arXiv:2302.05909v1 [math.GR] 12 Feb 2023

对合交换二值群的分类

V. M. Buchstaber、A.A. Gaifullin 和 A.P. Veselov

摘要。本文给出了有限生成对合交换二值群的完整分类。构造了这类二值群的三个系列：主系列、幂零系列和特殊系列，并证明任意有限生成对合交换二值群都同构于属于这三个系列之一的二值群。对于豪斯多夫情形和局部紧情形下的拓扑对合交换二值群，本文还得到了若干分类结果。此外，本文还讨论了一维情形下代数对合二值群的分类。

目录

1. 引言 2 2. 单生成对合二值群 8 3. 2 阶元素的子群 10 4. 特殊与非特殊二值群 11 5. 二值群的商群 13 6. 直积分解 16 7. 非特殊二值群的性质 18 8. 含有阶不为 1、2 或 4 的元素的二值群 21 9. 由阶为 1、2 和 4 的元素组成的非特殊二值群 31 10. 布尔群上的拟余循环 35 11. 特殊二值群 39 12. 有限生成情形下的分类结束 44 13. 非有限生成二值群 46 14. 拓扑二值群 50 15. 局部紧二值群 60 16. 代数二值群 62 17. 结束语 64 参考文献 65

2020 数学主题分类。20N99（主要）；08A05、14L99、22A30（次要）。V.M. Buchstaber 和 A. A. Gaifullin 的工作在 Steklov 国际数学中心完成，并得到俄罗斯联邦科学和高等教育部资助（协议编号：075-15-2022-265）。

1. 引言

多值群是普通群的一种推广，其任意一对元素的乘积都是一个多重集，即一个无序的元素集合（其中可能有重复元素）。对于给定的多值群，两个元素相乘所得结果的基数可以不同；这类多值乘法理论历史悠久，可追溯至 19 世纪，参见 [29]。

本文研究 n值群。定义 n值群的关键在于确定多重集的基数 n ，该多重集是两个元素的直积。 n值群的概念源自 V.M. Buch-staber 和 S.P. Novikov [11] 在向量丛特征类理论中的构造。 n值群代数理论的基础由 V.M. Buchstaber 的工作奠定。V.M. Buchstaber、他的学生（A.N. Kholodov、P.V. Yagodovsky 等）及合作者（E. Rees、A.P. Veselov、M.I. Monastyrsky、V. Dragovic 等）发展了这一理论及其应用，参见综述 [7]和 [17]中的参考文献。

本文只讨论二值群。我们用 $\mathrm{Sym}^2(X)$ 表示集合 X的第二对称幂，即由 X中的元素构成的所有二元多重集的集合。我们将使用方括号列举多重集中的元素。

定义 1.1.二值群是一个集合 X ，带有二值乘法 $*\colon X \times X \to \mathrm{Sym}^2(X)$，单位元 $e \in X$，以及逆元 $x \mapsto x^{-1}$ ，满足以下性质。

- 结合律：对于任意三个元素 x、 y、 $z \in X$，四个元素的多重集相等

$$x * (y * z) = (x * y) * z.$$

- 强单位元：对于任意元素 x ，等式成立

$$e * x = x * e = [x, x].$$

- 逆元的存在性与唯一性：对于任意元素 $x \in X$，多重集 $x*x^{-1}$ 和 $x^{-1}*x$ 各自都包含单位元 e；此外，若元素 y 使得多重集 $x*y$ 和 $y*x$ 中有一个包含单位元，则 $y = x^{-1}$。

若二值群满足交换律，则称其为交换的

$$x * y = y * x$$

对所有 $x, y \in X$。

注 1.2。二值群的原始定义（见 [7]）并未要求逆元的唯一性。这一附加条件见于 [15] 和 [17]。对于本文而言，这一条件后来证明十分重要。

n值群最重要的来源是陪集多值群的构造，见 [7, 第 6]节。陪集 n值群由一对对象构造而成，其中包括一个单值群 G 及其自同构群中的一个有限子群 H 。与此同时，n值群的理论并不局限于陪集群。首先，不同的对 (G, H) 可能导出同构的 n值群；其次，存在一类丰富的非陪集 n值群，见 [7], [15]。我们将需要以下陪集二值群的构造。

构造 1.3（陪集二值群）。设 G 是一个普通（单值）群， $\iota\colon G \to G$ 是它的对合自同构（即满足 $\iota^2 = \mathrm{id}$ 的自同构）。那么

商集 $X = G/\iota$ 被赋予二值群结构，使得

$$\pi(g) * \pi(h) = \big[\pi(gh), \pi(g\iota(h))\big]$$

对所有 $g, h \in G$，其中 $\pi\colon\ G \to X$ 是自然投影。该二值群的单位元是群 G的单位元的像，逆元由公式 $\pi(g)^{-1} = \pi(g^{-1})$定义。对于阿贝尔群 G，对合的一个重要例子是取逆元（对跖对合）： $\iota_{\mathbf{a}}(g) = g^{-1}$.

n值群理论的一个重要特点是分类和计数问题具有很高的复杂性。这是因为，在含有 k 个元素的集合上， n值群的同构类数量会随着 k 和 n的增长而极其迅速地增加。即使我们只考虑交换的n值群，同样的现象也会出现。据我们所知，曾有人尝试使用高性能计算技术，在给定 n 和 k 的情况下，对 n值群的同构类进行计数，但由于问题的计算复杂度，这些尝试并未取得显著成果。

因此，寻找这类 n 值群中可行分类问题的类别，自然具有重要意义。由 V.M. Buchstaber 和 A.P. Veselov 在 [17] 中为研究 Conway地形图而引入的对合二值群，是这类群中的一个重要类别。

定义 1.4. 若二值群 X 的元素 x 满足弱对合的条件$x^{-1} = x$，或者等价地，多重集 $x * x$ 包含单位元 e，则称其为弱对合。若元素 $x \in X$ 满足 $x * x = [e, e]$，则称其为强对合。若二值群 X 中的元素全是弱对合，即对所有 $x \in X$ 都有 $x^{-1} = x$，则称该群为对合的。

备注 1.5. 请注意，在 [15] 中，“对合 n 值群”的概念含义不同，具体指取逆元运算的对合性$x \mapsto x^{-1}$. 。显然，按 [15] 中的含义定义的对合群，包含文献 [17] 中所定义的对合群。文献 [15] 的主要结果证明，其中引入的对合 n 值群的群代数与所谓的组合代数相同，参见 [1]。本文中，“对合二值群”一词采用 [17] 中的含义。

本文的主要目标是对合交换二值群的分类。 [17]提出了这类二值群的分类问题。该文猜想，每个对合交换二值群都同构于形如 $A/\iota_{\mathbf{a}}$ 的陪集二值群，其中 A 是一个阿贝尔群，而 $\iota_{\mathbf{a}}(g) = g^{-1}$ 是该群上的对跖对合。我们将证明，即使对于有限二值群，这个猜想也不成立。

我们考虑以下各类对合交换二值群的分类问题:

- 有限生成二值群（定理 1.10，其证明占据第 2–12 节），
- 无拓扑的任意二值群（第 13 节），
- 豪斯多夫拓扑二值群（第 14 节），
- 局部紧豪斯多夫二值群（第 15 节），
- 代数二值群（第 16 节）。

对于有限生成群的情形（定理 1.10），以及没有小子群的紧拓扑群的情形（定理 15.8），我们将得到完整的分类。

本书的大部分内容将致力于有限生成情形。之后，我们将讨论如何把我们的方法推广到其他类别的二值群，以及在此过程中得到了哪些结果并提出了哪些新问题。

现在，我们来表述有限生成对合交换二值群的分类定理。我们将证明，除了由形如 $A/\iota_{\mathbf{a}}$ 的陪集二值群构成的 **主系列** 之外，有限生成对合交换二值群还存在另外两个系列；我们称之为 **幺幂级数** 和 **特殊系列**。有趣的是，幺幂级数中的二值群也可通过对阿贝尔群采用陪集构造得到，但所依据的是非对跖对合。特殊系列中的二值群并非陪集二值群，见下文命题 **4.4**。特别地，我们的结果给出了非陪集二值群的新构造。

现在，我们介绍这些对合交换二值群系列的构造。

在本文中，我们用 C_n 表示阶为 n 的循环群；其中包括 C_∞，它是一个无限循环群。对所有群（包括阿贝尔群）使用乘法记号会更方便。

1. 主系列。设 A 是一个（单值）阿贝尔群。考虑由公式 $\iota_{\mathbf{a}}(a) = a^{-1}$定义的对跖对合 $\iota_{\mathbf{a}}\colon\ A \to A$。那么陪集二值群

$$X_A^{\mathbf{a}} = A/\iota_{\mathbf{a}}$$

是一个幂等交换群。

如果 A 是有限生成阿贝尔群，那么众所周知，它可以唯一地（在同构意义下）表示为直积 $C_{d_1} \times C_{d_2} \times \cdots \times C_{d_k}$，其中 $2 \le d_i \le \infty$整除 d_{i+1}，对所有 $i = 1$，.....，$k-1$ 均成立（例如参见 [**42**]）。引入记号

$$X^{\mathbf{a}}_{d_1,\dots,d_k} = X^{\mathbf{a}}_{C_{d_1}\times\cdots\times C_{d_k}}.$$

可以直接验证，如果群 A 是有限群，那么二值群 $X_A^{\mathbf{a}}$ 中的元素个数等于

$$\frac{1}{2}(d_1 d_2 \cdots d_k + 2^r),$$

其中 r 是数字 d_1，.....，d_k中偶数的个数。

注 **1.6.** 主系列对合二值群中最简单但重要的情形是群 $X^{\mathbf{a}}_{m\times 2} = C_2^m/\iota_{\mathbf{a}}$（其中 $m\times 2$表示由 m 个 2 组成的序列 2，.....，2）。二值群 $X^{\mathbf{a}}_{m\times 2}$ 是群 C_2^m的所谓双重群。这意味着， $X^{\mathbf{a}}_{m\times 2}$ 作为集合与 C_2^m相同，而 $X^{\mathbf{a}}_{m\times 2}$ 中的运算是通过将 C_2^m中的运算加倍得到的，即 $x * y = [xy, xy]$。注意，任意群 G都可以定义双重群。所得结果总是二值群，并且在 [**15**]的意义下是对合的。只有当 G 是二元域 $\mathbb{F}_2$上的向量空间时，它才是交换的，并且在 [**17**] 的意义下是对合的。

注 **1.7.** 自然地，我们可以将二值群 $X^{\mathbf{a}}_{\infty,\dots,\infty}$ 视为**自由**反演交换二值群。文献 [**17**]，对二值群 $X^{\mathbf{a}}_{\infty} = C_\infty/\iota_{\mathbf{a}}$ 和 $X^{\mathbf{a}}_{\infty,\infty} = (C_\infty \times C_\infty)/\iota_{\mathbf{a}}$ 进行了详细研究，并分别称它们为*Buchstaber-Novikov* 二值群和*Conway* 二值群，分别记作 $\mathbb{X}_1$ 和 $\mathbb{X}_2$。

2. 幺幂级数。我们需要引入布尔群的概念。如果一个群的每个非单位元的阶都是 2，就称该群为布尔群，参见 [**21**, 第 1] 章。容易证明，任何这样的群都是阿贝尔群。因此，布尔群是二元域 $\mathbb{F}_2$ 上的向量空间，其运算采用乘法记法。对于布尔群 V，我们将 $\dim V$ 记作它作为向量空间的维数。

设 V为布尔群。考虑由公式确定的 幺幂对合 $\iota_{\mathbf{u}}$: $V \times V \to V \times V$,

$$\iota_{\mathbf{u}}(a, b) = (a, ab). \tag{1}$$

则陪集二值群

$$X_V^{\mathbf{u}} = (V \times V)/\iota_{\mathbf{u}}$$

是一个对合交换二值群。

注 1.8。利用由公式 $(a, b) \mapsto (ab, b)$ 定义的群 $V \times V$ 的自同构，对合 $\iota_{\mathbf{u}}$ 被转换为置换对合

$$\iota_{\mathbf{t}} : (a, b) \mapsto (b, a),$$

但就我们的目的而言，考虑幺幂形式（1）中的对合更为方便。这两个对合的等价性由众所周知的同构解释。

$$GL(2, \mathbb{F}_2) \cong S_3$$

该同构将其对应于一个三元素集合的置换群，其中所有二阶元素都彼此共轭。

可以直接验证，如果 $\dim V = n < \infty$，也就是说， $V \cong C_2^n$，那么该二值群

$$X_n^{\mathbf{u}} = X_{C_2^n}^{\mathbf{u}}$$

由 $2^{2n-1} + 2^{n-1}$ 个元素组成。

如果 $n = 1$，那么 $X_1^{\mathbf{u}} = X_{C_2}^{\mathbf{u}}$ 是一个有三个元素的群 $\{e, v, x\}$ ，其乘法表为$v * v = [e, e]$、$v * x = [x, x]$、 $x * x = [e, v]$。容易看出 $X_{C_2}^{\mathbf{u}} \cong X_{C_4}^{\mathbf{a}}$。

当 $n = 2$ 时，存在一个不太明显的 10 元二值群同构 $X_2^{\mathbf{u}} \cong X_{4,\,4}^{\mathbf{a}}$，也就是说，$X_{C_2 \times C_2}^{\mathbf{u}} \cong X_{C_4 \times C_4}^{\mathbf{a}}$ （见例 1.11 和第 9 节）。

因此，当 $\dim V \leq 2$ 时，二值群 $X_V^{\mathbf{u}}$ 属于主系列例子的范围。不过，正如我们将在下文看到的，对于 $\dim V \geq 3$，二值群 $X_V^{\mathbf{u}}$ 与主系列中的任何二值群都不同构。

注 1.9. 容易看出，陪集二值群 G/ι 是对合的，当且仅当对任意元素 $g \in G$ ，$g^{-1} = g$ 或 $g^{-1} = \iota(g)$这两个等式之一成立。第一种情况出现在幺幂级数的二值群中，第二种情况出现在主系列的二值群中。

3. 特殊系列。V. M. Buchstaber 和 E. Rees 提出了一种构造二值群的方法：在通常的（单值）群中添加一个额外元素，参见论文 [**13**] 第3节中的例（6）。对合交换二值群的特殊系列，是将这一构造应用于布尔群而得到的。

设 V 是一个以 e 为单位元的布尔群。我们在集合 V 中再添加一个元素，记为 s，并在

集合 $Y_V = V \cup \{s\}$ 上定义一个交换的二值运算，其公式为

$$\begin{aligned} x * y &= [xy, xy], && x, y \in V,\ x \neq y, \\ x * x &= [e, s], && x \in V,\ x \neq e, \\ s * x &= [x, x], && x \in V,\ x \neq e, \\ e * x &= [x, x], && x \in V \cup \{s\}, \\ s * s &= [e, e]. \end{aligned}$$

可以直接验证，所引入的运算定义良好、满足结合律，并使 Y_V 成为对合交换二值群。

若 $\dim V = n < \infty$，即 $V \cong C_2^n$，则该二值群

$$Y_n = Y_{C_2^n}$$

由 $2^n + 1$ 个元素组成。

对于 $n = 1$，二值群 Y_1 由三个元素 e、s 和 x 组成，其乘法表为 $s * s = [e, e]$、$s * x = [x, x]$、$x * x = [e, s]$。因此，$Y_1 \cong X^{\mathbf{a}}_{C_4} \cong X^{\mathbf{u}}_{C_2}$。不过，正如我们将在下文看到的（命题4.3），当 $\dim V \geq 2$ 时，二值群 Y_V 并非陪集，尤其不同构于主系列和幺幂级数中的任何二值群。（根据 [13] 中的命题3.1，也可以推得，当 $\dim V \geq 2$ 时，Y_V 并非陪集。）

再给出对二值群 Y_V 的一种解释。集合 $V \setminus \{e\}$ 可以自然地视为向量空间 V 的射影化 $\mathbb{P}(V)$。于是，Y_V 就是射影空间 $\mathbb{P}(V)$ 加上两个元素 e 和 s。乘法规则如下：

(1) e 是单位元，即对所有 $x \in Y_V$，$e * x = [x, x]$；(2) 若 x 和 y 是射影空间 $\mathbb{P}(V)$ 中两个不同的点，且 z 是经过 x 和 y 的直线上的第三个点，则 $x * y = [z, z]$；(3) 若 $x \in \mathbb{P}(V)$，则 $x * x = [e, s]$ 和 $s * x = [x, x]$；(4) $s * s = [e, e]$。

4. 与布尔群的直积。若 X 是一个对合交换二值群，而 W 是一个布尔群，则直积 $X \times W$ 也具有对合交换二值群的结构，其乘法由公式 $(x_1, w_1) * (x_2, w_2) = (x_1 * x_2, w_1 w_2)$ 定义。更确切地说，若 $x_1 * x_2 = [z_1, z_2]$，则

$$(x_1, w_1) * (x_2, w_2) = \big[(z_1, w_1 w_2), (z_2, w_1 w_2)\big].$$

如果我们取主系列的对合交换群作为 X，那么这种构造不会产生新的例子，因为对于任意阿贝尔群 A 和任意布尔群 W，都存在一个典范同构

$$X^{\mathbf{a}}_A \times W \cong X^{\mathbf{a}}_{A \times W}. \tag{2}$$

然而，如果我们取幂零系列和特殊系列的二值群作为 X，那么就会得到新的对合二值群例子。

现在我们可以陈述有限生成幂等交换二值群的分类定理。

定理 1.10。 每个有限生成对合交换二值群都同构于以下二值群之一：

(1) $X^{\mathbf{a}}_{d_1, \ldots, d_k}$, *where* $2 \leq d_i \leq \infty$ *and* $d_1 | d_2 | \cdots | d_k$;

(2) $X_n^{\mathbf{u}} \times C_2^m$，其中 $n \geq 1, m \geq 0$;

(3) $Y_n \times C_2^m$，其中 $n \geq 1, m \geq 0$。

对每个 $m \geq 0$，都存在同构

$$X_{m\times 2,4}^{\mathbf{a}} \cong X_1^{\mathbf{u}} \times C_2^m \cong Y_1 \times C_2^m, \tag{3}$$

$$X_{m\times 2,4,4}^{\mathbf{a}} \cong X_2^{\mathbf{u}} \times C_2^m, \tag{4}$$

其中 $m\times 2$ 表示由$2,\ldots,2$个 *2* 构成的序列。所示同构穷尽了所列二值群之间的所有同构。

例 1.11. 现在考虑 10 元二值群 $X_{4,4}^{\mathbf{a}} = C_4^2/\iota_{\mathbf{a}}$和 $X_2^{\mathbf{u}} = (C_2^2 \times C_2^2)/\iota_{\mathbf{u}}$，并给出它们之间的一个显式同构。用 a_1 和 a_2 表示群 C_4^2 中各因子的生成元，用 b_1 和 b_2 表示群 C_2^2中各因子的生成元。按公式定义映射 $f\colon C_4^2 \to C_2^2 \times C_2^2$

$$f(a_1^k a_2^l) = \left(b_1^k b_2^l, b_1^{[k/2]} b_2^{[l/2]}\right), \qquad 0 \leq k \leq 3,\ 0 \leq l \leq 3,$$

其中 $[r]$ 表示数 r的整数部分。映射 f 不是同态。不过，可以直接验证，对于任意元素 a、$c \in C_4^2$，元素 $f(ac)$与以下 4 个元素中的一个相同：$f(a)f(c)$、$f(a)\iota_{\mathbf{u}}\big(f(c)\big)$、$\iota_{\mathbf{u}}\big(f(a)\big)f(c)$以及 $\iota_{\mathbf{u}}\big(f(a)\big)\iota_{\mathbf{u}}\big(f(c)\big)$；此外，多重集相同

$$\begin{aligned}\big[f(ac), f(ac^{-1}), f(a^{-1}c), f(a^{-1}c^{-1})\big] = \\ \big[f(a)f(c), f(a)\iota_{\mathbf{u}}\big(f(c)\big), \iota_{\mathbf{u}}\big(f(a)\big)f(c), \iota_{\mathbf{u}}\big(f(a)\big)\iota_{\mathbf{u}}\big(f(c)\big)\big].\end{aligned}$$

因此，映射 f 诱导出一个良定义的同构 $X_{4,\,4}^{\mathbf{a}} \cong X_2^{\mathbf{u}}$。结合同构 (2)，即可得到同构 (4)。

例1.12. 考虑 5 元群 $Y_2 = Y_{C_2^2}$，它是特殊系列中第一个不包含于主系列的群。设 x、y 和 z 是 C_2^2中的三个非平凡元素。那么，二值群 Y_2 的乘法表形式如下:

$$\begin{aligned} &x*x = y*y = z*z = [e,s], \quad s*s = [e,e],\\ &x*y = [z,z], \quad y*z = [x,x], \quad z*x = [y,y],\\ &s*x = [x,x], \quad s*y = [y,y], \quad s*z = [z,z]. \end{aligned}$$

这个二值群与四元数构成的非阿贝尔 8 元群有关

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H},$$

其中 $\mathbb{H}$ 是四元数代数。在群 Q_8 上有共轭反自同构 σ, $\sigma(gh) = \sigma(h)\sigma(g)$，它固定元素 1 和 -1，并置换$i \leftrightarrow -i$、$j \leftrightarrow -j$、$k \leftrightarrow -k$。通过对合自同构构造陪集二值群，通常无法推广到反自同构的情形。然而，群 Q_8 的反自同构 σ 具有如下特殊性质：对于任意两个元素 g、$h \in Q_8$，四元多重集 $[gh, g\sigma(h)\ \sigma(g)h$、$\sigma(g)\sigma(h)]$ 是某个二元多重集的加倍。由此性质很容易推出，5元商集 Q_8/σ 具有定义良好的二值群结构。由于四元数单位的乘法在相差一个符号的意义下是交换的，二值群 Q_8/σ 是交换的。容易看出，它与二值群 Y_2 同构，同构为 $1 \mapsto e$、$-1 \mapsto s$、$\pm i \mapsto x$、$\pm j \mapsto y$ 和 $\pm k \mapsto z$。

例 1.13. 与前一个例子类似，9元二值群 Y_3 与16元集合之间存在联系

$$O_{16} = \{\pm 1, \pm e_0, \pm e_1, \dots, \pm e_6\} \subset \mathbb{O},$$

其中 $\mathbb{O}$ 是八元数代数，$1, e_0, \dots, e_6$ 是其标准基。由于八元数乘法不满足结合律，集合 O_{16} 甚至不是一个群，而只是所谓的*Moufang*拟群，见 [18, §7.1]。不过，共轭定义了这一代数结构的一个对合反自同构。可以直接验证，对于任意两个元素 g, $h \in O_{16}$，四元多重集 $[gh, g\sigma(h)\ \sigma(g)h, \sigma(g)\sigma(h)]$ 都是某个二元多重集的加倍。这再次表明，在9元商集O_{16}/σ 上存在定义良好的二值乘法。尽管O_{16} 中的乘法既不满足结合律，也不满足交换律，但其结合性和交换性在相差一个符号的意义下成立。利用这一点，可以直接验证，由 O_{16}/σ 得到的二值乘法满足结合律和交换律，并在该集合上定义了交换二值群的结构。同样可以直接验证，这个二值群与二值群 Y_3同构。

本文结构如下。第 2 节对单生成对合二值群进行分类。特别地，我们证明所有这类二值群都是交换的。第 3–12 节致力于有限生成情形下对合交换二值群的分类。第 13–15 节给出了拓扑情形中的若干分类结果。第 16 节讨论代数二值群的情形。最后，第 17 节讨论一些开放问题。

2. 单生成对合二值群

单生成通常群的分类问题非常简单：其答案是无限循环群以及所有可能的有限循环群。对于 n 值群，单生成群（甚至是交换二值群）的分类问题却很难，目前距离完整解决仍相去甚远。

有限群的不可约表示集合上的多值乘法，为单生成交换 n 值群提供了丰富的来源，参见 [7,第 10, 11] 节。更确切地说，有如下定理：如果有限群 G 具有忠实不可约表示 ρ，那么其不可约表示集合上的多值群是单生成的。证明基于伯恩赛德定理（见 [19]），该定理指出，在这种情形下，群 G 的任意不可约表示都包含在表示 ρ 的某个张量幂的分解中。

还要注意，单生成多值群的问题与离散时间多值动力系统的可积性问题密切相关，参见 [40], [16]。然而，对于本文所研究的对合二值群，即使没有交换性假设，单生成群分类问题也可以得到完全解决。结果表明，这一分类与通常群的情形一样简单（自由单生成二值群的情形曾在研究 Conway地形图时加以探讨，见 [17] ）。

定理 2.1. 任意单生成对合二值群都同构于形如 $X_C^{\mathbf{a}} = C/\iota_{\mathbf{a}}$ 的陪集群，其中 C 是一个循环群，且 $\iota_{\mathbf{a}}\colon\ C \to C$ 是对跖对合。特别地，每个这样的二值群都是交换的。

证明将分为几个引理，这些引理本身也对我们有所帮助。

引理 2.2. 设 X 是一个对合二值群，且元素 $x, y, z \in X$ 满足 z 属于多重集 $x * y$。那么 x 属于多重集 $y * z$。

证明。设 $x * y = [z, z']$。那么，由于二值群 X 的对合性，多重集 $(x*y)*z = [z*z, z'*z]$ 包含单位元 e。另一方面，由于结合律，这个多重集可以写成 $x*(y*z)$。由它包含 e 这一事实以及二值群 X 的对合性可知， $y * z$ 包含 x。□

引理 2.3。 设 X 是一个对合二值群。那么，对于任意元素 $x \in X$，存在唯一的序列 x^0， x^1， x^2，..... ，其元素属于二值群 X ，且满足 $x^0 = e$、 $x^1 = x$ ，并且

$$x * x^k = x^k * x = [x^{k-1}, x^{k+1}] \tag{5}$$

对于所有 $k \geq 1$。

证明。我们来证明，公式 (5) 与初始条件 $x^0 = e$、$x^1 = x$ 一起，定义了一个良定义的递推规则，用于唯一地构造序列 $\{x^k\}_{k\geq 0}$。假设 x^0、x^1、.....、x^n 中的元素（其中 $n \geq 1$）已定义，并且等式 (5) 对 $1 \leq k \leq n-1$ 成立；下面证明，可以唯一地定义 x^{n+1} ，使等式 (5) 对 $k = n$ 成立。

由 $1 \leq k \leq n-1$ 下的等式 (5) 可知，特别是，元素 x 与 x^0、x^1、.....、x^{n-1} 中的每个元素都交换。下面证明 x 与 x^n 交换。当 $n = 1$ 时这显然成立，因此假设 $n \geq 2$。我们有

$$x * x * x^{n-1} = x * [x^{n-2}, x^n] = [x * x^{n-2}, x * x^n],$$
$$x^{n-1} * x * x = [x^{n-2}, x^n] * x = [x^{n-2} * x, x^n * x].$$

由于 x 与 x^{n-1} 交换，因此 $x * x * x^{n-1} = x^{n-1} * x * x$。此外， $x * x^{n-2} = x^{n-2} * x$。因此 $x * x^n = x^n * x$。

现在，对三元组 (x^{n-1}, x, x^n) 应用引理 2.2，可得元素 x^{n-1} 属于多重集 $x * x^n = x^n * x$。因此，我们可以且应当取该多重集的第二个元素作为 x^{n+1}。□

对于 $k < 0$，根据定义，我们设 $x^k = x^{-k}$。那么，对于所有整数 k，等式 (5) 都成立。自然地，我们将元素 x^k 称为元素 x的第 次幂。

引理 2.4. 设 X 是一个对合二值群， x 是它的任意元素。那么

$$x^k * x^l = [x^{k+l}, x^{k-l}], \tag{6}$$
$$(x^k)^l = x^{kl} \tag{7}$$

对于所有整数 k 和 l,

证明。由 $x^n = x^{-n}$，只需证明非负 k 和 l时等式 (6) 成立。我们先证明 $0 \leq k \leq l$ 时的情形； $k \geq l$ 的情形完全类似。由于 $x^0 = e$，(6) 对 $k = 0$ 成立。对于 $k = 1$ ，该等式变为公式 (5)，而公式 (5) 曾用于构造序列 $\{x^k\}$；因此它也成立。我们通过对 k 作归纳法，证明 $2 \leq k \leq l$ 时等式 (6) 成立。根据归纳假设

$$x^{k-1} * x^l = [x^{k+l-1}, x^{k-l-1}].$$

将该等式两边从左侧乘以 x ，并应用公式 (5)，得到

$$x * x^{k-1} * x^l = [x^{k+l}, x^{k+l-2}, x^{k-l}, x^{k-l-2}].$$

关于 另一方面，再次利用归纳假设和公式 (5)，我们得到

$$x * x^{k-1} * x^l = [x^{k-2} * x^l, x^k * x^l] = [x^{k+l-2}, x^{k-l-2}, x^k * x^l],$$

由此可得 $x^k * x^l = [x^{k+l}, x^{k-l}]$。

特别由公式 (6) 可得，元素序列 x^{kl}，其中$l = 0$，1，2，.....，满足递推关系

$$x^k * x^{kl} = [x^{k(l-1)}, x^{k(l+1)}]$$

因此 $(x^k)^l = x^{kl}$。 □

推论 2.5。 每个单生成的对合二值群都是交换的。

引理 2.6。 设 X 是一个对合二值群， x 是其任意元素。那么，由所有满足 $x^k = e$ 的整数 k 构成的子集 $K \subseteq \mathbb{Z}$ 是一个子群。如果$k \in K$，那么对于所有 $l \in \mathbb{Z}$，都有 $x^{\pm l+k} = x^l$ 。反之，如果 $x^l = x^m$，那么要么 $l - m \in K$ ，要么$l + m \in K$。

证明。显然，对于所有 $k \in K$， $0 \in K$ 和 $-k \in K$ 都成立。由于 $e * x^l = [x^l, x^l]$，由公式 (6) 立即可得，对于所有 $k \in K$ 和 $l \in \mathbb{Z}$，都有 $x^{\pm l+k} = x^l$ 。特别地，如果 l 也属于 K，我们就得到 $x^{k+l} = e$，因此 $k + l \in K$。于是 $K \subseteq \mathbb{Z}$ 是一个子群。

现在假设 $x^l = x^m$。根据对合性，多重集 $x^l * x^m = [x^{l+m}, x^{l-m}]$ 包含 e。因此，要么 $x^{l+m} = e$ ，要么 $x^{l-m} = e$，所以要么 $l + m \in K$ ，要么 $l - m \in K$。□

使得 $x^k = e$ 成立的最小正整数 k 称为元素 x 的阶，记作 $\mathrm{ord}\, x$。如果对所有正整数 k， $x^k \neq e$ 都成立，那么我们称元素 x 的阶等于无穷大。显然，$\mathrm{ord}\, x = 1$ 当且仅当 $x = e$。下文将特别关注阶为 2 和 3 的元素。由定义和引理 2.6 可 쉽게得出，非单位元 x 的阶为 2 当且仅当$x * x = [e, e]$，阶为 3 当且仅当 $x * x = [e, x]$。特别地，阶为 1 和 2 的元素恰好是强对合，参见定义 1.4。

以下推论由引理 2.6 得出。

推论 2.7。 如果 x 是一个对合二值群中的元素，那么 $x^l = x^m$ 当且仅当数 $l-m$ 和 $l+m$ 中至少有一个可被 阶 x 整除。特别地，$x^l = e$ 当且仅当 l 可被 阶 x 整除。

定理 2.1 的证明。设 X 是一个由单个生成元生成的对合二值群，其生成元为 x。根据引理 2.4，对于任意 k、$l \geq 0$，等式 (6) 成立。由所有幂 x^k 构成的集合 X 的一个子集在乘法下封闭，并包含 $x.$。由于二值群 X 由元素 x 生成，我们得到幂 x^k、 $k \in \mathbb{Z}$ 穷尽了 X 的所有元素。

根据引理 2.6，由满足 $x^k = e$ 的所有整数 k 构成的子集 $K \subseteq \mathbb{Z}$ 是一个子群，并且对于所有 $k \in K$ 和 $l \in \mathbb{Z}$， $x^{\pm l+k} = x^l$ 。因此，对应关系$k \mapsto x^k$ 给出了一个定义良好的满射 φ: $(\mathbb{Z}/K)/\iota \to X$。由公式 (6) 可知，映射 φ 是二值群的同态；由引理 2.6 的最后一个陈述可知，映射 φ 是单射。因此， φ 是二值群的同构。□

3. 2 阶元素的子群

设 X 为一个对合交换二值群。我们在 X 上引入部分定义的单值乘法运算 $\cdot$，使得

(1) $x \cdot y = z$ 若 $x * y = [z, z]$(2) 当多重集 $x \cdot y$ 由两个不同元素组成时，表达式 $x * y$ 未定义。

由定义立即可得， $x \cdot y = y \cdot x$ 和 $x \cdot e = x$。此外，当 $\operatorname{ord} x \leq 2$时， $x \cdot x = e$；当 $\operatorname{ord} x > 2$时， $x \cdot x$ 未定义。

引理 3.1。 如果两个元素 x和 y 中至少有一个的阶为2，则多重集$x * y$ 由两个相同的元素组成，因此表达式 $x \cdot y$ 有定义。

证明。令 $\operatorname{ord} x = 2$ 和 $z \in x * y$。由引理 2.2，我们有 $y \in x * z$，也就是说，对于某个 y'，有 $x * z = [y, y']$。然后

$$(x * x) * z = [e, e] * z = [z, z, z, z],$$
$$x * (x * z) = x * [y, y'] = [x * y, x * y'],$$

因此 $x * y = [z, z]$。 □

命题 3.2。 设 X 是一个对合交换二值群， $V \subseteq X$ 是其由单位元 e 和所有阶为2的元素组成的子集。那么

(a) 集合 V 关于运算 $\cdot$构成一个布尔群；(b)运算 $\cdot$ 定义了群 V 在集合 X 上的作用；此外，若$x * y = [z_1, z_2]$，则

$$(v \cdot x) * y = [v \cdot z_1, v \cdot z_2] \tag{8}$$

对所有 $v \in V$；(c) 若 $v \in V \setminus \{e\}$ 和 $x \in X$，则 $v \cdot x = x$ 当且仅当 $x^2 = v$；特别地，等式 $v \cdot x = x$ 只有在 $\operatorname{ord} x = 4$ 时才能成立。

证明。陈述 (a) 和 (b) 由引理 3.1 以及二值群 X 的结合律、交换律和对合性立即得出。

我们来证明陈述 (c)。若 $x^2 = v$，则 $\operatorname{ord} x = 4$，于是 $x^3 = x$，因此 $v * x = x^2 * x = [x^3, x] = [x, x]$，故 $v \cdot x = x$。

反过来，假设 $v \cdot x = x$，即 $v * x = [x, x]$。由引理 2.2 可知，多重集 $x * x$ 包含元素 v。然而，群 X 是对合的，这一事实意味着该多重集也包含元素 e。由于 $v \neq e$，我们得到 $x * x = [e, v]$，即 $x^2 = v$。 □

二值群 X 关于群 V 在其上的作用 $\cdot$ 分解为若干轨道。我们将这些轨道称为 V-轨道；包含元素 x 的 V-轨道记作 Vx。

注 3.3. 下文中，我们通常用 xy 代替 $x \cdot y$，这应该不会造成混淆。

4. 特殊与非特殊二值群

定义 4.1. 由对合交换二值群中的元素构成的一对 (x, y)，若 $\operatorname{ord} x > 2$、$\operatorname{ord} y > 2$，但多重集 $x * y$ 由两个相同的元素组成，则称为特殊对。若一个对合交换二值群至少包含一对特殊元素，则称其为特殊群；否则称为非特殊群。

Rem注 4.2. 在 [17]，中，非特殊二值群称为强二值群 .

因此，若一个二值群是非特殊的，则当且仅当元素 x 和 y 中有一个的阶为 ≤ 2 时，值 $x \cdot y$ 才有定义。

命题 4.3. 所有形如 $X_A^{\mathfrak{a}}$ 和 $X_V^{\mathfrak{u}} \times W$ 的二值群都是非特殊的。当维数 $V \geq 2$时，二值群 $Y_V \times W$ 是特殊的。

证明。我们来证明二值群 $X_A^{\mathbf{a}}$ 的非特殊性。设 $\pi\colon A \to X_A^{\mathbf{a}}$ 是关于对跖对合的商映射。考虑元素 x、$y \in X_A^{\mathbf{a}}$。若 a、$b \in A$ 是满足 $x = \pi(a)$ 且 $y = \pi(b)$ 的元素，则 $x * y = [\pi(ab)\ \pi(ab^{-1})]$。假设元素 x 和 y 的阶大于 2。那么元素 a 和 b 的阶也大于 2。因此，元素 ab 和 ab^{-1} 既不相等，也互不为逆元。因此，多重集 $x * y$ 由两个不同的元素组成。由此，二值群 $X_A^{\mathbf{a}}$ 是非特殊的。

我们来证明二值群 $X_V^{\mathbf{u}} = (V \times V)/\iota_{\mathbf{u}}$ 的非特殊性，其中$\iota_{\mathbf{u}}(a,b) = (a, ab)$。设 $\pi\colon V \times V \to X_V^{\mathbf{u}}$为对合 $\iota_{\mathbf{u}}$ 对应的商映射。可以直接验证，二值群 $X_V^{\mathbf{u}}$ 中元素 $\pi(a,b)$ 的阶在 $a \neq e$ 时等于 4，而在 $a = e$ 且 $b \neq e$ 时等于 2。因此，任意两个阶大于 2 的元素都具有如下形式：$x = \pi(a_1, b_1)$、$y = \pi(a_2, b_2)$，其中 $a_1 \neq e$ 且 $a_2 \neq e$。于是 $x * y = [\pi(a_1a_2, b_1b_2)\ \pi(a_1a_2, a_1b_1b_2)]$。由于元素 $a_1b_1b_2$ 既不是 b_1b_2 也不是$a_1a_2b_1b_2$，所以多重集 $x * y$ 中的元素互不相同。因此，二值群 $X_V^{\mathbf{u}}$ 是非特殊的。容易看出，这意味着所有二值群 $X_V^{\mathbf{u}} \times W.$ 都是非特殊的。

现在考虑二值群 Y_V，其中 $\dim V \geq 2$。设 $x, y \in V$ 是两个不同的非单位元。那么，二值群 Y_V 中元素 x 和 y 的阶都等于 4，因为 $x * x = y * y = [e, s]$ 和 s 是一个二阶元素。此外，$x * y = [xy, xy]$，因此 (x, y) 是一个特殊对。由此，二值群 Y_V 是特殊的，进而所有二值群 $Y_V \times W$ 都是特殊的。□

命题 4.4。设 X 是一个特殊对合交换二值群。那么 X 不是陪集，也就是说，X 不同构于任何形如 G/ι 的二值群，其中 G 是通常群，ι 是 G 的自同构，且 $\iota^2 =$单位元。

证明。反设：令 $X \cong G/\iota$。记 $\pi\colon G \to X$ 关于自同构 ι 的商映射。令 (x, y) 为 X 中的特殊对，并令 $g, h \in G$ 为满足 $\pi(g) = x$ 且 $\pi(h) = y$ 的元素。

我们有 $x * x = \left[\pi(g^2)\ \pi\big(g\iota(g)\big)\right]$。由于 $\operatorname{ord} x > 2$，多重集 $x * x$ 必须由两个不同的元素组成，因此可得 $g^2 \neq g\iota(g)$，从而 $\iota(g) \neq g$。同样，$\iota(h) \neq h$。

多重集 $x * y = \left[\pi(gh)\ \pi\big(g\iota(h)\big)\right]$ 由两个相同的元素组成。因此，要么 $g\iota(h) = gh$，要么 $g\iota(h) = \iota(gh) = \iota(g)\iota(h)$，这意味着要么 $\iota(h) = h$，要么 $\iota(g) = g$。如前所证，这两种情况均不可能，证明完毕。□

注 4.5。请注意，一般而言，可以通过陪集构造从非交换单值群得到交换二值群。例如，如 [7]（另见 [17]）所示，二值 Buchstaber–Novikov 群$X_{C_\infty}^{\mathbf{a}} = C_\infty/\iota_{\mathbf{a}}$ 同构于陪集群 $(C_2 * C_2)/\sigma$，其中 $*$ 表示自由积，而 σ 是一个自同构，它交换因子 C_2的生成元。我们强调，命题 4.4 断言，特殊对合交换二值群不可能是任意群 G 关于其自同构的陪集二值群（该群不一定是交换的）。尽管如此，我们提醒读者，特殊二值群 Y_2（分别地，Y_3）可以通过一种类似陪集构造的方法得到：对非交换群 Q_8 的反自同构（分别地，对非交换且非结合的 Moufang拟群 O_{16}）使用该方法；参见例 1.12 和 1.13。

5. 二值群的商群

关于二值群的商群是否存在这一一般问题，需要单独研究。对于我们所讨论的对合交换二值群情形，这个问题的答案是肯定的。

5.1. 商群的存在性。 二值群 X 的子集 Y 若满足：对于 y_1、$y_2 \in Y$ 中的任意两个元素，多重集 $y_1 * y_2$ 中的两个元素都属于 Y，则称 Y 为子群 。

我们按照以下规则，为子群 Y 在二值群 X 上定义一个等价关系 $\sim$ ：当且仅当存在一个元素 $y \in Y$ 使得 $x' \in x*y$ 时，有 $x \sim x'$ 。

引理 5.1。（a）所定义的关系 $\sim$ 确实是一个等价关系 。（b） $x \sim e$ 当且仅当 $x \in Y$。

（c） 如果 $x_1 * x_2 = [z_1, z_2]$、$x_1' * x_2' = [z_1', z_2']$、$x_1 \sim x_1'$ 和 $x_2 \sim x_2'$，则 $[z_1, z_2] \sim [z_1', z_2']$，也就是说，要么 $z_1 \sim z_1'$ 且 $z_2 \sim z_2'$，要么 $z_1 \sim z_2'$ 且 $z_2 \sim z_1'$。

证明。关系 $\sim$ 具有自反性，因为对于所有 x，都有 $x \in x * e$ 。由引理 2.2 可立即得出关系 $\sim$ 的对称性。下面证明其传递性。设$x_1 \sim x_2$ 和 $x_2 \sim x_3$。那么存在 y_1、$y_2 \in Y$中的元素，使得 $x_2 \in x_1 * y_1$且 $x_3 \in x_2 * y_2$，由此可立即推出 $x_3 \in x_1 * y_1 * y_2$。另一方面，对于某些 y_3、$y_4 \in Y$中的元素，有$y_1 * y_2 = [y_3, y_4]$，因此

$$x_1 * y_1 * y_2 = [x_1 * y_3, x_1 * y_4].$$

因此，元素 x_3 属于多重集 $x_1 * y_3$ 和 $x_1 * y_4$中的一个。于是，$x_1 \sim x_3$，这就完成了对 $\sim$ 是等价关系的证明。

若 $x \in Y$，则由 $e \in x * x$ 可推出 $x \sim e$。反过来，若 $x \sim e$，则存在元素$y \in Y$使得 $e \in x * y$，因此由对合性可知 $x = y \in Y$。

由于二值群 X 满足交换律，且 $\sim$ 是一个等价关系，只需在 $x_2 = x_2'$的情形下证明命题 (c)。若$x_1 \sim x_1'$，则存在 $y \in Y$使得 $x_1' \in x_1 * y$。于是，对某个 p，有 $x_1 * y = [x_1', p]$，并且我们得到

$$[z_1 * y, z_2 * y] = (x_1 * x_2) * y = (x_1 * y) * x_2 = [x_1' * x_2, p * x_2] = [z_1', z_2', p * x_2].$$

必要时交换元素 z_1 和 z_2，我们可以假设 z_1' 属于多重集 $z_1 * y$；于是 $z_1 \sim z_1'$。此外，若元素 z_2' 也属于多重集 $z_2 * y$，则 $z_2 \sim z_2'$ ，因此结论成立。接下来只需考虑 $z_1 * y = [z_1', z_2']$的情形。于是 $z_1' \sim z_1 \sim z_2'$。由引理 2.2 可知，对某个 q，有 $x_1' * y = [x_1, q]$。于是

$$[z_1' * y, z_2' * y] = (x_1' * x_2) * y = (x_1' * y) * x_2 = [x_1 * x_2, q * x_2] = [z_1, z_2, q * x_2],$$

这意味着 z_2 属于多重集 $z_1' * y$ 和 $z_2' * y$ 之一。因此，所有四个元素 z_1、z_2、z_1' 和 z_2' 两两等价，这就证明了所述结论。□

引理 5.1 表明，集合 $X/Y = X/\sim$ 定义良好，并且群 X 中的二值乘法在集合 X/Y 上诱导出定义良好的二值乘法。

引理 5.2。 所引入的乘法使集合 X/Y 成为一个对合的、可交换的二值群。

证明。 X/Y 中二值乘法的交换律和结合律直接来自 X 中乘法的交换律和结合律。显然，单位元的等价类根据引理 5.1 的命题（b），

与子群 Y 重合，是所引入的二值乘法的（强）单位元；我们也将这个单位元记作 e。

让我们证明对合性（同时证明逆元的存在性和唯一性）。事实是，对所有 $x \in X$，$e \in x * x$ 立即意味着对所有 $z \in X/Y$，$e \in z * z$。因此，只需证明：如果 z_1 和 z_2 是来自 X/Y 的两个不同元素，那么 $e \notin z_1 * z_2$。为此，我们需要证明：如果 x_1 和 x_2 分别是两个不同等价类 z_1 和 z_2 的代表元，那么多重集 $x_1 * x_2$ 中不含有来自 Y 的元素。假设情况并非如此，即元素 $y \in Y$ 属于多重集 $x_1 * x_2$。那么，根据引理 2.2，$x_2 \in x_1 * y$，这意味着$x_1 \sim x_2$，进而得到 $z_1 = z_2$，这不成立。矛盾完成了该引理的证明。□

以这种方式定义的对合交换二值群 X/Y 称为二值群 X 关于其子群 Y 的**商群**。由引理 5.1 的 (b) 部分可知，自然投影 $\pi\colon X \to X/Y$ 的核确实与子群 Y 重合。（与普通群的情形一样，二值群同态的核 定义为单位元的原像。）

注 5.3。设 $V \subseteq X$ 是由所有阶为 ≤ 2 的元素组成的子集。由命题 3.2，集合 V 是一个布尔群，它作用于二值群 X 上。因此，若 $W \subseteq V$ 是一个子群，则记号 X/W 可以有两种含义：(i) 二值群 X 关于其子群 W 的商群；(ii) 群 W 在 X 上的作用的轨道空间，其中 W 被视为关于第 3 节中引入的运算 $\cdot$ 的单值群。然而，容易看出这两个集合相同。

5.2. 同态定理。 关于同态像的基本定理同样适用于对合交换二值群的情形。

命题 5.4. *设 $f\colon X \to Z$ 是对合交换二值群之间的一个同态。那么，它的核 $\ker f$ 和像 $\operatorname{im} f$ 分别是二值群 X 和 Z 的子群，并且 f 诱导出一个同构 $X/\ker f \cong \operatorname{im} f$。*

证明。显然，$\operatorname{im} f$ 是一个子群。若 $y_1, y_2 \in \ker f$ 且 $y_1 * y_2 = [z_1, z_2]$，则

$$[f(z_1), f(z_2)] = f(y_1) * f(y_2) = e * e = [e, e],$$

因此 $f(z_1) = f(z_2) = e$。所以，$\ker f$ 也是一个子群。令 $\sim$ 为上述定义的、对应于该子群的 X 上的等价关系。为完成命题的证明，只需证明元素 $z \in \operatorname{im} f$ 的原像点恰好是相对于 $\sim$ 的等价类。下面证明这一点。若 $x_1 \sim x_2$，则存在 $y \in \ker f$ 使得 $x_2 \in x_1 * y$。于是

$$f(x_2) \in f(x_1) * f(y) = f(x_1) * e = [f(x_1), f(x_1)],$$

因此 $f(x_2) = f(x_1)$。反过来，设 x_1 和 x_2 是 X 中的两个元素，使得 $f(x_1) = f(x_2)$。令 $x_1 * x_2 = [p, q]$。根据对合性，多重集 $[f(p)\ f(q)] = f(x_1) * f(x_2) = f(x_1) * f(x_1)$ 必须包含单位元。因此，p 和 q 中至少有一个属于 $\ker f$。不失一般性，假设 $p \in \ker f$。由引理 2.2 可知，元素 x_2 属于多重集 $x_1 * p$，因此 $x_1 \sim x_2$。□

已证明的命题使我们能够定义对合交换二值群的**正合序列**，并以与普通阿贝尔群情形完全相同的方式处理它们。

5.3. 二值群的 C_2-扩张。

定义 5.5。（对合交换） C_2-扩张 是对合交换二值群 X 的对合交换二值群正合序列

$$1 \to 2C_2 \to \widehat{X} \xrightarrow{\pi} X \to 1, \tag{9}$$

其中， $2C_2$ 是通过将群 C_2中的运算加倍得到的二元素二值群。

我们也可以研究所得群 X 不是幂等交换群的扩张，但这类扩张并非我们关注的对象。下文中， C_2-扩张均指幂等交换的 C_2-扩张。

二值群的像是一个二元子群，其中一个元素是单位元 e；另一个元素的阶为 2，我们记作 u。很容易看出， X 是通过对 X 取商得到的，所依据的是由第3节所述运算给出的群$C_2 = \{e, u\}$ 的作用。

我们将群 X 和 X 的单位元都记作 e，这不应造成混淆。

引理 5.6. (a) 若 $x \in X$ 是一个阶不等于 2的元素，则其原像 $\pi^{-1}(x)$ 由两个元素组成，且每个元素的阶要么是 $\operatorname{ord} x$，要么是 $2 \operatorname{ord} x$.

(b) 若 $x \in X$ 是一个阶为 2的元素，则其原像 $\pi^{-1}(x)$ 要么由两个阶为 2的元素组成，要么由一个阶为 4的元素组成。

证明。首先注意到 $\pi^{-1}(e) = \{e, u\}$，因此引理的结论对 $x = e$成立。

若 $\hat{x}$ 是 $\pi^{-1}(x)$中的一个元素，则 $\pi^{-1}(x) = \{\hat{x}, u\hat{x}\}$，因此我们只需确定元素 $\hat{x}$ 和 $u\hat{x}$ 的阶可能是多少，以及这两个元素何时可能彼此相同。

显然，对所有 $k \in \mathbb{Z}$都有 $\pi\left(\hat{x}^k\right) = x^k$ 。因此，若 $\hat{x}^k = e$，则 $x^k = e$。所以，$\operatorname{ord} \hat{x}$ 可被 $\operatorname{ord} x$整除。现在取 $k = \operatorname{ord} x$。于是 $x^k = e$，这意味着元素 $\hat{x}^k$ 属于集合 $\pi^{-1}(e) = \{e, u\}$，也就是说，要么是 $\hat{x}^k = e$ ，要么是 $\hat{x}^k = u$。在第一种情形下，$\operatorname{ord} \hat{x} = k$。在第二种情形下，$\operatorname{ord} \hat{x} > k$，但同时 $\hat{x}^{2k} = u^2 = e$，所以 $\operatorname{ord} \hat{x} = 2k$。

根据命题 3.2(c)，等式 $u\hat{x} = \hat{x}$ 成立，当且仅当 $\hat{x}^2 = u$。若如此，则 $x^2 = e$，于是 $\operatorname{ord} x = 2$，并且 $\operatorname{ord} \hat{x} = 4$。在这种情形下，原像 $\pi^{-1}(x)$ 只包含一个元素 $\hat{x}$。在所有其他情形下， $u\hat{x} \neq \hat{x}$，也就是说，原像 $\pi^{-1}(x)$ 包含两个不同的元素 $\hat{x}$ 和 $u\hat{x}$。最后需要指出，若 $\operatorname{ord} \hat{x} = \operatorname{ord} x = 2$，那么根据命题 3.2，$\operatorname{ord}(u\hat{x}) = 2$；因此 $\pi^{-1}(x)$ 包含两个 2 阶元素。□

回顾一下，根据命题 3.2(a)，由单位元 e 和所有 2 阶元素组成的子集 $V \subseteq X$ 是一个布尔群。记 $R \subset V$ 为由所有满足以下条件的 2 阶元素 x 组成的子集：原像 $\pi^{-1}(x)$ 只包含一个四阶元素。我们将称 R 扩张 *(9)* 的分支集。注意，单位元 e 从不属于集合 R。此外，以下结论成立。

引理 5.7. 集合 $V \setminus R$ 是群 V 的子群。

证明。设 x、$y \in V \setminus R$、$\hat{x}$ 和 $\hat{y}$ 分别是原像 $\pi^{-1}(x)$ 和 $\pi^{-1}(y)$ 中的某些元素。那么，$\operatorname{ord} \hat{x} = \operatorname{ord} \hat{y} = 2$。根据命题 3.2(a)，我们得到 $\operatorname{ord}(\hat{x}\hat{y}) = 2$。由于 $\hat{x}\hat{y} \in \pi^{-1}(xy)$，可知 $xy \in V \setminus R$。因此， $V \setminus R$ 是一个子群。□

6. 直积分解

回顾一下，在第 1 节中，我们定义了对合交换二值群 X 和布尔群 W 的直积运算；所得对合交换群 $X \times W$ 中的乘法运算由公式给出

$$(x_1, w_1) * (x_2, w_2) = \big[(z_1, w_1 w_2), (z_2, w_1 w_2)\big],$$

其中 $x_1 * x_2 = [z_1, z_2]$。

定义 6.1. 若对合交换二值群 X含有单值直因子，则称之为 X 同构于如下形式的二值群$X' \times W$，其中 X'是对合交换二值群， W是非平凡布尔群。否则，称 X 不含单值直因子。

我们希望将有限生成对合交换二值群的分类问题，归结为对不含单值直因子的二值群所进行的同一分类问题。为此，我们需要以下两个命题：第一个命题给出了判断二值群是否不含单值直因子的一个便捷判据，第二个命题则指出，二值群中最大的单值直因子在同构意义下唯一确定。

命题 6.2. 有限生成对合交换二值群 X不含单值直因子，当且仅当每个阶为 2 的元素 $v \in X$ 都是来自 X 的某个元素的平方。

命题 6.3. 任意有限生成对合交换二值群 X 都可以分解为一个不含单值直因子的有限生成对合交换二值群与一个有限布尔群的直积。若 $X = X_i \times W_i$，其中 $i = 1,2$，是两个这样的分解，则 $X_1 \cong X_2$ 和 $W_1 \cong W_2$。

在证明命题 6.2 和 6.3 之前，我们先确立对合交换二值群的两个有用性质。

引理 6.4. 设 X 是一个对合交换二值群， $x, y \in X$ 和 $x * y = [z_1, z_2]$。假设 $x^2 \neq y^2$ 和 $z_1 \neq z_2$，则 $z_1 * z_2 = [x^2, y^2]$。

证明。由引理 2.2，元素 y 属于多重集 $x * z_1$ 和 $x * z_2$。因此，单位元 e 属于多重集

$(x * z_1) * (x * z_2) = (x * x) * (z_1 * z_2) = [e, x^2] * (z_1 * z_2) = [z_1 * z_2, z_1 * z_2, x^2 * ($ $z_1 * z_2)]$.然而， $e \notin z_1 * z_2$ 因为 $z_1 \neq z_2$。因此， $e \in x^2 * (z_1 * z_2)$，这意味着 $x^2 \in z_1 * z_2$。类似地，我们有 $y^2 \in z_1 * z_2$。由于 $x^2 \neq y^2$，这就证明了引理。□

引理 6.5. 设 X 是一个对合交换二值群， $Q \subseteq X$ 是由 X中所有元素的平方构成的子集。那么 Q 是一个子群。

证明。我们需要证明，对于任意的 x、 $y \in X$，多重集 $x^2 * y^2$ 由平方构成。设 $x * y = [z_1, z_2]$，则

$$x * x * y * y = (x * x) * (y * y) = [e, x^2] * [e, y^2] = [e, e, x^2, x^2, y^2, y^2, x^2 * y^2],$$

$$x * x * y * y = (x * y) * (x * y) = [z_1, z_2] * [z_1, z_2] = [e, e, z_1^2, z_2^2, z_1 * z_2, z_1 * z_2].$$

如果 $x^2 \neq y^2$ 且 $z_1 \neq z_2$，那么 $z_1 * z_2 = [x^2, y^2]$，因此 $x^2 * y^2 = [z_1^2, z_2^2]$，结论得证。接下来还需分析 $x^2 = y^2$或 $z_1 = z_2$.的情形

如果 $x^2 = y^2$，那么 $x^2 * y^2 = [e,(x^2)^2]$，与结论一致。

如果 $z_1 = z_2$，那么 $x * x * y * y = [e, e, e, e, z_1^2, z_1^2, z_1^2, z_1^2]$，则多重集 $x^2 * y^2$由平方组成，由此完成证明。□

命题 6.2 的证明。命题陈述中的“当且仅当”的“仅当”部分显而易见：事实上，如果 $X = X' \times W$，其中 W 是一个非平凡的布尔群，那么对于任意元素 $w \in W \setminus \{e\}$，对 $(e, w) \in X$ 是一个不是平方的二阶元素。

反之，设在二值群 X 中存在一个 2 阶元素 w，它不是任何元素的平方。令 $W = \{e, w\}$，并证明单值群 $W \cong C_2$可以作为直因子从 X中分离出来。为此，只需构造一个二值群同态 $f\colon X \to W$，使得 $f(w) = w$。事实上，如果构造出了这样的同态，那么它与自然投影 $\pi\colon X \to X/W$一起将诱导出同构 $X \cong (X/W) \times W$。

如果我们将 W 视为二值群，那么其乘法由 th e 公式

$$e * e = [e, e], \qquad e * w = [w, w], \qquad w * w = [e, e].$$

因此，映射 $f\colon X \to W$ 是二值群同态，当且仅当对于 x中的任意元素 y、$z \in X$，只要 $z \in x * y$，就有等式

$$f(x)f(y)f(z) = e. \tag{10}$$

对所有满足 $z \in x * y$ 的三元组 $\{x, y, z\}$，这些等式构成了域 $\mathbb{F}_2$（采用乘法记号）上的一个关于变量 f（x）的齐次线性方程组，其中 $x \in X$。我们需要证明，这个方程组有一个满足附加条件 f（w）$= w$ 的解。为此，只需证明方程 f（w）$= e$ 不能由方程 (10) 推出。

反设不然。则方程 f（w）$= e$ 是方程 (10) 形式的方程在 $\mathbb{F}_2$ 上的一个线性组合。由于我们采用乘法记号，这意味着方程 f（w）$= e$ 是以下方程的乘积

$$f(x_i)f(y_i)f(z_i) = e, \qquad i = 1, \dots, m,$$

对某些满足 $z_i \in x_i * y_i$ 的三元组 $\{x_i, y_i, z_i\}$，考虑到对于所有 t，f（t）$^2 = e$。因此，这个含 $3m$ 个元素的多重集 $[x_1, y_1, z_1, \dots, x_m, y_m, z_m]$ 具有如下形式

$$\left[w, t_1, t_1, t_2, t_2, \dots, t_n, t_n\right]$$

对于某些 t_1、.....、$t_n \in X$，当然，$n = (3m - 1)/2$。

对于每个 i，由 $z_i \in x_i * y_i$ 可知，多重集 $x_i * y_i * z_i$ 包含单位元 e：

$$\begin{aligned} e \in (x_1 * y_1 * z_1) * \cdots * (x_m * y_m * z_m) &= w * (t_1 * t_1) * (t_2 * t_2) * \cdots * (t_n * t_n) \\ &= w * \left[e, t_1^2\right] * \left[e, t_2^2\right] * \cdots * \left[e, t_n^2\right]. \end{aligned}$$

由于二值群 X 是对合的，因此

$$w \in \left[e, t_1^2\right] * \left[e, t_2^2\right] * \cdots * \left[e, t_n^2\right].$$

因此，w 属于二值群 X 中由平方 t_i^2 生成的一个子群。于是，根据引理 6.5，元素 w 本身是一个平方，这是不可能的。这个矛盾意味着线性方程组 (10) 存在一个满足 $f(w) = w$的解。该解是一个二值群同态，它诱导出一个同构 $X \cong (X/W) \times W$。□

命题 6.3 的证明。若二值群 X 含有某个单值直因子，则取该直因子：$X = X' \times W'$，其中 dim $W' > 0$。若 X' 又含有某个单值直因子 $\widetilde{\qquad}$ $\widetilde{\qquad}$，则再次取该直因子：$X' = X'' \times W$，其中 dim $W > 0$，因而 $\widetilde{\qquad}$ $X = X'' \times W''$，其中 $W'' = W' \times W$，dim $W'' \geq 2$。以此类推，只要可能就继续进行；经过第 k 步后，我们将得到分解 $X = X^{(k)} \times W^{(k)}$，其中 dim $W^{(k)} \geq k$。我们需要证明这个过程会在某一步终止，也就是说，

经过一定步骤后，二值群 $X^{(k)}$ 将不再含有单值直因子。为此，注意到每个带有双重运算的群 $W^{(k)}$ 都是二值群 X 的商群。因此，如果二值群 X 由 N 个元素生成，那么群 $W_{(k)}$ 也由 N 个元素生成，因而由 $k \leq N$ 生成。因此，所讨论的过程最迟将在第 N 步终止，从而得到所需的分解。

现在设 $X = X_1 \times W_1 = X_2 \times W_2$ 是两个分解，使得 X_1 和 X_2 不含单值直因子。先假设 $W_1 = W_2$。那么，投影 $X \to X_1$ 和 $X \to X_2$ 都是关于同一个群 $W_1 = W_2$ 的作用取商，这立即推出 X_1 和 X_2 同构。

现在假设 $W_1 \neq W_2$。令 $Q \subseteq X$ 为由来自 X 的所有元素的平方组成的子集。那么 $Q \subseteq X_1$ 和 $Q \subseteq X_2$。根据引理 6.5，子集 Q 是一个子群。令 $V \subseteq X$ 为由所有阶为 ≤ 2 的元素组成的子集。那么 V 是一个布尔群，且 W_1 和 W_2 是其子群。由 Q 是二值群 X 的子群这一事实可知，$U = Q \cap V$ 是布尔群 V 的子群。由于 $Q \subseteq X_1$ 和 $Q \subseteq X_2$，因此 $U \cap W_1 = U \cap W_2 = \{e\}$。假设直积 $U \times W_1$ 不等于整个群 V。那么元素 $v \in V \setminus (U \times W_1)$ 经投影 $X = X_1 \times W_1 \to X_1$ 映射为一个 2 阶元素，而该元素不是来自 X_1 的任何元素的平方。根据命题 6.2，这与 X_1 不含单值直因子的事实矛盾。因此 $V = U \times W_1$。同理，$V = U \times W_2$。于是，W_1 和 W_2 是向量空间 V 中与子空间 U 互补的两个子空间，其中 V 定义在 $\mathbb{F}_2$ 上。因此，存在一个同态 $f\colon\ W_1 \to U$，使得公式 $w \mapsto wf\ (w)$ 定义了一个同构 $W_1 \cong W_2$；于是，由公式 $F\ (x,\ w) = (x,\ wf(w))$ 定义的映射 $F\colon\ X_1 \times W_1 \to X_1 \times W_1$ 是二值群 X 的一个自同构，它保持 X_1 不变并将 W_1 映射为 W_2。因此存在一个直积分解 $X = X_1 \times W_2$，这意味着 $X_1 \cong X_2$。□

7. 非特殊二值群的性质

回忆一下，如果对任意阶大于 2 的元素 x、$y \in X$，直积 $x * y$ 都由两个不同的元素组成，则称对合交换二值群 X 为 非特殊 。本节将证明这类二值群的若干有用性质。

本节所有陈述中，X 是非特殊对合交换二值群，而 $V \subseteq X$ 是由单位元 e 和所有 2 阶元素组成的子集。回忆一下，根据命题 3.2，集合 V 是一个作用于 X 上的布尔群。本节所有陈述中，除非另有说明，小写拉丁字母 x、y、z.....表示二值群 X 的元素。

引理 7.1。 等式 $x^2 = y^2$ 成立，当且仅当元素 x 和 y 位于同一个 V-轨道中。

证明。若 x 和 y 位于同一个 V-轨道中，即对某个 $v \in V$ 有 $y = vx$，则由公式 (8) 立即得到等式 $x^2 = y^2$。

证明逆向蕴含。若 $x^2 = y^2 = e$，则 x、y 属于 V，因此位于同一个 V-轨道中。假设 $x^2 = y^2 \neq e$。那么元素 x 和 y 的阶大于 2。由于对 $(x,\ y)$ 不是特殊的，因此可得 $x * y = [z_1, z_2]$，其中 $z_1 \neq z_2$。我们有

$$x * x * y * y = (x * x) * (y * y) = [e, x^2] * [e, x^2] = [e, e, e, x^2, x^2, x^2, x^2, x^4],$$
$$x * x * y * y = (x * y) * (x * y) = [z_1, z_2] * [z_1, z_2] = [e, e, z_1^2, z_2^2, z_1 * z_2, z_1 * z_2].$$

由 $z_1 \neq z_2$ 这一事实可知， $e \notin z_1 * z_2$。因此，要么 $z_1^2 = e$，要么 $z_2^2 = e$。不妨设 $z_1^2 = e$，从而 $z_1 \in V$。由于 $z_1 \in x * y$，根据引理 2.2，我们有 $y \in z_1 * x$，因此 $y = z_1 x$。□

LEMMA 7.2. *If* $x * y = [z_1, z_2]$, *then* $z_1 * z_2 = [x^2, y^2]$.

证明。首先假设元素 x 和 y 属于不同的 V-轨道，且它们都不属于 V。那么由引理 7.1 可得 $x^2 \neq y^2$。此外，由于所考虑的二值群 X 是非特殊的，因此可知 $z_1 \neq z_2$。于是，所需的等式由引理 6.4 得出。

剩下的情形是：元素 x 和 y 属于同一个 V-轨道，或者它们中至少有一个属于 V。如果 x 和 y 属于同一个 V-轨道，使得对于某个 $v \in V$ 有 $y = vx$，那么 $x * y = [v, vx^2]$ 和 $v * (vx^2) = [x^2, x^2] = [x^2, y^2]$。如果 $x \in V$，那么 $z_1 = z_2 = xy$ 和 $z_1 * z_2 = [e, y^2] = [x^2, y^2]$； $y \in V$ 的情形类似。□

COROLLARY 7.3. *If* $x * y = [z_1, z_2]$, *then* $z_2 \in x^2 * z_1$.

应用引理 7.2 两次，可得以下结论。

推论 7.4。如果 $x * y = [z_1, z_2]$，那么 $x^2 * y^2 = [z_1^2, z_2^2]$。

引理 7.5。设 $x * y = [z_1, z_2]$。

(a) 如果元素 x 和 y 的阶整除 4，那么 z_1 和 z_2 的阶也整除 4。因此，非特殊对合交换二值群 X 中所有阶整除4的元素构成一个子群。(b) 元素 z_1 和 z_2 属于同一个 V-轨道，当且仅当元素 x 和 y 中至少有一个的阶整除4。如果$\operatorname{ord} x$ 整除 *4*，那么 $z_2 = x^2 z_1$。(c) 如果三个元素 x、 z_1 和 z_2 都属于同一个 V-轨道，那么元素 y 的阶整除4。

证明。由推论 7.4 可得 $x^2 * y^2 = [z_1^2, z_2^2]$。现在设两个元素 x 和 y 的阶都整除 4。则 x^2 和 y^2 属于集合 V。因此，元素$z_1^2 = z_2^2 = x^2 y^2$ 也属于 V，所以 $z_1^4 = z_2^4 = e$，这就证明了命题（a）。

此外，利用所考虑的二值群 X 不是特殊群这一事实以及引理 7.1，我们得到以下等价关系链，从而证明命题（b）的第一部分：

$$(\operatorname{ord} x \mid 4) \vee (\operatorname{ord} y \mid 4) \Leftrightarrow (x^2 \in V) \vee (y^2 \in V) \Leftrightarrow z_1^2 = z_2^2 \Leftrightarrow V z_1 = V z_2 .$$

命题（b）的第二部分由推论 7.3 立即得到。

现在设三个元素 x、 z_1 和 z_2 都属于同一个 V-轨道，因此 $z_1 = v_1 x$ 和$z_2 = v_2 x$，其中 v_1、$v_2 \in V$，于是 $[x^2, y^2] = z_1 * z_2 = [v_1 v_2, v_1 v_2 x^2]$。因此，要么 $y^2 = v_1 v_2$，此时 $\operatorname{ord} y$ 整除 4；要么 $x^2 = v_1 v_2$和 $y^2 = v_1 v_2 x^2 = e$，此时 $\operatorname{ord}\ y$ 整除 2。□

引理 7.6. 若 $x * y = z * t$，则或者存在 $v \in V$ 使得 $z = vx$ 和$t = vy$，或者存在 $v \in V$ 使得 $z = vy$ 和 $t = vx$。

证明。引理 7.2 立即推出，若 $x * y = z * t$，则 $[x^2, y^2] = [z^2, t^2]$。设 $x^2 = z^2$ 和 $y^2 = t^2$；第二种情形完全类似。于是由引理 7.1，存在元素 v_1、 $v_2 \in V$，使得 $z = v_1 x$ 和 $t = v_2 y$。若 $v_1 = v_2$，则引理的陈述成立。

假设 $v_1 \neq v_2$ 且设 $w = v_1 v_2$，则 $w \neq e$。等式 $x * y = z * t$ 可改写为 $w(x * y) = x * y$。令 $x * y = [s_1, s_2]$，则有以下两种可能的情形。

1) $ws_1 = s_1$ 且 $ws_2 = s_2$。由命题 3.2 的 (c) 项可得$s_1^2 = s_2^2 = w$，这意味着根据引理 7.1，对于某个 $u \in V$，有 $s_2 = us_1$。现在由引理 7.2 可得

$$[x^2, y^2] = s_1 * s_2 = [u, us_1^2] = [u, uw].$$

不失一般性， $x^2 = u$ 和 $y^2 = uw$。于是 $ux = x$ 和 $uv_1v_2y = y$，因此 $z = v_1x = uv_1x$ 和 $t = v_2y = uv_1y$。由此，引理中的陈述对$v = uv_1$成立。

2) $ws_1 = s_2$ 和 $ws_2 = s_1$。由引理 7.2 可得

$$[x^2, y^2] = s_1 * s_2 = [w, ws_1^2].$$

不失一般性， $x^2 = w = v_1v_2$。于是 $v_1v_2x = x$，因此 $z = v_1x = v_2x$。由此，引理中的陈述对 $v = v_2$成立。□

引理 7.7. 设元素 x_1、 x_2和 x_3 属于两两不同的 V-轨道，且它们都不属于 V。则多重集 $x_1 * x_2 * x_3$ 由四个不同的元素组成。此外，若 $x_1 * x_2 = [p_3, q_3]$、 $x_2 * x_3 = [p_1, q_1]$和 $x_3 * x_1 = [p_2, q_2]$，则

$$x_1 * x_2 * x_3 = (x_1 * p_1) \cup (x_1 * q_1) = (x_2 * p_2) \cup (x_2 * q_2) = (x_3 * p_3) \cup (x_3 * q_3)$$

都是将四元素集 $x_1 * x_2 * x_3$ 划分为两个二元素子集的三种不同划分。换言之， $x_1 * p_1$、 $x_1 * q_1$、 $x_2 * p_2$、 $x_2 * q_2$、 $x_3 * p_3$ 和 $x_3 * q_3$ 恰好是四元素集 $x_1 * x_2 * x_3$的全部六个不同的二元素子集。

证明。我们先证明，6 个多重集 $x_1 * p_1$、 $x_1 * q_1$、 $x_2 * p_2$、 $x_2 * q_2$、 $x_3 * p_3$和 $x_3 * q_3$ 两两不同。假设结论不成立。这里有两种本质不同的情形： $x_1 * p_1 = x_1 * q_1$或 $x_1 * p_1 = x_2 * p_2$。其他情形都与这两种情形之一完全类似。我们依次考察这两种情形。

1) $x_1 * p_1 = x_1 * q_1$。于是根据引理 7.6，存在一个元素 $v \in V$，使得要么 $p_1 = q_1 = vx_1$，要么 $vx_1 = x_1$ 且 $vp_1 = q_1$。然而，等式 $p_1 = q_1$ 不可能成立，因为二值群 X 不是特殊的，并且 x_2、 $x_3 \notin V$。因此 $vx_1 = x_1$ 且$vp_1 = q_1$，并且 $v \neq e$。由命题 3.2 的 (c) 项可知，$\operatorname{ord} x_1 = 4$ 且 $v = x_1^2$；再由引理 7.5 的 (b) 项可知，元素 x_2 和 x_3 中有一个（不妨设为 x_2）的阶整除 4，且 $x_2^2 p_1 = q_1$。因此$x_1^2 x_2^2 p_1 = p_1$ 且 $x_1^2 x_2^2 q_1 = q_1$。然而，由于 x_1 和 x_2 属于不同的 V-轨道，根据引理 7.1 可知 $x_1^2 \neq x_2^2$，从而 $x_1^2 x_2^2 \neq e$。现在再由命题 3.2 的 (c) 项可知，$\operatorname{ord} p_1 = \operatorname{ord} q_1 = 4$ 且 $p_1^2 = q_1^2 = x_1^2 x_2^2$。再由推论 7.4 可知 $x_2^2 * x_3^2 = [x_1^2 x_2^2, x_1^2 x_2^2]$，从而 $x_2^2 x_3^2 = x_1^2 x_2^2$，进而$x_3^2 = x_1^2$。这与 x_1 和 x_3 属于不同的 V-轨道这一事实矛盾。

2) $x_1 * p_1 = x_2 * p_2$。由于 x_1 和 x_2 属于不同的 V-轨道，根据引理 7.6，存在一个元素 $v \in V$，使得 $p_2 = vx_1$ 和 $p_1 = vx_2$。于是由引理 2.2 可得$x_3 \in x_1 * p_2 = [v, vx_1^2]$，因此 $x_3 = vx_1^2$，因为 $x_3 \notin V$。类似地， $x_3 = vx_2^2$。所以 $x_1^2 = x_2^2$。这与 x_1 和 x_2 属于不同的 V-轨道这一事实矛盾。

因此，六个多重集 $x_1 * p_1$、 $x_1 * q_1$、 $x_2 * p_2$、 $x_2 * q_2$、 $x_3 * p_3$和 $x_3 * q_3$两两不同。每个多重集都由两个（可能相同的）元素组成，并且包含在四元多重集 $x_1 * x_2 * x_3$中。然而，如果四元多重集 $x_1 * x_2 * x_3$中有重复元素，那么其中所含的不同二元多重集的数量将严格少于 6。因此，多重集 $x_1 * x_2 * x_3$ 由四个不同的元素组成，这就完成了引理的证明。□

引理 7.8. 假设元素 x_1、 x_2 和 x_3 属于两两不同的 V-轨道，且它们都不属于 V。如果多重集 $y_1 * y_2$ 包含于多重集 $x_1 * x_2 * x_3$中，

那么存在一个由数字 $1,2$构成的置换 λ,μ，一个由数字 $1,2,3$构成的置换 i,j,k，以及一个元素 $v\in V$，使得 $y_\lambda = vx_i$ 和 $y_\mu \in v(x_j * x_k)$。

证明。令 $x_i * x_j = [p_k, q_k]$ 对数字 1、2、3 的每个置换 i,j,k。根据引理 7.7，我们知道 $x_1*p_1, x_1*q_1, x_2*p_2, x_2*q_2, x_3*p_3$ 和 x_3*q_3 恰好是四元素集 $x_1*x_2*x_3$ 的全部 6 个二元素子集，因此其中一个与多重集 y_1*y_2 重合。不失一般性，我们可以假设 $y_1*y_2 = x_1*p_1$。于是根据引理 7.6，存在一个元素 v，使得 $y_\lambda = vx_1$ 且 $y_\mu = vp_1 \in v\,(x_2*x_3)$，其中 λ,μ 是数字 1、2 的某个置换。□

8. 含有阶不是 1、2 或 4

本节将证明以下结果。

定理 8.1. 设 X 是一个非特殊对合交换二值群，其中至少含有一个阶既不是 1，也不是 2，也不是 4 的元素。那么 X 同构于一个形如 $X_A^{\mathbf{a}} = A/\iota_{\mathbf{a}}$ 的陪集二值群，其中 A 是一个阿贝尔群，而 $\iota_{\mathbf{a}}$ 是 A 上的对跖对合。

注 8.2. 该定理不要求二值群 X 有限生成。此外，容易验证，二值群 $A/\iota_{\mathbf{a}}$ 有限生成，当且仅当阿贝尔群 A 有限生成。

定理 8.1 的证明将通过显式构造阿贝尔群 A 给出。这一构造实质上取决于所选元素 $t\in X$，使得 $\operatorname{ord} t \notin \{1,2,4\}$。然而，正如将在第 12 节（命题 12.2）中说明的，对于有限生成的二值群 X，所得阿贝尔群 A 在同构意义下不依赖于元素 t 的选择。显然，即使不假设有限生成，这一点似乎也成立，但我们不知道这一事实的证明。

以下命题描述了阿贝尔群 A的显式构造。证明将分解为一系列引理，并构成本节余下的内容。

命题 8.3. 设 X 是一个非特殊对合交换二值群，$V\subseteq X$ 是由所有阶为 ≤ 2的元素构成的子集，且 $t\in X$ 是一个满足 阶$t\notin\{1,2,4\}$的元素。考虑集合

$$A = \{(x,p)\in X\times X \mid p\in t*x\}. \tag{11}$$

Then

(a) 若 $(x,p)\in A$，$(y,q)\in A$，$t*x=[p,p']$ 且 $t*y=[q,q']$，则存在唯一的一对 $(z,r)\in A$，使得

(i) z 属于三个多重集 $x*y$、$p*q'$ 和 $p'*q$中的每一个；(ii) r 属于两个多重集 $x*q$ 和 $p*y$中的每一个。(iii) 存在一个元素 r'，使得 $t*z=[r,r']$ 属于两个多重集 $x*q'$ 和$p'*y$中的每一个。(b) 通过公式定义乘法运算 $\bullet$: $A\times A\to A$

$$(x,p)\bullet(y,q) = (z,r),$$

其中，$(z,r)\in A$ 是唯一满足性质(i)、(ii) 和(iii)的对。于是，$(A,\bullet)$ 是一个交换（单值）群，其单位元为(e,t)，逆元由公式$(x,p)^{-1}=(x,p')$定义，其中 $t*x=[p,p']$。

(c) 到第一因子的投影 $A\to X, (x,p)\mapsto x$ 诱导了二值群 $A/\iota_{\mathbf{a}}\cong X$ 的一个同构，其中 $\iota_{\mathbf{a}}$ 是对跖对合：$\iota_{\mathbf{a}}(a)=a^{-1}$。

以下引理是命题 3.2 的直接推论。

引理 *8.4.* 群 V 按照公式 $v(x,p)=(vx,vp)$ 作用于集合 A，其中 $v\in V$，$(x,p)\in A$。若命题 *8.3* 的陈述 *(a)* 对集合 A 中的元素 $\alpha=(x,p)$ 和 $\beta=(y,q)$ 成立，则对于任意元素 u，$v\in V$，命题 *8.3* 的陈述 *(a)* 对元素 $u\alpha=(ux,up)$ 和 $v\beta=(vy,vq)$ 成立，且

$$(u\alpha)\bullet(v\beta)=uv(\alpha\bullet\beta). \tag{12}$$

引理 *8.5.* 当 (y,q) 是下列对之一时，命题 *8.3* 的陈述 *(a)* 在特殊情形下成立：(e,t)、(t,e)、(t,t^2)、(t^2,t)、(x,p)、(x,p')、(p,x)、(p',x) 和 (s,p)，其中$t*p=[x,s]$。我们有以下公式

$$(x,p)\bullet(e,t)=(x,p), \tag{13}$$
$$(x,p)\bullet(t,e)=(p',x), \tag{14}$$
$$(x,p)\bullet(t,t^2)=(p,s), \tag{15}$$
$$(x,p)\bullet(t^2,t)=(s',p') \tag{16}$$
$$(x,p)\bullet(x,p)=(x^2,f), \tag{17}$$
$$(x,p)\bullet(x,p')=(e,t), \tag{18}$$
$$(x,p)\bullet(p,x)=(t,e), \tag{19}$$
$$(x,p)\bullet(p',x)=(f',x^2), \tag{20}$$
$$(x,p)\bullet(s,p)=(t^2,t), \tag{21}$$

其中 $t*p'=[x,s']$、$x*p=[t,f]$ 和 $x*p'=[t,f']$。

证明。直接利用引理 2.2 和推论 7.3，即可验证公式（13）–（21）右侧的各对 (z,r) 属于集合 A，且具有性质 (i)、(ii) 和 (iii)。接下来只需证明在每种情形下，这样的对 (z,r) 是唯一的。

首先注意，若元素 x、p、p'、y、q 和 q' 中至少有一个属于 V，则对 (z,r) 必然唯一。事实上，

- 若 $x\in V$，则 $z\in x*y=[xy,xy]$ 和 $r\in x*q=[xq,xq]$，因此 $(z,r)=(xy,xq)$;
- 若 $p\in V$，则 $z\in p*q'=[pq',pq']$ 且 $r\in p*y=[py,py]$，因此 $(z,r)=(pq',py)$;
- 若 $p'\in V$，则 $z\in p'*q=[p'q,p'q]$ 且 $r'\in p'*y=[p'y,p'y]$，因此 $(z,r')=(p'q,p'y)$，之后元素 r 由 $t*z=[r,r']$的条件唯一确定;
- 情形 $y\in V$、$q\in V$和 $q'\in V$完全类似。

这些论证涵盖了情形 $(y,q)=(e,t)$、(t,e) 和 (t,t^2)。依次考虑其余情形，并假设元素 x、p、p'、y、q 和 q' 均不属于 V。

1. 在 $(y,q)=(t^2,t)$ 的情形下，我们有 $r\in x*q=[p,p']$，因此 $r=p$或$r=p'$。此外，我们还有 $r\in p*y=p*t^2$。首先假设 $p\notin p*t^2$。那么唯一可能的值是 $r=p'$。此外，元素 z 必须属于多重集$t*r=[x,s']$ 和 $x*y=x*t^2$。当 $x\notin x*t^2$ 时，这两个条件唯一确定 z。若 $x\in x*t^2$，则 $t^2\in x*x$，因此 $t^2=x^2$；由引理 7.1 可知，对某个$u\in V$，有 $x=ut$。于是 $[p,p']=x*t=[u,ut^2]$，这是不可能的，因为根据假设，元素 p 和 p' 均不属于 V。

现在假设 $p\in p*t^2$，于是 $t^2\in p*p$。那么 $t^2=p^2$，因此由引理 7.1 可得 $p=ut$，其中某个 $u\in V$。另一方面，$y=t^2$，所以 $t*y=[t,t^3]$ 和 $q'=t^3$。元素 z 必须属于多重集 $x*y=[u,ut^4]$ 和 $p*q'=[ut^2,ut^4]$。由于 $t^2\neq e$,

由此可得 $z = ut^4$。现在，元素 r 必须属于多重集 $t * z = [ut^3, ut^5]$ 和 $x * q = p * y = [ut, ut^3]$。若 $t^5 \neq t$，则唯一满足这两个条件的元素是 $z = ut^3$。若 $t^5 = t$，则或者 $t^4 = e$，或者 $t^6 = e$。第一个等式不可能成立，因为 ord $t \notin \{1, 2, 4\}$；第二个等式也不可能成立，因为在这种情况下，元素 $q' = t^3$ 会属于集合 V，这与我们的假设矛盾。

在讨论其余情形之前，我们先作一个一般性说明。我们已经证明，当 (y, q) 是 (e, t)、(t, e)、(t, t^2) 和 (t^2, t) 中的一对时，命题 (a) 成立；也就是说，当 y 和 q 中有一个等于 t 时，命题 (a) 成立。根据引理 8.4，这意味着如果 y 和 q 中有一个元素属于轨道 Vt，命题 (a) 就成立。类似地，如果 x 和 p 中有一个元素属于轨道 Vt，命题 (a) 也成立。因此，在证明命题 (a) 时，我们可以假设 x、p、y 和 q 均不属于 $Vt.$。根据引理 7.1，这等价于假设 x^2、p^2、y^2 和 q^2 中没有元素等于 $t^2.$。现在我们在这个附加假设下继续考察所有情形。

2. 在 $(y, q) = (x, p)$ 的情形下，我们有 $z \in x * x = [e, x^2]$ 和 $z \in p * p'$。若 $z = e$，则 $p = p'$；由于二值群 X 的非特殊性，这是不可能的，因为$x \notin V$和 $t \notin V$。因此，唯一可能的值是 $z = x^2$。进一步，我们有 $r \in x * p = [t, f]$和 $r \in x^2 * t$。若 $t \in x^2 * t$，则 $x^2 \in t * t = [e, t^2]$，这是不可能的，因为根据假设，$x \notin V$和 $x^2 \neq t^2$。因此 $t \notin x^2 * t$，故唯一可能的值是 $r = f$。

3. 在 $(y, q) = (x, p')$ 的情形下，元素 z 必须属于多重集$x * x = [e, x^2]$、$p * q' = p * p = [e, p^2]$和 $p' * q = p' * p' = [e, p'^2]$。若元素 x^2、p^2和 p'^2 不全相同，则可推出 $z = e$，进而得到 $r = t$。若 $x^2 = p^2 = p'^2$，则由引理 7.1 可得 $p = ux$ 和 $p' = u'x$，其中 u、$u' \in V$。接着，由引理 7.2，等式 $[x^2, t^2] = p * p' = [uu', uu'x^2]$ 成立。因此，要么 $t^2 = uu'$，要么$x^2 = uu'$和 $t^2 = uu'x^2 = e$。这两种情况都不可能，因为 ord $t \notin \{1, 2, 4\}$。因此，情形$x^2 = p^2 = p'^2$ 不可能。

4. 在 $(y, q) = (p, x)$ 的情形下，我们有 $r \in x * x = [e, x^2]$ 和 $r \in p * p = [e, p^2]$。若 $x^2 \neq p^2$，则可得 $r = e$，进而得到 $z = t$。令 $x^2 = p^2$。于是由引理 7.1 可知，对于某个 $u \in V$，有 $p = ux$，因此 $t \in x * p = [u, ux^2]$。由于 $t \notin V$，可知$t = ux^2$。于是 $t * x = [ux, ux^3]$，进而得到 $p' = ux^3$。因此，元素 z 属于多重集 $x * y = [u, ux^2]$ 和 $p' * q = [ux^2, ux^4]$。由于 $x^4 = t^2 \neq e$，唯一可能的值是 $z = ux^2 = t$。因此 $r \in z * t = [e, x^4]$。然而，上文已经指出 $r \in [e, x^2]$。此外，根据假设，我们有 $x^4 = t^2 \neq x^2$。所以唯一可能的值是$r = e$。

5. 在 $(y, q) = (p', x)$ 的情形下，我们有 $r \in x * q = [e, x^2]$ 和 $r \in p * y = p * p'$。然而，由于 $x \notin V$和 $t \notin V$，根据二值群 X 的非特殊性可知 $p \neq p'$。因此 $e \notin p * p'$，唯一可能的值是 $r = x^2$。进一步地，我们有 $z \in x * y = [t, f']$和 $z \in t * r = t * x^2$。如果包含关系 $t \in t * x^2$ 成立，那么将得到 $x^2 \in t * t = [e, t^2]$，但这是不可能的，因为 $x \notin V$ 和 $x^2 \neq t^2$。因此$t \notin t * x^2$，从而唯一可能的值是 $z = f'$。

6. 当 $(y, q) = (s, p)$ 时，我们有 $z \in p' * q = p' * p = [t^2, x^2]$（由引理 7.2）以及 $z \in x * s$。

假设 $x^2 \notin x * s$。那么唯一可能的值是 $z = t^2$，因此 $r = t$或 $r = t^3$。然而，元素 r必须属于多重集 $x * q = x * p = [t, f]$。如果 $t^3 = f$成立，那么根据引理 7.2，我们会得到 $[x^2, p^2] = t * f = [t^2, t^4]$，这是不可能的，因为根据假设，$x^2 \neq t^2$ 且 $p^2 \neq t^2$。所以 $t^3 \neq f$，因此唯一可能的值是 $r = t$。

现在假设 $x^2 \in x * s$。那么 $s \in x^2 * x = [x, x^3]$。然而，$x \neq s$，因为 $t, p \notin V$，且二值群 X 不是特殊的。因此 $s = x^3$。由引理 7.2 可得

$[t^2, p^2] = x * s = [x^2, x^4]$。由于 $x^2 \neq t^2$，可知 $t^2 = x^4$和 $p^2 = x^2$。因此，对于某些 u，$v \in V$，有 $p = ux$和 $t = vx^2$。于是 $[p, p'] = t * x = [vx, vx^3]$。若等式 $p' = vx$成立，那么由引理 7.2 可得 $[t^2, x^2] = p * p' = [uv, uvx^2]$，这将意味着 $t^2 = uv$ 或 $x^2 = uv$ 和 $t^2 = uvx^2 = e$，但这是不可能的，因为 $\mathrm{ord}\, t \notin \{1, 2, 4\}$。因此，$p = vx$ 和 $p' = vx^3$。此外，$[q, q'] = t * s = [vx, vx^5]$，故$q' = vx^5$。元素 z必须属于多重集 $x * y = [x^2, x^4]$ 和 $p * q' = [x^4, x^6]$。若等式 $x^2 = x^6$ 成立，则可推出 $x^8 = e$，进而得到 $t^4 =(vx^2)^4 = e$，这并不成立。因此 $x^2 \neq x^6$，故唯一可能的值是 $z = x^4$。此外，元素 r必须属于多重集 $x*q = [v, vx^2]$和 $p*y = [vx^2, vx^4]$。等式$x^4 = e$ 不可能成立，因为这将意味着 $t^2 = (vx^2)^2 = e$。因此，唯一可能的值是 $r = vx^2$。□

命题 8.3 的 (a) 部分证明。引理 8.4 和引理 8.5 表明，只要满足以下至少一个条件，关于对 (x, p) 和 (y, q) 的 (a) 部分陈述就成立：

(1) 轨道 Vx、Vy、Vp 和 Vq 中的一个与 V 或 Vt 重合；(2) 轨道 Vx 和 Vp 中的一个与轨道 Vy 和 Vq 中的一个重合。

接下来要考虑“一般位置”的情形，即上述两个条件均不满足的情况。由引理 7.7 可知，多重集 $t*x*y$ 由四个不同的元素组成，而 $(x*q) \cup (x*q')$ 和 $(p*y) \cup (p'*y)$ 是这个四元素集划分为两个二元素子集的两种不同划分。因此，集合 $x*q$ 和 $p*y$ 有一个公共元素，记为 r。此外，$t*x*y = (t*z) \cup (t*z')$，其中$x*y = [z, z']$，这意味着 r 恰好属于二元素集 $t*z$ 和 $t*z'$ 之一。根据需要重新命名元素 z 和 z'，可假设 $r \in t*z$ 和$r \notin t*z'$。那么，(z, r) 是 A 中唯一可能具有性质 (i)、(ii) 和 (iii) 的对。接下来只需证明它确实具有这些性质。性质 (ii) 和包含关系 $z \in x*y$ 按构造成立。

让我们证明性质（iii）。根据引理 7.7

$$t*x*y = (x*q) \cup (x*q') = (p*y) \cup (p'*y) = (t*z) \cup (t*z')$$

它们都是将四元素集 $t*x*y$ 划分为两个二元素子集的三种不同划分。因此，由于元素 r 属于子集 $x*q$、$p*y$ 和 $t*z$，可知子集 $t*z$ 中与 r 不同的元素 r' 属于子集 $x*q'$ 和 $p'*y$，这就是性质（iii）。

现在让我们证明 $z \in p*q'$。元素 z 属于多重集

$$x*y \subseteq (p*t)*y = p*(t*y) = (p*q) \cup (p*q').$$

因此，如果 $z \notin p*q'$，那么元素 z 必须属于多重集 $p*q$。假设确实如此。根据引理 7.7，对于三元组 (t, x, y)，多重集 $t*x*y$ 由四个不同的元素组成，而 $x*q$、$p*y$ 和 $t*z$ 是其中三个两两不同的二元素子集，且它们交于公共元素 r。因此，这三个子集的并集（不计元素的重数）恰好是整个集合 $t*x*y$。另一方面，由于 $x \in t*p$、$y \in t*q$和 $z \in p*q$，多重集 $x*q$、$p*y$和 $t*z$ 各自都包含于四元素多重集 $t*p*q$ 中。因此，$t*p*q = t*x*y$。于是，32 元多重集 $(t*p*q)*(t*x*y)$ 中单位元 e 的重数至少为 4。另一方面，对于某些 f、$g \in X$，我们有 $x*p = [t, f]$ 和 $y*q = [t, g]$；于是

$$\begin{aligned}(t*p*q)*(t*x*y) = (t*t)*(x*p)*(y*q) = (t*t)*[t, f]*[t, g] \\ = [t*t*t*t, t*t*t*f, t*t*t*g, t*t*f*g].\end{aligned}$$

与此同时，多重集

$$t*t*t*t=[e,t^2]*[e,t^2]=[e,e,e,t^2,t^2,t^2,t^2,t^4]$$

只包含 e，且其重数为 3，因为 $\operatorname{ord} t\neq\{1,2,4\}$。因此，元素 e 必须属于三个多重集 $t*t*t*f$、$t*t*t*g$ 和 $t*t*f*g$ 中的至少一个。

如果 $e\in t*t*t*f$，那么 $f\in t*t*t=[t,t,t,t^3]$，于是要么 $f=t$，要么 $f=t^3$。根据引理 7.2

$$[x^2,p^2]=t*f=\begin{cases}[e,t^2], & \text{если } f=t,\\ [t^2,t^4], & \text{если } f=t^3.\end{cases}$$

因此，$x^2=t^2$ 或 $p^2=t^2$，所以根据引理 7.1 可得 $Vx=Vt$ 或 $Vp=Vt$，这与条件（1）不满足的假设相矛盾。同样，假设 $e\in t*t*t*g$ 也会导致矛盾。如果 $e\in t*t*f*g$，那么根据引理 7.2，我们有

$$t*t*f*g=(t*f)*(t*g)=[x^2,p^2]*[y^2,q^2].$$

因此，等式 $x^2=y^2$、$x^2=q^2$、$p^2=y^2$ 和 $p^2=q^2$ 中必有一个成立；由引理 7.1 可知，条件（2）成立。这又导致了矛盾。

因此，$z\notin p*q$，故 $z\in p*q'$，同理，$z\in p'*q$。所以，对 (z,r) 确实具有性质 (i)、(ii) 和 (iii)。□

根据构造，运算 $\bullet$ 是交换的。由公式（13）可知，元素 $\varepsilon=(e,t)$ 是乘法 $\bullet$ 的单位元，也就是说，对于所有 $\alpha\in A$，都有 $\varepsilon\bullet\alpha=\alpha$。此外，由公式（18）可知，若 $t*x=[p,p']$，则 $(x,p)\bullet(x,p')=\varepsilon$。若 $\alpha=(x,p)\in A$，则我们将元素 (x,p') 记为 α^{-1}。那么 $(\alpha^{-1})^{-1}=\alpha$，且 $\varepsilon^{-1}=\varepsilon$。然而请注意，我们尚未证明逆元的唯一性，也就是说，尚未证明等式 $\alpha\bullet\beta=\varepsilon$ 蕴含 $\beta=\alpha^{-1}$。为了证明 $(A,\bullet)$ 是阿贝尔群，我们需要证明逆元的唯一性和乘法的结合律。证明将分为几个引理。

下一个引理可直接由以下事实得出：当 $p\leftrightarrow p'$、$q\leftrightarrow q'$ 和 $r\leftrightarrow r'$ 同时互换时，性质 (i)、(ii) 和 (iii) 不变。

引理 8.6. 对于任意两个元素 $\alpha,\beta\in A$，等式 $(\alpha\bullet\beta)^{-1}=\alpha^{-1}\bullet\beta^{-1}$ 成立。

引理 8.7. 对于任意两个元素 $\alpha,\beta\in A$，等式 $\alpha^{-1}\bullet(\alpha\bullet\beta)=\beta$ 成立。

证明。设 $\alpha=(x,p)$、$\beta=(y,q)$ 和 $\alpha\bullet\beta=(z,r)$；另设 $t*x=[p,p']$、$t*y=[q,q']$ 和 $t*z=[r,r']$。那么，三元组 (x,p,p')、(y,q,q') 和 (z,r,r') 满足性质 (i)、(ii) 和 (iii)。我们需要证明 $(x,p')\bullet(z,r)=(y,q)$。这意味着我们需要证明，若分别用三元组 (x,p',p)、(z,r,r') 和 (y,q,q') 替换三元组 (x,p,p')、(y,q,q') 和 (z,r,r')，性质 (i)、(ii) 和 (iii) 仍然成立。下面写出所需的性质：

(i') y 属于多重集 $x*z$、$p*r$ 和 $p'*r'$ 中的每一个；(ii') q 属于多重集 $x*r$ 和 $p'*z$ 中的每一个；(iii') q' 属于多重集 $x*r'$ 和 $p*z$ 中的每一个。

由引理 2.2 可立即得到，这三个性质的并集等价于最初的三个性质 (i)、(ii) 和 (iii) 的并集。□

推论 8.8. 对于任意元素 $\alpha\in A$，以 α 进行乘法运算会将集合 A 双射到其自身。特别地，如果 $\alpha\bullet\beta=\varepsilon$，那么 $\beta=\alpha^{-1}$，也就是说，逆元是唯一的。

对所有 $k \in \mathbb{Z}$，引入记号 $\tau = (t, e)$ 和 $\tau^k = (t^k, t^{k-1})$。用 $\mathcal{T} \subseteq A$表示由 τ^k, $k \in \mathbb{Z}$ 的所有元素构成的子集。通过直接验证性质 (i)、(ii) 和 (iii)，我们很容易得到以下结论。

引理 8.9. 等式 $\tau^k \bullet \tau^m = \tau^{k+m}$对所有 $k, m \in \mathbb{Z}$都成立。因此，集合 $\mathcal{T}$在运算 $\bullet$ 下是由元素 τ生成的循环群。

引理 8.10. 对于任意两个元素 $\alpha, \beta \in A$，等式 $\tau \bullet (\alpha \bullet \beta) = (\tau \bullet \alpha) \bullet \beta$成立。

证明。设 $\alpha = (x, p)$、$\beta = (y, q)$、$\alpha \bullet \beta = (z, r)$ 以及 $t * x = [p, p']$、$t * y = [q, q']$、$t * z = [r, r']$。则三元组 (x, p, p')、(y, q, q') 和 (z, r, r') 满足性质 (i)、(ii) 和 (iii)。根据公式（14），我们有 $\tau \bullet \alpha = (p', x)$ 和 $\tau \bullet (\alpha \bullet \beta) = (r', z)$。因此，我们需要证明

$$(p', x) \bullet (y, q) = (r', z). \tag{22}$$

让 $(p', x) \bullet (y, q) = (\zeta,$ {v8}。

我们先证明 $\rho = z$。事实上，根据乘法构造 $\bullet$，元素 ρ 必须属于多重集 $p' * q$ 和 $x * y$。然而，元素 z 也属于这两个多重集。假设 $\rho \neq z$。那么 $p' * q = x * y = [z, \rho]$。由引理 7.6 可知，存在一个元素 $u \in V$，使得 $p' = ux$ 和$q = uy$，或者 $p' = uy$ 和 $q = ux$。我们分别考察这两种情形。

1. 设 $p' = ux$ 和 $q = uy$。那么元素 t 属于多重集$x * p' = [u, ux^2]$ 和 $y * q = [u, uy^2]$。由于 $t \notin V$，可得 $t = ux^2 = uy^2$，因此$x^2 = y^2$。由引理 7.1 可知，对于某个元素 $v \in V$，有 $y = vx$。我们有$t * x = [ux, ux^3]$，因此 $p = ux^3$。于是，$\alpha = (x, ux^3)$，$\beta = (vx, uvx)$。现在由公式（18）可得 $\alpha \bullet \beta = (v, vt)$，也就是说，$z = v$ 和 $r = r' = vt$。我们需要证明的等式（22）可写为 $(ux, x) \bullet (vx, uvx) = (vt, v)$，这立即由公式（19）得出。

2. 令 $p' = uy$ 和 $q = ux$。由公式 (20) 和 (17) 可得

$$\alpha \bullet \beta = (x, p) \bullet (up', ux) = (uf', ux^2),$$
$$(\tau \bullet \alpha) \bullet \beta = (p', x) \bullet (up', x) = (up'^2, uf'),$$

其中 $x * p' = [t, f']$。由引理 7.2，得 $t * f' = [x^2, p'^2]$，因此（22）变为 es

$$\tau \bullet (uf', ux^2) = (up'^2, uf')$$

并可由公式（14）推出。

因此，我们已证明 $\rho = z$ 在所有情形下成立。我们需要证明 $\zeta = r'$。假设结论不成立。根据乘法构造，$\bullet$ 元素 ζ 必定属于多重集 $p' * y$ 和 $x * q'$。然而，元素 r' 也属于这两个集合。因此 $p' * y = x * q' = [\zeta, r']$。根据引理 7.6，这意味着存在一个元素 $u \in V$，使得 $p' = ux$ 和 $q' = uy$，或者 $p' = uy$ 和 $q' = ux$。我们分别考虑这些情形。

1. 设 $p' = ux$ 和 $q' = uy$。与上面的情形 1 类似，我们得到 $t = ux^2 = uy^2$ 和$y = vx$，其中 $v \in V$是某个元素。我们有 $t * x = [ux, ux^3]$，因此 $p = ux^3$。类似地，$q = uy^3 = uvx^3$。于是，$\alpha = (x, ux^3)$，$\beta = (vx, uvx^3)$。现在由公式 (17) 可得 $\alpha \bullet \beta = (vx^2, vf)$，其中 $x * p = [t, f]$。然而，$x * p = [ux^2, ux^4]$，所以 $f = ux^4$。因此 $z = vx^2 = uvt$ 和 $r = uvx^4$。我们有 $t * z = [uv, uvx^4]$，因此 $r' = uv$。等式 (22) 具有如下形式：$(ux, x) \bullet (vx, uvx^3) = (uv, uvt)$，这可由公式（18）立即推出。

2. 设 $p' = uy$ 和 $q' = ux$。由公式（19）可得

$$\alpha^{-1} \bullet \beta^{-1} = (x, p') \bullet (up', ux) = (ut, u) = u\tau.$$

因此，根据引理 8.6 和 8.9

$$\alpha \bullet \beta = u\tau^{-1},$$
$$\tau \bullet (\alpha \bullet \beta) = u\varepsilon,$$
$$(\tau \bullet (\alpha \bullet \beta)) \bullet \beta^{-1} = u\beta^{-1} = (p', x) = \tau \bullet \alpha,$$

因此，鉴于推论 8.8，我们得到所需的等式 (22)。

因此， $\zeta = r'$ 在所有情形下成立，由此完成引理的证明。 □

推论 8.11。 运算 $\bullet$ 限制在 $\mathcal{T} \times A \subseteq A \times A$ 上定义了循环群 $\mathcal{T}$ 在集合 A 上的作用，使得对于任意元素 α， $\beta \in A$ 以及任意整数 k，等式 $\tau^k \bullet (\alpha \bullet \beta) = (\tau^k \bullet \alpha) \bullet \beta$ 成立。

回想一下，公式 $v(x, p) = (vx, vp)$，$v \in V$, $(x, p) \in A$ 定义了交换群 V 在集合 A 上的作用。根据公式 (12)，该作用具有性质 $v(\alpha \bullet \beta) = (v\alpha) \bullet \beta$，对所有 $v \in V$, α, $\beta \in A$均成立。容易看出，群 V 和 $\mathcal{T}$ 在集合 A 上的作用彼此交换。因此，我们得到直积 $G = V \times \mathcal{T}$在集合 A上的作用，它具有如下性质

$$g(\alpha \bullet \beta) = (g\alpha) \bullet \beta \tag{23}$$

对于所有 $g \in G$、 α、 $\beta \in A$。容易看出，以下两个引理可由此性质以及关于运算 $\bullet$的逆元的唯一性推出。

引理 8.12。 运算 $\bullet$ 在 G-轨道 A/G的集合上诱导出良定义的交换的运算；关于此运算，轨道 $G\varepsilon$ 是单位元，并且每个轨道 $G\alpha$ 的逆元唯一，且与轨道 $G\alpha^{-1}$重合。

引理 8.13。 设集合 A 的元素 α_1、 α_2、 α_3、 β_1、 β_2、 β_3 满足：对于每个 i，元素 α_i和 β_i 属于同一个 G-轨道。那么，当且仅当 $(\beta_1 \bullet \beta_2) \bullet \beta_3 = \beta_1 \bullet (\beta_2 \bullet \beta_3)$ 时，有 $(\alpha_1 \bullet \alpha_2) \bullet \alpha_3 = \alpha_1 \bullet (\alpha_2 \bullet \alpha_3)$。

由上一个引理和引理 8.7，可轻易得出以下结论 s.

推论 8.14. 如果集合 A 的元素 α_1、 α_2、 α_3 满足：对于某个 i 或 α_i， α_i 属于 G-轨道 $G\varepsilon$，且对于某个 $i \neq j$, α_j^{-1} 属于同一个 G-轨道，那么$(\alpha_1 \bullet \alpha_2) \bullet \alpha_3 = \alpha_1 \bullet (\alpha_2 \bullet \alpha_3)$。

引理 8.15. 设集合 A 的元素 $\alpha = (x, p)$ 和 $\beta = (y, q)$ 满足： β与元素 α 和元素 α^{-1}均不属于同一个 G-轨道，并设$t * x = [p, p']$ 和 $t * y = [q, q']$。那么，元素 x、 p 和 p' 均不与元素 y、 q 和 q'中的任何一个属于同一个V-轨道。

证明。由等式 (14) 和 (15) 可知，元素 (x, p)、(p', x) 和 (p, s)（其中 $t * p = [x, s]$）属于同一个 G-轨道。类似地，元素 (y, q)、(q', y) 和 (q, z)（其中 $t * q = [y, z]$）也属于同一个 G-轨道。因此，如果元素 x、 p 和 p' 中的一个与元素 y、 q 和 q' 中的一个属于同一个 V-轨道，那么在元素 α 和 β 的 $\sim G$-轨道中，分别存在元素 $\widetilde{\alpha} = (\widetilde{x}, \widetilde{p})$ 和 $\beta = (\widetilde{y}, \widetilde{q})$, 使得对于某个 $v \in V$，有 $\widetilde{y} = v\widetilde{x}$。于是，要么 $\widetilde{q} = v\widetilde{p}$，要么 $\widetilde{q} = v\widetilde{p}'$，其中 $t * \widetilde{x} = [\widetilde{p}, \widetilde{p}']$。 ~因此，元素 β 与元素 $\widetilde{\alpha}$ 和 $\widetilde{\alpha}^{-1}$中的一个属于同一个 G-轨道，所以根据引理 8.12可知，元素 β 与元素 α 和 α^{-1}中的一个属于同一个 G-轨道。□

下一个引理直接由运算 $\bullet$ 的构造得出。

引理 8.16。 设 $\alpha_i=(x_i,\ p_i)$、 $i=1$、 2、 3 是集合 A *and* $t*x_i=[p_i,p_i']$ 的元素。设 $(z,\ r)=(\alpha_1\bullet\alpha_2)\bullet\alpha_3$ 以及 $t*z=[r,r']$。则

(1) 元素 z 属于多重集 $x_1*x_2*x_3$ 以及以下六个多重集中的每一个: $x_i*p_j*p_k'$, 其中 i、 j、 k 是数字 1、 2、 3 的所有可能排列; (2) 元素 r 属于三个多重集 $x_1*x_2*p_3$、 $x_1*p_2*x_3$和 $p_1*x_2*x_3$中的每一个; (3) 元素 r' 属于三个多重集 $x_1*x_2*p_3'$、 $x_1*p_2'*x_3$和 $p_1'*x_2*x_3$中的每一个。

引理 8.17. 设集合 A 中的元素 α_1、 α_2 和 α_3 分别属于两两不同的G-轨道。那么 $(\alpha_1\bullet\alpha_2)\bullet\alpha_3=\alpha_1\bullet(\alpha_2\bullet\alpha_3)\ =(\alpha_1\bullet\alpha_3)\bullet\alpha_2$.

证明。若元素 α_i 中任意一个属于 G-轨道 $G\varepsilon$ ，或者对某个 $i\neq j$，元素 α_i 和 α_j^{-1} 属于同一个 G- 轨道，则由推论 8.14 可得所需等式。因此，我们可以假设，元素 α_i 中没有任何一个与元素 ε 或任意一个元素 $\alpha_j^{\pm1}$ （其中 $j\neq i$）属于同一个 G-轨道。于是由引理 8.15 可知，首先，元素 x_i、 p_i 和 p_i'（其中 $i=1$、2、3）中没有任何一个属于 V 或 Vt; 其次，对于 $i\neq j$ ，元素 x_i、 p_i 和 p_i' 中没有任何一个与元素 x_j、 p_j 和 p_j' 中的任何一个属于同一个 V-轨道。

假设引理的陈述不成立，因此在所示的三种阶中的两种下，元素 α_1、α_2 和 α_3 的直积结果不同: $(z_1,r_1)\ \neq(z_2,r_2)$。设 $t*z_i=[r_i,r_i']$, $i=1,2$。注意，引理 8.16 中的性质 (1)–(3) 在元素 α_1、 α_2 和 α_3 的排列下保持不变，因此这些性质对两个三元组 (z_1,r_1,r_1') 和 (z_2,r_2,r_2') 均成立。

对数字 1、2、3 的每一种排列 i,j,k，令 $(y_i,q_i)\ =\alpha_j\bullet\alpha_k$。于是 $y_i\in x_j*x_k$和 $q_i\in t*y_i$。设 $x_j*x_k=[y_i,y_i']$ 和 $t*y_i=[q_i,q_i']$。

首先假设 $z_1\neq z_2$。根据引理 8.16 的性质 (1)，元素 z_1和 z_2 都属于多重集 $x_1*x_2*x_3$。然而，由于元素 x_1、x_2和 x_3 分别处于两两不同的 V-轨道中，由引理 7.7 可知，多重集 $x_1*x_2*x_3$ 由四个互不相同的元素组成，而 x_1*y_1 、 x_1*y_1'、 x_2*y_2、 x_2*y_2'、x_3*y_3和 x_3*y_3' 恰好是它的全部六个二元素子集。因此，这六个子集中有一个与集合 $[z_1,z_2]$重合。重新编号元素 α_1、 α_2、 α_3后，我们可以假设 $[z_1,z_2]=x_1*h$，其中 h 是元素 y_1 和 y_1'中的一个。

现在考虑多重集 $x_i*p_j*p_k'$，其中 i、 j、 k 是数 1、2、3 的排列。根据引理 8.16 的性质 (1)，这些多重集中的每一个都包含多重集 $[z_1,z_2]\ =\ x_1*h$。因此，由引理 7.8，对每个三元组 (x_i,p_j,p_k')，都存在一个元素 $v\in V$，使得该三元组中的一个元素等于 vx_1 和 vh 这两个元素之一，而该三元组中另外两个元素的直积包含 vx_1 和 vh 中剩下的那个元素。此外，根据已证明的结论，元素 x_2、 p_2、 p_2'、 x_3、 p_3、 p_3' 不可能属于轨道 Vx_1。另外，元素 p_1 和 p_1' 也不可能同时属于轨道 Vx_1，因为根据引理 7.5(c)，这将意味着 $\operatorname{ord}t$ 整除 4。分 3 种情形讨论。

1. 两个元素 p_1 和 p_1' 位于轨道 Vh中。 由于 p_1 和 p_1' 不可能同时位于轨道 Vx_1中，因此 $Vx_1\neq Vh$。由于 $\operatorname{ord}t\notin\{1,2,4\}$，根据引理 7.5(b)，我们有 $\operatorname{ord}x_1\in\{1,2,4\}$。元素 x_2、 p_2、 p_2'、 x_3、 p_3、 p_3'均不位于 Vx_1或$Vp_1=Vh$中。因此，根据引理 7.8，对于三元组 (x_i,p_j',p_k)、 $i=2$、3，可知多重集 x_2*p_3、 x_2*p_3'、 x_3*p_2和 x_3*p_2'都与轨道 Vx_1相交。于是，根据引理 2.2，多重集 x_1*x_2分别与轨道 Vp_3和 Vp_3'相交，而多重集 x_1*x_3分别与轨道 Vp_2和 Vp_2'相交。然而，由于

元素 x_1 的阶整除 4，因此根据引理 7.5(b)，多重集 x_1*x_2 和 x_1*x_3 各由两个属于同一 V-轨道的元素组成。因此，对于某些元素 w_2、$w_3 \in V$，有 $p_2' = w_2p_2$ 和 $p_3' = w_3p_3$。由于 $t * x_i = [p_i, p_i']$，现在根据引理 7.5(b)可知，元素 x_2 和 x_3 的阶也整除 4。注意，元素 t 属于二值群 X 中由集合 V 以及元素 x_1、x_2 和 x_3生成的子群。事实上，$t \in x_3 * p_3$，且元素 p_3 与多重集 $x_1 * x_2$中的元素处于同一 V-轨道。因此，根据引理 7.5(a)，我们得到元素 t 的阶整除 4，这就产生了矛盾。

2. 元素 p_1 和 p_1' 中的一个位于轨道 Vx_1 中，另一个属于轨道 Vh。由于 p_1 和 p_1' 不可能同时位于轨道 Vx_1 中，因此 $Vx_1 \neq Vh$。考虑 $p_1 \in Vx_1$ 和 $p_1' \in Vh$ 的情形；第二种情形完全类似。由以下事实：对于某个 $u \in V$，有 $p_1 = ux_1$，可推出 $t \in x_1 * p_1 = [u, ux_1^2]$，从而由于 $t \notin V$，有 $t = ux_1^2$。此外，由于 $t \notin V$，我们有 $x_1^2 \notin V$，这意味着元素 x_1 的阶不整除 4。于是，根据命题 3.2 的 (c) 项，所有元素 vx_1（其中 v 遍历群 V）两两不同。特别地，在 $v \neq e$ 下有 $vx_1 \neq x_1$，在 $v \neq u$ 下有 $vx_1 \neq ux_1$。此外，元素 x_2、p_2、p_2'、x_3、p_3、p_3' 中没有一个位于 Vx_1 或 $Vp_1 = Vh$ 中。因此，由三元组 (x_1, p_2, p_3')、(x_1, p_3, p_2')、(x_2, p_1, p_3') 和 (x_3, p_1, p_2') 的引理 7.8 可知，元素 h 同时属于多重集 $p_2 * p_3'$ 和 $p_3 * p_2'$，而元素 uh 同时属于多重集 $x_2 * p_3'$ 和 $x_3 * p_2'$。利用引理 2.2，我们由此得到，多重集 $h * p_2'$ 包含元素 ux_3 和 p_3，而多重集 $h * p_3'$ 包含元素 ux_2 和 p_2。如果等式 $p_2 = ux_2$ 成立，那么我们将得到 $t \in x_2 * p_2 = [u, ux_2^2]$，因而由于 $t \notin V$，有 $t = ux_2^2$。但由等式 $x_2^2 = ut = x_1^2$ 和引理 7.1 可推出，元素 x_1 和 x_2 位于同一个 V-轨道中，这是不正确的。因此，$ux_2 \neq p_2$，从而 $h * p_3' = [ux_2, p_2]$。同样，$ux_3 \neq p_3$ 且 $h * p_2' = [ux_3, p_3]$。于是由引理 7.2 可得，元素 h^2 属于多重集 $ux_2 * p_2$ 和 $ux_3 * p_3$。然而，元素 ut 也属于同样的两个多重集。此外，由引理 7.6 可知 $ux_2 * p_2 \neq ux_3 * p_3$，因为元素 x_2 和 p_2 中没有一个与元素 x_3 和 p_3 中的任何一个位于同一个 V-轨道中。因此，$h^2 = ut = x_1^2$，这根据引理 7.1 与 $Vh \neq Vx_1$ 矛盾。

3. 元素 p_1 和 p_1' 中至少有一个既不属于 Vx_1，也不属于 Vh。我们假设 $p_1' \notin Vx_1 \cup Vh$；第二种情形类似。在三元组 (x_2, p_3, p_1') 和 (x_3, p_2, p_1') 中，没有元素属于轨道 Vx_1；此外，元素 p_1' 不属于轨道 Vh。根据引理 7.8，对于这些三元组，元素 x_2 和 p_3 中至少有一个属于 Vh，而元素 x_3 和 p_2 中至少有一个属于 Vh。然而，元素 x_2 和 p_2 均不与元素 x_3 和 p_3 中的任何一个属于同一个 V-轨道。因此，要么 x_2、$p_2 \in Vh$ 且 x_3、$p_3 \notin Vh$，要么 x_2、$p_2 \notin Vh$ 且 x_3、$p_3 \in Vh$。这两种情形彼此类似，因此我们考虑第一种。令 $x_2 = uh$ 和 $p_2 = vh$，其中 u、$v \in V$。由等式 $p_2 = uvx_2$ 可得 $t \in x_2 * p_2 = [uv, uvx_2^2]$，因此 $t = uvx_2^2$，因为 $t \notin V$。现在回想一下，h 要么是 y_1，要么是 y_1'，因此 $h \in x_2 * x_3$。于是，$x_3 \in x_2 * h = [u, ux_2^2] = [u, vt]$，这与元素 x_3 既不属于 V 也不属于 Vt 矛盾。

所得矛盾证明了 $z_1 = z_2$。将该元素简单记为 z。考虑元素 $\beta_1 = \tau \bullet \alpha_1$、$\beta_2 = \alpha_2$、$\beta_3 = \alpha_3$ 组成的三元组。引理 8.10 意味着，对于数字 1、2、3 的所有排列 i、j、k，$\beta_i \bullet (\beta_j \bullet \beta_k) = \tau \bullet (\alpha_i \bullet (\alpha_j \bullet \alpha_k))$。因此，由元素 α_1、α_2 和 α_3 按两种不同顺序所得的直积分别等于 (z, r_1) 和 (z, r_2)，以及公式（14），可知元素 β_1、β_2 和 β_3 按相同的两种顺序所得的直积分别等于 $\tau \bullet (z, r_1) = (r_1', z)$ 和 $\tau \bullet (z, r_2) = (r_2', z)$，其中 $t * z = [r_1, r_1'] = [r_2, r_2']$。元素 β_1、β_2、

以及 β_3 也分别属于不同的 G-轨道。对它们重复上述关于元素 α_1、 α_2 和 α_3 的论证，即证明 $z_1 = z_2$，我们得到 $r_1' = r_2'$，因此 $r_1 = r_2$ □

引理 8.18。对于集合 A 中的任意元素 α ，我们有以下等式$(\alpha \bullet \alpha) \bullet (\alpha \bullet \alpha) = \alpha \bullet (\alpha \bullet (\alpha \bullet \alpha))$。

证明。考虑三个元素 α、 $\beta = \alpha \bullet (\alpha \bullet \alpha)$ 和 $\gamma = (\alpha \bullet \alpha)^{-1}$。首先假设 α 和 β 属于不同的 G-轨道，并且 β 和 γ 属于不同的 G-轨道。那么

$$(\alpha \bullet \beta) \bullet \gamma = \alpha \bullet (\beta \bullet \gamma). \tag{24}$$

事实上，若 α、 β 和 γ 属于三个两两不同的 G-轨道，则由引理 8.17 可得 (24)；若 α 和 γ 属于同一个 G-轨道，则根据引理 8.13，等式 (24) 等价于成立的等式 $(\alpha \bullet \beta) \bullet \alpha = \alpha \bullet (\beta \bullet \alpha)$。利用等式 (24) 和引理 8.7，我们得到

$$\begin{aligned}\big((\alpha \bullet \alpha) \bullet (\alpha \bullet \alpha)\big) \bullet (\alpha \bullet \alpha)^{-1} &= \alpha \bullet \alpha,\\ \big(\alpha \bullet (\alpha \bullet (\alpha \bullet \alpha))\big) \bullet (\alpha \bullet \alpha)^{-1} &= (\alpha \bullet \beta) \bullet \gamma = \alpha \bullet (\beta \bullet \gamma)\\ &= \alpha \bullet \big(\big(\alpha \bullet (\alpha \bullet \alpha)\big) \bullet (\alpha \bullet \alpha)^{-1}\big) = \alpha \bullet \alpha.\end{aligned}$$

应用推论 8.8，即得引理的结论。

剩下需要考虑的情形是：某些元素 α 和 γ 与元素 β位于同一个G-轨道中。

假设元素 α 和 $\beta = \alpha \bullet (\alpha \bullet \alpha)$ 位于同一个 G-轨道中。于是根据引理 8.12，元素 $\alpha \bullet \alpha$ 与元素 ε位于同一个 G-轨道中，因此元素 α 和 α^{-1} 位于同一个 G-轨道中。在这种情形下，所要证明的等式可由推论 8.14 应用于三元组 $\alpha, \alpha, \alpha \bullet \alpha$ 得出。

现在假设元素 $\beta = \alpha \bullet (\alpha \bullet \alpha)$ 和 $\gamma = (\alpha \bullet \alpha)^{-1}$ 位于同一个G-轨道中。那么对于某些 $v \in V, k \in \mathbb{Z}$，有 $\beta = v\tau^k \bullet \gamma$。于是根据引理 8.6

$$\alpha \bullet \alpha = \gamma^{-1} = v\tau^k \bullet \beta^{-1} = v\tau^k \bullet \left(\alpha^{-1} \bullet (\alpha \bullet \alpha)^{-1}\right).$$

应用引理 8.6 和 8.7 以及推论 8.11，我们得到

$$\begin{aligned}(\alpha \bullet \alpha) \bullet (\alpha \bullet \alpha) &= (\alpha \bullet \alpha) \bullet \left(v\tau^k \bullet \left(\alpha^{-1} \bullet (\alpha \bullet \alpha)^{-1}\right)\right)\\ &= v\tau^k \bullet \left((\alpha \bullet \alpha) \bullet \left(\alpha^{-1} \bullet (\alpha \bullet \alpha)^{-1}\right)\right) = v\tau^k \bullet \alpha^{-1},\\ \alpha \bullet (\alpha \bullet (\alpha \bullet \alpha)) &= \alpha \bullet \left(v\tau^k \bullet (\alpha \bullet \alpha)^{-1}\right) = v\tau^k \bullet \left(\alpha \bullet \left(\alpha^{-1} \bullet \alpha^{-1}\right)\right) = v\tau^k \bullet \alpha^{-1},\end{aligned}$$

至此，引理的证明完成。 □

引理 8.19. 对于集合 A中的任意元素 α 和 β，等式 $(\alpha \bullet \alpha) \bullet \beta = \alpha \bullet (\alpha \bullet \beta)$成立。

证明。首先假设元素 α 和 β^{-1} 均不与元素 $\alpha \bullet \beta$处于同一个 G-轨道中。利用引理 8.17、8.13 和 8.7，我们得到

$$(\alpha \bullet (\alpha \bullet \beta)) \bullet \beta^{-1} = \alpha \bullet ((\alpha \bullet \beta) \bullet \beta^{-1}) = \alpha \bullet \alpha.$$

将等式两边同乘 β，并再次利用引理 8.7，我们得到所需的等式 $\alpha \bullet (\alpha \bullet \beta) = (\alpha \bullet \alpha) \bullet \beta$。

接下来考虑某些元素 α 和 β^{-1} 与元素 $\alpha \bullet \beta$处于同一个G-轨道中的情形。

假设元素 α 和 $\alpha \bullet \beta$ 属于同一个 G-轨道。由公式（23）和引理 8.7 可知，元素 $\varepsilon = \alpha^{-1} \bullet \alpha$ 和 $\beta = \alpha^{-1} \bullet (\alpha \bullet \beta)$ 也属于同一个 G-轨道。在这种情形下，待证结论立即由推论 8.14 得出。

现在假设元素 $\alpha \bullet \beta$ 和 β^{-1} 属于同一个 G-轨道。由引理 8.12 和引理 8.7 可知，元素 α 与元素 $\beta^{-1} \bullet \beta^{-1}$属于同一个 G-轨道。因此，由引理 8.13 可知，三元组（α, α, β）所需满足的结合性等价于三元组$(\beta^{-1} \bullet \beta^{-1}, \beta^{-1} \bullet \beta^{-1}, \beta)$所需满足的结合性。然而，利用引理 8.18 和引理 8.7，我们得到

$$\begin{aligned}\big((\beta^{-1} \bullet \beta^{-1}) \bullet (\beta^{-1} \bullet \beta^{-1})\big) \bullet \beta &= \big(\big((\beta^{-1} \bullet \beta^{-1}) \bullet \beta^{-1}\big) \bullet \beta^{-1}\big) \bullet \beta \\ &= (\beta^{-1} \bullet \beta^{-1}) \bullet \beta^{-1} = (\beta^{-1} \bullet \beta^{-1}) \bullet \big((\beta^{-1} \bullet \beta^{-1}) \bullet \beta\big).\end{aligned}$$

引理得证。 □

现在我们终于可以完整地证明乘法的结合律 $\bullet$。

引理 8.20。 对于集合 A 中的任意元素 α_1、α_2 和 α_3，等式 $(\alpha_1 \bullet \alpha_2) \bullet \alpha_3 = \alpha_1 \bullet (\alpha_2 \bullet \alpha_3)$ 成立。

证明。若元素 α_1、α_2 和 α_3 分别属于两两不同的 G-轨道，则所需等式由引理 8.17 得出；若这三个元素中有两个属于同一个 G-轨道，则该等式由引理 8.19 和引理 8.13 得出。□

命题 8.3 的命题（b）由推论 8.8 和引理 8.20 得出；命题（c）则直接由命题（a）和（b）得出。

9. 由阶为 1、2 和 4 的元素构成的非特殊二值群

定理 9.1。 设 X 是一个有限生成的非特殊幂等交换二值群，不含单值直因子，且完全由阶为 1、2 和4 的元素组成。那么， X 同构于以下两个系列中的某个群：

(1) $X^{\mathbf{a}}_{n\times 4} = C_4^n/\iota_{\mathbf{a}}$，其中 $\iota_{\mathbf{a}}(a) = a^{-1}$；(2) $X^{\mathbf{u}}_n = (C_2^n \times C_2^n)/\iota_{\mathbf{u}}$，其中 $\iota_{\mathbf{u}}(a,\ b) = (a,\ ab)$。

两个二值群 $X^{\mathbf{a}}_{n\times 4}$ 和 $X^{\mathbf{u}}_n$ 均由 $2^{2n-1}+2^{n-1}$ 个元素组成。当 $n \le 2$ 时，这两个二值群同构；而当 $n \ge 3$ 时，它们不同构。

设 X 是一个满足定理 9.1 条件的二值群，$V \subseteq X$ 是由所有阶为 1 和 2 的元素组成的子群。对于每个元素 $x \in X \setminus V$，其阶为 4，因此其平方 x^2 的阶为 2，即 $x^2 \in V \setminus \{e\}$。对于每个元素 $v \in V$，记 $X_v \subseteq X$ 为由所有满足 $x^2 = v$ 的元素 x 组成的子集。于是，对于 $v \ne e$，$X_e = V$ 和 X_v 均由 4 阶元素组成。根据命题 6.2，X 不含单值直因子这一事实意味着所有子集 X_v 都非空。此外，引理 7.1、推论 7.4 和引理 7.5(b) 立即推出以下陈述。

引理 9.2. 每个集合 X_v 都是一个 V-轨道。对于 $v \ne e$，该轨道中元素的稳定子是二元群 $\{e, v\}$。如果 $x \in X_u$、$y \in X_v$ 和 $x * y = [z_1, z_2]$，那么$z_1, z_2 \in X_{uv}$ 和 $z_2 = uz_1 = vz_1$。

推论 9.3. 如果二值群 X 是有限生成的，那么布尔群 V 是有限的。

证明。令 X 由 x_1、……、x_N中的元素生成，并令 $x_i \in X_{v_i}$ 位于 $i = 1$、……、N之下。于是，任何形如 $x_{i_1} * \cdots * x_{i_k}$的多重集都由属于轨道 X_v的元素组成，其中 $v = v_{i_1}^{\pm 1} \cdots v_{i_k}^{\pm 1}$。因此，轨道 X_v的并集（其中 v遍历由元素 v_1、……、v_N生成的子群）就是整个二值群 X。所以，元素 v_1、……、v_N生成整个群 V，故 $\dim V \le N$。□

推论 9.4。 若维数$V = n < \infty$，则二值群 X 恰好由$2^{2n-1} + 2^{n-1}$ 个元素组成。

在每个子集 X_v、 $v \in V$ 中，我们选取一个代表元 x_v，并将单位元 e 作为 x_e 。引理 9.2 推出

$$x_u * x_v = \big[\varphi(u,v)x_{uv}, u\varphi(u,v)x_{uv}\big] = \varphi(u,v)[x_{uv}, ux_{uv}] \tag{25}$$

存在某个元素 $\varphi(u,v) \in V$，满足

$$\varphi(u,v) \equiv \varphi(v,u) \pmod{\langle u,v\rangle}, \tag{26}$$

$$\varphi(u,u) \equiv e \pmod{\langle u\rangle}, \tag{27}$$

$$\varphi(e,u) \equiv \varphi(u,e) \equiv e \pmod{\langle u\rangle}, \tag{28}$$

其中，我们用 $\langle v_1$、……、 $v_k\rangle$ 表示由 v_1、……、 v_k 中的元素生成的子群。

注意，条件 (25) 并不能唯一确定元素 $\varphi(u,v)$，而只能将其确定到相差子群 $\langle u,v\rangle$ 中的一个元素的乘法。该子群由 u 和 v 生成。事实上，分别乘以元素 u 和 v ，只会重新排列多重集 $x_u * x_v$ 中的元素。

容易看出，二值群 X 中的乘法可以由构造出的映射 $\varphi\colon V \times V \to V$ 完全恢复。现在我们写出条件，使得满足 (26)–(28) 的映射 φ 确实定义了 X 上的结合乘法。对任意的 u、 v、 $w \in V$，有

$$\begin{aligned}(x_u * x_v) * x_w &= \varphi(u,v)[x_{uv}, ux_{uv}] * x_w \\ &= \varphi(u,v)\varphi(uv,w)[x_{uvw}, ux_{uvw}, vx_{uvw}, wx_{uvw}]\end{aligned}$$

and

$$\begin{aligned}x_u * (x_v * x_w) &= x_u * \varphi(v,w)[x_{vw}, vx_{vw}] \\ &= \varphi(v,w)\varphi(u,vw)[x_{uvw}, ux_{uvw}, vx_{uvw}, wx_{uvw}].\end{aligned}$$

由于元素 x_{uvw} 被群 V 中的元素 e 和 uvw 稳定，而不被该群的任何其他元素稳定，因此这两个多重集相同这一条件可写为一个包含关系

$$\varphi(u,v)\varphi(uv,w)\varphi(u,vw)\varphi(v,w) \in \langle u,v,w\rangle \tag{29}$$

如果我们不选择集合 X_v 的代表元集合 $\{x_v\}$，而改选另一个代表元集合 $\{x'_v\}$，其中同样有 $x'_e = e$，那么对于某个 $\chi(v) \in V$，有 $x'_v = \chi(v)\, x_v$，使得 $\chi(e) = e$。此时，映射 φ 将被公式给出的映射取代

$$\varphi'(u,v) = \varphi(u,v)\chi(u)\chi(v)\chi(uv).$$

鉴于如上所述，值 $\varphi(u, v)$ 仅在相差群 $\langle u$ 中某个元素的乘法意义下确定，因此更准确地说，应当由某个映射 φ' 取代 φ，使得

$$\varphi'(u,v) \equiv \varphi(u,v)\chi(u)\chi(v)\chi(uv) \pmod{\langle u,v\rangle}. \tag{30}$$

我们将满足条件 (28) 和 (29) 的映射 $\varphi\colon V \times V \to V$ 称为布尔群 V 上的拟余循环。如果拟余循环 φ 满足条件 (26)，则称其为对称的；如果满足条件 (27)，则称其为对合的。如果存在映射 $\chi\colon V \to V$，使得 $\chi(e) = e$，并且对于所有 u、 $v \in V$，同余式 (30) 成立，则称两个拟余循环 φ 和 φ' 是上同调等价的。特别地，如果一个拟余循环与恒等于 1 的拟余循环上同调等价，则称其为上同调平凡的。

由于公式 (25) 中的拟余循环 φ 的值 $\varphi(u,v)$ 仅在乘以来自 $\langle u、\ v\rangle$ 的元素的意义下确定，因此，称 V 上的两个拟余循环 φ 和 φ' 是等价的，如果对于所有 $u、\ v\in V$，都有同余式 $\varphi(u,v)\equiv\varphi'(u,v)$ (模 $\langle u、\ v\rangle$)。

以下命题可由上述内容立即得到。

命题 9.5。有限生成的非特殊对合交换二值群 X 不含单值直因子，并且由阶为 1、2 或 4 的元素组成，则完全由一个布尔群 V 和一个对合对称拟余循环 φ: $V\times V\to V$ 确定。与各对 $(V,\ \varphi)$ 和 $(V',\ \varphi')$ 相对应的二值群同构，当且仅当存在群 V 与 V' 的一个同构，将拟余循环 φ 映射为一个与拟余循环 φ' 上同调等价的拟余循环。

上述术语的由来如下。设 G 是一个群，A 是一个采用加法记号的阿贝尔群。回顾上同调群 $H^*(G;\ A)$ 的定义，参见 [2, 第 III 章，§1]。

对于每个 $k\geq 0$，考虑由以下映射组成的群 $\mathcal{C}^k(G;A)$

$$\varphi\colon \underbrace{G\times\cdots\times G}_{k}\to A$$

使得若元素 g_i 中至少有一个等于 e，则 $\varphi(g_1,\ldots,g_k)=0$。微分$\delta$: $\mathcal{C}^k(G;\ A)\to\mathcal{C}^{k+1}(G;\ A)$ 由以下公式定义

$$(\delta\varphi)(g_1,g_2,\ldots,g_{k+1})=\varphi(g_2,\ldots,g_{k+1})+\sum_{i=1}^{k}(-1)^i\varphi(g_1,\ldots,g_ig_{i+1},\ldots,g_{k+1})+(-1)^{k+1}\varphi(g_1,\ldots,g_k).$$

属于该映射的核的映射 φ 称为群 G上取值于 A 的 k-余循环 。上同调群 $H^k(G;A)$ 按定义是由群 G 上取值于 A 的 k-余循环所成的群，模去子群 $\delta\mathcal{C}^{k-1}(G;A)$ 后得到的商群。

若群 A 是布尔群，且我们对其使用乘法记号，则 2-余循环的方程可写为

$$\varphi(u,v)\varphi(uv,w)\varphi(u,vw)\varphi(v,w)=e \tag{31}$$

对所有 $u、\ v、\ w\in G$ 均成立。此外，两个余循环 φ 和 φ' 上同调等价，当且仅当存在映射 χ: $G\to A$，使得 $\chi(e)=e$，并且

$$\varphi'(u,v)=\varphi(u,v)\chi(u)\chi(v)\chi(uv)$$

对所有 $u,v\in G$ 均成立。因此，上述拟余循环的定义是这些条件的弱化版本。

命题 9.5 将我们的分类问题——分类不含单值直因子且由阶为 1、2 和 4 的元素构成的有限生成非特殊对合交换二值群——归结为在上同调意义下分类布尔群上的对合对称拟余循环。在 V 上的对合对称拟余循环的上同调类集合 $\mathcal{H}(V)$ 上，乘法运算定义了阿贝尔群的结构。我们的任务是计算这个群。在解决这个问题之前，我们注意到，对于严格满足方程 (31) 的真正余循环，一个类似的问题是显然的。

引理 9.6。 设 V 和 W 为布尔群，且 $\varphi\colon\ V\times V\to W$ 是一个对合对称余循环，也就是说，它是满足余循环方程 (31)及以下方程的映射

$$\varphi(u,v)=\varphi(v,u), \tag{32}$$

$$\varphi(u,u)=\varphi(e,u)=\varphi(u,e)=e. \tag{33}$$

于是 φ 是上同调平凡的，也就是说，对于某个 $\chi\colon\ V\to W$，有 $\varphi=\delta\chi$，使得 $\chi(e)=e$。

证明。显然，只需证明 $W=\mathbb{F}_2$这一情形下的引理。（在这种情形下，当然我们将用加法记号表示 $\mathbb{F}_2$。）设 $\dim V=n$，且 $b_1,\dots,b_n$是布尔群 V作为 $\mathbb{F}_2$上向量空间的一组基。于是

$$H^*(V;\mathbb{F}_2)=H^*\left((\mathbb{RP}^\infty)^n;\mathbb{F}_2\right)=\mathbb{F}_2[t_1,\dots,t_n],$$

其中 $t_1,\dots,t_n$是空间 $H^1(V;\mathbb{F}_2)=\mathrm{Hom}(V,\mathbb{F}_2)$ 的一组基，它与基 $b_1,\dots,b_n$对偶。因此，余循环 φ的上同调类具有如下形式$\sum\lambda_i t_i^2+\sum_{i<j}\mu_{ij}t_it_j$，其中 $\lambda_i,\mu_{ij}\in\mathbb{F}_2$。由上同调中的乘法定义立即可得，$\lambda_i=\varphi(b_i,b_i)$，且 $\mu_{ij}=\varphi(b_i,b_j)+\varphi(b_j,b_i)$。因此，由方程 (32) 和 (33) 可知，余循环 φ 的上同调类为零。□

现在给出一个对合对称拟余循环的非平凡例子。设$\mathcal{B}=\{b_i\}_{i\in\Lambda}$ 是布尔群 V（作为 $\mathbb{F}_2$上的向量空间）的一组基。于是，该群的每个元素 V都可以唯一地写成 $b_I=\prod_{i\in I}b_i$的形式，其中 $I\subseteq\Lambda$ 是一个有限子集；特别地，$b_\varnothing=e$。令

$$\varphi_{\mathcal{B}}(b_I,b_J)=b_{I\cap J}. \tag{34}$$

条件 (26)–(29) 可以直接验证，因此 $\varphi_{\mathcal{B}}$确实是 V上的对合对称拟余循环。关于群 $\mathcal{H}(V)$，我们的主要结果如下。

命题 9.7。 (1) 如果$\dim V\le 2$，那么 V上的每个对合对称拟余循环都是平凡的，因此群 $\mathcal{H}(V)$ 是平凡群。

(2) 如果 $3\le\dim V<\infty$，则由公式(34) 定义的拟余循环 $\varphi_{\mathcal{B}}$ 是上同调非平凡的。在这种情形下，V上的每个对合对称拟余循环都与平凡拟余循环或拟余循环 $\varphi_{\mathcal{B}}$ 中的一个上同调等价。（特别地，与不同基 $\mathcal{B}$ 相对应的拟余循环 $\varphi_{\mathcal{B}}$ 彼此上同调等价。）因此，$\mathcal{H}(V)$ 是阶为2的循环群。

我们将把这一命题的证明推迟到下一节，现在先说明定理 9.1 如何由此推出。为此，我们计算与二值群 $X^{\mathbf{a}}_{n\times 4}$ 和 $X^{\mathbf{u}}_n$ 对应的拟余循环 φ。

1. 考虑二值群 $X=X^{\mathbf{u}}_n=(C_2^n\times C_2^n)/\iota_{\mathbf{u}}$，其中 $\iota_{\mathbf{u}}(a,b)=(a,ab)$。二值群 X 中的 2 阶元素所成的群恰好是子群$V=\{e\}\times C_2^n\subset C_2^n\times C_2^n$，它由对合 $\iota_{\mathbf{u}}$ 固定的元素组成。将v与 (e,v) 对应起来，我们将 C_2^n 与 V 对应起来。对于任意 $v\in V=C_2^n$，子集 $X_v\subset X$ 由以下元素在投影 $\pi\colon C_2^n\times C_2^n\to X$下的像组成：所有形如 (v,w) 且满足 $w\in C_2^n$ 的元素。我们在此子集中选取一个代表元 $x_v=\pi(v,e)=\pi(v,v)$。于是

$$x_u*x_v=[x_{uv},ux_{uv}],$$

因此，二值群 $X^{\mathbf{u}}_n$ 对应于群 C_2^n上的平凡拟余循环。

2. 考虑二值群 $X=X^{\mathbf{a}}_{n\times 4}=C_4^n/\iota_{\mathbf{a}}$，其中 $\iota_{\mathbf{a}}(a)=a^{-1}$。令$\{a_i\}_{i\in\Lambda}$ 为直积 C_4^n 的标准生成元系。X 中阶为 2 的元素所成的群恰好是子群 $V=C_2^n\subset C_4^n$，它由在对合 $\iota_{\mathbf{a}}$下不变的元素组成。布尔群 V的基 $\mathcal{B}=\{b_i\}_{i\in\Lambda}$ 由以下元素组成：

$b_i = a_i^2$。群 V的任意元素都具有形式 $b_I = \prod_{i\in I} b_i$，其中$I \subseteq \Lambda$ 是一个有限子集。作为子集 $X_{b_I} \subset X$ 的代表元 x_{b_I}，我们取元素 $a_I = \prod_{i\in I} a_i$在投影 π下的像： $C_4^n \to X$。我们有 $a_I a_J = b_{I\cap J} a_{I\Delta J}$,$a_I^{-1} a_J = b_{I\setminus J} a_{I\Delta J}$，其中 $I\Delta J$是集合 I与 J的对称差。因此

$$x_{b_I} * x_{b_J} = [b_{I\cap J} x_{b_{I\Delta J}}, b_{I\setminus J} x_{b_{I\Delta J}}] = b_{I\cap J}[x_{b_{I\Delta J}}, b_I x_{b_{I\Delta J}}].$$

因此，二值群 $X^{\mathbf{a}}_{n\times 4}$ 对应于群 C_2^n上的拟余循环 $\varphi_{\mathcal{B}}$。

定理 9.1 由上述计算以及命题 9.5 和 9.7 立即得出。还请回忆，例 1.11 中描述了二值群$X^{\mathbf{a}}_{4,\ 4}$与 $X_2^{\mathbf{u}}$之间的显式同构。

10. 布尔群上的拟余循环

本节将证明命题 9.7。由 $\dim V \le 2$ 时，任意一对不同的非平凡元素 u、$v \in V$ 都满足 $\langle u\ 、\ v\rangle = V$ 这一事实可立即得出， V 上的每个对合对称拟余循环都等价，因此与平凡拟余循环上同调等价。由此，命题 9.7 的陈述 (1) 得证。

我们将陈述 (2) 的证明分成几个引理。

引理 10.1。 设 V 是含8 个元素的布尔群，也就是说，它是 $\mathbb{F}_2$ 上的三维向量空间。那么 $\mathcal{H}(V)$ 是一个二阶循环群。如果 $\mathcal{B}$ 是布尔群 V 的一组基，那么拟余循环 $\varphi_{\mathcal{B}}$ 的上同调类是群 $\mathcal{H}(V)$ 的一个生成元。

证明。设 φ 是 V 上的一个对合对称拟余循环。如果 u 和 v 是 V 中不同的非平凡元素，那么群 V 关于子群 $\langle u、\ v\rangle$只有两个陪集。若 $\varphi(u,v) \in \langle u,\ v\rangle$，则令 $\lambda(u,v) = 0$；若 $\varphi(u,v) \notin \langle u,\ v\rangle$，则令 $\lambda(u,v) = 1$。于是 $\lambda(u,v) = \lambda(v,u)$。三元组 (u,v,uv) 的余循环条件 (29) 可写为 $\lambda(u,v) = \lambda(v,uv)$，这意味着值 $\lambda(u,v)$ 仅取决于二维子空间 $\langle u、\ v\rangle \subset V$，而与其基 u、v 的具体选择无关。此外，向量空间 V 的二维子空间与对偶向量空间 $V^* = \mathrm{Hom}(V,\mathbb{F}_2)$ 的非平凡元素之间存在自然的一一对应。因此，我们得到一个良定义映射 $\lambda\colon V^*\setminus\{e\} \to \mathbb{F}_2$。容易看出，等价的拟余循环 φ 导出相同的映射 λ，并且拟余循环 φ 在等价意义下可由映射 λ 唯一确定。

现在我们来证明，对于任意映射 $\lambda\colon V^*\setminus\{e\} \to \mathbb{F}_2$，都对应着一个拟余循环的等价类。为此，我们首先计算与拟余循环 $\varphi_{\mathcal{B}}$相对应的映射 $\lambda_{\mathcal{B}}$，其中 $\mathcal{B} = \{b_1,b_2,b_3\}$ 是布尔群 V的一组基。直接计算可得 $\lambda_{\mathcal{B}}(\xi_{\mathcal{B}}) = 1$，其中 $\xi_{\mathcal{B}} \in V^*$是一个元素，满足 $\xi_{\mathcal{B}}(b_1) = \xi_{\mathcal{B}}(b_2) = \xi_{\mathcal{B}}(b_3) = 1$，且对所有 $\xi \ne \xi_{\mathcal{B}}$都有 $\lambda_{\mathcal{B}}(\xi) = 0$。关于逐点乘法， V 上的拟余循环构成一个群，拟余循环的直积对应于相应映射 λ的逐点加法。因此，很容易看出，对于不同的 $\mathcal{B}$，将拟余循环 $\varphi_{\mathcal{B}}$ 相乘，可以得到任意映射 $\lambda\colon V^*\setminus\{e\} \to \mathbb{F}_2$作为 λ。由于集合 $V^*\setminus\{e\}$ 含有 7 个元素， V 上恰有 128 个拟余循环的等价类。

现在我们来看看，如何用映射 λ 来改写两个余循环的上同调等价。对于映射 $\lambda\colon V^*\setminus\{e\} \to \mathbb{F}_2$，我们定义

$$\sigma(\lambda) = \sum_{\xi\in V^*\setminus\{e\}} \lambda(\xi).$$

我们来证明，与映射 λ 和 λ' 对应的拟余循环上同调等价，当且仅当 $\sigma(\lambda) = \sigma(\lambda')$。

对于两个元素 a、$b \in V \setminus \{e\}$，考虑映射 $\chi_{a,\,b}$: $V \to V$使得 $\chi_{a,\,b}(a) = b$且 $\chi_{a,\,b}(u) = e$ 在 $u \neq a$ 下成立。考虑通过映射 $\chi_{a,\,b}$使彼此上同调等价的两个拟余循环:

$$\varphi'(u,v) = \varphi(u,v)\chi_{a,b}(u)\chi_{a,b}(v)\chi_{a,b}(uv),$$

并比较与它们对应的映射 λ、λ': $V^* \setminus \{e\} \to \mathbb{F}_2$。直接计算表明

$$\lambda'(\xi) = \begin{cases} \lambda(\xi) + 1, & \text{if } \xi(a) = 0 \text{ and } \xi(b) = 1, \\ \lambda(\xi), & \text{otherwise.} \end{cases}$$

因此，如果 $a = b$，则拟余循环 φ 和 φ' 等价且 $\lambda = \lambda'$；如果$a \neq b$，则对于恰好两个元素 $\xi \in V^* \setminus \{e\}$，$\lambda'(\xi) \neq \lambda(\xi)$。因此，首先，$\sigma(\lambda') = \sigma(\lambda)$；其次，通过选取一对 (a,b)，我们可以改变集合 $V^* \setminus \{e\}$ 中任意两个预先指定元素上的映射 λ。由于任意映射 χ: $V \to V$ 都可以表示为不同的对 (a,b) 所对应的形如 χ_{a}、$_{b}$ 的映射的逐点乘积，我们得到：与映射 λ、λ': $V^* \setminus \{e\} \to \mathbb{F}_2$ 对应的拟余循环的等价类属于同一个上同调类，当且仅当 $\sigma(\lambda) = \sigma(\lambda')$。因此，$\mathcal{H}(V)$ 是二阶循环群。由于对于群 V 的任意基 $\mathcal{B}$，$\sigma(\lambda_{\mathcal{B}}) = 1$，所有拟余循环 $\varphi_{\mathcal{B}}$ 都是上同调等价的，并且它们的上同调类生成群 $\mathcal{H}(V)$。□

设 V为一个布尔群，且 φ: $V \times V \to V$为一个拟余循环。若 $U \subset V$为一个子群，且 Π: $V \to U$ 为一个投影，则映射

$$U \times U \subset V \times V \xrightarrow{\varphi} V \xrightarrow{\Pi} U$$

我们将其称为沿投影 Π将拟余循环 φ 限制到子群 U 上的限制。容易看出，这是 U上的一个拟余循环。此外，如果原拟余循环是对合的且对称的，那么所得的 U上的拟余循环也具有相同性质。沿投影 Π 取限制的运算诱导出一个同态Π_*: $\mathcal{H}(V) \to \mathcal{H}(U)$。

引理 10.2。设 V为一个有限布尔群，满足维数 $V > 3$，且 Π: $V \to U$为到某个子群 $U \subset V$ 上的投影，并满足维数$U = 3$。则同态Π_*: $\mathcal{H}(V) \to \mathcal{H}(U)$ 是满射。

证明。设 $\mathcal{B}$ 是布尔群 V 的一个基，其中一部分是子群 U 的一个基 $\mathcal{A}$。那么，拟余循环 $\varphi_{\mathcal{B}}$ 沿 Π 的限制与拟余循环 $\varphi_{\mathcal{A}}$ 重合。这立即推出同态 Π_* 的满射性，因为根据引理 10.1，群 $\mathcal{H}(U)$ 由拟余循环 $\varphi_{\mathcal{A}}$ 的上同调类生成。□

引理 10.3。设 V 是一个有限布尔群，Π: $V \to U$ 是到 $U \subset V$ 的某个子群上的投影，且 维数 $U \geq 3$。则同态 Π_*: $\mathcal{H}(V) \to \mathcal{H}(U)$ 是单射。

证明。注意，只需证明子群 U 在 V 中余维 1 时的情形（若将 V 视为 $\mathbb{F}_2$ 上的向量空间）即可；一般情形将通过归纳法自动推出。记 Π 的投影的一维核的生成元为 c。于是 $V = U \times \langle c \rangle$。

设 φ 是定义在 V 上的对合对称拟余循环，ψ 是沿 Π 对其在 U 上的限制。我们需要证明，若 ψ 上同调平凡，则 φ 也上同调平凡。

由拟余循环 ψ 的上同调平凡性可知，存在映射 $\xi\colon U \to U$，使得 $\xi(e) = e$ 且 $\varphi(u_1,u_2)\xi(u_1)\xi(u_2)\xi(u_1u_2) \in \langle u_1,u_2,c\rangle$ 对任意 $u_1,u_2 \in U$ 均成立。我们令 $\chi(u) = \xi(u)$，且对所有 $u \in U$，令 $\chi(uc) = \xi(u)\varphi(u,c)$，并考虑由公式定义在 V 上的对合对称拟余循环 φ'

$$\varphi'(v,w) = \varphi(v,w)\chi(v)\chi(w)\chi(vw).$$

于是，拟余循环 φ' 与 φ 上同调等价，并且

$$\varphi'(u_1,u_2) \equiv c^{\lambda(u_1,u_2)} \pmod{\langle u_1,u_2\rangle}, \qquad u_1,u_2 \in U, \tag{35}$$

其中 $\lambda\colon U\times U \to \mathbb{F}_2$ 是满足 $\lambda(u_1,u_2) = \lambda(u_2,u_1)$ 且 $\lambda(u,u) = \lambda(u,e) = 0$的映射。此外，对于所有 $u \in U$，$\varphi'(u,c) \in \langle u,\ c\rangle$。

由三元组 (c,c,u) 的条件 (29)（其中 $u \in U$）可得，$\varphi'(uc,c) \in \langle u,\ c\rangle$。现在，由三元组 (c,u_1,u_2) 的条件 (29)（其中 u_1、$u_2 \in U$）可得，$\varphi'(u_1c,u_2) \in \langle u_1,\ u_2,\ c\rangle$。因此，

$$\varphi'(u_1c,u_2) \equiv c^{\mu(u_1,u_2)} \pmod{\langle u_1c,u_2\rangle}, \tag{36}$$

其中 $\mu\colon U\times U \to \mathbb{F}_2$ 是满足 $\mu(e,u) = \mu(u,e) = 0$的映射。

最后，由三元组 (u_1,c,u_2c) 的条件 (29)（其中 u_1、$u_2 \in U$）可得，$\varphi'(u_1c,u_2c) \in \langle u_1,\ u_2,\ c\rangle$。因此，

$$\varphi'(u_1c,u_2c) \equiv c^{\nu(u_1,u_2)} \pmod{\langle u_1c,u_2c\rangle}, \tag{37}$$

其中 $\nu\colon U\times U \to \mathbb{F}_2$ 是满足 $\nu(u_1,u_2) = \nu(u_2,u_1)$ 且 $\nu(u,u) = \nu(u,e) = 0$的映射。现在，对于三元组 (u_1,u_2,u_3)、(u_1c,u_2,u_3) 和 (u_1c,u_2c,u_3)，其中u_1、u_2、$u_3 \in U$，条件 (29) 可写成以下方程组

$$\lambda(u_2,u_3) + \lambda(u_1u_2,u_3) + \lambda(u_1,u_2u_3) + \lambda(u_1,u_2) = 0, \tag{38}$$

$$\lambda(u_2,u_3) + \mu(u_1u_2,u_3) + \mu(u_1,u_2u_3) + \mu(u_1,u_2) = 0 \quad \text{for } u_1 \notin \langle u_2,u_3\rangle, \tag{39}$$

$$\mu(u_2,u_3) + \lambda(u_1u_2,u_3) + \nu(u_1,u_2u_3) + \nu(u_1,u_2) = 0 \quad \text{对于 } u_1 \notin \langle u_3\rangle, u_2 \notin \langle u_3\rangle. \tag{40}$$

(39) 中的限制 $u_1 \notin \langle u_2,u_3\rangle$ 和 (40) 中的限制 $u_1 \notin \langle u_3\rangle$, $u_2 \notin \langle u_3\rangle$ 至关重要。这些限制与以下事实有关：恰好在这些限制下，元素 c 不属于所讨论的三元组所生成的子群，因此我们可以写出条件：对应同余式 (29) 左端的元素 c 的出现次数等于零。

等式 (38) 正是 λ 的通常余循环条件。引理 9.6 意味着存在映射 $\eta\colon U \to \mathbb{F}_2$ 使得 $\eta(e) = 0$ 并且

$$\lambda(u_1,u_2) = \eta(u_1) + \eta(u_2) + \eta(u_1u_2). \tag{41}$$

如果元素 $u,u' \in U$ 互不相同，且都不等于 e，那么三元组 $(u_1,u_2,u_3) = (u,u,u')$ 的等式 (40) 给出

$$\mu(u,u') = \nu(u,uu'). \tag{42}$$

注意，如果元素 u 和 u' 中有一个等于 e，那么等式 (42) 仍然成立，因为 $\mu(u,e) = \mu(e,u) = e$ 并且 $\nu(u,u) = \nu(u,e) = \nu(e,u) = e$。然而，条件$u \neq u'$ 至关重要。

现在假设 u_1、u_2、$u_3 \in U$ 的元素满足 $u_1 \notin \langle u_2$、$u_3\rangle$。那么每一对 $(u_1u_2,\ u_3)$、$(u_1,\ u_2u_3)$ 和 $(u_1,\ u_2)$ 都由互不相同的元素组成。因此，将 (41) 和 (42) 代入 (39)，得到方程

$$\nu(u_1u_2,u_1u_2u_3) + \nu(u_1,u_1u_2u_3) + \nu(u_1,u_1u_2) = \eta(u_2) + \eta(u_3) + \eta(u_2u_3).$$

在此方程中作替换 $a_1 = u_1$、 $a_2 = u_1u_2$、 $a_3 = u_1u_2u_3$ ，并引入一个新函数

$$\rho(u, u') = \nu(u, u') + \eta(uu'), \tag{43}$$

我们得到

$$\rho(a_1, a_2) + \rho(a_2, a_3) + \rho(a_3, a_1) = 0 \tag{44}$$

只要 a_1 不等于元素 e、 a_1a_2、 a_2a_3 和 a_3a_1中的任何一个。最后一个条件的确切含义是，元素 a_1、 a_2、 a_3 和 $a_1a_2a_3$ 中没有一个等于 e。注意，函数 ν 的对称性立即意味着函数 ρ的对称性。此外，对于所有 $u \in U$，有 $\rho(u, u) = \nu(u, u) + \eta(e) = 0$。

到目前为止，我们从未使用过关键条件 $\dim U \geq 3$；没有该条件，引理便不成立。我们来证明，在此条件下，对于集合 $U \setminus \{e\}$ 的所有元素三元组 (a_1, a_2, a_3)，等式 (44) 都成立，而无需假设 $a_1a_2a_3 \neq e$。事实上，设 a_1、 a_2 和 a_3 是 $U \setminus \{e\}$ 中的元素，使得 $a_1a_2a_3 = e$。那么 $\dim\langle a_1$、 a_2、 $a_3\rangle = 2$。因此，由条件 $\dim U \geq 3$ 可知，存在元素 $b \in U$，它不属于子群 $\langle a_1$、a_2、 $a_3\rangle$。于是，正如已经证明的那样，等式 (44) 对三元组 (a_1, a_2, b)、(a_2, a_3, b) 和 (a_3, a_1, b) 中的每一个都成立。将这些等式相加，即可得到初始三元组 (a_1, a_2, a_3) 的等式 (44)。

由等式 (44) 对集合 $U \setminus \{e\}$ 中所有元素三元组 (a_1, a_2, a_3) 均成立这一事实可立即推出，存在一个函数 $\zeta\colon U \setminus \{e\} \to \mathbb{F}_2$，使得

$$\rho(u, u') = \zeta(u) + \zeta(u'), \qquad u, u' \neq e. \tag{45}$$

事实上，任取一个元素 $u_0 \in U \setminus \{e\}$，我们可以令 $\zeta(u) = \rho(u_0, u)$，对所有$u \in U \setminus \{e\}$ 均成立。于是，等式 (45) 可由等式 (44) 推出。由 (42)、(43) 和 (45) 可得

$$\mu(u, u') = \zeta(u) + \eta(u') + \zeta(uu'), \qquad u \neq u', \tag{46}$$

$$\nu(u, u') = \zeta(u) + \zeta(u') + \eta(uu'), \qquad u, u' \neq e. \tag{47}$$

我们通过令 $\zeta(e) = 0$，将函数 ζ 扩展到整个 U。不过请注意，如果 u 和 u' 中的某个元素等于 e，公式 (45) 和 (47) 未必成立；如果 $u = u'$，公式 (46) 也同样如此。

考虑映射 $\theta\colon V \to V$ 以及对合对称拟余循环

$$\varphi''\colon V \times V \to V$$

由公式定义

$$\theta(u) = c^{\eta(u)}, \quad u \in U,$$

$$\theta(uc) = c^{\zeta(u)}, \quad u \in U,$$

$$\varphi''(v, w) = \varphi'(v, w)\theta(v)\theta(w)\theta(vw), \qquad v, w \in V.$$

由公式（35）、（36）、（37）、（41）、（46）和（47）可得

$$\varphi''(v, w) \in \langle v, w\rangle \tag{48}$$

对所有 v、 $w \in V$ 均成立，也就是说，拟余循环 φ'' 等价于平凡拟余循环。注意，在例外情形（v、w）=（uc、u）和（v、w）=（uc、c）中，公式（46）和（47）可能不成立，但包含关系（48）仍然成立，因为在这些情形下 $c \in \langle v$、 $w\rangle$。由于根据构造， φ'' 与 φ 上同调等价，因此得到引理的结论。

□

命题 9.7 的陈述（2）由引理 10.1、10.2 和 10.3 推出。

11. 特殊二值群

在本截面中，我们将证明以下定理。

定理 11.1。 任何不含单值直因子的特殊对合交换二值群都同构于二值群 Y_V，其中 V 是一个满足 维数$V \geq 2$的布尔群。

引理 11.2。 如果(x, y) 是对合交换二值群 X 和 $x * y = [z, z]$中的一个特殊对，那么 $x^2 = y^2 = z^2$ 以及5 个元素 e、 x、 y、 z 和 $s = x^2$ 两两不同，并构成二值群 X 的一个子群，其乘法表为

$$
\begin{aligned}
&x * x = y * y = z * z = [e, s], \quad s * s = [e, e],\\
&x * y = [z, z], \quad y * z = [x, x], \quad z * x = [y, y],\\
&s * x = [x, x], \quad s * y = [y, y], \quad s * z = [z, z],
\end{aligned}
$$

也就是说，这是一个同构于二值群 Y_2的子群。特别地， x、 y 和 z 是阶为4的元素。

Proof. 令 $x * y = [z, z]$。根据引理 2.2，我们有 $y * z = [x, x']$，其中某个 x'。于是

$$
\begin{aligned}
&x * y * z = (x * y) * z = [z, z] * z = [e, e, z^2, z^2],\\
&x * y * z = x * (y * z) = x * [x, x'] = [e, x^2, x * x'].
\end{aligned}
$$

然而，我们知道 $x^2 \neq e$，因为 $\operatorname{ord} x > 2$。因此 $x^2 = z^2$。此外，我们看到单位元 e 包含在多重集 $x * x'$中，这意味着 $x' = x$。于是，$y * z = [x, x]$。类似地，我们有 $y^2 = x^2$和 $x * z = [y, y]$。令 $s = x^2 = y^2 = z^2$，则 $x * x = y * y = z * z = [e, s]$。

我们有

$$
\begin{aligned}
&x * y * y = (x * y) * y = [z, z] * y = [x, x, x, x],\\
&x * y * y = x * (y * y) = x * [e, s] = [x, x, x * s],
\end{aligned}
$$

所以 $x * s = [x, x]$，从而 $x^3 = x$。由于 $\operatorname{ord} x > 2$，可得 $\operatorname{ord} x = 4$。因此 $\operatorname{ord} s = 2$，也就是说， $s * s = [e, e]$。类似地，由等式 $x * s = [x, x]$ 可证明$y * s = [y, y]$和 $z * s = [z, z]$。于是，e、 s、 x、 y、 z这 5 个元素构成二值群 X 的一个子群，该子群与 Y_2同构。□

由此引理可知，如果（x, y）是一个特殊对，且 $x * y = [z, z]$，那么（x, z）和（y, z）也都是特殊对，并且 $x * z = [y, y]$ 和 $y * z = [x, x]$。我们将这样的元素三元组（x, y, z）称为特殊三元组。特殊三元组中的元素的阶总是 4，并且 $x^2 = y^2 = z^2$ 对它们成立。

命题 11 .3. 设 X 是一个特殊的对合交换二 -值群 . *Then*

(a) 二值群 X 的所有元素的阶都是1、2 或4；(b) 二值群 X 的所有阶为4 的元素都有相同的平方，即存在一个元素 $s \in X$，使得 $x^2 = s$ 对 $x \in X$ 中所有阶为4的元素都成立。

此命题的证明将分为若干个引理。

引理 11.4. 设在对合交换二值群 X 中，元素 x 的阶为 4，而元素 q 的阶既不是 1，也不是 2，也不是 4。设 $s = x^2$。则存在一个由二值群 X 的元素构成的序列 $\{x_n\}_{n \in \mathbb{Z}}$，使得

使得 $x_0 = x$ 和

$$q^k * x_n = [x_{n-k}, x_{n+k}], \qquad k, n \in \mathbb{Z}, \tag{49}$$

$$sx_n = x_{-n}, \qquad n \in \mathbb{Z}, \tag{50}$$

$$x * x_1 = [q, sq], \tag{51}$$

$$x_1 * x_1 = [e, sq^2]. \tag{52}$$

此外，这样的序列在指标 n的符号反转意义下是唯一的，也就是说，在同时置换 $x_n \leftrightarrow x_{-n}$ （对所有 n）的意义下是唯一的。同时， $x_1 \neq x_{-1}$ ，且每个元素 x_1 和 x_{-1} 的阶既不是 1，也不是 2，也不是 4。

证明。设 $x_0 = x$。由于 ord $q \neq 4$，由引理 11.2 可知，对 (q, x) 不是特殊的。由于 q 和 x 的阶大于 2，因此存在元素 x_1、$x_{-1} \in X$ ，使得 $q*x = [x_1, x_{-1}]$，且 $x_1 \neq x_{-1}$。

元素 $s = x^2$ 的阶为 2，且我们有以下等式

$$[x * x_1, x * x_{-1}] = x * (x * q) = (x * x) * q = [e, s] * q = [q, q, sq, sq].$$

此外，我们还有

$$s(x * x_1) = (sx) * x_1 = x * x_1.$$

因此

$$x * x_1 = x * x_{-1} = [q, sq].$$

Fro由事实 $q \in x * x_1$ 可知，元素 q^2 属于多重集 t

$$(x * x_1) * (x * x_1) = (x * x) * (x_1 * x_1) = [e, s] * [e, x_1^2] = [e, e, s, s, x_1^2, x_1^2, sx_1^2, sx_1^2].$$

如果元素 x_1 的阶等于 1、2 或 4，那么元素 x_1^2 的阶将等于 1 或 2，而多重集 $(x * x_1)$ $* (x * x_1)$ 将由阶为 1 和 2 的元素组成。但这不可能成立，因为元素 q^2 的阶既不是 1 也不是 2。因此，ord $x_1 \notin \{1, 2, 4\}$。同理，ord $x_{-1} \notin \{1, 2, 4\}$。

现在由命题 3.2(c)可知， $sx_1 \neq x_1$ 和 $sx_{-1} \neq x_{-1}$。然而，同时

$$[sx_1, sx_{-1}] = s[x_1, x_{-1}] = s(x * q) = (sx) * q = x * q = [x_1, x_{-1}].$$

因此， $sx_1 = x_{-1}$ 和 $sx_{-1} = x_1$。

带有 $k = 1$ 的等式 (49) 具有如下形式

$$q * x_n = [x_{n-1}, x_{n+1}]. \tag{53}$$

这些等式使得我们能够递归地唯一确定序列 $\{x_n\}$ 的元素，从已定义的元素 x_0、 x_1 和 x_{-1} 开始。事实上，正指标对应的元素 x_n 按照 n 的升序依次定义。根据构造，对于 $n \geq 1$，元素 x_n 属于多重集 $q * x_{n-1}$，因此，由引理 2.2 可知，多重集 $q * x_n$ 确实包含元素 x_{n-1} ，我们可以且必须取该多重集的第二个元素作为 x_{n+1}。同理，负指标对应的元素 x_n 按照 n 的降序依次唯一确定。

让我们对 k 使用归纳法证明 $q^k * x_n = [x_{n+k}, x_{n-k}]$。对于 $k = 0$ 和 $k = 1$，根据构造这显然成立。对于 $k \geq 2$，我们假设该命题对 $k-2$ 和 $k-1$ 成立，并对此进行证明。我们有

$$q * q^{k-1} * x_n = q * (q^{k-1} * x_n) = q * [x_{n+k-1}, x_{n-k+1}] = [x_{n+k}, x_{n+k-2}, x_{n-k+2}, x_{n-k}],$$

$$q * q^{k-1} * x_n = (q * q^{k-1}) * x_n = [q^{k-2}, q^k] * x_n = [x_{n+k-2}, x_{n-k+2}, q^k * x_n],$$

因此 $q^k * x_n = [x_{n+k}, x_{n-k}]$。

只需对 $n \geq 0$ 证明等式 (50)，这同样通过对 n 使用归纳法完成。事实上，对于 $n = 0$ 和 $n = 1$，归纳基成立。归纳步骤通过元素 s 作用于等式 (53) 得到：如果 $sx_{n-1} = x_{-n+1}$ 和 $sx_n = x_{-n}$，那么

$$[x_{-n+1}, x_{-n-1}] = q * x_{-n} = q * (sx_n) = s(q * x_n) = s[x_{n+1}, x_{n-1}] = [sx_{n+1}, x_{-n+1}],$$

因此 $sx_{n+1} = x_{-n-1}$。

现在来证明等式 (51) 和 (52)。

由于 $q * x = [x_1, sx_1]$，x_1 属于多重集 $q * x$ 和 $(sq) * x$。根据引理 2.2，这意味着元素 q 和 sq 属于多重集 $x * x_1$。然而，$\operatorname{ord} q \neq 4$，因此根据命题 3.2(c)，$q \neq sq$。于是 $x * x_1 = [q, sq]$。

最后，我们有

$$(sq^2) * x_1 = q^2 * (sx_1) = q^2 * x_{-1} = [x_1, x_{-3}],$$

因此，根据引理 2.2，可知元素 sq^2 属于多重集 $x_1 * x_1$。由于 $\operatorname{ord} q \neq 4$，那么 $\operatorname{ord} q^2 \neq 2$，从而 $sq^2 \neq e$。因此，$x_1 * x_1 = [e, sq^2]$。□

引理 11.5. 设 (x, y, z) 是 X 中的特殊三元组，$s = x^2 = y^2 = z^2$，而 $q \in X$ 是一个阶既不是 1、也不是 2、也不是 4 的元素。设 $\{x_n\}_{n\in\mathbb{Z}}$、$\{y_n\}_{n\in\mathbb{Z}}$ 和 $\{z_n\}_{n\in\mathbb{Z}}$ 是满足引理 *11.4* 中关于对 (x, q)、(y, q) 和 (z, q) 的条件的序列。则对所有 $n \in \mathbb{Z}$，以下等式成立：

$$\begin{aligned}
&x_n * y = [z_n, sz_n], && y_n * z = [x_n, sx_n], && z_n * x = [y_n, sy_n],\\
&x * y_n = [z_n, sz_n], && y * z_n = [x_n, sx_n], && z * x_n = [y_n, sy_n].
\end{aligned}$$

此外，如有必要，同时对所有 $n \in \mathbb{Z}$ 改变 $z_n \leftrightarrow z_{-n}$，即可确保以下等式成立：

$$\begin{aligned}
&x_1 * y_1 = [z, z_2], && x_2 * y_1 = x_1 * y_2 = [z_1, z_3],\\
&y_1 * z_1 = [x, x_2], && y_2 * z_1 = y_1 * z_2 = [x_1, x_3],\\
&z_1 * x_1 = [y, y_2], && z_2 * x_1 = z_1 * x_2 = [y_1, y_3].
\end{aligned}$$

证明。我们有

$$\begin{aligned}
q^n * x * y &= (q^n * x) * y = [x_n, sx_n] * y = [x_n * y, s(x_n * y)],\\
q^n * x * y &= q^n * (x * y) = q^n * [z, z] = [z_n, sz_n, z_n, sz_n],
\end{aligned}$$

因此 $x_n * y = [z_n, sz_n]$。关于 $y_n * z$、$z_n * x$、$x * y_n$、$y * z_n$ 和 $z * x_n$ 的公式可类似证明。

我们有

$$\begin{aligned}
(x * y) * (q * q) &= [z, z] * [e, q^2] = [z, z, z, z, z_2, z_2, sz_2, sz_2],\\
(q * x) * (q * y) &= [x_1, sx_1] * [y_1, sy_1] = [x_1 * y_1, x_1 * y_1, s(x_1 * y_1), s(x_1 * y_1)].
\end{aligned}$$

由于 $sz = z$，可知 $x_1 * y_1 = [z, z_2]$ 或 $x_1 * y_1 = [z, sz_2] = [z, z_{-2}]$。在第二种情形下，我们需要对 $z_n \leftrightarrow z_{-n}$ 同时进行置换，使其对所有 n 都成立。因此，我们得到等式 $x_1 * y_1 = [z, z_2]$。于是

$$\begin{aligned}
q * x_1 * y_1 &= (q * x_1) * y_1 = [x, x_2] * y_1 = [z_1, sz_1, x_2 * y_1],\\
q * x_1 * y_1 &= q * (x_1 * y_1) = q * [z, z_2] = [z_1, sz_1, z_1, z_3],
\end{aligned}$$

因此 $x_2 * y_1 = [z_1, z_3]$。类似地，$x_1 * y_2 = [z_1, z_3]$。

类似地，我们得到 $y_1 * z_1 = [x, x_2]$ 或 $y_1 * z_1 = [x, x_{-2}]$。然而，现在我们不能再进行置换 $x_n \leftrightarrow x_{-n}$，因为这会破坏已经证明的等式 $x_1 * y_1 = [z, z_2]$。因此，我们需要用另一种方式证明等式 $y_1 * z_1 = [x, x_2]$成立。注意，在 $x_2 = x_{-2}$ 的情形下，这个等式已经

得到证明。因此，我们只需考虑情形 $x_2 \neq x_{-2}$。在这种情形下 $x_2 \neq x$。事实上，如果等式 $x = x_2$ 成立，那么等式 $x_{-2} = sx_2 = sx = x = x_2$ 就成立。现在注意，由已经证明的等式 $x * y_1 = [z_1, sz_1]$ 和 $x_2 * y_1 = [z_1, z_3]$ 以及引理 2.2 可知，元素 x 和 x_2 属于多重集 $y_1 * z_1$。由于 $x_2 \neq x$，这就推出了所需的等式 $y_1 * z_1 = [x, x_2]$。类似地，我们有 $z_1 * x_1 = [y, y_2]$。

现在可以仿照 $x_2 * y_1$ 和 $x_1 * y_2$ 的公式，证明 $y_2 * z_1$、$y_1 * z_2$、$z_2 * x_1$、$z_1 * x_2$ 的公式。□

引理 11.6. 设 (x, y) 是对合交换群 X 中的一个特殊对。那么在 X 中不存在满足 $q^2 = x$ 的元素 q。

证明。假设这样的元素 q 存在。设 $x * y = [z, z]$、$s = x^2 = y^2 = z^2$、$\{x_n\}_{n\in\mathbb{Z}}$、$\{y_n\}_{n\in\mathbb{Z}}$ 和 $\{z_n\}_{n\in\mathbb{Z}}$ 是满足引理 11.5 条件的序列。我们有

$$[x_2, sx_2] = q^2 * x = x * x = [e, s],$$

因此，要么 $x_2 = e$，要么 $x_2 = s$。所以，要么 $x_2 * y_1 = [y_1, y_1]$，要么 $x_2 * y_1 = [sy_1, sy_1]$。然而，根据引理 11.5，我们有 $x_2 * y_1 = [z_1, z_3]$，这意味着要么 $y_1 = z_1$，要么 $sy_1 = z_1$，也就是说，$y_1 = z_{-1}$。在上述每种情形下，我们都得到多重集 $q * y_1$ 包含元素 y 和 z。由于 $y \neq z$，我们有 $q * y_1 = [y, z]$。最后，

$$[y_1, y_1, x * y_1] = [e, x] * y_1 = (q * q) * y_1 = q * (q * y_1) = q * [y, z] = [y_1, y_{-1}, z_1, z_{-1}] = [y_1, y_{-1}, y_1, y_{-1}],$$

因此 $x * y_1 = [y_{-1}, y_{-1}]$。然而，根据引理 11.5 中的公式，我们有 $x * y_1 = [y_1, y_{-1}]$。由于 $y_1 \neq y_{-1}$，这就产生了矛盾，从而完成了引理的证明。□

引理 11.7。特殊对合交换二值群 X 不能包含阶为3的元素。

证明。反设：令 $q \in X$ 为一个阶为 3 的元素，则 $q^2 = q$，也就是说，$q * q = [e, q]$。设 (x, y, z) 是 X 中的某个特殊三元组，$s = x^2 = y^2 = z^2$ 和 $\{x_n\}_{n\in\mathbb{Z}}$，$\{y_n\}_{n\in\mathbb{Z}}$ 以及 $\{z_n\}_{n\in\mathbb{Z}}$ 是满足引理 11.5 条件的序列。我们有

$$[x_2, x_{-2}] = q^2 * x = q * x = [x_1, x_{-1}].$$

因此，要么是 $x_2 = x_1$，要么是 $x_2 = x_{-1} = sx_1$。如果等式 $x_2 = x_1$ 成立，那么我们就会得到 $q * x_1 = [x_1, x]$，因此，

$$[x_1, x_1, x_1, x] = [e, q] * x_1 = (q * q) * x_1 = q * (q * x_1) = q * [x, x_1] = [x_1, x_{-1}, x_1, x].$$

这不成立，因为 $x_1 \neq x_{-1}$。因此，$x_2 = sx_1$。同理，$y_2 = sy_1$ 且 $z_2 = sz_1$。

现在，利用等式 $x_1 * x_1 = [e, sq]$、$x_1 * z = [y_1, sy_1]$、$x_1 * y_1 = [z, z_2]$和 $x_1 * z_1 = [y, y_2]$，我们得到

$$(x_1 * x_1) * y_1 = [e, sq] * y_1 = [y_1, y_1, sy_2, sy] = [y_1, y_1, y_1, y],$$
$$x_1 * (x_1 * y_1) = x_1 * [z, z_2] = x_1 * [z, sz_1] = [y_1, sy_1, sy, sy_2] = [y_1, y_{-1}, y, y_1],$$

这导致矛盾，因为 $y_1 \neq y_{-1}$。引理的证明至此完成。□

命题 11.3(a) 的证明。假设二值群 X 包含一个元素 q，其阶既不为 1，也不为 2 或 4。根据引理 11.7，q的阶不等于 3；因此 $\operatorname{ord} q > 4$。设 (x, y, z) 是 X 中的某个特殊三元组，

$s = x^2 = y^2 = z^2$ 和 $\{x_n\}_{n\in\mathbb{Z}}$、 $\{y_n\}_{n\in\mathbb{Z}}$ 和 $\{z_n\}_{n\in\mathbb{Z}}$ 是满足引理 11.5 条件的序列。利用这些序列的性质，我们得到

$$q * y_1 * x_2 = q * (y_1 * x_2) = q * [z_1, z_3] = [z, z_2, z_2, z_4],$$
$$q * y_1 * x_2 = (q * y_1) * x_2 = [y, y_2] * x_2 = [z_2, sz_2, x_2 * y_2],$$

这意味着元素 sz_2 与三个元素 z、 z_2 和 z_4中的一个重合。

如果等式 $sz_2 = z_2$ 成立，那么我们将得到 $q^2 * z = [z_2, z_2]$。由于 $\operatorname{ord} q^2 > 2$ 和 $\operatorname{ord} z = 4$，可推出 (q^2, z) 是一个特殊对，这根据引理 11.6 是不可能的。因此， $sz_2 \neq z_2$

如果等式 $sz_2 = z$ 成立，那么我们将再次得到

$$sz_2 = z = sz = z_2,$$

正如我们已经证明的，这是不可能的。因此 $sz_2 \neq z$。

因此， $sz_2 = z_4$。于是

$$[z_3, z_5] = q * z_4 = q * (sz_2) = s(q * z_2) = s[z_1, z_3] = [sz_1, sz_3].$$

如果 $z_3 = sz_3$，那么 $q^3 * z = [z_3, z_3]$。因此，$\operatorname{ord} q^3 \leq 2$，或者 (q^3, z) 是一个特殊对，于是根据引理 11.2，元素 q^3 的阶等于 4。因此，无论哪种情形，元素 q^3 的阶都整除 4，从而元素 q 的阶整除 12。另一方面，元素 q 的阶大于 4，所以 $\operatorname{ord} q = 6$，或 $\operatorname{ord} q = 12$。于是 q^2 或 q^4 的阶为 3，这根据引理 11.7 是不可能的。因此 $z_3 \neq sz_3$，所以 $z_3 = sz_1$。于是

$$[z_2, z_4] = q * z_3 = q * (sz_1) = s(q * z_1) = s[z, z_2] = [z, sz_2] = [z, z_4],$$

因此 $z = z_2$。但又有 $sz_2 = z_2$，而正如我们已经证明的，这是不可能的。由此得到的矛盾完成了命题 (a) 部分的证明。□

引理 11.8。 设 x 和 p 是对合交换二值群 X 中阶为 4 的两个元素，且 $x^2 \neq p^2$。那么存在一个阶为 4 的元素 $a \in X$，使得 $a^2 = x^2p^2$ 且

$$x * p = [a, x^2a], \qquad x * a = [p, x^2p], \qquad p * a = [x, p^2x].$$

证明。由于 $x^2 \neq p^2$，由引理 11.2 可知，对 (x, p) 不是特殊的。因此，对于某个 $a \neq b$，有 $x * p = [a, b]$。引理 2.2 现在推出 $p \in x * a$。与此同时，一方面，

$$x^2(x * a) = (x^2x) * a = x * a,$$

另一方面， $x^2p \neq p$ （根据命题 3.2(c)，因为 $p^2 \neq x^2$）。因此 $x*a = [p, x^2p]$。类似地，$p * a = [x, p^2x]$。

现在我们有

$$(x * x) * (a * a) = [e, x^2] * [e, a^2] = [e, e, x^2, x^2, a^2, a^2, x^2a^2, x^2a^2],$$
$$(x * a) * (x * a) = [p, x^2p] * [p, x^2p] = [e, e, x^2, x^2, p^2, p^2, x^2p^2, x^2p^2],$$

因此，要么 $a^2 = p^2$，要么 $a^2 = x^2p^2$。同理，由对直积 $p * p * a * a$ 的考察可知，要么 $a^2 = x^2$，要么 $a^2 = x^2p^2$。由于 $x^2 \neq p^2$，可知 $a^2 = x^2p^2$。

由于 x^2 和 p^2 是不同的 2 阶元素，我们得到 $\operatorname{ord} a^2 = 2$，因此 $\operatorname{ord} a = 4$。此外，我们看到 $a^2 \neq x^2$，因为 $p^2 \neq e$。因此，根据命题 3.2(c)$x^2a \neq a$。然而，

$$[x^2a, x^2b] = x^2(x * p) = (x^2x) * p = x * p = [a, b],$$

因此 $b = x^2a$。 □

命题 11.3(b) 的证明。设 (x,y,z) 是 X and$s = x^2 = y^2 = z^2$ 中的某个特殊三元组。假设存在一个 4 阶元素 $p \in X$，使得$p^2 = t \neq s$。将引理 11.8 应用于对 (x,p)、(y,p) 和 (z,p)，可得群 X 中存在 4 阶元素 a、b 和 c，使得

$$\begin{gathered} a^2 = b^2 = c^2 = st, \\ x*p = [a, sa], \quad x*a = [p, sp], \quad p*a = [x, tx], \\ y*p = [b, sb], \quad y*b = [p, sp], \quad p*b = [y, ty], \\ z*p = [c, sc], \quad z*c = [p, sp], \quad p*c = [z, tz]. \end{gathered}$$

我们有

$$\begin{aligned} x*y*p &= (x*y)*p = [z,z]*p = [c,c,sc,sc], \\ x*y*p &= x*(y*p) = x*[b,sb] = [x*b, s(x*b)]. \end{aligned}$$

此外，根据引理 11.2，对 (x,b) 不是特殊的，因为 $x^2 \neq b^2$。因此，多重集 $x*b$ 由两个不同的元素组成。因此 $x*b = [c, sc]$。现在由引理 2.2 可知，元素 x 属于多重集 $b*c$。因此，元素$tx = stx = b^2x$ 也属于多重集

$$b^2(b*c) = (b^2b)*c = b*c.$$

同时，根据命题 3.2(c)，$tx \neq x$，因为 $x^2 \neq t$。因此，$b*c = [x, tx]$。最后，我们得到

$$[c,c,c,c] = [e,c^2]*c = [e,b^2]*c = (b*b)*c = b*(b*c) = b*[x,tx] = \\ [c, sc, tc, stc] = [c, sc, sc, c],$$

所以 $sc = c$，根据命题 3.2(c) 这是不可能的，因为 $c^2 \neq s$。因此，对于 $p \in X$ 的所有 4 阶元素，$p^2 = s$。□

定理 11.1 的证明。根据命题 11.3，二值群 X 的所有元素的阶为 1、2 或 4；此外，在 X 中存在一个 2 阶元素 s，使得对于所有 4 阶元素 $x \in X$，$s = x^2$。由于 X 不包含单值直因子，由命题 6.2 可知，s 是 X 中唯一的 2 阶元素。因此，对于所有元素 $x \in X$，除 e 和 s 外，$x^2 = s$。元素 e 和 s 构成二值群 X 的二元子群。考虑二值商群 $V = X/\{e,s\}$。对于所有元素 x，除 e 和 s 外，我们有 $sx = x$，因此V 不过是集合 X，其中两个元素 e 和 s 被合并为一个元素 e，且不作其他合并。在二值群 V 中，等式 $x^2 = s$ 变为等式 $x^2 = e$。因此，二值群 V 的所有非平凡元素的阶均为 2。根据命题 3.2，我们得到 V 是一个带有加倍乘法的布尔群，因此 $X \cong Y_V$。□

12. 有限生成情形下分类的结束

在本节中，我们汇总第 2–11 节的结果，并证明定理 1.10。由命题 6.3 以及定理 8.1、9.1 和 11.1 可知，每个有限生成对合交换二值群 X 都同构于下列某个二值群 $X_A^{\mathbf{a}} \times C_2^m$，其中 A 是有限生成阿贝尔群，$X_n^{\mathbf{u}} \times C_2^m$或 $Y_n \times C_2^m$. 考虑到同构 $X_A^{\mathbf{a}} \times C_2^m \cong X_{A \times C_2^m}$，我们看到 X 同构于定理 1.10 中列出的某个二值群。

现在我们需要证明，除以下例外情况外，所有这些二值群均两两不同构：

$$X^{\mathbf{a}}_{m\times 2,4} \cong X^{\mathbf{u}}_1 \times C_2^m \cong Y_1 \times C_2^m,$$
$$X^{\mathbf{a}}_{m\times 2,4,4} \cong X^{\mathbf{u}}_2 \times C_2^m.$$

第一个例外同构显而易见；第二个由同构 $X^{\mathbf{a}}_{4,4} \cong X^{\mathbf{u}}_2$ 得出，参见例 1.11 和定理 9.1。

二值群分为两种类型：特殊和非特殊，不同类型的二值群彼此不同构。根据命题 4.3，二值群 $Y_n \times C_2^m$with $n \geq 2$ 是特殊的，而定理 1.10 中列出的其他所有二值群都是非特殊的。

特殊二值群 $Y_n \times C_2^m$ 由 $2^m(2^n+1)$ 个元素组成，因此对于不同的对 (n,m)，这些群两两不同构。

二值群 $X^{\mathbf{u}}_n \times C_2^m$ 由 $2^m(2^{2n-1}+2^{n-1})$ 个元素组成，因此对于不同的对 (n,m)，这些群也两两不同构。

为了完成定理 1.10 的证明，我们还需证明以下两个命题。

命题 12.1。 若 $n \geq 3$ 且 $m \geq 0$，则二值群 $X^{\mathbf{u}}_n \times C_2^m$ 不同构于主系列中的任何二值群 $X^{\mathbf{a}}_A$。

命题 12.2。 设 A 和 B 是有限生成阿贝尔群，且二值群 $X^{\mathbf{a}}_A$ 和 $X^{\mathbf{a}}_B$ 同构。则群 A 和 B 也同构。

我们从以下简单的引理开始，它将在两个命题的证明中使用。

引理 12.3。 设 A 是一个阿贝尔群，$\pi\colon\ A \to X^{\mathbf{a}}_A$ 是关于对跖对合 $\iota_{\mathbf{a}}$ 的商映射。则对于所有 $a \in A$，有 阶 $\pi(a) =$阶 a。

证明。根据陪集二值群的定义，我们有

$$\pi(a^k) * \pi(a) = \left[\pi(a^{k-1}), \pi(a^{k+1})\right]$$

对所有 k。由这个等式可容易地通过归纳法得出，对所有 $a \in A$和 $k > 0$，$\pi(a)^k = \pi(a^k)$。由于 ord $\pi(a)$按定义是满足 $\pi(a)^k = e$ 的最小 k，且二值群 $X^{\mathbf{a}}_A$ 中单位元在映射 π 下的逆像仅包含群 A 的单位元，因此 ord $\pi(a)$ = ord a。□

命题12.1 的证明。二值群 $X^{\mathbf{u}}_n \times C_2^m$由阶为 1、2 和 4 的元素组成。因此，同构 $X^{\mathbf{u}}_n \times C_2^m \cong X^{\mathbf{a}}_A$ 成立的必要条件是，二值群 $X^{\mathbf{a}}_A$ 的所有元素的阶都为 1、2 和 4。根据引理 12.3，这等价于阿贝尔群 A 的所有元素的阶都为 1、2 和 4，也就是说，对于某个 p，有 $A \cong C_4^p \times C_2^q$ $q \geq 0$。于是，二值群 $X^{\mathbf{a}}_A$ 由 2^q个（$2^{2p-1}+2^{p-1}$）元素组成，因此 $p = n$ 且 $q = m$。这样，主系列中唯一可能与二值群 $X^{\mathbf{u}}_n \times C_2^m$同构的二值群就是二值群 $X^{\mathbf{a}}_{C_4^n \times C_2^m} \cong X^{\mathbf{a}}_{n\times 4} \times C_2^m$。容易看出，在二值群$X^{\mathbf{a}}_{n\times 4}$ 和 $X^{\mathbf{u}}_n$ 中，所有 2 阶元素都是平方。因此，根据命题 6.2，这两个二值群不含单值直因子。于是，根据命题 6.3，同构 $X^{\mathbf{u}}_n \times C_2^m \cong X^{\mathbf{a}}_{n\times 4} \times C_2^m$将推出同构 $X^{\mathbf{u}}_n \cong X^{\mathbf{a}}_{n\times 4}$。最后注意到，根据定理 9.1，当 $n \geq 3$时，二值群 $X^{\mathbf{u}}_n$ 和 $X^{\mathbf{a}}_{n\times 4}$ 不同构。□

用 $N_k(A)$（分别用 $N_k(X)$）表示阿贝尔群 A （分别表示对合交换二值群 X）中阶为 k 的元素个数。有限阿贝尔群的这一众所周知的性质可由其分类定理轻易推出。

引理 12.4. 若有限阿贝尔群 A 和 B 满足：对所有 k， $N_k(A) = N_k(B)$ ，则 A 和 B 同构。

推论 12.5.若有限生成阿贝尔群 A 和 B 满足：对所有 k ，$N_k(A) = N_k(B)$ ，且阿贝尔群 A 和 B的自由部分的秩相等，则 A 和 B 同构。

引理 12.6.若 A 是有限生成阿贝尔群，则对所有 $k > 2$， $N_2(X_A^{\mathbf{a}}) = N_2(A)$且 $N_k(X_A^{\mathbf{a}}) = N_k(A)/2$ 。

证明。在投影 $\pi\colon A \to X_A^{\mathbf{a}}$下，群 A 中每一对 $\{a, a^{-1}\}$互逆元素都被合并为二值群 $X_A^{\mathbf{a}}$中的一个元素。此外，若 $\operatorname{ord} a = 2$，则 $a = a^{-1}$；若 $\operatorname{ord} a > 2$，则 $a \neq a^{-1}$。因此，结论由引理 12.3 立即得出。□

引理 12.7. 设 A 是一个有限生成阿贝尔群。那么，该群 A 的自由部分的秩等于元素系统 $x_1, \ldots, x_r \in X_A^{\mathbf{a}}$ 的最大基数，其中 $x_1^{n_1} * \cdots * x_r^{n_r}$ 的多重集中没有一个包含单位元 e；这里 $n_1, \ldots, n_r \in \mathbb{Z}$，且数字 n_i 中至少有一个非零。

证明。若 $a_1, \ldots, a_r$ 是群 A 的元素，且 $x_i = \pi(a_i)$， $i = 1, \ldots, r$，那么多重集 $x_1^{n_1} * \cdots * x_r^{n_r}$ 由 2^{r-1} 个元素组成，这些元素对应于所有可能的符号选择 $\pm$。因此，若数字 n_i 中至少有一个非零，则这些元素均不等于 e ，这一条件等价于不存在非平凡关系 $a_1^{m_1} \cdots a_r^{m_r} = e$。 □

命题 12.2 的证明。根据引理 12.6 和 12.7，数目$N_k(A)$以及有限生成阿贝尔群 A 的自由部分的秩，由二值群 $X_A^{\mathbf{a}}$的结构唯一确定。因此，命题 12.2 由推论 12.5 得出。□

至此，定理 1.10 得证。

13. 非有限生成二值群

现在我们来讨论，分类定理在多大程度上可以推广到非有限生成的对合交换二值群。这个问题有两种自然的表述方式：我们可以考察不带拓扑的二值群，也可以考察拓扑二值群。第一种问题将在本节讨论，第二种将在第 14 节和第 15 节讨论。显然，无论哪种情形，我们都不能指望得到像有限生成情形下定理 1.10 那样的完整分类定理。事实上，在非有限生成情形下，即使对于单值交换群，也不存在分类定理。因此，我们所能期望的最佳结果，是在单值交换群的分类基础上，解决对合交换二值群的分类问题。

本节的主要结果是以下定理。

定理13.1。每个对合交换二值群都同构于以下某个二值群

(1) $X_A^{\mathbf{a}}$，其中 A 是阿贝尔群；

(2) $X_V^{\mathbf{u}} \times W$，其中 V和 W是布尔群，且维数 $V \geq 3$；(3) $Y_V \times W$，
其中 V和 W是布尔群，且维数 $V \geq 2$。

来自不同系列的二值群彼此永不同构。两个二值群若都属于系列 2 或都属于系列 3，则它们同构，当且仅当相应的布尔群 V 同构，且相应的布尔群 W 也同构。

为了使定理 13.1 的表述完整，我们希望回答以下问题。

问题 13.2。阿贝尔群 A 和 B 不同构，而二值群 $X_A^{\mathbf{a}}$ 和 $X_B^{\mathbf{a}}$ 却同构，这种情况可能发生吗?

对于任意阿贝尔群，这个问题的答案尚不得而知。回想一下，在有限生成阿贝尔群的情形中，命题 12.2 给出了否定的答案。这个结论是通过计算不同阶的元素的个数证明的；当然，这种证明方法无法推广到非有限生成的情形。

定理 13.1 的证明沿用定理 1.10 的证明思路。设 X 是任意一个对合交换二值群。与定理 1.10 的证明一样，我们分三种情形讨论：

(1) X 含有一个阶既不是 1、也不是 2、也不是 4 的元素（此时 X 必定是非特殊的）；(2) X 是非特殊的，并且只由阶为 1、2 和 4 的元素组成；(3) X 是特殊的。

在第一种情形下，根据定理 8.1，二值群 X 同构于形如 $X_A^{\mathbf{a}}$的陪集二值群，其中 A 是一个阿贝尔群。回顾一下，在定理 8.1 的证明中，我们从未用到有限生成性质，见注 8.2。

在第二种和第三种情形下，我们首先注意到，命题 6.2 和命题 6.3 很容易推广到非有限生成情形。唯一的区别是，在命题 6.3 的证明中，必须按照标准方法用超限归纳取代通常按维数进行的归纳法。因此，任意一个对合交换二值群中的极大单值直因子（它是一个布尔群）都可以唯一地分出，且唯一性限于同构意义下。这使我们能够将分类定理归结为不含单值直因子的二值群 X 的情形，也就是说（根据命题 6.2），这类二值群 X中的每个 2 阶元素都是某个 4 阶元素的平方。如果这样的二值群 X 是特殊的，那么根据定理 11.1， X 同构于形如 Y_V 的群；该定理的证明中也从未用到有限生成性质。

我们还需考虑这样的情形： X 是一个非特殊二值群，其中所有元素的阶均为 1、2 或 4，且每个 2 阶元素都是某个 4 阶元素的平方；并证明在此情形下， X 同构于以下两种群之一： $X_{C_4^\omega}^{\mathbf{a}}$，其中 ω 是某个（可能无限的）基数；或者 $X_V^{\mathbf{u}}$，其中 $V \cong C_2^\omega$是一个（可能无限的）布尔群。这里， A^ω 表示 ω 个阿贝尔群 A的直和（不是直积）。这是最重要的情形，除第 9 节和第 10 节中的内容外，还需要作一些补充考量。更准确地说，对于不一定有限生成的二值群 X （因此，其所有 2 阶元素组成的布尔群 V 也不一定有限），第 9 节和第 10 节中的所有论证，除引理 10.3 的证明外，都可逐字照搬。因此，我们只需证明以下命题。

引理 13.3。设 V 是一个无限布尔群，且 $\Pi\colon\ V \to U$ 是到某个有限子群 $U \subset V$ 的投影，其中维数 $U \geq 3$。那么，同态 $\Pi_*\colon\ \mathcal{H}(V) \to \mathcal{H}(U)$ 是单射。

我们需要以下两个技术性引理。

引理 13.4. 设 φ 是布尔群 W 上的对合对称拟余循环，并且满足以下条件

$$\varphi(u,v) = \varphi(v,u), \tag{54}$$
$$\varphi(u,u) = \varphi(e,u) = \varphi(u,e) = e \tag{55}$$

恰好成立。考虑由公式给出的映射 $\delta\varphi\colon\ W \times W \times W \to W$

$$(\delta\varphi)(u,v,w) = \varphi(v,w)\varphi(uv,w)\varphi(u,vw)\varphi(u,v). \tag{56}$$

拟余循环 φ 是上同调平凡的，当且仅当存在映射 $\lambda\colon\ W \times W \to \mathbb{F}_2$，使得 $\lambda(u,u) = \lambda(e,u) = \lambda(u,e) = 0$ 对所有 $u \in W$ 均成立，并且

$$(\delta\varphi)(u,v,w) = u^{\lambda(uv,w)+\lambda(u,vw)+\lambda(u,v)} v^{\lambda(v,w)+\lambda(uv,w)+\lambda(vw,u)+\lambda(v,u)} w^{\lambda(w,v)+\lambda(w,uv)+\lambda(wv,u)} \tag{57}$$

对所有 $u,v,w \in W$ 均成立。

证明. 容易看出，任何与拟余循环 φ 上同调等价且满足条件 (54)、(55) 的拟余循环都具有如下形式

$$\varphi'(u,v) = \varphi(u,v)\chi(u)\chi(v)\chi(uv)u^{\lambda(u,v)}v^{\lambda(v,u)}$$

对于某些映射 $\chi\colon\ W \to W$ 和 $\lambda\colon\ W \times W \to \mathbb{F}_2$，使得 $\chi(e) = e$ 且 $\lambda(u,u) = \lambda(e,u) = \lambda(u,e) = 0$ 对所有 $u \in W$ 都成立。于是

$$(\delta\varphi')(u,v,w) = (\delta\varphi)(u,v,w)u^{\lambda(uv,w)+\lambda(u,vw)+\lambda(u,v)} v^{\lambda(v,w)+\lambda(uv,w)+\lambda(vw,u)+\lambda(v,u)} w^{\lambda(w,v)+\lambda(w,uv)+\lambda(wv,u)}.$$

如果拟余循环 φ 是上同调平凡的，那么我们可以将平凡拟余循环作为 φ'，从而恰好得到等式（57）。

反之，如果存在满足（57）的映射 λ，那么拟余循环 φ 等价于一个真正的对合对称余循环

$$\varphi'(u,v) = \varphi(u,v)u^{\lambda(u,v)}v^{\lambda(v,u)},$$

对于该余循环，条件 $(\delta\varphi')(u,v,w) = 1$ 以及条件（54）、（55）均精确成立。根据引理 9.6，余循环 φ' 是上同调平凡的，因此拟余循环 φ 也上同调平凡。□

引理 13.5. 无限布尔群 V 上的对合对称拟余循环，若其沿所有可能投影对每个有限子群的限制都是上同调平凡的，则该拟余循环上同调平凡。

证明。设 φ 是 V 上的对合对称拟余循环，其沿所有可能投影到有限子群的限制均为上同调平凡。将拟余循环 φ 替换为与之等价的拟余循环后，我们可以假设条件 (54)、(55) 严格成立。考虑由公式 (56) 给出的映射 $\delta\varphi\colon\ V \times V \times V \to V$。

用 $\mathcal{F}$ 表示群 V 的有限子群集合。根据引理 13.4，对于每个 $U \in \mathcal{F}$，存在一个映射 $\lambda\colon\ U \times U \to \mathbb{F}_2$，使得对所有 $u \in U$，$\lambda(u,u) = \lambda(u,e) = \lambda(e,u) = 0$，并且等式 (57) 对所有 $u,v,w \in U$ 都成立。用 Λ_U 表示所有具有这些性质的映射 λ 的集合。那么 Λ_U 是一个非空有限集。显然，如果

$U' \subset U$，那么对于每个 $\lambda \in \Lambda_U$， $\lambda|_{U'} \in \Lambda_{U'}$。（为简便起见，以下我们用 $\lambda|_{U'}$ 代替 $\lambda|_{U' \times U'}$。）

我们来证明，可以选取代表元 $\lambda_U \in \Lambda_U, U \in \mathcal{F}$，使得对于任意两个子群 U_1，$U_2 \in \mathcal{F}$，映射 λ_{U_1} 和 λ_{U_2} 在 $U_1 \cap U_2$ 上的限制相同。选择方式如下。根据策梅洛定理，集合 $\mathcal{F}$ 可以良序为 $\prec$。此外，我们可以假设在此良序下最小的是平凡子群 $\{e\}$。我们按照良序 $\prec$ 给出的次序，使用超限递归选取 λ_U 的代表元。每个代表元 λ_U 的选取都满足以下性质：

(∗) 对于任意有限集子群 $U_1, \ldots, U_k \in \mathcal{F}$，只要 $U_1 \prec \cdots \prec U_k = U$ 成立，并且对于任何包含子群 $U_1, \ldots, U_k$ 的子群 $W \in \mathcal{F}$，都存在一个映射 $\mu \in \Lambda_W$，使得 $\mu|_{U_i} = \lambda_{U_i}$ 且满足 $i = 1, \ldots, k$。

递归从平凡子群 $\{e\}$ 上的平凡映射 $\lambda_{\{e\}}$ 开始。

我们来证明，如果前面的代表元 $\lambda_{U'}, U' \prec U$ 的选取满足条件（∗），那么代表元 λ_U 确实可以按照条件（∗）选取。反设：集合 Λ_U 中的映射若选作 λ_U，没有一个会满足条件（∗）。设 $\lambda_1, \ldots, \lambda_N$ 是有限集 Λ_U 的所有元素。那么对于每个映射 λ_j，都存在一组子群 $U_{(j)1}, \ldots, U_{k_j}^{(j)} \in \mathcal{F}$，使得 $U_1^{(j)} \prec \cdots \prec U_{(j)k_j} = U$；并且存在一个包含 $U_{(j)1}, \ldots, U_{(j)^{k_j}}$ 的子群，使得映射 $\lambda_{U_1^{(j)}}, \ldots, \lambda_{U_{k_j-1}^{(j)}}, \lambda_j$ 这一组无法扩展为一个属于

集合 Λ_{W_j}。合并子群集合 $U_{(j)1}$、……、$U_{k_j}^{(j)}$、 $j = 1$、……、N，去除重复项，并使用 $\prec$ 对得到的子群有限集排序。由此得到子群的有限序列 $U_1 \prec \cdots \prec U_k = U$。设 W 是由所有子群 W_1、……、W_N 生成的群 V 的有限子群。那么对于所有 j，映射集合 λ_{U_1}、……、$\lambda_{U_{k-1}}$、λ_j 都无法扩展为属于集合 Λ_W 的映射。然而，由子群 $U_{k-1} \prec U$ 的条件（∗）可知，存在映射 $\mu \in \Lambda_W$，使得 $\mu|_{U_i} = \lambda_{U_i}$、 $i = 1$、……、$k - 1$。由于 $\mu|_U$ 是映射 λ_1、……、λ_N 之一，因此我们得到矛盾，从而完成了映射 λ_U 可构造性的证明。

由条件（∗）可知，特别地，对于任意两个子群 U_1、$U_2 \in \mathcal{F}$，映射 λ_{U_1} 和 λ_{U_2} 在交集 $U_1 \cap U_2$ 上的限制相同。因此，映射 λ_U 可合并为一个映射 $\lambda\colon\ V \times V \to \mathbb{F}_2$，使得对所有 $u \in V$，$\lambda(u, u) = \lambda(u, e) = \lambda(e, u) = 0$，且等式（57）对所有 u、v、$w \in V$ 均成立。因此，根据引理 13.4，拟余循环 φ 是上同调平凡的。□

引理 13.3 可由引理 10.2、10.3 和 13.5 得出。

由此，我们证明了任意对合交换二值群都属于定理 13.1 中列出的三个系列之一。

第三系列的二值群是特殊的，因此不同构于前两个系列的二值群。第一和第二系列的二值群（仅含阶为 1、2 和 4 的元素时）彼此不同，因为相应的拟余循环并非上同调等价。为完成定理 13.1 的证明，我们需要证明，可以从第二或第三系列的二值群 X 中唯一地恢复一对布尔群 (V, W)（在同构意义下）。事实确实如此：布尔群 W 是分解 $X \cong X' \times W$ 中的极大单值直因子；根据命题 6.3 的类比，该直因子在同构意义下是唯一的；而 V 则是第二系列中 X' 的所有 2 阶元素构成的布尔群，或是第三系列中 X' 的所有 4 阶元素构成的布尔群。

14. 拓扑二值群

如果 Y 是一个拓扑空间，那么我们在 $Y \times Y$ 上赋予直积拓扑，并由此在对称平方 $\mathrm{Sym}^2(Y)$ 上赋予商拓扑。

定义 14.1.拓扑二值群是一个拓扑空间 X ，具有二值群结构，且二值乘法运算 $X \times X \to \mathrm{Sym}^2(X)$和取逆元运算 $X \to X$ 均连续。

我们只考虑豪斯多夫拓扑二值群；非豪斯多夫情形显然要复杂得多。容易看出，若 A 是单值交换豪斯多夫拓扑群，且 ι是群 A的对合连续自同构，那么陪集二值群 A/ι自然具有豪斯多夫拓扑二值群结构。因此，对于任意豪斯多夫拓扑阿贝尔群 A ，拓扑二值群 $X_A^{\mathbf{a}}$ 有良好定义；对于豪斯多夫拓扑布尔群 V，拓扑二值群 $X_V^{\mathbf{u}}$ 也有良好定义。（此处及下文所说的拓扑布尔群，是指所有非平凡元素的阶均为 2 的拓扑群。）

再次，我们有三种本质不同的情形：
(1) X 包含一个阶既不是 1、也不是 2、也不是 4 的元素；(2) X 是非特殊的，且完全由阶为 1、2 和 4 的元素组成；(3) X 是特殊的。

我们分别讨论这些情形。在情形 (1) 和 (3) 中，我们将得到分类定理 8.1 和 11.1 的类似结果。情形 (2) 更为复杂。在这种情形下，分类问题仍未解决。我们将构造一个非平凡例子，说明分类定理 9.1 的直接类似结果并不成立。

含有一个元素的拓扑二值群 X ，该元素满足 t使得$\operatorname{ord} t \notin \{1,2,4\}$。 在这种情形下，定理 8.1 有一个直接类似结果，但其证明需要额外的论证。

定理 14.2。 设 X 是一个对合交换豪斯多夫拓扑二值群，且至少包含一个阶既不是 1、也不是 2、也不是 4 的元素。那么 X 同构于一个形如 $X_A^{\mathbf{a}} = A/\iota_{\mathbf{a}}$ 的陪集拓扑二值群，其中 A 是一个交换豪斯多夫拓扑群，而 $\iota_{\mathbf{a}}$ 是 A上的对跖对合。

如第 8 节中所述，我们将所需的拓扑群定义为集合

$$A = \{(x,p) \in X \times X \mid p \in t * x\} \tag{58}$$

其乘法和逆元运算由命题 8.3 定义。赋予集合 A 由 $X \times X$ 上的直积拓扑诱导的拓扑。在第 8 节中已经证明，由此得到的交换群结构定义良好，因此我们只需证明群 A 中所引入的乘法和逆元运算是连续的。（显然，由到第一因子的投影给出的同构 $A/\iota_{\mathbf{a}} \to X$ 在两个方向上都是连续的。）为了证明运算的连续性，我们需要 Smith-Dold 分歧覆盖的概念，见 [**37**], [**20**]。

~定义 14.3。设 $\pi\colon\ Y \to Y$ 是拓扑空间之间的连续满射，且点的原像点是有限的。映射 π 称为 Smith-Dold 意义下的 d重分歧覆盖，如果存在连续映射 $\tau\colon\ Y \to \mathrm{Sym}^d(\widetilde{Y})$ ，使得

~(1) 对任意点 $\tilde{y} \in Y$， $\tilde{y} \in \tau \circ \pi(\tilde{y})$；(2) 对任意点 $y \in Y$， $\mathrm{Sym}^d(\pi) \circ \tau(y) = \big[\underbrace{y, \ldots, y}\big]$.$_d$

注14.4. 在上述定义中，我们遵循 [14]。L. Smith 的等价原始定义如下。称连续满射 $\pi\colon Y \to Y$ 为**分歧覆盖**，如果存在一个映射 $\mu\colon Y \to \mathbb{Z}_{>0}$，称为**重数映射**，并且满足以下两个条件。

(1) 对任意点 $y \in Y$

$$\sum_{\tilde{y}\in\pi^{-1}(y)} \mu(\tilde{y}) = d.$$

(2) 映射 $\tau\colon Y \to \mathrm{Sym}^d(\widetilde{Y})$，使得 y 映入多重集 $\pi^{-1}(y)$，其中每个点 $\tilde{y}$ 均按重数 $\mu(\tilde{y})$计数，该映射是连续的。

重数映射 μ 可由定义 14.3 中的映射 τ 恢复，即为点 $\tilde{y}$ 在多重集 $\tau\circ\pi(\tilde{y})$中出现的重数。

通俗地说，d重分歧覆盖是一个连续映射，它具有一个连续的 d值逆元。

设 $\pi\colon A \to X$ 为到第一因子的投影。由于二值群 X 中的乘法是连续的，映射 $x \mapsto (x, t*x)$ 是映射 π的连续二值逆。因此，投影 π 是二重分歧 Smith-Dold 覆盖。正如 A. Dold 在豪斯多夫情形下的第 1], 节中指出的，从多重集中移除一个元素这一部分定义的运算

$$\mathrm{Sym}^d(Y) \times Y \dashrightarrow \mathrm{Sym}^{d-1}(Y), \qquad (\sigma, y) \mapsto \sigma \setminus y$$

在其定义域上连续。这立即推出群 A 中取逆元运算的连续性，该运算由公式 $(x,p)^{-1} = (x,p')$ 定义，其中 $[p,p'] = x*t$。

注14.5. 请注意二重 Smith-Dold 分歧覆盖的特点：在此类覆盖的全空间上，总存在一个交换各片的连续对合。在我们的情形中，这个对合是群 A上的对跖对合。~对于 d 重 Smith-Dold 分歧覆盖 $Y \to Y$ （其中 $d > 2$ ），情况~则更为复杂：一般来说，空间 Y 本身上并不存在阶为 d 的群作用。尽管如此，Buchstaber 和 Rees [14], 利用 Dold 的结果 [20],构造了一个关联的 $d!$ 重分歧覆盖 E，它覆盖 Y，并带有置换群 S_d的作用~，使得 $Y = E \times_{S_d} \{1, \ldots, d\}$。

为了证明直积运算的连续性，我们需要以下技术性引理。

~引理 14.6。设 $\pi\colon Y \to Y$是豪斯多夫拓扑空间的 ***Smith-Dold*** 分歧覆盖，$s\colon Y \to Y$是其集合论截面，即满足 $\pi\circ s = \mathrm{id}_Y$的映射。~假设该截面的图像 $\Gamma_s \subset Y \times Y$ 是闭的，则 s 是连续的。

~证明。将 Γ_s 与其在嵌入 $\pi\times\mathrm{id}: Y \to Y \times Y$ 下的原像等同起来，~~~我们可以假设 $\Gamma_s \subset Y$。子集 Γ_s 在 Y中是闭的，因为它在 $Y \times Y$中是闭的。下面证明截面 s 在任意点 $y \in Y$ 处的连续性。任取点 $s(y)$ 的一个邻域 U。设 $y_1 = s(y)$ $y_2, \ldots, y_k$是点 y 在映射 π 下的所有不同原像，不计重数。点 $y_2, \ldots, y_k$不属于图像 Γ_s。因此，由于图像是闭的，它们分别有开邻域 $U_2, \ldots, U_k$与 Γ_s不相交。现在，由投影 π 的多值逆映射的连续性可知，点 y在 Y中有一个开邻域 V，使得集合 $\pi^{-1}(V)$ 包含于

邻域 $U \cup U_2 \cup \cdots \cup U_k$ 的并集中。因此，集合 $s(V)$ 包含于该邻域并集与图像 Γ_s 的交集中，因而也包含于原邻域 U中。于是，映射 s 在点 y处连续。□

让我们从引理 14.6 推导出命题 8.3 中构造的乘法运算 $\bullet$的连续性。考虑由满足条件 $z \in x * y$的所有三元组 $\big((x,p),(y,q),(z,r)\big)$ 组成的闭子集 $B \subset A \times A \times A$，以及到前两个因子的直积上的投影 $\sigma\colon\ B \to A \times A$。容易看出，$\sigma$ 是四重 Smith-Dold 分歧覆盖。事实上，一个连续的四值逆映射会为每个对$\big((x,p),(y,q)\big)$ 指定四个（按重数计）三元组 $\big((x,p),(y,q),(z,r)\big)$，使得 $z \in x*y$ 且$r \in t*z$。根据命题 8.3 中的构造，作为乘积 $(x,p)\bullet(y,q)$，我们需要取满足条件 $\big((x,p),(y,q),(z,r)\big) \in \sigma^{-1}\big((x,p),(y,q)\big)$的 (z,r)，此外还需满足条件 $z \in x*y$, $z \in p*q'$, $z \in p'*q$, $r \in x*q$, $r \in p*y$, $r' \in x*q'$和 $r' \in p'*y$，其中 $t*x=[p,p']$, $t*y=[q,q']$ 且 $t*z=[r,r']$；这些条件总能唯一确定所需的点 (z,r)。这样，

$$s\colon \big((x,p),(y,q)\big) \mapsto \big((x,p),(y,q),(x,p)\bullet(y,q)\big)$$

是分歧覆盖 σ 的集合论截面。如前所述，由豪斯多夫性质可知，点 p'、q' 和 r' 分别连续地依赖于对 (x,p)、(y,q) 和 (z,r)。因此，所列出的每个条件都在 $A \times A \times A$ 中确定一个闭子集。截面 s 的图像是所有这些闭子集与闭集 B 的交集。因此，它是闭的，进而由引理 14.6 可知，截面 s 连续，从而完成定理 14.2 的证明。

特殊拓扑二值群。设 V 是一个具有离散拓扑的布尔群，$\dim V \geq 2$，U 是任意豪斯多夫拓扑布尔群，且 $s \in U$ 是一个不同于 e 的任意元素。考虑带有商拓扑（它总是豪斯多夫的）的商空间 $W = U/\langle s\rangle$。令 $\pi\colon\ U \to W$ 为投影。

现在考虑拓扑空间

$$Y_{V,U,s} = (\{e\} \times U) \sqcup \big((V \setminus \{e\}) \times W\big), \tag{59}$$

其中 $\sqcup$ 表示不交并，并通过公式定义其上的交换的二值乘法

$$(e,u_1)*(e,u_2) = \big[(e,u_1u_2),(e,u_1u_2)\big], \qquad u_1,u_2 \in U,$$
$$(e,u)*(v,w) = \big[(v,\pi(u)w),(v,\pi(u)w)\big], \qquad u \in U,\ v \in V\setminus\{e\},\ w \in W,$$
$$(v,w)*(e,u) = \big[(v,w\pi(u)),(v,w\pi(u))\big], \qquad u \in U,\ v \in V\setminus\{e\},\ w \in W,$$
$$(v_1,w_1)*(v_2,w_2) = \begin{cases} \big[(e,\pi^{-1}(w_1w_2)),(e,\pi^{-1}(w_1w_2))\big], & v_1=v_2^{-1},\ w_1=w_2,\\ \big[(v_1v_2,w_1w_2),(v_1v_2,w_1w_2)\big], & v_1 \neq v_2^{-1}, \end{cases} \qquad v_1,v_2 \in V\setminus\{e\},\ v_1 \neq v_2,\ w_1,w_2 \in W.$$

可以直接验证，$Y_{V,\,U,\,s}$ 是一个特殊的豪斯多夫拓扑二值群。此外，若忽略拓扑，这个二值群与二值群 $Y_V \times W$ 同构。

定理 14.7。任意特殊反演交换豪斯多夫拓扑二值群 X 都同构于以下形式的某个拓扑二值群：$Y_{V,\,U,\,s}$。两个拓扑二值群 $Y_{V_i,\,U_i,\,s_i}$, $i=1,2$ 彼此同构，当且仅当 $V_1 \cong V_2$ 作为抽象群同构，并且存在一个拓扑群同构 $U_1 \cong U_2$，将 s_1 映到 s_2。

证明。定理 13.1 立即推出，若忽略拓扑，则 X 同构于某个形如 $Y_{V,\,U,\,s}$ 的二值群。因此，定理 14.7 的第一条陈述由以下命题得出。

命题 14.8。集合 $Y_{V,\,U,\,s}$ 上的任何豪斯多夫拓扑，只要其上引入的二值乘法运算是连续的，就具有如下形式：某个定义在 $\{e\}\times U = U$ 上的拓扑与 $(V\setminus\{e\})\times W$ 上的积拓扑的不连通并；其中，$\{e\}\times U = U$ 上的拓扑使 U 成为 ***Hausdorff*** 拓扑群，集合 $V\setminus\{e\}$ 赋予离散拓扑，而集合 W 则赋予由 U 上所选拓扑诱导的商拓扑。

证明。考虑二值群 $Y = Y_{V,U,s}$上的任意 Hausdorff 拓扑 $\mathcal{T}$，并假设在此拓扑下二值乘法运算是连续的。我们将子集 $\{e\}\times U$ 与 U 等同，并将二值群 Y的元素 (e,u) 简单记作 u。注意，当且仅当元素 x 属于二值群 Y的子集 $(V\setminus\{e\})\times W$ 时，$s\in x*x$ 成立。由于 Y中的乘法运算是连续的，条件 $s\in x*x$ 在 Y中刻画了一个闭子集。因此，子集$\{e\}\times U$在 Y中是开集。记 $\mathcal{T}_U$为拓扑 $\mathcal{T}$在 U上的限制；则 $(U,\mathcal{T}_U)$ 是一个拓扑群。记 $\mathcal{T}_W$ 为拓扑 $\mathcal{T}_U$ 在投影 $\pi\colon U\to W$下的商拓扑。

我们还需证明，集合 $\{v\}\times W$ 中的每一个集合在 Y中也是开集，并证明拓扑 $\mathcal{T}|_{\{v\}\times W}$ 与 $\mathcal{T}_W$ 在将 $\{v\}\times W$与 W作标准等同后所得的商拓扑一致。令 $y = (v,e)$；则公式 $x\mapsto x*y$定义了一个连续映射 $\mu_y\colon Y\to \mathrm{Sym}^2(Y)$。首先注意，集合 $\{v\}\times W$与映射 μ_y下开集 $\mathrm{Sym}^2(U)$ 的逆像一致，因此 $\{v\}\times W$ 是开集。其次，将映射 μ_y 限制在集合 $\{e\}\times U$上时，其两个分支重合，并定义了一个连续映射 $\nu_y\colon \{e\}\times U\to\{v\}\times W$，该映射与映射 $(e,u)\mapsto\big(v,\pi(u)\big)$一致。第三，映射 $\mu_y|_{\{v\}\times W}$是映射 ν_y的连续二值逆。因此，ν_y 是一个二重 Smith-Dold 分歧覆盖，这立即说明集合 $\{v\}\times W$ 上的拓扑与商拓扑 $\mathcal{T}_W$一致。□

定理 14.7 的第二个断言由以下事实得出：从拓扑二值群 $Y = Y_{V,\,U,\,s}$ 可以在同构意义下唯一恢复拓扑布尔群 U、其元素 s 以及离散布尔群 V。事实上，$U\subset Y$ 是由单位元和所有 2 阶元素构成的子群，其拓扑取自子集拓扑；s是所有 4 阶元素的平方，而 $V\cong Y/U$。□

由阶为 1、2 和 4 的元素构成的非特殊拓扑二值群。这里我们给出一个例子，说明在这种情形下会出现根本性的新效应，而且定理 9.1 的直接类比并不成立。

首先，我们注意到，拓扑二值群不存在直接因子分解结果的类似结论，例如命题 6.2 和命题 6.3。这是因为，即便对于通常的交换豪斯多夫拓扑群，也不存在定义良好的取商群运算，能使结果仍属于豪斯多夫拓扑群范畴（例如，当一个子群在群中稠密时）。因此，在拓扑情形下，自然的做法是将幺幂级数 $X_V^{\mathbf{u}}\times W$ 的定义推广如下。

我们需要以下范畴 $\mathcal{P}$，称为豪斯多夫拓扑布尔群对范畴。此范畴的对象是对 (V,U)，其中

- V和 U 是豪斯多夫拓扑布尔群，分别关于某些拓扑 $\mathcal{T}_V$ 和 $\mathcal{T}_U$（它们是结构的一部分）；
- U 是群 V的子群，且包含映射 $U\subset V$ 关于拓扑 $\mathcal{T}_U$ 和 $\mathcal{T}_V$是连续的。

请注意，我们并未要求拓扑 $\mathcal{T}_U$ 与拓扑 $\mathcal{T}_V$ 在 U上的限制相同；定义仅意味着 $\mathcal{T}_U$ 的拓扑要么与其

限制相同，要么比它更精细。在范畴 $\mathcal{P}$ 中，从对象（V_1, U_1）到对象（V_2, U_2）的态射是一个交换图

$$\begin{array}{ccc} U_1 & \xrightarrow{\alpha} & U_2 \\ \cap & & \cap \\ V_1 & \xrightarrow{\beta} & V_2 \end{array}$$

其中，α 是关于拓扑 $\mathcal{T}_{U_1}$ 和 $\mathcal{T}_{U_2}$连续的同态，而 β是关于拓扑 $\mathcal{T}_{V_1}$ 和 $\mathcal{T}_{V_2}$连续的同态。我们将范畴 $\mathcal{P}$ 豪斯多夫拓扑布尔群对中的对象称为.....

设(V, U)是范畴 $\mathcal{P}$中的一对。考虑由公式确定的连续幺幂对合$\iota_{\mathbf{u}}$: $U \times V \to U \times V$

$$\iota_{\mathbf{u}}(u, v) = (u, uv).$$

那么，陪集二值群

$$X^{\mathbf{u}}_{V,U} = (U \times V)/\iota_{\mathbf{u}} \tag{60}$$

是一个对合交换豪斯多夫拓扑二值群。

在子群 U 被指定为拓扑直因子 $V = U \times W$，且拓扑 $\mathcal{T}_V$为直积拓扑这一特殊情形下，此构造得到拓扑二值群$X^{\mathbf{u}}_{V,\ U} \cong X^{\mathbf{u}}_{U} \times W$。

记 $\mathcal{C}$ 为由阶为 1、2 和 4 的元素及其连续同态组成的非特殊对合交换豪斯多夫拓扑二值群范畴。定理 9.1 的一个自然类比是：范畴 $\mathcal{C}$ 中的任一拓扑二值群都同构于以下两种形式之一：其一是形如 $X^{\mathbf{a}}_{A}$的二值群，其中 A 是由阶为 1、2 和 4 的元素组成的豪斯多夫拓扑群；其二是形如$X^{\mathbf{u}}_{V,\ U}$的二值群，其中(V, U)是豪斯多夫拓扑布尔群对。然而，下文将给出一个例子，说明这一说法并不成立。

在构造这个例子之前，我们先讨论如何将第 9 节和第 10 节中的上同调分类方法应用于这里考虑的拓扑情形，以及过程中会出现哪些问题。

设 X 是范畴 $\mathcal{C}$ 中的一个拓扑二值群。用 V 表示 X 中所有阶为 1 或 2 的元素构成的布尔群，其上赋予由嵌入 $V \subset X$ 诱导的豪斯多夫拓扑 $\mathcal{T}_V$。用 $U \subset V$ 表示由所有满足 $x \in X.$ 的元素 x^2 构成的子群。与引理 9.2 类似，对于每个元素 $u \in U$，集合 X_u （由所有满足 $x^2 = u$ 的 x 构成）是一个 V-轨道。此外，该轨道中各元素的稳定子为子群 $\{e, u\} \subset V$；并且，若 $x \in X_u$、$y \in X_w$ 且 $x * y = [z_1, z_2]$，则 z_1、$z_2 \in X_{uw}$ 且 $z_2 = uz_1 = wz_1$。因此，存在一个典范双射 $X/V \leftrightarrow U$，而 U 中的（单值）乘法由 X 中的二值乘法诱导。我们在 U 上赋予商拓扑 $\mathcal{T}_{U.}$。先验地说，这个拓扑是否为豪斯多夫拓扑并不明显。不过，我们注意到，X 中平方运算的连续性蕴含嵌入 $X/V = U \subset V$ 的连续性，其中 U 赋予商拓扑 $\mathcal{T}_U$，而 V 赋予子空间拓扑 $\mathcal{T}_V$。因此，拓扑 $\mathcal{T}_U$ 是豪斯多夫的，并且有序对 (V, U) 是范畴 $\mathcal{P}$ 中的一个对象。因此，所构造的对应

$$X \mapsto (V, U)$$

定义了一个从 $\mathcal{C}$ 范畴到 $\mathcal{P}$范畴的函子，我们将其记为 Φ。

可以直接验证，对于范畴 $\mathcal{P}$ 中的任意一对 (V, U)，$\Phi(X^{\mathbf{u}}_{V,\ U}) = (V, U)$。特别地，这意味着拓扑二值群 $X^{\mathbf{u}}_{V_1,\ U_1}$ 和 $X^{\mathbf{u}}_{V_2,\ U_2}$

当且仅当拓扑布尔群的对 (V_1, U_1) 和 (V_2, U_2) 同构时，它们才同构。

函子 Φ 使我们能够将对范畴 $\mathcal{C}$ 中拓扑二值群 X 进行分类的问题，拆分为若干独立问题：对每个给定的（在同构意义下）对 $\Phi(X) = (V, U)$，分别对所有可能的 X 进行分类。若在每个 V-轨道 X_u（其中 $u \in U$）中选取一个代表元 x_u（使得 $x_e = e$），那么二值群 X 中的乘法便由代表元 x_u的乘法规则唯一确定，其形式如下

$$x_u * x_v = \varphi(u, v)[x_{uv}, ux_{uv}], \qquad u, v \in U, \tag{61}$$

某些 对合对称拟余循环 φ: $U \times U \to V$，也就是说，一个满足以下条件的映射 t

$$\varphi(u, v) \equiv \varphi(v, u) \pmod{\langle u, v\rangle}, \tag{62}$$

$$\varphi(u, u) \equiv \varphi(e, u) \equiv \varphi(u, e) \equiv e \pmod{\langle u\rangle}, \tag{63}$$

$$\varphi(u, v)\varphi(uv, w)\varphi(u, vw)\varphi(v, w) \in \langle u, v, w\rangle \tag{64}$$

对所有 u、v、$w \in U$,

到目前为止，与第 9 节中的情况相比，唯一的区别是群 U 不一定与 V相同。不过，现在我们需要确保由公式 (61) 给出的乘法是连续的。自然地，为了保证乘法的连续性，我们希望从 V-轨道 $u \mapsto x_u$ 中选取代表元的映射 $U \to X$ 是连续的（相对于 U 上的拓扑 $\mathcal{T}_U$）。如果范畴 $\mathcal{C}$ 中的拓扑群 X 具有从 V-轨道 $u \mapsto x_u$中选取代表元的连续映射，我们就称它为驯服的；若不存在这样的连续映射，则称它为野性的。由此便引出了第一个基本问题。

问题 14.9. 范畴 $\mathcal{C}$ 中是否包含野性的拓扑二值群?

作者目前尚不清楚这个问题的答案。一方面，没有合理的论据支持否定的回答，尤其是考虑到拓扑空间 U 并非单连通。另一方面，迄今为止，我们未能构造出一个野性二值群的例子。

接下来，我们将重点研究范畴 $\mathcal{C}$中的驯顺二值群，并证明即使在这些群中，也存在一个既不属于主系列、也不属于幺幂级数的拓扑群。首先，我们证明，作为拓扑空间，二值群 X 与幺幂二值群$X^{\mathbf{u}}_{V,\,U} = (U \times V)/\iota_{\mathbf{u}}$同胚。

命题 *14.10.* 设 X 是范畴 $\mathcal{C}$中的一个驯拓扑二值群，且 $\Phi(X) = (V, U)$。那么，作为拓扑空间，二值群 X 与幺幂二值群 $X^{\mathbf{u}}_{V,U} = (U \times V)/\iota_{\mathbf{u}}$同胚。更确切地说，若 $u \mapsto x_u$ 是二值群 X的 V-轨道中代表元选择的连续映射，则由公式 $g(u, v) = vx_u$ 定义的映射 g: $U \times V \to X$ 诱导出一个同胚 $\bar{g}$: $(U \times V)/\iota_{\mathbf{u}} \approx X$。

证明。由于群 V 作用于轨道 Vx_u 上时，每个元素的稳定子都等于 $\{e, u\}$，可知 $\bar{g}$ 是一个双射。映射 g （因此映射 $\bar{g}$）的连续性，来自映射 $u \mapsto x_u$ 的连续性以及二值群 X 中乘法的连续性。记 $X \to X/V = U$ 的（连续）投影为 π。映射 g 存在一个二值连续逆映射 $X \to \mathrm{Sym}^2(U \times V)$，其定义由公式 $x \mapsto [\pi(x)\ x * x_{\pi(x)}]$ 给出。（因此， g 是一个二重 Smith-Dold 分歧覆盖。）由此立即可得映射 $\bar{g}^{-1}$ 的连续性。□

因此，任意一个满足 $\Phi(X) = (V, U)$ 的驯顺二值群 X，都可以视为幺幂级数 $X^{\mathbf{u}}_{V,\ U}$ 的二值群，其乘法按照公式 (61) 由一个对合对称拟余循环 φ 变形而来。（回想一下，正如第 9 节所示，平凡拟余循环对应于二值群 $X^{\mathbf{u}}_{V,\ U}$ 本身。）我们将用记号 $X_{V,\ U,\ \varphi}$ 表示具有乘法 (61) 的二值群。

容易验证，要使二值群 $X_{V,\ U,\ \varphi}$ 中的乘法连续，必要且充分条件是拟余循环 φ 在以下意义下拟连续。事实上，回顾一下，每个值 $\varphi(u, v)$ 并非唯一确定，而是相差一个来自 $\langle u, v\rangle$ 的元素的乘法。若拟余循环φ: $U \times U \to V$的四值映射 $U \times U \to \mathrm{Sym}^4(V)$ 由公式定义，且拟连续，则称其为拟连续：

$$(u, v) \mapsto \big[\varphi(u, v), u\varphi(u, v), v\varphi(u, v), uv\varphi(u, v)\big],$$

是连续的。

若不选择 V-轨道 x_u 的代表元集合，而改选另一组代表元 x'_u，其中仍有 $x'_e = e$，则对于某个映射 χ: $U \to V$，有 $x'_u = \chi(u)x_u$，使得$\chi(e) = e$。此时，拟余循环 φ 将替换为拟余循环 φ'，满足

$$\varphi'(u, v) \equiv \varphi(u, v)\chi(u)\chi(v)\chi(uv) \pmod{\langle u, v\rangle}. \tag{65}$$

此外，当且仅当映射 χ 在以下意义下拟连续时，向新代表元集合 x'_u 的转换才连续依赖于 u：由公式给出的二值映射$U \to \mathrm{Sym}^2(V)$

$$u \mapsto \big[\chi(u), u\chi(u)\big]$$

是连续的。

因此，自然地，若两个拟连续对合对称拟余循环 φ和 φ' 上同调等价，即存在某个拟连续映射 χ，使得它们满足关系式 (65)： $U \to V$ 其中 $\chi(e) = e$，那么以下命题 9.5 的类似结论成立。

命题14.11. 拓扑二值群 $X_{V,\ U,\ \varphi}$ 和 $X_{V',\ U',\ \varphi'}$ 同构，当且仅当存在拓扑布尔群对 $(V,\ U)$ 和 $(V',\ U')$ 之间的一个同构，将拟连续拟余循环 φ 映为一个与 φ' 上同调等价的拟连续拟余循环。特别地，$X_{V,\ U,\ \varphi}$ 同构于 $X^{\mathbf{u}}_{V,\ U}$，当且仅当拟连续拟余循环 φ 上同调平凡。

记 $\mathcal{H}_{\mathrm{qc}}(U, V)$ 为拟连续拟余循环 $U \times U \to V$ 的上同调类所构成的布尔群。因此，满足 X 使得 $\Phi(X) = (V, U)$ 的驯拓扑二值群的分类归结为以下问题。

问题 14.12： 描述群 $\mathcal{H}_{\mathrm{qc}}(U,\ V)$。

自然存在一个遗忘拓扑同态

$$f\colon \mathcal{H}_{\mathrm{qc}}(U, V) \to \mathcal{H}(U, V),$$

其中， $\mathcal{H}(U, V)$ 是由任意映射 χ（同样不要求拟连续性）定义的上同调等价类所构成的布尔群，其元素为所有拟余循环（不要求拟连续性）。利用引理 9.6，容易验证同构 $\mathcal{H}(U, V) \cong \mathcal{H}(U)$ 总是成立，因此当 $\dim U \leq 2$ 时，群 $\mathcal{H}(U, V)$ 是平凡的；当 $\dim U \geq 3$ 时， $\mathcal{H}(U, V) \cong C_2$。显然，在一般情形下，同态 f 既不是单射，也不是满射。

现在我们给出同态 f 的核中的一个元素示例，由此可以从范畴 $\mathcal{C}$ 构造一个驯拓扑二值群，它既不属于对踵族 $X_A^{\mathbf{a}}$，也不属于幂零族 $X_{V,\,U}^{\mathbf{u}}$。在我们的例子中，$U = V$，因此从现在起，我们将用 $\mathcal{H}_{\mathrm{qc}}(V)$ 代替 $\mathcal{H}_{\mathrm{qc}}(V,V)$，并用 $X_{V,\,\varphi}$ 代替 $X_{V,\,V,\,\varphi}$。

为构造上述例子，我们需要自由拓扑布尔群这一概念。设 Y 是一个完全正则豪斯多夫拓扑空间。A.A. Markov [30] 引入了以 Y 为基的自由拓扑群和自由阿贝尔拓扑群的概念。我们将需要一个类似的、以 Y 为基的自由布尔群 $B(Y)$ 概念，见 [36]。从代数角度看，$B(Y)$ 就是一个布尔群 C_2^Y，也就是说，它是域 $\mathbb{F}_2$ 上的向量空间，其基为集合 Y。在 $B(Y)$ 上，我们取一个与群结构相容并满足以下两个条件的拓扑：

(1) 基 $Y \hookrightarrow B(Y)$ 的嵌入是到其像上的同胚；(2) 将空间 Y 映射到任意布尔拓扑群中的任意连续映射，都可延拓为从群 $B(Y)$ 到该拓扑群的连续同态。

这样的拓扑存在且唯一；同时，在所有与群结构相容并满足条件（1）的拓扑中，它是最细的，而在所有与群结构相容并满足条件（2）的拓扑中，它是最粗的。关于自由拓扑群和自由阿贝尔拓扑群中这些陈述的类似结论的证明，见 [30] 和 [23]；将这些结果推广到布尔情形所需的内容可见 [36]。

群 $B(Y)$ 的元素可以解释为空间 Y 的有限子集（按通常意义，即不计重数）。在这种情形下，群中的运算是子集的对称差，单位元是空集。为方便起见，我们将子集 u 与 v 的对称差记作 uv。

我们关注 Y 为带有度量 d 的紧致度量空间的情形。此时，$B(Y)$ 上的自由拓扑布尔群的拓扑可以如下描述，见 [23], [36]。

对于每个子集 $v \in B(Y)$，定义其 范数 $\|v\|$，其取值于 $\mathbb{R}_{\geq 0} \cup \{+\infty\}$，如下所示：

- 如果集合 v 包含偶数个元素，则 $\|v\|$ 是以下各和的最小值

$$\sum_{i=1}^{k} d(p_i, q_i)$$

其中遍历将集合 v 划分为两两不交的配对 $\{p_1, q_1\}$、……、$\{p_k, q_k\}$ 的所有划分；

- 如果集合 v 包含奇数个元素，则 $\|v\| = +\infty$。

所构造的函数在以下意义下是一个范数：

- $\|v\| \geq 0$ 对所有 v，且当且仅当 $v = e$ 时，$\|v\| = 0$；
- $\|uv\| \leq \|u\| + \|v\|$。

引入的范数类似于 A. A. Markov [30] 和 M.I. Graev [23] 针对拓扑布尔群所定义的半范数；具体公式见 [36, 第 2] 节。因此，函数

$$\rho(u, v) = \|uv\|$$

定义了 $B(Y)$ 上取值于 $\mathbb{R}_{\geq 0} \cup \{+\infty\}$ 的良定义 ∞-度量。我们可以考察 $B(Y)$ 上相应的度量拓扑，但那并不是我们所需要的拓扑。我们需要的拓扑更精细，具体构造如下。

对于每个 $k \geq 0$，我们用 $B_k(Y)$ 表示群 $B(Y)$ 的子集，该子集由所有至多包含 k 个元素的 $v \subset Y$ 的子集组成。赋予每个集合 $B_k(Y)$ 由度量 ρ 诱导的度量拓扑。 $B(Y)$ 上自由拓扑布尔群的所需拓扑，就是这些度量拓扑的归纳极限拓扑。这意味着，集合 U 在 $B(Y)$ 中是开的，当且仅当交集 $U \cap B_k(Y)$ 在 $\big(B_k(Y)\ \rho\big)$ 中对每个 k 都是开的。

非形式地说， $B(Y)$可视为 Y 上有限点集的一个构形空间，其规则是：当一对点发生碰撞时，它们都会消失。特别地，容易看出，若 Y 是道路连通的，则 $B(Y)$由两个道路连通分支组成： $B_{even}(Y)$和 $B_{odd}(Y)$，它们分别由所有基数为偶数和奇数的子集构成。

例 14.13。设 $K \subset \mathbb{R}^d$ 为维数 $d \geq 1$的有限维欧几里得空间中的一个紧凸体（即内部非空的凸集）。考虑一个自由拓扑布尔群 $B(K)$。

我们通过以下公式定义一个拟余循环 φ: $B(K) \times B(K) \to B(K)$

$$\varphi(u,v) = \prod_{p\in u}\prod_{q\in v}\left\{\frac{p+q}{2}\right\}, \tag{66}$$

其中， $\{\cdot\}$ 表示一个单点子集。可以直接验证，映射 φ 满足条件（62）–（64），即它确实是一个对合对称拟余循环。此外，显然映射 φ 是连续的，并且还是拟连续的。

命题 14.14. 设 φ: $B(K) \times B(K) \to B(K)$ 是由公式(66)给出的拟余循环。那么

(a) 若不考虑布尔群 $B(K)$上的拓扑，拟余循环 φ 便成为上同调平凡的；换言之，φ 在群 $\mathcal{H}(B(K))$中表示一个平凡类；(b)拟余循环 φ 作为拟连续拟余循环是上同调非平凡的，也就是说，它在群 $\mathcal{H}_{\mathrm{qc}}(B(K))$中表示一个非平凡类。

证明。我们来证明陈述 (a)。定义一个不连续映射 χ_0: $B(K) \to B(K)$，其公式为

$$\chi_0(v) = \prod_{\{p,q\}\subset v,\ p\neq q}\left\{\frac{p+q}{2}\right\}, \tag{67}$$

其中，直积遍历集合 v 的所有无序子集 $\{p,q\}$ 。容易看出

$$\varphi(u,v) = \chi_0(u)\chi_0(v)\chi_0(uv) \tag{68}$$

对所有 $u, v \in B(K)$ 均成立，由此立即得到陈述 (a)。注意，由公式 (67) 定义的映射 χ_0 不是拟连续的，因此等式 (68) 并不能推出拟余循环 φ 在群 $\mathcal{H}_{\mathrm{qc}}(B(K))$中的上同调平凡性。

我们用反证法证明命题（b）。假设 φ 作为拟连续拟余循环是上同调平凡的。那么存在一个拟连续映射χ: $B(K) \to B(K)$，使得 $\chi(e) = e$ 并且

$$\varphi(u,v) \equiv \chi(u)\chi(v)\chi(uv) \pmod{\langle u,v\rangle}$$

对于所有的 u， $v \in B(K)$。

将 χ 限制在集合 K 的单元素子集上，我们得到映射 $K \to B(K)$,$q \mapsto \chi(\{q\})$。这个映射是拟连续的，具体来说，二值映射

$$q \mapsto \big[\chi(\{q\}), \{q\}\chi(\{q\})\big] \tag{69}$$

是连续的。现在注意，在两个元素 $\chi(\{q\})$ 和 $\{q\}\chi(\{q\})$ 中，恰有一个总是落在连通分支 $B_{even}(K)$ 中，另一个则落在 $B_{odd}(K)$ 中。因此，如果我们总是从这两个元素中选取落在 $B_{even}(K)$ 中的那个，就得到了二值映射 (69) 的一个连续单值分支。

$$\psi(\{q\}) = \begin{cases} \chi(\{q\}) & \text{if } \chi(\{q\}) \in B_{even}(K), \\ \{q\}\chi(\{q\}) & \text{if } \chi(\{q\}) \in B_{odd}(K). \end{cases}$$

于是，映射 $q \mapsto \psi(\{q\})$ 是连续的。我们通过如下设定，将映射 ψ 扩展为连续同态 $\psi\colon B(K) \to B_{even}(K)$:

$$\psi(v) = \prod_{q \in v} \psi(\{q\}).$$

我们用新映射 $\widetilde{\chi}\colon B(K) \to B(K)$ 替换映射 χ，使得

$$\widetilde{\chi}(v) = \chi(v)\psi(v)$$

对所有 $v \in B(K)$ 均成立。由于 ψ 是同态，我们仍有 $\widetilde{\chi}(e) = e$，并且

$$\varphi(u, v) \equiv \widetilde{\chi}(u)\widetilde{\chi}(v)\widetilde{\chi}(uv) \pmod{\langle u, v\rangle} \tag{70}$$

对所有 $u, v \in B(K)$ 均成立。此外，由同态 ψ的连续性可知，映射 $\widetilde{\chi}$ 仍然是拟连续的。

根据构造，对于任意点 $q \in K$，要么 $\widetilde{\chi}(\{q\}) = e$，要么 $\widetilde{\chi}(\{q\}) = \{q\}$。设 p和 q 是集合 K中的两个不同点。对有序对 (u, v) 应用同余 (70) $= (\{p\}, \{q\})$，可得

$$\left\{\frac{p+q}{2}\right\} \subseteq \widetilde{\chi}(\{p, q\}) \subseteq \left\{\frac{p+q}{2}, p, q\right\}.$$

此外，注意集合 $\{p, q\}$ 与空集 e属于空间 $B(K)$ 的同一个连通分支 $B_{even}(K)$。映射 $\widetilde{\chi}$ 的拟连续性意味着，无序对 $\big[\widetilde{\chi}(w)\ w\widetilde{\chi}(w)\big]$ 随 w连续变化。若 $w = e$，则该对中的两个集合均为空，因此都属于 $B_{even}(K)$。因此，集合 $\widetilde{\chi}(\{p, q\})$ 和 $\{p, q\}\widetilde{\chi}(\{p, q\})$ 也都属于 $B_{even}(K)$。所以，$\widetilde{\chi}(\{p, q\})$ 是这两个集合之一：$\{(p+q)/2, p\}$ 或 $\{(p+q)/2, q\}$。

现在设 p、q 和 r 是集合 K 中的三个点，使得 6 个点 p、q、r、$(p+q)/2$、$(q+r)/2$、$(r+p)/2$ 两两不同。于是，由关于对 $(u, v) = (\{p, q\}, \{r\})$ 的同余 (70) 可知，集合 $\widetilde{\chi}(\{p, q, r\})$ 恰好包含点 p 和 q中的一个。然而，同理，该集合恰好包含点 p 和 r中的一个，也恰好包含点 q 和 r中的一个。综合这三条结论便会导出矛盾，从而完成命题的证明。□

推论 14.15。驯服的拓扑二值群 $X_{B(K),\,\varphi}$ 不同构于（作为拓扑群）任何主系列的二值群 $X_A^{\mathbf{a}}$，也不同构于任何幂零系列的二值群 $X_{V,\,U}^{\mathbf{u}}$。

证明。由命题 14.14 的陈述 (a) 可知，作为抽象二值群，也就是说，忘掉拓扑之后，二值群$X_{B(K),\,\varphi}$ 与幺幂级数的二值群 $X_{B(K)}^{\mathbf{u}}$ 同构。由此立即可得（根据定理 13.1），即使不考虑拓扑，$X_{B(K),\,\varphi}$ 也不与主系列中的任何群 $X_A^{\mathbf{a}}$ 同构。

我们有 $\Phi\big(X_{B(K),\varphi}\big) = \big(B(K)\ B(K)\big)$。因此，拓扑二值群 $X_{B(K),\varphi}$ 显然不可能同构于任何幺幂级数中的拓扑二值群

除了二值群$X^{\mathbf{u}}_{B(K),B(K)} = X^{\mathbf{u}}_{B(K)}$之外。拓扑群 $X^{\mathbf{u}}_{B(K)}$ 和 $X_{B(K),\varphi}$ 不同构，这可由拟余循环 φ 在群 $\mathcal{H}_{\mathrm{qc}}(B(K))$ 中的上同调非平凡性以及命题 14.11 得出。□

注 14.16。余循环 φ 的构造可以有相当大的变化，使得命题 14.14 和推论 14.15 仍然成立（而且它们的证明完全相同）。具体而言，我们可以考虑任意具有以下形式的拟余循环

$$\varphi(u,v) = \prod_{p\in u}\prod_{q\in v} F(p,q),$$

其中 $F\colon\ K\times K\to B_{odd}(K)$ 是任意对称连续映射，满足 $F(q,q) = \{q\}$ 对所有 $q\in K$ 均成立。在这种情形下，只需集合 K 具有路径连通性，凸性并不重要：我们之所以需要凸性，仅仅是为了使所选的特定映射 $F(p,q) = \{(p+q)/2\}$ 定义良好。

15. 局部紧二值群

最重要的一类拓扑群是局部紧（豪斯多夫）拓扑群。这类群具有丰富的结构理论，其发展主要与希尔伯特第五问题的解决相关。对这个问题最常见的表述如下：每一个作为拓扑流形的拓扑群是否都同构于某个李群？

关于本文讨论的问题，我们主要关注交换局部紧群。它们的结构理论基础由 L.S. Pontryagin [34], [35]的著作奠定；尤其是，他为交换群的希尔伯特第五问题给出了肯定的解答。E. Gleason [22] 以及 D. Montgomery 和 L. Zippin [31]则为一般情形下的希尔伯特第五问题给出了肯定的解答。后来，针对局部紧群，人们又得到了更强的结构定理。

对我们而言，最重要的是下面这个关于无小子群的局部紧群的定理。根据定义，若一个拓扑群包含一个不含非平凡子群的单位元邻域，则称该群没有小子群。

定理15.1（Gleason–Yamabe 定理）。设 G 是一个没有小子群的局部紧豪斯多夫拓扑群，则 G 同构于一个李群。

注 15.2. 该定理的结论由 E. Gleason [22] 在群为有限维这一附加假设下证明；一般情形则由 H. Yamabe [46] 证明，另见专著 [38, 推论 1.5.8]。

众所周知，任意交换李群都可以表示为紧致环面（$(S^1)^m$）、向量群 $\mathbb{R}^n$和离散阿贝尔群的直积。因此，在交换情形下，Gleason–Yamabe 定理可表述如下。

推论15.3。设 G 是一个没有小子群的交换局部紧豪斯多夫拓扑群。那么 $G\cong (S^1)^m\times\mathbb{R}^n\times A$，其中 $m\ge 0$、$n\ge 0$ 和 A 是离散阿贝尔群。

自然的问题是，如何将这一结果推广到对合交换二值群的情形。与普通群的情形一样，我们称一个拓扑二值群没有小子群，如果它包含一个不含非平凡二值子群的单位元邻域。

定理 15.4。 设 X 是一个没有小子群的对合交换局部紧豪斯多夫拓扑二值群。那么以下两种情况必有其一：

(1) $X \cong \big((S^1)^m \times \mathbb{R}^n \times A\big)/\iota_{\mathbf{a}}$，其中 $m \geq 0$、 $n \geq 0$、 $m+n>0$、 A 是一个离散阿贝尔群，且 $\iota_{\mathbf{a}}$ 是对跖对合；(2) X 是离散的。

注 15.5. 离散二值群当然总是局部紧的，并且不含小子群。离散对合交换二值群的分类由定理 13.1 给出。

为了证明定理 15.4，我们需要两个简单的引理。

引理 15.6. 设 X 是一个豪斯多夫拓扑二值群，其单位元为 e。假设单元素集合 $\{e\}$ 是开集。则 X 是离散的。

证明。在 $\mathrm{Sym}^2(X)$ 中考虑子集 W ，它由所有形如 $[e,x]$ 的多重集组成，其中 $x \in X$。集合 $\{e\}$ 在 X 中是开集这一事实，立即推出集合 W 在 $\mathrm{Sym}^2(X)$ 中是开集。对于任意元素 $y \in X$，乘以 y 定义了一个连续映射 $\mu_y\colon X \to \mathrm{Sym}^2(X)$。由于 $e \in x*y$ 当且仅当 $x=y$，于是 $\mu_y^{-1}(W) = \{y\}$。因此，所有单元素集合 $\{y\}$ 都是开集，故 X 上的拓扑是离散的。□

引理 15.7. 设 X 满足定理 *15.4* 的条件。那么在 X 中存在一个不含 *2* 阶和 *4* 阶元素的单位元邻域。

证明。设 U 是二值群 X的一个不含非平凡二值子群的单位元开邻域。令 U' 为由 $x \in X$ 中所有满足 $x^2 \in U$的元素组成的集合。由于映射 $x \mapsto x^2$ 是连续的， U' 也就是单位元的一个开邻域。

注意，集合 U 不含 2 阶元素。事实上，若 U 中存在一个 2 阶元素，也就是说，存在一个元素 $x \neq e$ 满足 $x*x=[e,e]$，那么集合 $\{e,x\}$ 就是包含于 U中的一个非平凡二值子群。任意四阶元素的平方都是一个 2 阶元素。此外， U'中元素的平方属于 U。因此，集合 U'不含四阶元素。于是，我们可以取集合 $U \cap U'$作为所需的邻域。□

定理 15.4 的证明。根据引理 15.7，设 V 是单位元的一个开邻域，其中不含 2 阶或 4 阶元素。假设二值群 X 不是离散的。那么根据引理 15.6，单元素集合 $\{e\}$ 不是开集。因此，邻域 V 至少包含一个不同于 e 的元素 t。于是 $\operatorname{ord} t \notin \{1,2,4\}$。根据定理 14.2，存在一个同构 $X \cong G/\iota_{\mathbf{a}}$，其中 G 是交换豪斯多夫拓扑群， $\iota_{\mathbf{a}}$ 是对跖对合。利用投影 $G \to X$ 是二重 Smith-Dold 分歧覆盖这一事实，容易从二值群 X 的局部紧性推得群 $G.$ 的局部紧性。现在，由于 X 不是离散的，根据 Gleason–Yamabe 定理，存在一个同构 $G \cong (S^1)^m \times \mathbb{R}^n \times A$ ，使其与 $m+n>0$ 同构。□

对于没有小子群的紧二值群，定理 15.4 导出了一个类似于定理 1.10 的完整分类。

定理 15.8。 设 X 是一个没有小子群的带对合的交换紧豪斯多夫拓扑二值群。那么 X 同构于以下二值群之一：

(1) $X^{\mathbf{a}}_{d_1,\dots,d_k}(m) = \big((S^1)^m \times C_{d_1} \times \cdots \times C_{d_k}\big)/\iota_{\mathbf{a}}$, *where* $2 \leq d_i < \infty$ *and* $d_1 | d_2 | \cdots | d_k$;

(2) $X_n^{\mathbf{u}} \times C_2^m$，其中 $n \geq 1$、 $m \geq 0$;

(3) $Y_n \times C_2^m$，其中 $n \geq 1$、 $m \geq 0$。

所列二值群之间的所有同构均由定理 *1.10* 中的同构 (3)、(4) 穷尽。

证明。该定理几乎立即由定理 15.4 和定理 1.10 得出。我们只需验证：对应于不同集合（m； d_1，...， d_k）的拓扑二值群 $X^{\mathbf{a}}_{d_1,\ ...,\ d_k}(m)$ 两两不同构；并且对于 $m \geq 1$, 它们不同构于幂零系列和特殊系列中的二值群。为此，注意到二值群 $X = X^{\mathbf{a}}_{d_1,\ ...,\ d_k}(m)$ 中单位元的连通分支是群 $X_0 = X^{\mathbf{a}}_{\varnothing}(m) = (S^1)^m/\iota_{\mathbf{a}}$，而商群 X/X_0 同构于二值群 $X^{\mathbf{a}}_{d_1,\ ...,\ d_k}$。此外，拓扑二值群 $X^{\mathbf{a}}_{\varnothing}(m)$ 两两不同构，因为它们具有不同的维数；二值群 $X^{\mathbf{a}}_{d_1,\ ...,\ d_k}$ 则根据引理 1.10 两两不同构。定理得证。□

16. 代数双值群

现在，我们按照 [6,7, 17] 讨论交换对合群的代数版本。为简单起见，我们将在复数域 $\mathbb{C}$. 上进行研究。

在最简单的情形下，代数双值乘法律 $(x, y) \mapsto z = x*y$ 在局部坐标中由方程 $F(x, y, z) = 0$ 给出，其中 $F(x, y, z)$ 是一个多项式，它关于变量 x, y, z 对称，且对每个变量的次数均为 2。二值乘法律必须满足结合律条件

$$(x * y) * z = x * (y * z)$$

按照对应理论的意义，即方程组

$$\begin{cases} F(x, y, u) = 0, \\ F(u, z, w) = 0 \end{cases}$$

and

$$\begin{cases} F(y, z, v) = 0, \\ F(x, v, w) = 0 \end{cases}$$

消去 u 和 v 后，定义同一个集合 $(x, y, z, w) \in \mathbb{C}^4$. 。我们还假设

$$F(0, y, z) = (z - y)^2,$$

这意味着 0 是群的（强）单位元。注意，由于对称性，我们有等式 $F(x, y, 0) = (x - y)^2$, , 这意味着相应的群自动是对合的。反过来，对合二值群的加法律必定关于全部三个变量对称，见引理 2.2。

此类群已在 [6, 17], 中分类，其中证明了相应的多项式必须具有如下形式

$$F(x, y, z) = (x + y + z - a_2 xyz)^2 - 4(1 + a_3 xyz)(xy + xz + yz + a_1 xyz), \tag{71}$$

其中， a_1、 a_2、 a_3 是任意参数。一般而言，这种多项式的方程 $F = 0$ 定义了陪集群 $\mathcal{E}/\iota_{\mathbf{a}}$，其中 $\mathcal{E}$ 是椭圆曲线（视为阿贝尔群），而 $\iota_{\mathbf{a}}$: $\mathcal{E} \to \mathcal{E}$ 是对跖对合。

更准确地说，考虑一条标准魏尔斯特拉斯形式的椭圆曲线

$$v^2 = 4u^3 - g_2 u - g_3$$

以及其上的一个点 α，并将相应参数设为

$$a_1 = 3\wp(\alpha), \quad a_2 = 3\wp(\alpha)^2 - \frac{g_2}{4}, \quad a_3 = \frac{1}{4}(4\wp(\alpha)^3 - g_2\wp(\alpha) - g_3), \tag{72}$$

其中，$\wp$是满足方程的经典魏尔斯特拉斯椭圆函数

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3.$$

定理 16.1（[6, 17]）。方程 $F(x, y, z) = 0$，其中对称多项式 $F(x, y, z)$，满足条件 $F(0, y, z) = (z-y)^2$, 当且仅当 F 具有形式（*71*）时，定义了一个代数双值群的结构。

通过变量变换，具有参数（*72*）的形式（*71*）的乘法律 $F(x, y, z) = 0$ 可化为形式 $X \pm Y \pm Z = 0$，其中 F具有形式（*71*）

$$x = (\wp(X) + \wp(\alpha))^{-1}, \quad y = (\wp(Y) + \wp(\alpha))^{-1}, \quad z = (\wp(Z) + \wp(\alpha))^{-1}. \tag{73}$$

相应的二值群与对合陪集双值群$\mathcal{E}/\iota_{\mathbf{a}} = \mathbb{CP}^1$同构，其中 $\mathcal{E}$ 是由方程给出的椭圆曲线

$$v^2 = u^3 + a_1u^2 + a_2u + a_3, \tag{74}$$

而 $\iota_{\mathbf{a}}$ 是其对合 $v \mapsto -v$.

当右侧多项式的根重合时，椭圆曲线退化为有理曲线，相应的对合二值群分别同构于陪集群 $\mathbb{C}^*/\iota_{\mathbf{a}}$ 和 $\mathbb{C}/\iota_{\mathbf{a}}$，其中 $\iota_{\mathbf{a}}(z) = z^{-1}$ 和 $\iota_{\mathbf{a}}(z) = -z$。

有趣的是，一般族 (71) 包含了形式二值群的所有情形；这类群最早由 V. M. Buchstaber 和 S.P. Novikov 在拓扑学中提出 [11,3, 4]: $a_1 = 0$ 的情形对应椭圆上同调，$a_2 = a_3 = 0$ 的情形对应 K-理论，而最退化的情形 $a_1 = a_2 = a_3 = 0$ 对应普通上同调（详情参见 [17]）。

注意，根据参数化 (73)，从代数几何的观点来看，一般方程 (71) 定义了特殊库默尔曲面 $\mathcal{E} \times \mathcal{E}/\pm I$ 的（仿射部分）。V. M. Buchstaber 和 V. Dragovic [8] 结合可积台球讨论了与亏格为 2 的曲线的雅可比簇对应的一般库默尔曲面。嵌入在 $\mathbb{CP}^3$ 中的库默尔曲面上的相应二值群，可用 Klein$_\wp$-函数的加法律 [9] 明确描述。

自然可以假设，一般的代数双值交换对合群是通过陪集构造由阿贝尔簇及其退化得到的，但精确表述的细节仍有待澄清。A. Pillay [33], 运用模型论中的赫鲁绍夫斯基定理所得的结果，可能有助于证明。

一维形式双值群的一般理论实际上已由 V.M. Buchstaber 在 [4], [5]中完成。特别是，那里引入了典范不变算子 d_n 这一概念，并证明，对于由以下关系给出的双值形式加法律

$$z^2 - \Theta_1(x, y)z + \Theta_2(x, y) = 0,$$

典范算子 d_1 的形式为

$$d_1 = \frac{1}{2}\varphi_1(x)\frac{d}{dx} + \frac{1}{8}\varphi_2(x)\frac{d^2}{dx^2}, \tag{75}$$

其中

$$\varphi_1(x)=\frac{\partial\Theta_1(x,y)}{\partial y}|_{y=0},\qquad \varphi_2(x)=\frac{\partial\sigma(x,y)}{\partial y}|_{y=0},$$
$$\sigma(x,y)=\Theta_1^2(x,y)-4\Theta_2(x,y).$$

文中还证明，不变算子代数由典范算子 d_1 自由生成，并为这类群的指数函数给出了一个一般公式。

容易验证，对于代数双值群 (71)，参数化 (73) 中的典范算子 (75) 就是椭圆坐标 X 下的二阶微分算子 $\frac{d^2}{dX^2}$ （或者说，是 Lam´e 算子 $\mathcal{L}=\frac{d^2}{dX^2}-m(m+1)\wp(X)$ 在 $m=0$ 时的特殊情形）。该算子生成一个微分算子代数，此代数在椭圆曲线 (74) 上的平移以及对合 $\iota_{\mathbf{a}}$ 下保持不变。相应的指数函数已在 [6] 中用椭圆函数明确写出。

17. 结语

n 值群的结构理论才刚刚起步，大多数问题仍未解决。

本文完成了有限生成情形以及若干重要拓扑类中二值交换对合群的分类。

一般情形下，最有前景的方向似乎是发展 n值李群理论。特别是，对于由李群 G 通过陪集构造定义的 n值群 G/H,$H\subset\operatorname{Aut}G$ ，自然的研究方向是考察 G上的微分算子代数，这些算子在 G上的（例如左）平移以及自同构群 H. 的作用下保持不变。相应的代数可视为 n值李群的泛包络代数的类似物；一般情形下对此进行研究，似乎是一个重要而有趣的问题。

椭圆二值群的例子表明，二维球面上存在二值李群结构，而它并不具有通常的群结构。关于 n值群结构的拓扑障碍这一问题极具研究价值。正如 H. Hopf [27], 所证明的，如果一个拓扑空间具有带单位元的（单值）乘法，那么该空间的上同调环具有 Hopf 代数结构。不存在这种结构，便构成拓扑空间上存在乘法的障碍。V. M. Buchstaber 和 E. Rees [12, 13] （另见 [14]）证明，空间上存在 n值乘法会导出一种类似的结构，他们称之为 $Hopf$ n-代数。对于四维流形，相应的障碍由 T.E. Panov [32] 进行了研究。他明确列出了上同调具有 Hopf 2-代数结构的四维流形的同伦型。因此，只有该列表中的流形才可能具有二值乘法。值得注意的是，单连通奇异库默尔簇 $\mathcal{E}\times\mathcal{E}/\pm I\approx T^4/\iota_{\mathbf{a}}$是一个二值群，它实现了 Panov 指出的第二 Betti 数为 6 的情形。D.V. Gugnin [25]取得了若干关于球面上多值乘法的结果。

在形式二值群理论中，20 世纪 70 年代，V.M. Buchstaber 的研究取得了重大进展 [3, 4], , 其研究动机是配边理论中的应用 [11]。这些研究尤其揭示了该理论与 Delsarte-Levitan 广义移位算子理论之间的深刻联系 [28]（另见沿此方向的论文 [26]）。论文 [3, 4], 中的方法，以及与.....理论的联系

量子群和霍普夫代数 [12, 13], , 可能有助于在我们问题的更一般背景下开展研究。

在 n值群理论中，存在源自数学多个分支的重要构造。其中一种构造是在非交换群的不可约表示集合上定义 n值群结构，见 [7]。很自然地，可以将这一构造视为用群论术语诠释田中–克莱因对偶性（见 [1]）；它是庞特里亚金对偶在非交换群情形下的类似物。 n值群的对偶理论见 [10], [44], [45]。

再提及一种构造。陪集 n值群的群代数是原群的群代数的一个子代数，由自同构群作用下各轨道中的点之和所生成。一个更一般的、源自群的例子是所谓的舒尔环（见 [43]）。围绕舒尔环问题， [15]中运用数论方法构造了一些非陪集 n值群的例子。

最后，多值映射理论与可积系统理论之间也有重要联系 [16,40, 41], , 其中仍有许多问题尚未解决（例如，参见综述 [17]中的讨论和参考文献）。特别是，A.P. Veselov 的著作 [39, 41] 提出了一种研究多值映射可积性的方法，即考察其迭代的像的数量增长。 [16]讨论了这种方法与多值群理论之间的联系。值得注意的是，Gromov 关于有限生成的多项式增长群几乎都是幂零群这一卓越定理的原始证明，运用了 E. Gleason、D. Montgomery 和 L. Zippin 的研究成果，参见 [24]。

参考文献

[1] E. Bannai, T. Ito 组合代数 I：关联方案。The Benjamin/Cummings Pub- lishing Co., Inc., Menlo Park, CA，1984，xxiv+425页。[2] K.S. Brown 群上同调，Graduate Texts in Math. 87, Springer-Verlag，纽约–柏林，1982，x+306 页。[3] V.M. Buchstaber 二值形式群的分类。Uspekhi Mat. Nauk 28:3(171) (1973)，173–174（俄文）。[4] V.M. Buchstaber 二值形式群。代数理论及其在配边理论中的应用。I。Izv. Akad. Nauk SSSR Ser. Mat. 39:5 (1975)，1044–1064（俄文）；英文译本：Izv. Math., 9:5 (1975)，987–1006。[5] V.M. Buchstaber 二值形式群。代数理论及其在配边理论中的应用。II。Izv. Akad. Nauk SSSR Ser. Mat. 40:2 (1976)，289–325（俄文）；英文译本：Izv. Math., 10:2 (1976)，271–308。[6] V.M. Buchstaber 与椭圆函数加法定理及二值代数群相关的函数方程，Uspekhi Mat. Nauk 45:3(273) (1990)，185–186（俄文）；英文译本：Russian Math. Surveys 45:3 (1990)，213–215。[7] V.M. Buchstaber n值群：理论与应用，Mosc. Math. J., 6:1 (2006)，57–84。[8] V.M. Buchstaber, V. I. Dragovi´c 二值群、库默尔簇与可积台球，Arnold Math. J. 4:1 (2018)，27–57。[9] V.M. Buchstaber, D.V. Leikin 平面代数曲线雅可比簇上的加法律，非线性动力学，论文集，Trudy Mat. Inst. Steklova 251，Nauka，MAIK ‘Nauka/ Interperiodika’，M.，2005，54–126（俄文）；英文译本：Proc. Steklov Inst. Math. 251 (2005)，49–120。[10] V.M. Buchstaber, M.I. Monastyrsky 具有非交换对称性的自旋系统的广义克拉默斯–旺尼尔对偶，J. Phys. A 36:28 (2003)，7679–7692。[11] V.M. Buchstaber, S.P. Novikov 形式群、幂系统与亚当斯算子，Mat. Sb. (N.S.) 84(126):1 (1971)，81–118（俄文）；英文译本：Math. USSR-Sb. 13:1 (1971)，80–116。[12] V.M. Buchstaber, E.G. Rees 多值群与 Hopf n代数，Uspekhi Mat. Nauk, 51:4(310) (1996)，149–150（俄文）；英文译本：Russian Math. Surveys, 51:4 (1996)，727–729。

[13] V.M. Buchstaber, E.G. Rees 多值群、其表示与霍普夫代数，Transform. Groups 2:4 (1997), 325–349。[14] V.M. Buchstaber, E.G. Rees Frobenius n同态、转移与分歧覆盖，Math. Proc. Camb. Phil. Soc. 144:1 (2008)，1–12。[15] V.M. Buchstaber, A.M. Vershik, S.A. Evdokimov, I.N. Ponomarenko 组合代数与多值对合群，Funktsional. Anal. i Prilozhen. 30:3 (1996)，12–18（俄文）；英文译本：Funct. Anal. Appl. 30:3 (1996)，158–162。[16] V.M. Buchstaber, A.P. Veselov 多值群的可积对应与代数表示，Internat. Math. Res. Notices 1996:8 (1996)，381–400。[17] V.M. Buchstaber, A.P. Veselov，Conway地形图、 $PGL_2(\mathbb{Z})$-动力学与二值群，Us- pekhi Mat. Nauk, 74:3(447) (2019)，17–62（俄文）；英文译本：Russian Math. Surveys, 74:3 (2019)，387–430。[18] J.H. Conway, D.A. Smith 四元数与八元数：其几何、算术与对称性。A. K. Peters, Ltd.，Natick, MA，2003，xii+159 页。[19] C.W. Curtis, I. Reiner 有限群表示论与结合代数，Pure Appl. Math. XI，Interscience Publishers（John Wiley & Sons, Inc.旗下部门），纽约–伦敦，1962，xiv+685 页。[20] A. Dold 分歧覆盖、轨道投影与对称幂，Math. Proc. Cambridge Philos. Soc. 99:1 (1986)，65–72。[21] S. Givant, P. Halmos 布尔代数导论，Undergrad. Texts Math.，Springer，纽约，2009，xiv+574 页。[22] A.M. Gleason 无小子群的群，Ann. of Math. (2), 56:2 (1952)，193–212。[23] M.I. Graev 自由拓扑群，Izv. Akad. Nauk SSSR Ser. Mat. 12:3 (1948)，279–324（俄文）。[24] M. Gromov 多项式增长群与扩张映射，Inst. Hautes ´Etudes Sci. Publ. Math. 53 (1981)，53–73。[25] D.V. Gugnin 流形与 nH空间的分歧覆盖，Funktsional. Anal. i Prilozhen. 53:2 (2019)，68–71（俄文）；英文译本：Funct. Anal. Appl., 53:2 (2019)，133–136。[26] D.I. Gurevich 关于多值李群，Uspekhi Mat. Nauk, 39:6(240) (1984)，195–196（俄文）；英文译本：Russian Math. Surveys, 39:6 (1984)，213–214。.[27] H. Hopf 关于群流形及其推广的拓扑，Ann. of Math. (2), 42:1 (1941), 22–52。[28] B.M. Levitan 广义位移算子理论。Nauka，莫斯科，1973，312页（俄文）。[29] G.L. Litvinov 超群与超群代数。Itogi Nauki i Tekhniki. Ser. Sovrem. Probl. Mat. Nov. Dostizh. 26, VINITI，莫斯科，1985，57–106（俄文）；英文译本：J. Soviet. Math. 38:2 (1987)，1734–1761。[30] A.A. Markov 关于自由拓扑群，Izv. Akad. Nauk SSSR Ser. Mat. 9:1 (1945)，3–64（俄文）。[31] D. Montgomery, L. Zippin 有限维群的小子群，Ann. of Math. (2), 56:2 (1952)，213–241。[32] T.E. Panov 关于四维流形的 Hopf 上同调 2-代数的结构，Uspekhi Mat. Nauk 51:1(307) (1996), 161-162（俄文）；英文译本：Russian Math. Surveys, 51:1 (1996)，155–157。[33] A. Pillay 关于多值代数群的一则 टिप्पणी，Proc. Amer. Math. Soc. 137:7 (2009)，2175–2180。[34] L. Pontrjagin 拓扑交换群理论，Ann. of Math. (2), 35:2 (1934)，361–388。[35] L.S. Pontrjagin 拓扑交换群理论，Uspekhi Mat. Nauk 2 (1936)，177–195（俄文）。[36] O. Sipacheva 自由布尔拓扑群，Axioms 4:4 (2015)，492–517。[37] L. Smith 转移与分歧覆盖，Math. Proc. Cambridge Philos. Soc. 93:3 (1983), 485–493。[38] T. Tao 希尔伯特第五问题及相关主题，Grad. Stud. Math. 153，Amer. Math. Soc., Providence, RI，2014，xiv+338页。[39] A.P. Veselov 多值映射迭代下一个点的像的数量增长，Mat. Zametki 49:2 (1991)，29–35（俄文）；英文译本：Math. Notes 49:2 (1991)，134–139。[40] A.P. Veselov 可积映射，Uspekhi Mat. Nauk 46:5(281) (1991)，3–45（俄文）；英文译本：Russian Math. Surveys, 46:5 (1991)，1–51。

[41] A.P. Veselov映射动力学中的增长与可积性, Comm. Math. Phys. **145**:1 (1992), 181–193.[42] E.B. Vinberg 代数教程。 Factorial Press, 莫斯科, 2001, 544 pp. (俄文); 英译本：Grad. Stud. Math. **56**, Amer. Math. Soc., 罗得岛州普罗维登斯, 2003, x+511 pp.[43] H. Wielandt 有限置换群, 德文译本, Academic Press, 纽约–伦敦, 1964, x+114 pp.[44] P.V. Yagodovskii 对偶多值群。 Uspekhi Mat. Nauk **64**:5(389) (2009), 183–184 (俄文); 英译本：Russian Math. Surveys, **64**:5 (2009), 955–957.[45] P.V. Yagodovsky有限交换多值群理论中的对偶性, 表示论、动力系统、组合方法。第 XVIII 部分, Zap. Nauchn. Sem. POMI **378**, POMI, 圣彼得堡, 2010, 184–227 (俄文); 英译本：J. Math. Sci. **174**:1 (2011), 97–119.[46] H. Yamabe *Gleason*定理的推广, Ann. of Math. (2), **58**:2 (1953), 351–365.

Victor M. Buchstaber

俄罗斯科学院斯捷克洛夫数学研究所，俄罗斯莫斯科

俄罗斯莫斯科国立罗蒙诺索夫大学

国家研究型大学“高等经济学院”，俄罗斯莫斯科电子邮箱地址：buchstab@mi-ras.ru

Alexander A. Gaifullin

俄罗斯科学院斯捷克洛夫数学研究所，俄罗斯莫斯科

俄罗斯斯科尔科沃科学技术研究院

俄罗斯莫斯科国立罗蒙诺索夫大学

俄罗斯科学院信息传输问题研究所（Kharkevich研究所），莫斯科电子邮箱：agaif @mi-ras.ru

Alexander P. Veselov

英国拉夫堡大学电子邮箱:
A.P.Veselov@lboro.ac.uk