 p 群，可以通过分析不同的 p 子群和共轭关系，来推导出 p 群的具体结构。

定理 3.8 (Frattini 论断) [4]设 $N \lhd G$，$H \geq N_G(P)$，则 $H = N_G(P)$。

定理 3.9 设 $H \in Syl_p(G)$，$H \geq N_G(P)$，则 $H = N_G(P)$。

证明 因为 $H \lhd N = N_G(P)$，并且 P 也是 H 的 Sylow p-子群，由定理 3.8 可得，$N = H \cdot N_N(P) \leq H \cdot N_G(P) \leq H$，于是有 $H = N$。

值得注意的是，对于一般的有限群，分类和描述的问题非常复杂，但对于有限 p 群，由于其特殊的结构，能够得到相对简洁的结论。有限 p 群的结构定理给出了在有限群的分类中一个重要的例子，对于理解有限群的结构和性质有着重要的意义。

4. 有限群的应用领域

有限群在数学以外的领域中也有广泛的应用。下面列举了一些常见的应用领域。

4.1. 几何学

对称性与立体几何[6]：有限群是对称性的重要工具。例如，正方体具有 48 种不同的对称操作，这些操作可以表示为一个有限群的元素。几何学家通过研究这些对称操作，发现了很多正方体的性质。

曲面理论：有限群也被广泛应用于曲面理论研究中。通过考虑群作用在曲面上的不动点，可以获得许多曲面的性质。例如，通过在球面上考虑群作用，可以得到五种不同的对称性类型，这些类型可以被用于分类球面上的几何结构。

张量积分与变换[7]：有限群也被广泛应用于算法设计和数据分析中。例如，在图像处理中，图像可以被看作是函数在欧几里得空间中的采样。利用 *Fourier* 变换和群的理论，可以从这些采样数据中提取特征并进行分析。

状态空间搜索[8]：有限群也被应用于求解状态空间搜索问题。例如，在机器人路径规划中，搜索问题可以被看作是在有向图上找到一条路径，该路径经过一系列的状态。通过将状态编码为群的元素，可以通过群的理论解决这些问题，例如求解机器人在工厂中最短路径或最短时间内访问多个地点的问题。

4.2. 数论

有限群在代数数论中起着重要作用，例如，通过研究有限域上的剩余类群，我们可以解决一些数论问题，如费马大定理和二次互反律。有限群的性质也有助于研究模形式、椭圆曲线和整数解等数论问题。

4.3. 物理学

有限群在物理学中的应用非常广泛，特别是在对称性研究、粒子物理学和量子力学中都有应用：

对称性与粒子物理学[9]：有限群的对称性在粒子物理学中起着重要的作用。例如，内禀对称性群描述了基本粒子的内禀性质，如自旋和荷电。同时，空间对称性群描述了物理系统的对称性，例如晶体中的格点对称性。通过研究这些对称性群，我们可以解释和预测粒子的性质和相互作用。

能带理论与固体物理学[10]：能带理论描述了电子在晶体中运动的方式。通过考虑晶体的对称性群，可以推导出电子态的分类和能带结构，从而解释晶体的导电性和光学性质。

场论和粒子物理[11]：有限群在场论和粒子物理的对称性研究中也有重要应用。例如，规范对称性群描述了基本粒子相互作用的规范场理论。通过研究这些对称性群的表示论，我们可以解释和预测粒子的相互作用和动力学行为。

4.4. 密码学

有限群在密码学中作为一种重要的代数结构，被广泛应用于构造公钥密码学和对称密码学的安全算法，例如 NTRU 公钥密码体制，工作原理如下：

第一步：密钥生成

从 RNTRU 中随机选取两个小多项式 $f(x)$ 和 $g(x)$ (系数是稀疏的，即系数中 0 的比例很高)，且满足 $f(x)$ 在 RNTRU 中 $\bmod p$ 和 $\bmod q$ 均是可逆的，其逆元分别表示为 $F_p(x)$， $F_q(x)$，即

$$F_p(x)*f(x)\equiv 1(\bmod p),$$

$$F_q(x)*f(x)\equiv 1(\bmod q).$$

计算

$$h(x)\equiv pF_q(x)*g(x)(\bmod q).$$

其中以 $h(x)$ 为公钥， $f(x)$ 为私钥，接收者同时保存 $F_q(x)$。

第二步：加密

对明文消息 $m(x)\in R_{NTRU}/p$ ($m(x)$ 的系数取自 $0,1,\cdots,p-1$)进行加密，在 RNTRU 中随机选取一个小多项式 $r(x)$ (即范数 $|r(x)|=\left(\sum_{i=0}^{n-1}r_i^2\right)^{\frac{1}{2}}$ 很小)

$$r(x)=r_{n-1}x^{n-1}+\cdots+r_1x+r_0,$$

然后计算

$$c(x)\equiv h(x)*r(x)+m(x)(\bmod q).$$

第三步：解密

接收者利用私钥 $f(x)$ 进行解密，计算

1) $a(x)\equiv f(x)*c(x)(\bmod q)$， $a(x)$ 的系数选在区间 $\left(-\frac{q}{2},\frac{q}{2}\right]$ 内；

2) $F_p(x)*a(x)(\bmod\ p)$ 即可恢复明文 $m(x)$。

总结起来，有限群是群论中重要的一个分支，具有严谨的数学证明和推理，同时在数学、物理学、化学和密码学等领域具有广泛的应用价值，具体原因如下：

1) 数学领域：有限群是抽象代数学中的一个重要研究对象，它们可以帮助我们深入理解群论、表示

论、域论等数学分支的基本概念和结构。有限群的研究还涉及到许多重要的数学问题，如数论中的费马大定理和椭圆曲线密码系统中的离散对数问题。

2) 物理学领域：有限群是物理学中对称性的研究工具，特别是在粒子物理学和固体物理学中。基本粒子的相互作用和物理系统的性质都与其对称性有关。有限群的表示论可以帮助我们研究分子和晶体的对称性、粒子物理学中的标准模型以及凝聚态物理学中的拓扑相变等。

3) 化学领域：有限群对于描述和分类分子的对称性以及化学反应的对称特征非常重要。有限群在化学中的应用包括判断分子的光谱特性、分析化学反应的对称特征以及预测分子晶体的结构等。有限群论为化学家提供了一种系统研究和理解分子的工具。

4) 密码学领域：有限群的离散对数问题在密码学中具有重要的应用。基于有限群的密码系统，如椭圆曲线密码系统和 RSA 密码系统，是现代互联网通信和电子商务中广泛使用的加密算法。有限群的离散对数问题的复杂性保证了这些密码系统的安全性。

综上所述，有限群的研究在数学、物理学、化学和密码学等领域具有广泛的应用和重要的意义。

5. 有限群的未解问题

尽管有限群的分类与研究已经有了广泛而深入的探索，但仍有一些关键问题没有得到解决。下面列举了一些有限群的未解问题：

有限单群分类问题：简单群是有限群中最基本的结构，但目前仍未完全分类出有限单群(即没有正规子群的简单群)的形态。

巴拿赫－塔尔斯基问题：这是一道著名的分割问题，假设有一颗实心球，能否将其分割成有限个部分，再通过旋转和移动这些部分，重组成为两颗完全相同的实心球？该问题的解答构建在有限群论的基础上。

黑白染色问题：这是一个古老的问题，以棋盘为例，假设我们使用两种颜色(黑色和白色)对棋盘上的格子进行染色，如何用有限个染色步骤，能够实现将任意一个全部染成黑色或白色的棋盘达成目标。该问题的解答同样基于有限群论。

这些未解问题在有限群的研究中具有重要意义，对于理解群论的深层结构和应用也有一定的推动作用。除了以上未解决问题，有限群的研究具有广阔的未来研究方向和潜在前景，以下是其中一些可能的发展方向：

1) 群论和群表示论：有限群的基础研究将继续在数学领域推进。人们可能会进一步深入研究群的性质、结构和分类，探索群的新类型和新构造。

2) 应用于物理学和化学：有限群在物理学和化学中的应用将继续扩展。例如，对称性和群论在凝聚态物理学和拓扑物理学中的研究将不断推动新的发现。在化学中，有限群的应用可能在化学反应动力学、催化剂设计和材料科学等领域发挥更大的作用。

3) 密码学和信息安全性：在密码学领域，有限群的离散对数问题将继续成为关键的研究方向。随着量子计算的发展，研究者将致力于开发基于有限群的抗量子攻击的密码系统，并研究其他形式的密码学算法和协议，以应对不断演变的威胁。

4) 应用于计算机科学和人工智能：有限群也在计算机科学和人工智能领域发挥着重要作用。例如，在图像处理、模式识别和机器学习中，群表示论可以用于分析和处理结构化数据。未来的研究可能会更多地关注群的计算、群算法和群在复杂网络中的应用。

总之，有限群的研究具有广泛的前景和应用潜力。随着技术的不断进步和不同学科之间的交叉融合，有理由相信有限群的研究将进一步深化我们对自然界、数学领域和信息安全的理解。

综上所述，有限群研究的未来展望是多样化和广泛的，从理论推广到应用探索，与其他数学领域的联系也将进一步加强。

基金项目

本文系“塔里木大学校长基金硕士人才项目《商群的循环子群个数与群结构》《删失数据下半参分位数回归模型的变量选择》”(项目编号：TDZKSS202247；TDZKSS202231)的研究成果。

参考文献

[1] 李朝霞. 有限群与两类关联结构[D]: [硕士学位论文]. 杭州: 杭州电子科技大学, 2013.

[2] 胡俊美. 有限单群分类的历史研究[D]: [博士学位论文]. 石家庄: 河北师范大学, 2009.

[3] 哈金才, 李若雪, 哈瑞. 魔方的数学模型研究及其应用[J]. 创新创业理论研究与实践, 2018, 1(19): 83-86.

[4] 徐明曜. 有限群初步[M]. 北京: 科学出版社, 2014.

[5] 徐明曜, 曲海鹏. 有限 p 群[M]. 北京: 北京大学出版社, 2010.

[6] 方煜, 黄东枫, 孔祥涛. 二维投影在二面体群的分子对称性教学中的应用[J]. 安阳师范学院学报, 2020(5): 139-143.

[7] 朱婷婷. 广义二面体群上表示的张量积分解[D]: [硕士学位论文]. 扬州: 扬州大学, 2014.

[8] 李俊日. 基于改进状态空间模型与蚁群混合算法的机器人路径规划[D]: [硕士学位论文]. 长沙: 长沙理工大学, 2023.

[9] 叶笑蓉. 晶体学对称群的代数基础及其应用[D]: [硕士学位论文]. 湘潭: 湘潭大学, 2002.

[10] 高嘉成. 磁性拓扑能带理论与拓扑材料的搜索[D]: [博士学位论文]. 北京: 中国科学院大学(中国科学院物理研究所), 2023.

[11] 王树聪. 奇异摄动重整化群方法的一个动力学应用[D]: [硕士学位论文]. 长春: 吉林大学, 2019.