arXiv:2301.03683v1 [math.GR] 9 Jan 2023

阿贝尔群扩张循环群型穆芳环路

ˇ´ ˇ´ALES DRAPAL AND PETR VOJTECHOVSKY

Abstract. 我们研究阿贝尔群扩循环穆芳环路。我们利用阿贝尔群上的所谓穆芳置换（X, $+$）构造所有分裂的 3-可除阿贝尔群扩张循环群型穆芳群环。所谓穆芳置换，是指与阿贝尔群（$X,+$）上的某个自同构仅相差一个交替双加映射（满足某些性质）的置换。更一般地，我们还利用所谓构造对构造出其他阿贝尔群扩循环穆芳环路。顺带一提，我们证明：在由（$X,+$）上的构造对得到的穆芳环路 Q 中，阿贝尔正规子群（$X,+$）当且仅当 Q 是一个群时才会诱导出 Q 的阿贝尔同余。

1. 引言

穆芳环路最初发表于 1935 [32] 此后一直受到研究。然而，我们对穆芳环路基本结构概念的理解仍存在严重不足。造成这种情况的原因之一是缺乏构造方法。

本文开始系统研究交换群扩循环穆芳环路的构造，即具有阿贝尔正规子群 Q X 且 Q/X 为循环群的穆芳环路。主要结果包括定理 4.7 （根据所谓的构造对构造出大量交换群扩循环穆芳环路），定理 10.1 （在穆芳环路中， a 的每个共轭在 X 上的限制都是所谓的穆芳置换，且子环$\langle a^3\rangle X$ 上的乘法恰如定理 4.7中的抽象乘法公式），定理 10.4 （所有 3-可除交换群扩循环穆芳环路都是由定理 4.7 得到的环路的同态像，其构造对由穆芳置换导出），以及定理10.6 （对分裂的三可除阿贝尔群扩张循环群型穆芳群环的刻画）。

1.1. 穆芳环构造简述。 穆芳环最重要且最具启发性的例子，来自非零八元数的乘法环 [2, 11, 31, 41]。这些八元数穆芳环具有一些并非所有穆芳环都具备的重要结构性质。例如，在实八元数基本单位构成的16元环 $\mathbb{O}_{16}$ 中，每个平方都与所有元素满足结合律（因此它是 $\mathbb{O}_{16}$ 一个额外环 [10, 16]），而且实际上只有一个非单位元平方（因此它是 $\mathbb{O}_{16}$ 一个码环 [9, 24]）。所有非结合有限单穆芳环，都是有限域上分裂八元数代数的单位元环的中心因子 [30, 36, 44]。

另一类有趣的穆芳环路是 Moufang p-环路。Moufang p-环路是中心幂零的（奇数情形见 [20] ， p；另一情形见 [21] ， $p = 2$；关于两种情形的最新初等

2020年数学主题分类：20N05。关键词和短语：阿贝尔商循环穆芳环，穆芳环路，穆芳环中的共轭，Moufang置换，可解性，同余可解性。ˇ A. Dr´apal 受到捷克共和国教育、青年和体育部的 INTER-EXCELLENCE 项目 LTAUSA19070 资助。P. Vojtˇechovsk´y 受到西蒙斯基金会数学与物理科学数学家合作资助，资助编号 855097。

证明见 p）。利用几何方法，Bol [4] 构造了一个阶为 3^4 的非结合交换穆芳环路（所有阶小于 3^6 的交换穆芳环路也见 [25] ）。后来，Bruck [5] 为每个素数 p 构造了一个阶为 p^5 的非结合穆芳环路；Nagy 和 Valsecchi [27] 则分类了所有素数 $p > 3$ 下阶为 p^5 的穆芳环路。通过计算方法研究中心扩张，文献 [34] （分别是 [40]）对阶为 2^6 和 3^4 的所有穆芳环路进行了分类。前面提到的码环，也可以等价地描述为具有一个阶为 2 的中心子圈 Z 、且满足 Q/Z 为初等阿贝尔 2-群的 Moufang 2-环路 Q ，参见 [1, 24]。文献 [35] 枚举了阶为 $\leq 2^9$ 的码环。Moufang p-环路的构造通常具有组合性质，对于非素数幂阶的穆芳环路则鲜有说明。

另一个构造来源与一个尚未解决的问题有关：对于哪些整数 n ，存在阶为 n 的非结合穆芳环路？Chein 在 [7] 中描述了所有阶小于 32 的穆芳环路，并在 [8] 中描述了所有阶小于 64 的穆芳环路（另见 [22, 33] ，其中列出了所有阶小于 64 的非结合穆芳环路）。Chein 对小阶穆芳环路的分类中出现的构造，包括众所周知的群 G 的 Chein 双环路 M（G，2），以及 Chein 双环路的若干详尽变体。Leong 和 Rajah [28] 证明，若穆芳环路的阶 $p^\alpha q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ 是奇素数，且满足 $p < q_1 < \cdots < q_k$ 和 $\alpha \leq 3$ ，则它是一个群；对于 $p > 3$ 和 $\alpha = 4$ 的情形，结论也类似。Rajah 与多位合作者深入研究了介于这一指数下界与非结合穆芳 p-环路所提供的上界之间的阶的中间因数分解情形，例如参见 [6, 39]。鉴于问题本身的性质，这一研究领域中的构造大多是特设的，因为对于任何给定的阶，只需找到一个非结合例子，就能解决相应的存在性问题。

关于穆芳环路的一般构造，Kinyon 和 Kunen 在额外环背景下研究半直积，取得了重要成果 [26]。对于（不一定是额外环的）穆芳环路，第一步是 Gagola 发现的一个公式 [19]，参见我们的（2.12），该公式给出了存在一个穆芳环路（它是乘积中的正规子圈）与一个阶和 3 互素的循环群的半直积的必要条件。随后，Drapal 给出了存在这种半直积的充分条件´[13]。 [13] 的条件以对正规子圈的半自同构提出某些要求的形式给出，因而难以处理。本文受 [13] 启发，但与其相互独立。

最后，我们还想提及论文 [18, 23, 29]，这些论文讨论了穆芳环路的半直积和／或分裂扩张。

1.2. 主要结果概述。以下定义是构造许多交换群扩循环穆芳环路的关键：

定义 1.1. 设 $(X, +)$ 是一个阿贝尔群， g 是 X 的一个置换，且 $\gamma\colon X \times X \to X$ 是一个映射。若 γ 是一个对称交替双加映射，则 (g, γ) 是 $(X, +)$ 上的一个构造对，

$$g^{-1}(g(x) + g(y)) = x + y + \gamma(x, y) + g^{-1}(\gamma(x, y)) + g^{-2}(\gamma(x, y)) \tag{C1}$$

对所有 $x, y \in X$ 均成立，

$$\gamma(\gamma(x, y)\ z) = 0 \tag{C2}$$

对所有 $x, y, z \in X$ 均成立，且

$$g^{-1}(\gamma(x,y)) = \gamma(g(x), y) \tag{C3}$$

对所有 $x, y \in X$ 均成立。

注意，条件（C2）也可等价地表述为：γ 的像包含于根 $\mathrm{Rad}(\gamma) = \{x \in X : \ \gamma(x,y) = 0$ 对所有 $y \in X\}$ 属于 γ。

对于 $i, j \in \mathbb{Z}$，定义 $\mathbb{Z}$ 的区间 $I(i,j)$ 如下：

$$I(i,j) = \begin{cases} \emptyset, & \text{if } i = j, \\ \{i, i+1, \dots, j-1\}, & \text{if } i < j, \\ \{j, j+1, \dots, i-1\}, & \text{if } j < i. \end{cases} \tag{1.1}$$

给定一个阿贝尔群 $(X, +)$ 和一个循环群 $C = \langle b \rangle$，我们证明，公式

$$(b^i, x) \cdot (b^j, y) = \left(b^{i+j}, g^{-j}(x) + y + \sum_{k \in I(i+j,-j)} g^{-k}(\gamma(x,y)) \right) \tag{1.2}$$

在且仅在以下条件之一成立时，才能在 $C \times X$ 上正确地定义乘法：C 是无限的；或者 C 是有限的，$|g|$ 整除 $|C|$，且对所有 $x \in X$，$\sum_{0 \le k < |C|} g^k(x) \in \mathrm{Rad}(\gamma)$。（条件 $\sum_{0 \le k < |C|} g^k(x) \in \mathrm{Rad}(\gamma)$ 在 $|C|$ 有限、$|g|$ 整除 $|C|$ 且 $\mathrm{Rad}(\gamma)$ 不含 3 阶元素时成立。）在这种情况下，所得广群实际上是一个穆芳环路 $Q = C \ltimes_{(g,\gamma)} X$，其中包含一个正规子圈 $1 \times X$，使得 $Q/(1 \times X)$ 与 C 同构，参见定理 4.7。此外，$(C \times 0) \cap (1 \times X) = 1$，因此 Q 是 X 被 C 扩张得到的分裂扩张。

这些环路的若干关键性质 $C \ltimes_{(g,\gamma)} X$ 将在第5节中建立，例如逐元素交换子的公式、逐元素结合子的公式、结合子子圈、换位子子圈、导出子圈、核和中心。

在简短的第6 节中，我们证明，在穆芳环路 $Q = C \ltimes_{(g,\gamma)} X$ 中，正规子圈 $1 \times X$ 在 Q 上诱导阿贝尔同余，当且仅当 Q 是一个群。这与我们目前另一条研究方向有关，该方向关注环路中可解性的两种概念，参见 [15, 42, 43]。第6 节的结果在论文其他部分不会用到。

论文其余部分关注定理4.7的一个部分逆命题。

容易看出，定理4.7并未涵盖所有交换群扩循环穆芳环路。例如，四元数群 Q_8 是交换群扩循环的，但它不是分裂的，因此无法由定理4.7的构造得到。（最小的非结合、非分裂的交换群扩循环穆芳环路的阶为 32。）事实上，定理4.7 也未涵盖所有分裂的交换群扩循环穆芳环路。例如，阶为 81、指数为 3 的非结合交换穆芳环路是 $X = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ 由$C = \mathbb{Z}_3$作分裂扩张得到的，但定理4.7 并未涵盖任何非结合交换穆芳环路，参见推论 5.4。

另一方面，定理 4.7 给出了所有分裂且 3-可除的交换群扩循环穆芳环路，参见定理 10.6。为证明这一事实，我们需要引入以下与构造对类似的概念：

定义 1.2. 设 $(X, +)$ 是一个阿贝尔群。若映射 $\beta : X \times X \to X$ 定义为

$$\beta(x,y) = f^{-1}(f(x) + f(y)) - x - y \tag{P1}$$

是（对称）交错且双加性的，

$$\beta(\beta(x,y),z)=0 \tag{P2}$$

对所有 x、y、$z\in X$ 均成立，并且

$$\beta(f(x),f(y))=f(\beta(f^3(x),y)) \tag{P3}$$

对所有 x、$y\in X$均成立。当 f 是一个穆芳置换，且 β 由 (P1) 定义时，我们称β 为与 f 相关联的双加映射，并称元组 (f,β) 为一个 Moufang 对。

构造对与 Moufang 对之间的关系是：若 (f,β) 是一个 Moufang 对，则 (f^3,β) 是一个构造对，参见命题 9.8。特别地，当定理 4.7 的其余假设均满足时，我们可以将乘法公式 (1.2) 与 $(g,\gamma)=(f^3,\beta)$ 配合使用。此外，若对某个 $b=a^3$ 有 $a\in C$(这在 C为 3-可除时必然成立)，公式 (1.2) 就变为

$$(a^{3i},x)\cdot(a^{3j},y)=\Big(a^{3(i+j)},f^{-3j}(x)+y+\sum_{k\in I(i+j,-j)}f^{-3k}(\beta(x,y))\Big). \tag{1.3}$$

在第 7 节和第 8节中，我们导出了关于由内映射诱导的穆芳环路伪自同构和半自同构的一些相当一般的结果。随后我们证明，对于穆芳环路 Q的每个阿贝尔正规子群 X 以及每个元素 $a\in Q$，“共轭” T_a 在 X 上的限制是 X上的一个穆芳置换，参见命题 8.4。

在第 9 节中，我们研究穆芳置换 f 及其幂的抽象性质。除其他结果外，我们还推导出表达式 $f^{-i}(f^i(x)+f^i(y))$ 的公式，参见命题9.5。

接着，我们在定理 10.1 中证明，若 $(X,+)$ 是穆芳环路 Q 的一个阿贝尔正规子群，且 $a\in Q$ 则

$$a^{3i}x\cdot a^{3j}y=a^{3(i+j)}\Big(f^{-3j}(x)+y+\sum_{k\in I(i+j,-j)}f^{-3k}(\beta(x,y))\Big) \tag{1.4}$$

对所有 $i,j\in\mathbb{Z}$和 $x,y\in X$成立，其中 f是 T_a在 X上的限制；由命题 8.4 可知，它是 $(X,+)$ 上的一个穆芳置换。本文中，若 $(X,+)$ 是 $(Q,\cdot)$ 的正规子圈，我们记 $x+y$或 $x\cdot y$ 为 $x,y\in X$在 Q中的乘积。

注意，(1.4) 不一定描述 所有 由 Q中元素组成的数对的乘法。不过，容易推出（参见推论 10.2），若 $(X,+)\trianglelefteq Q$ 且 $Q=\langle a^3\rangle X$对于某个 $a\in Q$成立，则 (1.4) 完整地描述了 Q的乘法。

接下来不难证明，所有 3-可除的交换群扩循环穆芳环路 $Q=CX$ 都是环路 $C\ltimes_{(f^3,\beta)}X$ 的同态像，其中 (f,β) 是 $(X,+)$ 上的 Moufang 对。这里，$|f^3|$ 必须整除 $|C|$，否则 $C\ltimes_{(f^3,\beta)}X$ 甚至没有定义。同态的核由命题 10.5 描述。最后，分裂的 3-可除交换群扩循环穆芳环路 $Q=CX$ 恰好是环路 $C\ltimes_{(f^3,\beta)}X$，其中 (f,β) 是 $(X,+)$ 上的 Moufang 对，参见定理 10.6。

让我们以几点说明来总结主要结果。

乘法公式（1.4）看起来可能相当复杂且不自然。推导该公式的出发点是以下重要恒等式

$$a^{3i}x \cdot ya^{3j} = a^{3(i+j)}T_a^{-i-2j}(T_a^{i-j}(x)T_a^{i-j}(y))$$

对所有穆芳环路都成立。我们在命题 2.6 中记录这一恒等式及其所有变式，其中包括前面提到的 Gagola 恒等式（2.12） [19]。

结果表明，在有限情形下，每个关于（X，$+$）的构造对（g，γ）都会导出一个整数 m 以及一个映射 $U \times U \to V$，该映射是关于 R 的交替双线性映射，其中 $U = X/$根(γ)，$V = \langle$像$(\gamma)\rangle$ 且 $R = \mathbb{F}_2[x]/(x^m - 1)$。因此，要描述给定阿贝尔群（$X$，$+$）的构造对，就意味着首先对相关的交替双线性映射进行分类，然后再加入若干提升步骤。我们打算在未来的一篇论文中研究如何得到构造对，以及如何将由此得到的穆芳环路按同构分类。

2. Background

2.1. 映射。设（X，$+$）是一个阿贝尔群。称映射 $\gamma\colon X \times X \to X$ 为对称的，如果对所有 x、$y \in X$，都有 $\gamma(x,y) = \gamma(y,x)$；称其为反对称的，如果对所有 x、$y \in X$，都有 $\gamma(x,y) = -\gamma(y,x)$；称其为交错的，如果对所有 $x \in X$，都有 $\gamma(x,x) = 0$；称其为双加性的，如果对所有 x、y、$z \in X$，都有 $\gamma(x+y,z) = \gamma(x,z) + \gamma(y,z)$，且 $\gamma(x,y+z) = \gamma(x,y) + \gamma(x,z)$。

注意，双加映射满足 $\gamma(0,x) = 0 = \gamma(x,0)$，$\gamma(-x,y) = -\gamma(x,y) = \gamma(x,-y)$，$\gamma(x-y,z) = \gamma(x,z) - \gamma(y,z)$ 和 $\gamma(x,y-z) = \gamma(x,y) - \gamma(x,z)$，对所有 $x,y,z \in X$ 均成立。事实上，$\gamma(0,x) = \gamma(0+0,x) = 2\gamma(0,x)$ 推出 $\gamma(0,x) = 0$，接着 $0 = \gamma(x+(-x)\ y) = \gamma(x,y) + \gamma(-x,y)$ 蕴含 $\gamma(-x,y) = -\gamma(x,y)$，最后 $\gamma(x-y,z) = \gamma(x,z) + \gamma(-y,z) = \gamma(x,z) - \gamma(y,z)$

交替双加映射是反对称的，因为 $0 = \gamma(x+y,x+y) = \gamma(x,x) + \gamma(x,y) + \gamma(y,x) + \gamma(y,y) = \gamma(x,y) + \gamma(y,x)$。因此，对称交替双加映射满足 $2\gamma(x,y) = \gamma(2x,y) = 0$，因为 $\gamma(x,y) = \gamma(y,x) = -\gamma(x,y)$。本文中将不再特别指出，而直接使用这些性质。

任意映射 g 的像记为 Img(g)。与导论中一样，对于对称映射 $\gamma\colon X \times X \to X$，$\gamma$ 的根定义为

$$\mathrm{Rad}(\gamma) = \{x \in X : \gamma(x,y) = 0 \text{ for all } y \in X\}.$$

如果 γ 是对称且双加性的，那么 Rad(γ) 是 $(X,+)$ 的一个子群。

记号。为提高可读性，我们常常省略一元映射自变量周围的括号。例如，若 $g\colon X \to X$ 且 $\gamma\colon X \times X \to X$，我们可能写作 $g\gamma(x,y)$，而不写 $g(\gamma(x,y))$；写作 $\gamma(gx,y)$，而不写 $\gamma(g(x)\ y)$。

2.2. 环路。有关环路理论的导论，请参见[5, 37] 。

若集合 Q 配备二元运算 $\cdot$ 和元素 $1 \in Q$，且对每个 $x \in Q$ 都有 $x \cdot 1 = 1 \cdot x = x$，并且平移

$$L_x : Q \to Q,\ L_x(y) = x \cdot y \quad \text{and} \quad R_x : Q \to Q,\ R_x(y) = y \cdot x$$

是 Q 的置换。由此导出的除法运算记作 $x\backslash y = L_x^{-1}(y)$ 和 $x/y = R_y^{-1}(x)$。

结合子环称为子群。若环路 Q 中的每个元素都生成一个子群，则称该环路 Q 幂结合。若环路 Q 中任意两个元素都生成一个子群，则称该环路 Q 二元结合。

记号。我们常用 xy 代替 $x\cdot y$，并用 $\cdot$ 表示乘法的优先级，例如，$x\cdot yz$ 表示 $x\cdot(y\cdot z)$。

圈 Q 的乘法群是置换群 $\mathrm{Mlt}(Q)=\langle L_x,R_x:\ x\in Q\rangle$，而 Q 的内映射群 $\mathrm{Inn}(Q)$ 是 $\mathrm{Mlt}(Q)$ 中 1 的稳定子。众所周知，$\mathrm{Inn}(Q)=\langle T_x,L_{x,\ y},R_{x,\ y}:\ x,y\in Q\rangle$，其中

$$T_x=R_x^{-1}L_x,\quad L_{x,y}=L_{xy}^{-1}L_xL_y\quad\text{and}\quad R_{x,y}=R_{xy}^{-1}R_yR_x.$$

我们将内映射 T_x 称为共轭映射。

Q 的核 $\mathrm{Nuc}(Q)$ 由所有满足以下条件的 $x\in Q$ 构成：对所有 $y,z\in Q$，$x(yz)=(xy)z$、$y(xz)=(yx)z$ 且 $y(zx)=(yz)x$。Q 的中心 $Z(Q)$ 由所有满足对任意 $y\in Q$ 均有 $xy=yx$ 的 $x\in\mathrm{Nuc}(Q)$ 构成。$x,y\in Q$ 的交换子 $[x,y]$ 定义为 $(yx)[x,y]=xy$。$x,y,z\in Q$ 的结合子 $[x,y,z]$ 定义为 $(x\cdot yz)[x,y,z]=xy\cdot z$。

2.3. 态射与拓扑。用 $\mathrm{Sym}(Q)$ 表示 Q 上的对称群。三元组 $(c,f)\in Q\times\mathrm{Sym}(Q)$ 是 Q 的一个（左）伪自同构，当且仅当

$$cf(x)\cdot f(y)=cf(xy)\tag{2.1}$$

对每个 $x,y\in Q$ 都成立。元素 c 称为 f 的伴随元。Q 的所有伪自同构在以下运算下构成一个群 $\mathrm{Psa}_\ell(Q)$：

$$(c,f)(d,g)=(cf(d),fc)\quad\text{and}\quad(c,f)^{-1}=(f^{-1}(c\backslash 1),f^{-1}).\tag{2.2}$$

置换 $f\in\mathrm{Sym}(Q)$ 是 Q 的半自同构，当且仅当 $f(1)=1$ 且

$$f(x\cdot yx)=f(x)\cdot f(y)f(x)\tag{2.3}$$

对所有 $x,y\in Q$ 都成立。如果 f 是幂结合圈 Q 的半自同构，那么对于每个 $i\in\mathbb{Z}$，都有 $f(x^i)=f(x)^i$。

条件（2.3）可以写成 $fL_xR_x=L_{f(x)}R_{f(x)}f$，因此也可以写成

$$L_{f(x)}^{-1}fL_x=R_{f(x)}fR_x^{-1}.\tag{2.4}$$

因此，圈 f 的任意置换 Q，只要满足 $f(1)=1$ 和（2.4），就是半自同构。圈 Q 的一个α、β、γ）是 Q 的置换三元组，且满足

$$\alpha(x)\beta(y)=\gamma(xy)$$

对所有 x、$y\in Q$ 均成立。Q 的自拓扑可以按分量进行复合和求逆，从而构成自拓扑群 $\mathrm{Atp}(Q)$。

注意，(c,f) 是 Q 的伪自同构，当且仅当 (L_cf,f,L_cf) 是 Q 的自拓扑。我们在证明以下关于自拓扑的观察时会用到这一事实，其中中间分量固定单位元。

引理 2.1. 设 $(Q,\cdot,1)$ 是一个圈。假设 $(\alpha,\beta,\gamma)\in\mathrm{Atp}(Q)$ 且 $\beta(1)=1$。那么 $(\alpha(1)\ \beta)\in\mathrm{Psa}_\ell(Q)$。

证明。设 $c=\alpha(1)$。根据我们的假设，对于每个 $x\in Q$，$\alpha(x)=\alpha(x)\beta(1)=\gamma(x\cdot 1)=\gamma(x)$，且 $c\beta(x)=\alpha(1)\beta(x)=\gamma(1\cdot x)=\gamma(x)$。因此 $(\alpha,\beta,\gamma)=(L_c\beta,\beta,L_c\beta)$。□

2.4. 穆芳环路。若一个圈 Q 满足任意一个等价的穆芳恒等式，则称其为穆芳的

$$xy \cdot zx = (x \cdot yz)x, \tag{M1}$$
$$xy \cdot zx = x(yz \cdot x), \tag{M2}$$
$$x(y \cdot zy) = (xy \cdot z)y, \tag{M3}$$
$$x(y \cdot xz) = (xy \cdot x)z. \tag{M4}$$

我们总结一些关于穆芳环路的事实，包括一些简单的观察以及关于穆芳环路的标准结果[5]。

恒等式（M1）可表述为（L_x， R_x， R_xL_x） $\in \mathrm{Atp}(Q)$ 。这是用自拓扑刻画穆芳环路的一种有用方式。

根据穆芳定理[12, 32], ，若穆芳环路中的三个元素 x、 y 和 z 满足结合律，即 x（yz） = （xy）z，则子环 $\langle x$、 y、 $z\rangle$ 是一个群。因此，穆芳环路是二元结合的、幂结合的，满足柔性律 x（yx） = （xy）x、逆元性质x^{-1}（xy） $= y =$ （yx）x^{-1}，等等。我们利用穆芳环路中的二元结合性，并明确地写作 xyx、 $x^y = y^{-1}xy$、 $[x, y] = x^{-1}y^{-1}xy$ 等。

引理 2.2. [15] 设 Q 是一个穆芳环路。那么

$$x^{-1}(xy \cdot z) = yx^{-1} \cdot xz, \tag{2.5}$$
$$(z \cdot yx)x^{-1} = zx \cdot x^{-1}y \tag{2.6}$$

对每个 $x, y, z \in Q$均成立。

穆芳环路的所有内映射都可以视为伪自同构，并具有适当的伴随元。特别地，

$$(x^{-3}, T_x), \quad ([y, x], R_{x,y}) \quad \text{and} \quad ([x^{-1}, y^{-1}], L_{x,y}) \tag{2.7}$$

在穆芳环路中是伪自同构。穆芳环路的每个伪自同构都是半自同构。

引理 2.3. 设 Q 是一个穆芳环路， $c \in Q$ 和 $f \in$ 属于 Sym(Q)。那么 $(c, f) \in \mathrm{Psa}_\ell(Q)$ 当且仅当

$$xc^{-1} \cdot cy = f(f^{-1}(x)f^{-1}(y))$$

对所有 $x, y \in Q$均成立。

证明。将 $f^{-1}(x)$ 代入 x，并将 $f^{-1}(y)$ 代入 y，再代入 $cf(x) \cdot f(y) = cf(xy)$，得到 $cx \cdot y = cf(f^{-1}(x)f^{-1}(y))$。在左侧乘以 c^{-1} 并应用 (2.5)，即可完成证明。□

推论 2.4。设 Q 是一个穆芳环路。那么

$$xa^{-3} \cdot a^3y = T_a^{-1}(T_a(x)T_a(y))$$

对所有 a、 x、 $y \in Q$，均成立。

方程（2.8）对本文至关重要。

命题 2.5。设 Q 是一个穆芳环路。那么

$$a^{3i}x \cdot ya^{3j} = a^{3i} \cdot T_a^{j-i}(T_a^{i-j}(x)T_a^{i-j}(y)) \cdot a^{3j} \tag{2.8}$$

对所有 a、 x、 $y \in Q$ 以及所有 i、 $j \in \mathbb{Z}$。

证明。令 $b = a^{3i}$ 和 $\delta = i - j$。由二结合律和（M1），$b^i x \cdot y b^j = b^j (b^\delta x) \cdot y b^j = b^j (b^\delta x \cdot y) b^j$。由（2.5）和推论 2.4，

$$b^\delta x \cdot y = b^\delta (x b^{-\delta} \cdot b^\delta y) = b^\delta T_{a^{-\delta}}(T_{a^\delta}(x) T_{a^\delta}(y)) = b^\delta T_a^{-\delta}(T_a^\delta(x) T_a^\delta(y)),$$

在最后一步中，我们使用了 $T_{a^k} = T_a^k$。结合起来，得到

$$b^i x \cdot y b^j = b^j (b^\delta x \cdot y) b^j = b^j \cdot b^\delta T_a^{-\delta}(T_a^\delta(x) T_a^\delta(y)) \cdot b^j = b^i \cdot T_a^{-\delta}(T_a^\delta(x) T_a^\delta(y)) \cdot b^j. \qquad \square$$

下面是恒等式（2.8）的一些变式：

命题 2.6. 设 Q 是一个穆芳环路。那么

$$a^{3i}x \cdot a^{3j}y = a^{3(i+j)} T_a^{-i-2j}(T_a^{i-j}(x) T_a^{i+2j}(y)) = T_a^{2i+j}(T_a^{i-j}(x) T_a^{i+2j}(y)) a^{3(i+j)}, \tag{2.9}$$

$$a^{3i}x \cdot y a^{3j} = a^{3(i+j)} T_a^{-i-2j}(T_a^{i-j}(x) T_a^{i-j}(y)) = T_a^{2i+j}(T_a^{i-j}(x) T_a^{i-j}(y)) a^{3(i+j)}, \tag{2.10}$$

$$x a^{3i} \cdot a^{3j}y = a^{3(i+j)} T_a^{-i-2j}(T_a^{-2i-j}(x) T_a^{i+2j}(y)) = T_a^{2i+j}(T_a^{-2i-j}(x) T_a^{i+2j}(y)) a^{3(i+j)}, \tag{2.11}$$

$$x a^{3i} \cdot y a^{3j} = a^{3(i+j)} T_a^{-i-2j}(T_a^{-2i-j}(x) T_a^{i-j}(y)) = T_a^{2i+j}(T_a^{-2i-j}(x) T_a^{i-j}(y)) a^{3(i+j)} \tag{2.12}$$

对所有 a、x、$y \in Q$ 以及所有 i、$j \in \mathbb{Z}$ 均成立。

证明。注意到 $a^k z = a^k z a^{-k} a^k = T_a^k(z)\, a^k$，因此只需证明每个（2.9）–（2.12）中的第一个等式。由 $u = T_a^{j-i}(T_a^{i-j}(x)\, T_a^{i-j}(y))$，方程（2.8）给出

$$a^{3i}x \cdot y a^{3j} = a^{3i} u a^{3j} = T_a^{3i}(u) a^{3i} a^{3j} = T_a^{2i+j}(T_a^{i-j}(x) T_a^{i-j}(y)) a^{3(i+j)},$$

这就是（2.10）。其余恒等式随后由（2.10）推出：$a^{3i}x \cdot a^{3j}y = a^{3i}x \cdot T_a^{3j}(y)\, a^{3j}$，$x a^{3i} \cdot a^{3j} y = a^{3i} T_a^{-3i}(x) \cdot T_a^{3j}(y)\, a^{3j}$ 以及 $x a^{3i} \cdot y a^{3j} = a^{3i} T_a^{-3i}(x) \cdot y a^{3j}$。$\square$

3. Construction pairs and their properties

构造对在导论中已定义，参见定义 1.1。本节将建立（g，γ）在（X，$+$）上的构造对的基本性质。条件（C1）常以如下形式使用

$$g(x) + g(y) = g(x + y + \gamma(x, y) + g^{-1}(\gamma(x, y)) + g^{-2}(\gamma(x, y))).$$

引理 3.1。设 (g, γ) 是 $(X, +)$ 上的构造对，且 i 是一个整数。那么：

（i） $g(0) = 0$, $g(2x) = 2g(x)$ 且 $g(-x) = -g(x)$ 对所有 $x \in X$ 均成立，（ii）$\mathrm{Img}(\gamma) \subseteq \mathrm{Rad}(\gamma)$，$2X \subseteq \mathrm{Rad}(\gamma)$ 且 $2\mathrm{Img}(\gamma) = 0$，（iii） g^i 置换 $\mathrm{Img}(\gamma)$ 和 $\mathrm{Rad}(\gamma)$，（iv）当 $\{x, y\} \cap \mathrm{Rad}(\gamma) \neq \emptyset$ 时，$g^i(x + y) = g^i(x) + g^i(y)$，（v） g^i 限制为 $\mathrm{Rad}(\gamma)$ 上的一个自同构。

证明.（i）根据双加性，我们有 $\gamma(x, 0) = 0$。因此，由 (C3) 可得 $g^{-1}(0) = g^{-1}\gamma(0, 0) = \gamma(g(0), 0) = 0$，进而得到 $g(0) = 0$。由于 γ 是交错的，且 $g(0) = 0$，由 (C1) 可得 $0 = \gamma(x, x) + g^{-1}\gamma(x, x) + g^{-2}\gamma(x, x) = g^{-1}(g(x) + g(x)) - x - x = g^{-1}(2g(x)) - 2x$，从而得到 $2g(x) = g(2x)$。最后，$\gamma(x, -x) = -\gamma(x, x) = 0$，因此，由 (C1) 可得 $0 = \gamma(x, -x) + g^{-1}\gamma(x, -x) + g^{-2}\gamma(x, -x) = g^{-1}(g(x) + g(-x))$，进而得到 $g(x) + g(-x) = 0$。

（ii）条件 $\mathrm{Img}(\gamma) \subseteq \mathrm{Rad}(\gamma)$ 是对 (C2) 的另一种表述。任意对称交替双加映射都满足 $0 = \gamma(2x, y) = 2\gamma(x, y)$。

（iii）我们有 $x \in \mathrm{Rad}(\gamma)$ 当且仅当 $\gamma(x, y) = 0$ 对所有 $y \in X$ 当且仅当 $g^{-1}\gamma(x, y) = g^{-1}(0) = 0$ 对所有 $y \in X$ 当且仅当 $\gamma(g(x)\ y) = 0$ 对所有 $y \in X$ 由 (C3) 得，当且仅当 $g(x) \in \mathrm{Rad}(\gamma)$。类似地，$z \in \mathrm{Img}(\gamma)$ 当且仅当

$z = \gamma(x, y)$ 对某些 $x, y \in X$ 当且仅当 $g^{-1}(z) = g^{-1}\gamma(x, y) = \gamma(g(x)\ y)$ 对某些 $x, y \in X$ 由 得， (C3) 当且仅当 $g^{-1}(z) \in \mathrm{Img}(\gamma)$。

（iv）不失一般性，设 $x \in \mathrm{Rad}(\gamma)$。于是 $\gamma(x, y) = 0$，并且根据（i），对所有 i，都有 $g^i\gamma(x, y) = 0$。因此，由（C1）可得 $0 = \gamma(x, y) + g^{-1}\gamma(x, y) + g^{-2}\gamma(x, y) = g^{-1}(g(x) + g(y)) - x - y$，进而可得 $g(x + y) = g(x) + g(y)$。设该结论对某个 i 成立。根据（iii），对每个整数 k，都有 $g^k(x) \in \mathrm{Rad}(\gamma)$。由归纳假设，便有$g^{i+1}(x + y) = g^i(g(x + y)) = g^i(g(x) + g(y)) = g^i(g(x)) + g^i(g(y)) = g^{i+1}(x) + g^{i+1}(y)$。此外，$g^i(g^{-i}(x) + g^{-i}(y)) = g^i(g^{-i}(x)) + g^i(g^{-i}(y)) = x + y$，因此 $g^{-i}(x + y) = g^{-i}(x) + g^{-i}(y)$。故该结论对每个 i 都成立。

第（v）部分由（iii）和（iv）推出。 □

引理 3.2. 设 (g, γ) 是关于 $(X, +)$ 的构造对。那么

$$\gamma(g^i x, g^j y) = g^{-i-j}\gamma(x, y) \tag{3.1}$$

对所有 $x, y \in X$ 和 $i, j \in \mathbb{Z}$ 均成立。

证明. 只需证明

$$\gamma(g^i x, y) = g^{-i}\gamma(x, y) \tag{3.2}$$

对所有 $i \in \mathbb{Z}$ 均成立，因为由 γ 的对称性可得 $\gamma(g^i x, g^j y) = g^{-i}\gamma(x, g^j y) = g^{-i}\gamma(g^j y, x) = g^{-i}g^{-j}\gamma y(x, =) g^{-i-j}\gamma x(y, \gamma)$。下面证明 (3.2)。对于 $i = 0$，无需证明；对于 $i = 1$，则可得到 (C3)。若 (3.2) 对 i 成立，则 $\gamma(g^{i+1}x, y) = \gamma(g^i gx, y) = g^{-i}\gamma(gx, y) = g^{-i}g^{-1}\gamma(x, y) = g^{-i-1}\gamma(x, y)$ 表明 (3.2) 对 $i + 1$ 也成立。为证明 (3.2) 对 $i = -1$ 成立，在 (C3) 中用 $g^{-1}(x)$ 代替 x，得到 $g^{-1}\gamma(g^{-1}x, y) = \gamma(x, y)$，因此 $\gamma(g^{-1}x, y) = g\gamma(x, y)$。最后，若 (3.2) 对 i 成立，则 $\gamma(g^{i-1}x, y) = \gamma(g^i g^{-1}x, y) = g^{-i}\gamma(g^{-1}x, y) = g^{-i}g\gamma(x, y) = g^{-i+1}\gamma(x, y)$ 表明 (3.2) 对 $i - 1$ 也成立。□

引理 3.3. 设 (g, γ) 是 $(X, +)$ 上的一个构造对。那么 $(g^{-1}, g\gamma)$ 是 $(X, +)$ 上的一个构造对。

证明. 由 γ 的对称性，我们有 $g\gamma(x, y) = g\gamma(y, x)$。由引理 3.1 可知 $g(0) = 0$，因此我们有$g\gamma(x, x) = g(0) = 0$。由于 g 在 $\mathrm{Rad}(\gamma)$ 上限制为一个自同构，且由引理 3.1 可知 $\mathrm{Img}(\gamma) \subseteq \mathrm{Rad}(\gamma)$，所以我们有 $g\gamma(x + y, z) = g(\gamma(x, z) + \gamma(y, z)) = g\gamma(x, z) + g\gamma(y, z)$。这证明了 $g\gamma$ 是对称、交错且双加性的。

现在，$g\gamma(g\gamma(x, y)\ z) = gg^{-1}\gamma(\gamma(x, y)\ z) = \gamma(\gamma(x, y)\ z) = 0$，由 (C3) 和 (C2) 可得。因此 $\mathrm{Img}(g\gamma) \subseteq \mathrm{Rad}(g\gamma)$。

最后，由引理 3.1 可得 $g(x) + g(y) = g(x + y + \gamma(x, y) + g^{-1}\gamma(x, y) + g^{-2}\gamma(x, y)) = g(x + y) + g\gamma(x, y) + \gamma(x, y) + g^{-1}\gamma(x, y)$。将 $g^{-1}(x)$ 代入 x，将 $g^{-1}(y)$ 代入 y，并利用 (3.1)，得到 $x + y = g(g^{-1}x + g^{-1}y) + g^3\gamma(x, y) + g^2\gamma(x, y) + g\gamma(x, y)$。由于由引理 3.1 可得 $\gamma(x, y) = -\gamma(x, y)$ 且 $g(-z) = -g(z)$，我们推得

$$g(g^{-1}x + g^{-1}y) = x + y + g\gamma(x, y) + g^2\gamma(x, y) + g^3\gamma(x, y),$$

这对应于 (C1) 中 $(g^{-1}$、$g\gamma)$ 的对应形式。 □

引理 3.4列表 的基本性质（1.1）中的区间 $I(i, j)$。对于子集 $U, V \subseteq \mathbb{Z}$，设

$$U \oplus V = (U \cup V) \setminus (U \cap V)$$

为 U an 与 V 的对称差。

引理 3.4. 设 i、j、k 为整数。则：

(i) $I(i,j) = I(j,i)$, (ii) I
$(i,j) + k = I(i+k, j+k)$, (ii) I
$(i,k) \oplus I(j,k) = I(i,j)$。

证明。由 $I(i,j)$ 的定义可知，（i）和（ii）显然成立。对于（iii），由对称性，只需讨论三种情形 $i \le j \le k$、$i \le k \le j$ 和 $k \le i \le j$。注意此时 $I(i,j) = [i,j) = \{i, i+1, \dots, j-1\}$。若 $i \le j \le k$，则 $I(i,k) \oplus I(j,k) = [i,k) \oplus [j,k) = [i,j)$；若 $i \le k \le j$，则 $I(i,k) \oplus I(j,k) = [i,k) \oplus [k,j) = [i,j)$；若 $k \le i \le j$，则 $I(i,k) \oplus I(j,k) = [k,i) \oplus [k,j) = [i,j)$。□

引理 3.5. 设 (g,γ) 是定义在 $(X,+)$ 上的构造对。则

$$g^{-i}(g^i x + g^i y) = x + y + \sum_{k \in I(0,3i)} g^{-k}\gamma(x,y) \tag{3.3}$$

对所有 $x,y \in X$ 和 $i,j \in \mathbb{Z}$ 均成立。

证明。对于 $i = 0$，无需证明 $I(0,0) = \emptyset$。对于 $i = 1$，我们得到 $I(0,3i) = I(0,3) = \{0,1,2\}$，并由此恢复 (C1)。若 (3.3) 对某个 $i \ge 0$成立，则

$$g^{-i-1}(g^{i+1}x + g^{i+1}y) = g^{-1}g^{-i}(g^i gx + g^i g(y)) = g^{-1}\Big(gx + gy + \sum_{k \in I(0,3i)} g^{-k}\gamma(gx, gy)\Big).$$

我们有 $\gamma(gx, gy) = g^{-2}\gamma(x, y)$，由 (3.1) 得到。根据引理 3.1，$g^{-k}\gamma(gx, gy) \in$像$(\gamma) \subseteq$根$(\gamma)$，且当至少有一个加项属于根$(\gamma)$ 时，g 的幂表现为同态。因此 $g^{-i-1}(g^{i+1}x + g^{i+1}y)$ 等于

$$g^{-1}(gx+gy) + \sum_{k \in I(0,3i)} g^{-1}g^{-k}g^{-2}\gamma(x,y) = g^{-1}(gx+gy) + \sum_{k \in I(0,3i)} g^{-k-3}\gamma(x,y)$$
$$= x + y + \sum_{k \in \{0,1,2\}} g^{-k}\gamma(x,y) + (g^{-3}\gamma(x,y) + \cdots + g^{-3i-2}\gamma(x,y)) = x + y + \sum_{k \in I(0,3(i+1))} g^{-k}\gamma(x,y),$$

这就给出了3.3) 对于 $i+1$。

由引理 3.3，$(g^{-1}, g\gamma)$ 是 $(X, +)$ 上的一个构造对。对于 $i = -1$，我们得到 $I(0,3i) = I(0,-3) = \{-3,-2,-1\}$，而 (3.3) 变为

$$g(g^{-1}x + g^{-1}y) = x + y + g\gamma(x,y) + g^2\gamma(x,y) + g^3\gamma(x,y),$$

这是 (C1) 对于 $(g^{-1}, g\gamma)$ 的对应形式。如果对于某个 $i \le 0$，3.3) 成立，那么

$$g^{-i+1}(g^{i-1}x + g^{i-1}y) = gg^{-i}(g^i g^{-1}x + g^i g^{-1}y) = g\Big(g^{-1}x + g^{-1}y + \sum_{k \in I(0,3i)} g^{-k}\gamma(g^{-1}x, g^{-1}y)\Big).$$

由 $(g^{-1}x, g^{-1}y) = g^2\gamma(x, y)$ 可得 γ3.1。如上所述，利用引理 3.1，我们可知$g^{-i+1}($ $g^{i-1}x + g^{i-1}y)$ 等于

$$g(g^{-1}x + g^{-1}y) + \sum_{k \in I(0,3i)} gg^{-k}g^2\gamma(x,y) = g(g^{-1}x + g^{-1}y) + \sum_{k \in I(0,3i)} g^{-k+3}\gamma(x,y)$$
$$= x + y + \sum_{k \in \{1,2,3\}} g^k\gamma(x,y) + (g^4\gamma(x,y) + \cdots + g^{3i+3}\gamma(x,y)) = x + y + \sum_{k \in I(0,3(i-1))} g^{-k}\gamma(x,y),$$

从而得到（3.3），其中 $i-1$。 □

Coro推论 3.6. 设 (g,γ) 是 $(X,+)$ 上的构造对，并设 $i\in\mathbb{Z}$。 n

$$g^{-i}(x+y)=g^{-i}(x)+g^{-i}(y)+\sum_{k\in I(-2i,i)}g^{-k}\gamma(x,y) \tag{3.4}$$

对每个 $x,y\in X$。

证明。 由（3.3）可得

$$g^{-i}(x+y)=g^{-i}(g^ig^{-i}x+g^ig^{-i}y)=g^{-i}(x)+g^{-i}(y)+\sum_{k\in I(0,3i)}g^{-k}\gamma(g^{-i}x,g^{-i}y).$$

由引理 3.2， γ（$g^{-i}x$， $g^{-i}y$） $=g^{2i}\gamma$（x， y）。因此

$$\sum_{k\in I(0,3i)}g^{-k}\gamma(g^{-i}x,g^{-i}y)=\sum_{k\in I(0,3i)}g^{-k+2i}\gamma(x,y)=\sum_{k\in I(0,3i)-2i}g^{-k}\gamma(x,y).$$

由于 I（0， $3i$） $-2i=I$（$-2i$， i）满足引理 3.4，证毕。 □

4. 从构造对得到的穆芳环路

本节在 $C\times X$ 上引入一个乘法公式，对应于循环群 C 以及g， γ）在（X， $+$）上的构造对（4.2）。我们给出所得圈成为穆芳环路的充要条件。

为进一步简化第 3 节中使用的记号，令

$$\sum_U(x,y)=\sum_{k\in U}g^{-k}\gamma(x,y),$$

对于固定的构造对 (g,γ) on $(X,+)$ 以及任意的 $U\subseteq\mathbb{Z}$ and $x,y\in\mathbb{Z}$。

引理 4.1. 设 (g,γ) be a construction pair on $(X,+)$， $U,V\subseteq\mathbb{Z}$, $x,y\in X$ and $i,j\in\mathbb{Z}$. 则:

（i） $\sum_U(g^ix,g^jy)=\sum_{U+i+j}(x,y)$,
（ii） $g^i\sum_U(x,y)=\sum_{U-i}(x,y)$, （iii）
$\sum_U(x,y)+\sum_V(x,y)=\sum_{U\oplus V}(x,y)$

证明。 对于 （3.1），我们可以利用得到

$$\sum_U(g^ix,g^jy)=\sum_{k\in U}g^{-k}\gamma(g^ix,g^jy)=\sum_{k\in U}g^{-k-i-j}\gamma(x,y)=\sum_{k\in U+i+j}g^{-k}\gamma(x,y)=\sum_{U+i+j}(x,y).$$

由引理 3 .1， g 限制为 Rad(γ) 和 Img(γ) 上的自同构 $\subseteq\mathrm{Rad}(\gamma)$。Hen ce

$$g^i\sum_U(x,y)=g^i\sum_{k\in U}g^{-k}\gamma(x,y)=\sum_{k\in U}g^ig^{-k}\gamma(x,y)=\sum_{k\in U}g^{-(k-i)}\gamma(x,y)=\sum_{U-i}(x,y),$$

证明（ii）。（iii）立即由引理 3.1 中的 $2\mathrm{Img}(\gamma)=0$ 得出。 □

对于 (g,γ) 上的构造对 $(X,+)$，令 $r(g,\gamma)$ 为满足下列条件的最小正整数 r

$$\sum_{0\le k<r}g^k(x)\in\mathrm{Rad}(\gamma) \tag{4.1}$$

对于每个 $x\in X$，如果存在这样的 r。否则，令 $r(g,\gamma)=\infty$。

引理 4.2. 设 (g,γ) 是 $(X,+)$ 上的一个构造对。对于整数 n 和 $x\in X$，以下条件等价：

（i）$\sum_{0\le k<|n|} g^k(x)\in$ 根(γ)，（ii）$\sum_{I(0,n)}(x,y)=0$ 对所有 $y\in X$成立，（iii）$\sum_{I(i,i+n)}(x,y)=0$ 对所有 $y\in X$ 和 $i\in\mathbb{Z}$成立。

证明。若 $n=0$，则这三个和均显然等于 0。设 $n\neq 0$。根据引理 4.1，我们有 $g^{-i}\sum_{I(0,n)}(x,y)=\sum_{I(0,n)+i}(x,y)=\sum_{I(i,i+n)}(x,y)$。由于 $g(0)=0$，条件（ii）和（iii）等价。下面证明（i）和（ii）等价。注意，将 n 替换为 $-n$时，条件（i）不变。由于 $g^n\sum_{I(0,n)}(x,y)=\sum_{I(-n,0)}(x,y)=\sum_{I(0,-n)}(x,y)$，且 $g(0)=0$，将 n 替换为 $-n$时，条件（ii）也不变。因此我们不妨设 $n>0$。现在，根据引理 3.2 以及 γ的双加性，有 $\sum_{I(0,n)}(x,y)=\sum_{0\le k<n} g^{-k}\gamma(x,y)=\sum_{0\le k<n}\gamma(g^kx,y)=\gamma(\sum_{0\le k<n} g^kx,y)$。因此（i）和（ii）等价。□

引理 4.3. 设 (g,γ) 是 $(X,+)$ 上的构造对，且 $r=r(g,\gamma)$。对于整数 n，以下条件等价：

（i）$n=0$ 或 r 整除 n，（ii）对于所有 $x\in X$，$\sum_{0\le k<|n|} g^k(x)\in$ 根(γ)，（iii）对于所有 $x,y\in X$，$\sum_{I(0,n)}(x,y)=0$，（iv）对于所有 $x,y\in X$ 和 $i\in\mathbb{Z}$，$\sum_{I(i,i+n)}(x,y)=0$。

证明. 若 $n=0$，则这三个条件显然等价，因此假设 $n\neq 0$。（ii）、（iii）和（iv）的等价性由引理 4.2 得出。下面证明（i）和（iii）等价。与引理 4.2 的证明相同，不失一般性，可设$n>0$。注意，若 r 有限，则引理 4.2 蕴含对于每个 i，$\sum_{I(i,i+r)}(x,y)=0$。

假设（i）成立。那么，对于某个正整数 q，$r<\infty$ 和 $n=qr$。由于$I(0,n)=I(0,r)\cup I(r,2r)\cup\cdots\cup I((q-1)r,n)$，我们有 $\sum_{I(0,n)}(x,y)=\sum_{I(0,r)}(x,y)+\sum_{I(r,2r)}(x,y)+\cdots+\sum_{I((q-1)r,n)}(x,y)=0$。反过来，假设（ii）成立，这又意味着 $r<\infty$。为导出矛盾，假设对于某个 $0<t<r$，$n=qr+t$。那么$\sum_{I(0,t)}(x,y)=\sum_{I(0,n)}(x,y)-\sum_{I(t,n)}(x,y)=\sum_{I(0,n)}(x,y)-g^{-t}\sum_{I(0,qr)}(x,y)=0-g^{-t}(0)=0$ 对所有 $x,y\in X$ 都成立。于是，根据引理 4.2，对所有 $x\in X$，$\sum_{0\le k<t} g^kx\in$ Rad(γ)，这与 r的极小性矛盾。□

引理 4.4. 设 $(X,+)$ 是一个阿贝尔群，(g,γ) 是 $(X,+)$ 上的一个构造对，且$C=\langle b\rangle$ 是一个循环群。那么以下条件等价：

（i）公式

$$(b^i,x)\cdot(b^j,y)=\Big(b^{i+j},g^{-j}(x)+y+\sum_{k\in I(i+j,-j)} g^{-k}\gamma(x,y)\Big)\tag{4.2}$$

在 $C\times X$ 上正确定义了一个乘法。

（ii）要么 C 是无限的，要么 C 是有限的，$|g|$ 整除 $|C|$，且对每个 $x\in X$，$\sum_{0\le k<|C|} g^k(x)\in$ 根(γ)。（iii）要么 C 是无限的，要么 C 是有限的，$|g|$ 整除 $|C|$，且 $r(g,\gamma)$ 整除 $|C|$。

证明。（ii）与（iii）的等价性由引理 4.3得出。下面证明（i）与（ii）的等价性。

假设乘法 (4.2) 定义良好。若 C 是无限的，结论即得，因此假设 $|C| = n$ 是有限的。根据引理 3.1，回顾 $\gamma(x, 0) = 0$ 且 $g(0) = 0$。于是，对每个 $x \in X$，乘积 $(b^0, x) \cdot (b^0, 0)$ 的计算结果为 (b^0, x)，并且等于 $(b^n, x) \cdot (b^0, 0) = (b^0, g^{-n}(x))$，因此 $g^n(x) = x$ 且 $|g|$ 整除 n。此外，对每个 $x, y \in X$，乘积 $(b^0, x) \cdot (b^0, y) = (b^0, x + y)$ 等于 $(b^n, x) \cdot (b^0, y) = (b^0, x + y + \sum_I(n, 0)(x, y))$，因此 $\sum_I(0,n)(x, y) = 0$，从而根据引理 4.3，$\sum_{0\le k<n} g^k(x) \in \mathrm{Rad}(\gamma)$。

反过来，如果 C 是无限的，那么乘法显然是良定义的。假设$|C| = n$，$|g|$ 整除 n 且 $\sum_{0\le k<n} g^k(x) \in \mathrm{Rad}(\gamma)$ 对每个 $x \in X$都成立。我们只需检验，当用 4.2式中的 i 替换为 $i + n$，并将 j 替换为 $j + n$时，公式给出的结果相同。由于我们假设 $|g|$ 整除 n，所以只需检验

$$\sum_{I(i+n+j,-j)}(x, y) = \sum_{I(i+j,-j)}(x, y) = \sum_{I(i+j+n,-j-n)}(x, y).$$

回想一下，符号在此不起作用，因为 $2\mathrm{Img}(\gamma) = 0$。对于第一个等式，注意到$I(i + n + j, -j) \oplus I(i + j, -j) = I(i + j + n, i + j)$，由引理 3.4 可知，因此我们需要检验 $\sum_I(i+j+n, i+j)(x, y) = 0$。由引理 4.3，这成立，因为对每个 $x \in X$，$\sum_{0\le k<n} g^k(x) \in \mathrm{Rad}(\gamma)$。对于第二个等式，现在只需证明 $\sum_I(i+n+j,-j)(x, y) = \sum_I(i+j+n,-j-n)(x, y)$，这等价于 $\sum_I(-j, -j-n)(x, y) = 0$；由引理 3.4，这再次成立，而这又由引理 4.3 得出。□

下面的结果表明（结合引理 4.3）可知，引理 $\sum_{0\le k<|C|} g^k(x) \in \mathrm{Rad}(\gamma)$ 的必要条件 4.4 在 $|g|$ 整除 $|C|$ 且 $\mathrm{Rad}(\gamma)$不含 3 阶元素时会自动满足。

引理 4.5. 设 (g, γ) 是 $(X, +)$ 上的构造对，且 $r = r(g, \gamma)$。若 $|g| < \infty$，则 r 整除 $3|g|$。若 $|g| < \infty$ 且 $\mathrm{Rad}(\gamma)$ 不含 3 阶元素，则 r 整除 $|g|$。

证明. 设 $m = |g| < \infty$。由 (3.3)，$x + y = g^{-m}(g^m x + g^m y) = x + y + \sum_I(0,3m)(x, y)$，因此 $\sum_I(0,3m)(x, y) = 0$，并且由引理 4.3 得 r 整除 $3m$。再假设 $\mathrm{Rad}(\gamma)$ 不含 3 阶元素。由于对每个 k 都有 $g^k = g^{k+m}$，我们得到 $0 = \sum_I(0,3m)(x, y) = 3\sum_I(0,m)(x, y)$。和 $\sum_I(0,m)(x, y)$ 由引理 3.1 属于 $\mathrm{Rad}(\gamma)$。由于 $\mathrm{Rad}(\gamma)$ 不含 3 阶元素，我们推出 $\sum_I(0,m)(x, y) = 0$，进而由引理 4.3 得 r 整除 m。□

下面给出论文的主要构造：

定义 4.6。设 $(X, +)$ 是一个阿贝尔群，(g, γ) 是 $(X, +)$ 上的一个构造对，并且 $C = \langle b\rangle$ 是一个循环群。如果 C 是有限的，进一步设 $|g|$ 整除 $|C|$，且$r(g, \gamma)$ 整除 $|C|$。那么，带有乘法 $(C \times X, \cdot)$（4.2）的广群 $C \ltimes_{(g,\gamma)} X$ 将记作 $\langle b\rangle \ltimes_{(g,\gamma)} X$或 $\langle b\rangle \ltimes_{(g,\gamma)} X$。每当我们使用这一记号时，都隐含地假设该定义所要求的所有条件均已满足。

注意，$C \times 0$ 是 $Q = C \ltimes_{(g,\gamma)} X$的子环。映射 $(b^i, x) \mapsto b^i$ 是从 $Q = C \ltimes_{(g,\gamma)} X$ 到 C 上的一个同态，其核为 $1 \times X$。因此，$1 \times X$ 是Q 的正规子圈，并且 $Q/(1 \times X)$ 同构于 C。显然，$(C \times 0) \cap (1 \times X) = 1$，所以 Q 是分裂的。

定理 4.7。设 $Q = C \ltimes_{(g,\gamma)} X$为定义 4.6中的广群。则 Q是一个穆芳环路，其幺元为 $(1, 0)$，其逆元为 $(b^i, x)^{-1} = (b^{-i}, -g^i(x))$。

证明。 我们将自由使用引理 3.1、3.4 和 4.1 。由引理 4.4，乘法定义良好。

幺元。将 $(1,0) = (b^0, 0)$ 代入 (4.2) 中的 (b^i, x)，得到 $(b^0,0)\cdot(b^j,y) = (b^j, g^{-j}(0) + y + \sum_I(j,-j)(0,y))$。由于 $\gamma(0,y) = 0 = g(0)$，乘积化简为 (b^j,y)。类似地，$(b^i,x)\cdot(b^0,0) = (b^i, g^{-0}(x) + 0 + \sum_I(i,0)(x,0)) = (b^i,x)$。

双侧逆元。我们将证明 $(b^{-i}, -g^i(x))$ 是 (b^i,x) 的双侧逆元。我们有 $(b^i,x)\cdot(b^{-i},-g^i(x)) = (1, g^i(x) - g^i(x) + \sum_I(0,i)(x,-g^i(x)))$。由于 $\gamma(x,-g^i(x)) = -g^{-i}\gamma(x,x) = -g^{-i}(0) = 0$，乘积化简为 $(1,0)$。类似地，$(b^{-i},-g^i(x))\cdot(b^i,x) = (1, g^{-i}(-g^i(x)) + x + \sum_I(0,-i)(-g^i(x)\ x)) = (1,0)$，因为和再次为零，且 $g^k(-x) = -g^k(x)$。

逆性质环路。 众所周知，参见 [38], ，具有幺元和双侧逆元的广群是逆性质环路，当且仅当 $x^{-1}(xy) = y = (yx)x^{-1}$ 对所有x，y都成立。我们将验证这两个恒等式。以下用 $b^i x$ 代替$(b^i,\ x$。于是有

$$\begin{aligned} b^{-i}(-g^i x)\cdot(b^i x\cdot b^j y) &= b^{-i}(-g^i x)\cdot b^{i+j}(g^{-j}x + y + \sum_{I(i+j,-j)}(x,y)) \\ &= b^j(g^{-i-j}(-g^i x) + g^{-j}x + y + \sum_{I(i+j,-j)}(x,y) + \sum_{I(j,-i-j)}(-g^i x, g^{-j}x + y)). \end{aligned}$$

注意，由于 γ 是双加性且交错的，$\gamma(g^a x, g^b x + y) = \gamma(g^a x, g^b x) + \gamma(g^a x, y) = g^{-a-b}\gamma(x,x) + \gamma(g^a x, y) = \gamma(g^a x, y)$。因此

$$\sum_{I(j,-i-j)}(-g^i x, g^{-j}x + y) = \sum_{I(j,-i-j)}(-g^i x, y) = -\sum_{I(j,-i-j)}(g^i x, y) = -\sum_{I(i+j,-j)}(x,y).$$

此外，$g^{-i-j}(-g^i x) = -g^{-i-j}g^i(x) = -g^{-j}x$。结合起来可得 $b^{-i}(-g^i x)\cdot(b^i x\cdot b^j y) = b^j y$。类似地，

$$\begin{aligned} (b^i x\cdot b^j y)\cdot b^{-j}(-g^j y) &= b^{i+j}(g^{-j}x + y + \sum_{I(i+j,-j)}(x,y))\cdot b^{-j}(-g^j y) \\ &= b^i(g^j(g^{-j}(x) + y + \sum_{I(i+j,-j)}(x,y)) - g^j y + \sum_{I(i,j)}(g^{-j}x + y, -g^j y)), \end{aligned}$$

这里利用了 $\sum_{I(i+j,\ -j)}(x,\ y) \in$ 像$(\gamma) \subseteq$ 根$(\gamma$。根据推论 3.6，

$$\begin{aligned} g^j(g^{-j}(x) + y + \sum_{I(i+j,-j)}(x,y)) &= g^j(g^{-j}x) + g^j(y + \sum_{I(i+j,-j)}(x,y)) + \sum_{I(2j,-j)}(g^{-j}x, y) \\ &= x + g^j y + g^j\sum_{I(i+j,-j)}(x,y) + \sum_{I(2j,-j)}(g^{-j}x, y) \\ &= x + g^j y + \sum_{I(i,-2j)}(x,y) + \sum_{I(j,-2j)}(x,y) = x + g^j y + \sum_{I(i,j)}(x,y). \end{aligned}$$

此外，

$$\sum_{I(i,j)}(g^{-j}x + y, -g^j y) = -\sum_{I(i,j)}(g^{-j}x, g^j y) = -\sum_{I(i,j)}(x,y).$$

综合可得 $(b^i x\cdot b^j y)\cdot b^{-j}(-g^j y) = b^i x$。

穆芳恒等式。 剩下需要证明 $(C\times X,\cdot)$ 满足某个穆芳恒等式。我们将证明 (M2). 首先求出 $b^ix\cdot(b^jy\cdot b^ix)$ 的公式。我们有

$$\begin{aligned} b^ix\cdot(b^jy\cdot b^ix) &= b^ix\cdot b^{i+j}(g^{-i}y+x+\sum_{I(i+j,-i)}(x,y)\\ &= b^{2i+j}(g^{-i-j}x+g^{-i}y+x+\sum_{I(i+j,-i)}(x,y)+\sum_{I(2i+j,-i-j)}(x,g^{-i}y+x)). \end{aligned}$$

由于

$$\sum_{I(2i+j,-i-j)}(x,g^{-i}y+x) \;=\; \sum_{I(2i+j,-i-j)}(x,g^{-i}y) \;=\; \sum_{I(i+j,-2i-j)}(x,y)$$

且 $I(i+j,-2i-j)\oplus I(i+j,-i) = I(-i,-2i-j)$，我们得到

$$b^ix\cdot(b^jy\cdot b^ix) = b^{2i+j}(g^{-i-j}x+x+g^{-i}y+\sum_{I(-i,-2i-j)}(x,y). \tag{4.3}$$

在下面第二个等式中使用（4.3），我们有

$$\begin{aligned} b^ix\cdot((b^jy\cdot b^kz)\cdot b^ix) &= b^ix\cdot(b^{j+k}(g^{-k}y+z+\sum_{I(j+k,-k)}(y,z))\cdot b^ix)\\ &= b^{2i+j+k}(g^{-i-j-k}x+x+g^{-i}(g^{-k}y+z)+g^{-i}\sum_{I(j+k,-k)}(y,z)+\sum_{I(-i,-2i-j-k)}(x,g^{-k}y+z)). \end{aligned}$$

接下来，我们将改写最后一个等式中的某些三个加项，第一个加项使用推论 3.6 。我们得到:

$$\begin{aligned} g^{-i}(g^{-k}y+z) &= g^{-i-k}y+g^{-i}z+\sum_{I(-2i,i)}(g^{-k}y,z) = g^{-i-k}y+g^{-i}z+\sum_{I(-2i-k,i-k)}(y,z),\\ g^{-i}\sum_{I(j+k,-k)}(y,z) &= \sum_{I(i+j+k,i-k)}(y,z),\\ \sum_{I(-i,-2i-j-k)}(x,g^{-k}y+z) &= \sum_{I(-i-k,-2i-j-2k)}(x,y) \;+\; \sum_{I(-i,-2i-j-k)}(x,z). \end{aligned}$$

合并关于 (y,z) 的两个和可知，$b^ix\cdot((b^jy\cdot b^kz)\cdot b^ix) = b^{2i+j+k}u$，其中 u 等于

$$g^{-i-j-k}x+x+g^{-i-k}y+g^{-i}z+\sum_{I(-i-k,-2i-j-2k)}(x,y) \;+\; \sum_{I(-i,-2i-j-k)}(x,z) \;+\; \sum_{I(i+j+k,-2i-k)}(y,z).$$

另一方面,

$$(b^ix\cdot b^jy)\cdot(b^kz\cdot b^ix) = b^{i+j}(g^{-j}x+y+\sum_{I(i+j,-j)}(x,y))\cdot b^{i+k}(g^{-i}z+x+\sum_{I(i+k,-i)}(x,z))$$

等于 $b^{2i+j+k}v$，其中 v 是

$$g^{-i-k}(g^{-j}x+y)+g^{-i-k}\sum_{I(i+j,-j)}(x,y)+g^{-i}z+x+\sum_{I(i+k,-i)}(x,z) \;+\; \sum_{I(2i+j+k,-i-k)}(g^{-j}x+y,g^{-i}z+x).$$

再次关注某些三个加项，我们得到

$$g^{-i-k}(g^{-j}x+y)=g^{-i-j-k}x+g^{-i-k}y+\sum_{I(-2i-2k,i+k)}(g^{-j}x,y)=g^{-i-j-k}x+g^{-i-k}y+\sum_{I(-2i-j-2k,i-j+k)}(x,y),$$

$$g^{-i-k}\sum_{I(i+j,-j)}(x,y)=\sum_{I(2i+j+k,i-j+k)}(x,y),$$

$$\sum_{I(2i+j+k,-i-k)}(g^{-j}x+y,g^{-i}z+x)=\sum_{I(2i+j+k,-i-k)}(x,y)\quad+\sum_{I(i+k,-2i-j-k)}(x,z)\quad+\sum_{I(i+j+k,-2i-k)}(y,z).$$

因此，(x,y) 对 $(b^ix\cdot b^jy)\cdot(b^kz\cdot b^ix)$ 的总体贡献为

$$\begin{aligned}&I(-2i-j-2k,i-j+k)\oplus I(2i+j+k,i-j+k)\oplus I(2i+j+k,-i-k)\\&\quad=I(-2i-j-2k,2i+j+k)\oplus I(2i+j+k,-i-k)=I(-i-k,-2i-j-2k),\end{aligned}$$

而 (x,z) 的总体贡献为

$$I(i+k,-i)\oplus I(i+k,-2i-j-k)=I(-i,-2i-j-k).$$

综合以上可知 $v=u$ 以及 (M2) 成立。 □

5. Properties of the Moufang loops obtained from construction pairs

本节将确立定理 $C\ltimes_{(g,\gamma)}X$ 4.7中的穆芳环路的一些结构性质。我们将直接使用引理 3.1、3.4 和 4.1。

引理 5.1。设 $Q=\langle b\rangle\ltimes_{(g,\gamma)}X$。对于所有 $i,j\in\mathbb{Z}$ 以及 $x,y\in X$，我们有

$$[(b^i,x),(b^j,y)]=\Big(1,-x+g^{-j}x+y-g^{-i}y+\sum_{I(-i,-j)}(x,y)+\sum_{I(-i-j,i+j)}(x,y)\Big).\tag{5.1}$$

证明。设（1，u）是（5.1）右侧的表达式。我们需要验证（b^j，y）（b^i，x）·（1，u）=（b^i，x）（b^j，y）。设

$$\begin{aligned}v&=\sum_{I(i+j,0)}(g^{-i}y+x,-x+g^{-j}x+y-g^{-i}y)\\&=\sum_{I(i+j,0)}(g^{-i}y,x)+\sum_{I(i+j,0)}(g^{-i}y,g^{-j}x)+\sum_{I(i+j,0)}(x,y)+\sum_{I(i+j,0)}(x,g^{-i}y)\\&=\sum_{I(i+j,0)}(g^{-i}y,g^{-j}x)+\sum_{I(i+j,0)}(x,y)=\sum_{I(0,-i-j)}(x,y)+\sum_{I(i+j,0)}(x,y)=\sum_{I(-i-j,i+j)}(x,y).\end{aligned}$$

Then

$$
\begin{aligned}
&(b^j,y)(b^i,x)\cdot(1,u) = (b^{i+j}, g^{-i}y + x + \sum_{I(i+j,-i)}(x,y))\cdot(1,u)\\
&= (b^{i+j}, g^{-i}y + x + \sum_{I(i+j,-i)}(x,y) - x + g^{-j}x + y - g^{-i}y + \sum_{I(-i,-j)}(x,y) + \sum_{I(-i-j,i+j)}(x,y) + v)\\
&= (b^{i+1}, g^{-j}x + y + \sum_{I(i+j,-i)}(x,y) + \sum_{I(-i,-j)}(x,y) + \sum_{I(-i-j,i+j)}(x,y) + \sum_{I(-i-j,i+j)}(x,y))\\
&= (b^{i+j}, g^{-j}x + y + \sum_{I(i+j,-j)}(x,y)) = (b^i,x)(b^j,y). \qquad \square
\end{aligned}
$$

引理 5.2. 设 $Q = \langle b\rangle \ltimes_{(g,\gamma)} X$。对于所有 i、j、$k \in \mathbb{Z}$ 和 x、y、$z \in X$，我们有

$$
[(b^i,x),(b^j,y),(b^k,z)] = \Big(1, \sum_{I(i+j,i+j+k)}(x,y) + \sum_{I(i+k,i+j+k)}(x,z) + \sum_{I(j+k,i+j+k)}(y,z)\Big). \tag{5.2}
$$

证明。 设 $(1,u)$ 为结合子公式 (5.2) 的右侧。我们的目标是验证等式 $((b^i,x)\cdot(b^i,x)(b^j,y)\cdot(b^k,z)$。直接计算可得

$$
(b^i,x)\cdot(b^j,y)(b^k,z) = (b^{i+j+k}, g^{-j-k}x + g^{-k}y + z + \sum_{I(i+j,-j-2k)}(x,y) + \sum_{I(i+j+k,-j-k)}(x,z) + \sum_{I(j+k,-k)}(y,z)).
$$

注意到 t hat $u \in$ 根(γ)，我们看到 $((b^i,x)\cdot(b^j,y)(b^k,z))(1,u)$ 因此等于 t o

$$
(b^{i+j+k}, g^{-j-k}x + g^{-k}y + z + \sum_{I(i+j+k,-j-2k)}(x,y) + \sum_{I(i+k,-j-k)}(x,z) + \sum_{I(i+j+k,-k)}(y,z)).
$$

利用推论 3.6进行第三个等式的计算，得到

$$
\begin{aligned}
&(b^i,x)(b^j,y)\cdot(b^k,z) = (b^{i+j}, g^{-j}x + y + \sum_{I(i+j,-j)}(x,y))(b^k,z)\\
&= (b^{i+j+k}, g^{-k}(g^{-j}x + y) + g^{-k}\sum_{I(i+j,-j)}(x,y) + z + \sum_{I(i+j+k,-k)}(g^{-j}x + y, z)\\
&= (b^{i+j+k}, g^{-j-k}x + g^{-k}y + \sum_{I(-2k,k)}(g^{-j}x,y) + z + \sum_{I(i+j+k,-j+k)}(x,y) + \sum_{I(i+k,-j-k)}(x,z) + \sum_{I(i+j+k,-k)}(y,z)).
\end{aligned}
$$

由于

$$
\sum_{I(-2k,k)}(g^{-j}x,y) + \sum_{I(i+j+k,-j+k)}(x,y) = \sum_{I(-j-2k,-j+k)}(x,y) + \sum_{I(i+j+k,-j+k)}(x,y) = \sum_{I(i+j+k,-j-2k)}(x,y),
$$

我们就完成了。 $\square$

对于圈 Q，交换子子圈 Com(Q)（分别地，结合子子圈 Asc(Q)，以及导出子圈 Q'）是使得 Q/N 成为交换的（分别地，成为结合的、成为阿贝尔群）的最小正规子圈 N。因此，Com(Q)（分别地，Asc(Q)，以及 Q'）是由所有交换子（分别地，结合子，以及交换子和结合子）生成的 Q 的正规子圈。

命题 5.3。设 $Q = \langle b\rangle \ltimes_{(g,\gamma)} X$。那么

$$
1 \times \langle \mathrm{Img}(\gamma)\rangle = \mathrm{Asc}(Q) \le \mathrm{Com}(Q) = Q' = 1 \times \langle \mathrm{Img}(\gamma) \cup \mathrm{Img}(1-g)\rangle.
$$

证明。 由引理 5.1 和 5.2 可知，Com(Q)、Asc(Q) 和 Q' 都是$1 \times X$的子环。由于 X 是一个阿贝尔群，因此 Com(Q)（分别地，Asc(Q)、 Q'）是由所有交换子（分别地，结合子、交换子和结合子）生成的 Q 子环，也就是说，无须取正规闭包。

令 $A = \langle$像$(1-g) \cup$像$(\gamma)\rangle \leq X$。我们首先证明 Com(Q) $= 1 \times A$。有$g^{i+1}x - g^i x = g(g^i x) - g^i x \in$像$(g-1) \subseteq A$，对所有 i均成立，因此 $g^j x - x = (g^j x - g^{j-1}x) + (g^{j-1}x - g^{j-2}x) + \cdots + (gx - x) \in A$，对所有 $j \geq 0$均成立。由于 $g^{-j}x - x = -(g^j g^{-j}x - g^{-j}x)$，对所有 j均有 $g^j x - x \in A$。此外，$\sum_I(i,j)(x,y) \in A$，因为 g 置换了像 $(\gamma) \subseteq A$。由 (5.1),

$$[(b^i, x), (b^j, y)] = \Big(1, -x + g^{-j}x + y - g^{-i}y + \sum_{I(-i,-j)}(x,y) + \sum_{I(-i-j,i+j)}(x,y)\Big).$$

由此可知， $1 \times A$包含所有交换子，因此 Com(Q) $\leq 1 \times A$。反过来，设 Com(Q) $= 1 \times Y$，其中某个 $Y \leq X$。有 $[(b^i, x), (b^j, 0)] =$ (1, $-x + g^{-j}x$) $\in$ Com(Q)。特别地，像$(1-g) \subseteq Y$。于是交换子公式推出 $\sum_I(-i,-j)(x,y) + \sum_I(-i-j,i+j)(x,y) \in Y$。结合 $j = -i$，得到 $\sum_I(-i,i)(x,y) \in Y$，因而 $\sum_I(-i-j,i+j)(x,y) \in Y$且 $\sum_I(-i,-j)(x,y) \in Y$。于是 $\gamma(x,y) = \sum_I(0,1)(x,y) \in Y$，并且像 $(\gamma) \subseteq Y$。这表明 $1 \times A \leq$ Com(Q)。

结合子公式（5.2）表明 Asc(Q) $\leq \langle$Img$(\gamma)\rangle \leq$ Com(Q)，因此 Com(Q) $= Q'$。将 $i = j = 0$、$k = 1$ 和 $z = 0$ 代入（5.2）得到 $\gamma(x,y) = \sum_{I(0,1)}(x,y) \in$ Asc(Q)，因此 $\langle$Img$(\gamma)\rangle \leq$ Asc(Q)。□

C推论 5.4. 设 $Q = \langle b\rangle \ltimes_{(g,\gamma)} X$。如果 Q 是交换的，则 Q 是一个群 p.

证明。 如果 Q 是交换的，则 $1 = \mathrm{Com}(Q)$。由于 Asc(Q) $\leq \mathrm{Com}(Q)$，根据命题 5.3，Q 是一个群。□

回顾参数 $r(g,\gamma)$（4.1），可能带有 $r(g,\gamma) = \infty$。

命题 5.5. 设 $Q = \langle b\rangle \ltimes_{(g,\gamma)} X$，并设 $r = r(g,\gamma)$。

$$\text{Nuc}(Q) = \{(b^i, x)\colon \ x \in \text{Rad}(\gamma), \text{ 且 } i = 0 \text{ 或 } r \text{ 整除 } i\},$$
$$Z(Q) = \{(b^i, x) \in \text{Nuc}(Q)\colon \ |g| \text{ 整除 } i, \text{ 且 } g(x) = x\}.$$

证明。由引理 5.2，$(b^i, x) \in$Nuc(Q) 当且仅当 $\sum_I(i+j,i+j+k)(x,y) + \sum_I(i+k,i+j+k)(x,z) + \sum_I(j+k, i+j+k)(y,z) = 0$ 对所有 $j,k \in \mathbb{Z}$ 及 $y,z \in X$成立。设 $(b^i, x) \in$Nuc(Q)。令 $j = 0$, $k = 1$ 及 $z = 0$，得到 $0 = \sum_I(i,i+1)(x,y) = g^{-i}\gamma(x,y)$，故 $x \in$ Rad(γ)。那么，$\sum_I(j+k,i+j+k)(y,z) = 0$ 推出 $\sum_I(0,i)(y,z) = 0$。由引理 4.3， $i = 0$ 或 r 整除 i。反之，若 $i = 0$ 或 r 整除 i，则由引理 4.3，对于所有 j,k,y,z，$\sum_I(j+k,i+j+k)(y,z) = 0$ 成立。若另有 $x \in$ Rad(γ)，则可推出 $(b^i, x) \in$ Nuc(Q)。

假设 $(b^i, x) \in$Nuc(Q)。根据引理 5.1，$(b^i, x) \in Z(Q)$ 当且仅当对所有 $j \in \mathbb{Z}$ 和 $y \in X$， $-x + g^{-j}x + y - g^{-i}y = 0$。假设 $(b^i, x) \in Z(Q)$。令 $j = -1$ 和 $y = 0$，得到 $x = g(x)$。那么，对所有 y， $y = g^{-i}y$ 意味着 $|g|$ 整除 i。反过来，若 $|g|$整除 i 且 $x = g(x)$，则 $-x + g^{-j}x + y - g^{-i}y = 0$ 且 $(b^i, x) \in Z(Q)$。□

6. A note on abelian congruences in Moufang loops

环路的可解性理论有两种：一种是基于群论中标准可解性定义的经典可解性，另一种则基于一种一般的

同余模簇中的可解性理论。参见 [17] 关于同余模簇中的可解性，[42] 关于环路中同余可解性的导论，以及 [15] 关于环路可解性的详细讨论。

在群中，可解性的这两个概念是一致的；但在环路中，同余可解性严格强于经典可解性。穆芳环路中的这两个可解性概念是否一致，仍是一个悬而未决的问题。我们在 [15] 中证明了奇数阶穆芳环路是同余可解的，从而加强了 Glauberman 奇数阶定理对穆芳环路 [20]的结论。

主要困难在于，与群不同，穆芳环路的阿贝尔正规子群 Q 未必会诱导出 Q 的阿贝尔同余（见下文）。例如，在 [15] 中，我们构造了一类幂零穆芳环路 Q，它们具有一个阿贝尔正规子群，但该子群不会诱导出 Q的阿贝尔同余。

环路 Q 的正规子圈 X 诱导出 Q的同余 $\rho_X = \{(a,b) \in Q : aX = bX\}$。根据 [42] 和 [3], 的结果， Q 的同余 ρ、 σ 的交换子 $[\rho,\sigma]_Q$ 是由以下元素生成的 Q 的同余

$$\{(T_{b_1}(a), T_{c_1}(a)),\ (L_{b_1,b_2}(a), L_{c_1,c_2}(a)),\ (R_{b_1,b_2}(a), R_{c_1,c_2}(a)) : 1\rho a,\ b_1\sigma c_1,\ b_2\sigma c_2\}. \tag{6.1}$$

Q 的同余 ρ 是阿贝尔的，当且仅当 $[\rho,\rho]_Q = \{(a,a) : a \in Q\}$。

下面的结果表明，由定理 4.7 所给出的穆芳环路往往含有一个阿贝尔正规子群，但它并不诱导阿贝尔同余。

命题 6.1. 设 $Q = \langle b\rangle \ltimes_{(g,\gamma)} X$。那么， Q的阿贝尔正规子群 $1 \times X$ 诱导 Q 的阿贝尔同余，当且仅当 Q 是一个群。

证明. 若 Q 是一个群，则 Q 的每个阿贝尔正规子群都会诱导 Q的阿贝尔同余。反过来，设 ρ 是由 $1 \times X$诱导的同余，因此 ρ 的等价类恰好是 Q中 $1 \times X$ 的陪集。回忆一下，穆芳环路中有 $T_{a^{-1}} = T_a^{-1}$。因此，要证明 ρ 不是阿贝尔的，只需找出 $x, y, z \in X$，使得$T^{-1}_{(b,y)}(1,x) \neq T^{-1}_{(b,z)}(1,x)$，参见 (6.1)。现在， $T_u^{-1}(v) = u^{-1}vu = v(v^{-1}u^{-1}vu) = v[v,u]$。由引理 5.1，得

$$\begin{aligned} T^{-1}_{(b,y)}(1,x) &= (1,x)[(1,x),(b,y)] = (1,x)(1,-x+g^{-1}(x)+y-y+\sum_{I(0,-1)}(x,y)+\sum_{I(-1,1)}(x,y)) \\ &= (1,x)(1,-x+g^{-1}(x)+\sum_{I(0,1)}(x,y)) = (1,x)(1,-x+g^{-1}(x)+\gamma(x,y)) \\ &= (1, g^{-1}(x)+\gamma(x,y)). \end{aligned}$$

假设对于所有 $x, y, z \in X$，均有 $T^{-1}_{(b,y)}(1,x) = T^{-1}_{(b,z)}(1,x)$。那么对于所有$x, y, z \in X$，均有 $\gamma(x,y) = \gamma(z,y)$，因此对每个 $y \in Q$， $y \in \mathrm{Rad}(\gamma)$，且 $\mathrm{Img}(\gamma) = 1$。由命题 5.3， Q 是一个群。□

7. Pseudoautomorphisms induced by pseudoautomorphisms

现在我们开始为定理 4.7 的部分逆命题做准备。虽然本节和下一节的表述比所需范围更一般，但其主要目的是证明：穆芳环路中限制在阿贝尔正规子圈上的每个共轭都会产生一个穆芳置换，参见命题 8.4和定义 1.2。

本节中，设 Q 是一个穆芳环路， X 是 Q 的一个正规子圈。对于 Q 和 $x \in Q$ 上的置换 f，定义 Q 上的置换 $\mu_{f,x}$ 如下

$$\mu_{f,x} = R_x^{-1} f^{-1} R_{f(x)} f. \tag{7.1}$$

注意，如果 $f(1) = 1$，那么 $\mu_{f,x}(1) = R_x^{-1} f^{-1} f(x) = 1$。

设 f 是 Q 的伪自同构，参见 (2.1)。根据命题 7.1， $\mu_{f,x}$ 也是 Q 的伪自同构，我们称 $\mu_{f,x}$ 为由 f 诱导的伪自同构，记作 x。在特殊情形下，若 f 是 Q 的内映射，命题 7.2 表明，诱导的伪自同构 $\mu_{f,x}$ 作用于 X，并给出了 $\mu_{f,x}$ 的伴随元属于 X 的必要条件。特别地，如果 $x \in X$ 且 $f \in$ 属于 $\mathrm{Inn}(Q)$，那么 $\mu_{f,x}$ 在 X 上的限制是 X 的伪自同构，参见推论 7.3。最后，若对某个 $a \in Q$ 有 $f = T_a$，则 $R_x \mu_{f,x} R_x^{-1}$ 可用 f 和左平移表示，参见命题 7.7。

注意到，对于群的伪自同构而言，这一概念是平凡的。群的每个伪自同构都是自同构，因此，$(f^{-1} R_{f(x)} f) = R_x^{-1} R_{f^{-1}(f(x))} = R_x^{-1} R_x = \mathrm{id}_Q$。

命题 7.1. 设 Q 为穆芳环路，$(c, f) \in \mathrm{Psa}_\ell(Q)$ 且 $x \in Q$。则

$$(x^{-1} f^{-1}(c^{-1} f(x) c),\ \mu_{f,x}) \in \mathrm{Psa}_\ell(Q).$$

证明. 设 $\theta_x = (L_x, R_x, L_x R_x)$ 且 $\varphi = (L_c f, f, L_c f)$。注意，由于 Q 是穆芳环路， $\theta_x \in \mathrm{Atp}(Q)$；又由于 $(c, f) \in \mathrm{Psa}_\ell(Q)$， $\varphi \in \mathrm{Atp}(Q)$。因此， $\psi = \theta_x^{-1} \varphi^{-1} \theta_{f(x)} \varphi \in \mathrm{Atp}(Q)$。 ψ 的中间坐标等于 μ_f，$_x = R_x^{-1} f^{-1} R_{f(x)} f$。由于对于穆芳环路的任意伪自同构 f， $f(1) = 1$ 成立，因此有 $\mu_{f,x}(1) = 1$。 ψ 的第一个坐标将 1 映射为 $L_x^{-1} f^{-1} L_c^{-1}(f(x)c) = x^{-1} f^{-1}(c^{-1} f(x) c)$，由引理 2.1 即得证。□

命题 7.2. 设 Q 是一个穆芳环路， $X \trianglelefteq Q$ 和 $x \in Q$。设 $f \in \mathrm{Inn}(Q)$，并设当将 f 视为伪自同构时，c 是 f 的伴随元。那么 $\mu_{f,x}(X) = X$。此外，$\mu_{f,x}$ 的伴随元 $x^{-1} f^{-1}(c^{-1} f(x) c)$ 属于 X，当且仅当 $[f(x)\ c]$ 属于 X。

证明。由命题 7.1，$(x^{-1} f^{-1}(c^{-1} f(x) c)\ \mu_{f,x}) \in \mathrm{Psa}_\ell(Q)$。由于 $X \trianglelefteq Q$ 且 $f \in \mathrm{Inn}(Q)$，因此 $f(X) = X$。于是，利用 X 的正规性，可得 $\mu_{f,x} = R_x^{-1} f^{-1} R_{f(x)} f$ 置换 X 当且仅当 $Xf(x) = f(Xx)$，当且仅当 $c \cdot Xf(x) = cf(Xx)$，当且仅当 $cX \cdot f(x) = cf(Xx)$。条件 $cX \cdot f(x) = cf(Xx)$ 成立，因为 $f(X) = X$ 且 $(c, f) \in \mathrm{Psa}_\ell(Q)$，也就是说，对每个 $y \in X$， $cf(y) \cdot f(x) = cf(yx)$。

伴随元 $x^{-1} f^{-1}(c^{-1} f(x) c)$ 属于 X 当且仅当 $c^{-1} f(x) c \in f(xX)$，当且仅当存在 $y \in X$ 使得 $f(x)c = cf(xy) = cf(x) \cdot f(y)$，这等价于 $(cf(x))^{-1} f(x) c = [f(x)\ c] \in X$。□

命题 $[f(x)\ c] \in X$ 中7.2的条件 $x \in X$ 显然成立，因为 $[f(x)\ c] = f(x)^{-1} c^{-1} f(x) c$ 且 $f(x) \in X$， $c^{-1} f(x) c \in X$。因此有：

推论 7.3。设 Q 是一个穆芳环路， $X \trianglelefteq Q$ 且 $x \in X$。设 $f \in \in \mathrm{Inn}(Q)$，并设 c 是 f 的伴随元。设 ρ 是 $\mu_{f,x}$ 在 X 上的限制。那么 $(x^{-1} f^{-1}(c^{-1} f(x) c)\ \rho) \in \mathrm{Psa}_\ell(X)$。

推论 7.4. 设 Q 为一个穆芳环路， X 为 Q的正规子群， $x \in X$ 且 $f \in \mathrm{Inn}(Q)$。那么 $\mu_{f,x}$ 限制为 X的一个自同构。

注 7.5. 推论7.4 给出了半自同构 g 群 X 由某个穆芳环路的某个内映射诱导而来的必要条件 Q，该环路包含

X 作为正规子群。也就是说，如果存在 $x \in X$ 使得 $R_x^{-1}g^{-1}R_{g(x)}g$ 不是 X的自同构，那么 g 就不是由此诱导而来的。

注意，$R_x\mu_{f,\ x}R_x^{-1} = f^{-1}R_{f(x)}fR_x^{-1}$。右端将在下一个引理中讨论。

引理 7.6. 设 Q为一个穆芳环路，并假设（c，f）$\in \mathrm{Psa}_\ell$（Q）满足 f（c^{-1}）$=c^{-1}$。则

$$L_{f^3(x)}^{-1}fL_{f^2(x)}f^{-1} = f^{-1}R_{f(x)}fR_x^{-1} \tag{7.2}$$

当且仅当对所有 $x \in Q$ 均成立

$$(cx)^{-1}(cxc^{-1}\cdot y) = (f^{-3}(x)c)^{-1}\cdot f^{-3}(x)y \tag{7.3}$$

对所有 x、$y \in Q$均成立。

证明。 注意，（7.2）对所有 $x \in Q$ 成立，当且仅当

$$L_x^{-1}fL_{f^{-1}(x)}f^{-1} = f^{-1}R_{f^{-2}(x)}fR_{f^{-3}(x)}^{-1} \tag{7.4}$$

对所有 $x \in Q$均成立。将（7.4）的左端应用于 $y \in Q$ 可得

$$x^{-1}\cdot f(f^{-1}(x)f^{-1}(y)) \overset{2.3}{=} x^{-1}(xc^{-1}\cdot cy) \overset{(2.5)}{=} x^{-1}(c^{-1}(cx\cdot y)).$$

由于 $f(c^{-1}) = c^{-1}$，(2.2) 得出 $(c, f)^{-1} = (f^{-1}(c^{-1})\ f^{-1}) = (c^{-1}, f^{-1}) \in \mathrm{Psa}_\ell(Q)$。令$z = f^{-3}(x)$。将 (7.4) 的右端应用于 y，得到

$$f^{-1}(f(yz^{-1})\cdot f(z)) \overset{2.3}{=} (yz^{-1}\cdot c)(c^{-1}z) \overset{(2.5)}{=} c((c^{-1}\cdot yz^{-1})z),$$

其中我们应用了引理 2.3 于 $(c^{-1}, f^{-1}) \in \mathrm{Psa}_\ell(Q)$。将 (7.4) 的两边左乘 c^{-1}，因此可见 (7.4) 成立，当且仅当乘积

$$c^{-1}(x^{-1}(c^{-1}(cx\cdot y)) \overset{(M4)}{=} c^{-1}(cx)^{-1}\cdot(cx\cdot y) \overset{(2.5)}{=} (cx)^{-1}(cxc^{-1}\cdot y)$$

等于

$$(c^{-1}\cdot yz^{-1})z \overset{(2.6)}{=} c^{-1}z^{-1}\cdot zy = (zc)^{-1}zy,$$

于是证明完毕。 □

命题 7.7。 设 Q 是一个穆芳环路，且 $a \in Q$。若 $f = T_a$ 则 (7.2) 对每个$x \in Q$都成立。

证明。 的伴随元 $c = a^{-3}$ 等于 。当然， $T_a(c^{-1}) = c^{-1}$ 由幂结合律成立。令 $z = f^{-3}(x) = T_a^{-3}(x) = a^{-3}xa^3 = cxc^{-1}$。根据引理 7.6，只需验证 (7.3)。现在，$(cx)^{-1}(cxc^{-1}\cdot y) = x^{-1}c^{-1}\cdot zy = (zc)^{-1}\cdot zy$。 □

8. Inducing from a semiautomorphism of an abelian group

现在我们研究以下情形： f 是阿贝尔群（X，$+$）的半自同构，且$\mu_{f,\ x}$ 的（7.1）是（X，$+$）的自同构。

命题 8.1。设 f 是阿贝尔群（$X, +$）的半自同构，使得对于每个 $x \in X$，置换

$$\mu_x = \mu_{f,x} = R_x^{-1}f^{-1}R_{f(x)}f$$

是（$X, +$）的一个自同构。令

$$x \oplus y = f^{-1}(f(x) + f(y))$$

对所有的 $x, y \in X$ 均成立。则：

（i） f 是从（X， $\oplus$）到（X， $+$）的同构，且（X， $\oplus$）是一个阿贝尔群，其单位元为 0，逆元为 $\ominus x = -x$；（ii）对于所有 x、$y \in X$， $x \oplus y = \mu_y$（x）$+ y = x + \mu_x$（y）；（iii）对于所有 $x \in X$， μ_x（x）$= x$、$\mu_x R_x = R_x \mu_x$和 $\mu_x = f^{-1} R_{f(x)} f R_x^{-1}$；（iv）对于所有 x、$y \in X$， $x + y = x \oplus \mu_x$（y）；（v）对于所有 x、$y \in X$， $\mu_x = \mu_x^{-1} = \mu_{-x}$ 和 $\mu_x \mu_y = \mu_{x \oplus y}$；（vi）映射 $x \mapsto \mu_x$ 是（X， $+$）在 X 上的作用，当且仅当对每个 $x \in X$， $\mu_x \in$ 属于 Aut（X， $\oplus$）。

证明。（i）根据定义， $\oplus$ 表明 f 是从广群（X， $\oplus$）到（X， $+$）的同构。特别地，（X， $\oplus$）必定是阿贝尔群。由于 f 是（X， $+$）的半自同构，对于每个整数 k，都有 f（kx）$= kf$（x）。因此， $f(0) = 0$ 是（X， $\oplus$）的单位元，而 $x \oplus$（$-x$）$= f^{-1}$（f（x）$+ f$（$-x$））$= f^{-1}$（f（x）$- f$（x））$= f^{-1}(0) = 0$ 表明，$-x$ 是 x 在（X， $\oplus$）中的逆元。

（ii）根据定义， $x \oplus y = f^{-1}$（f（y）$+ f$（x））$= f^{-1} R_{f(y)} f$（x）$= R_y R_y^{-1} f^{-1} R_{f(y)} f$（$x$）$= R_y$（$\mu_y$（$x$））$= \mu_y$（$x$）$+ y$，因此，由于 $\oplus$的交换性，也有 $x \oplus y = y \oplus x = \mu_x$（$y$）$+ x$。

（iii）由（ii）， $\mu_x(x) + x = x \oplus x = f^{-1}(2f(x)) = f^{-1}(f(2x)) = 2x$，因此 $\mu_x(x) = x$。于是$\mu_x($ $y) + x = \mu_x(y) + \mu_x(x) = \mu_x(y + x)$，这说明 $R_x \mu_x = \mu_x R_x$，进而推出$\mu_x = R_x \mu_x R_x^{-1} = f^{-1} R_{f(x)} f R_x^{-1}$。

（iv）由于 f 是同构 $(X\oplus) \to (X, +)$，我们有 $f(x \oplus \mu_x(y)) = f(x) + f(\mu_x(y))$。由（iv）， f $(\mu_x(y)) = f f^{-1} R_{f(x)} f R_x^{-1}(y) = f(y - x) + f(x)$。结合可得， $f(x \oplus \mu_x(y)) = f(x) + f(y - x) + f$ $(x) = f(x + (y - x) + x) = f(x + y)$，因为 f 是 $(X, +)$ 的半自同构。因此 $x + y = x \oplus \mu_x(y)$。

（v）由（iv）和（ii）， $x \oplus \mu_x(y) = x + y = x + \mu_x(\mu_x^{-1}(y)) = x \oplus \mu_x^{-1}(y)$，因此 $\mu_x = \mu_x^{-1}$。接着我们计算 $x + \mu_x(y) + \mu_{x \oplus y}(z) = (x \oplus y) + \mu_{x \oplus y}(z) = (x \oplus y) \oplus z = x \oplus (y \oplus z) = x + \mu_x(y \oplus z) = x + \mu_x(y + \mu_y(z))$ $= x + \mu_x(y) + \mu_x(\mu_y(z))$，其中最后一步用到了 $\mu_x \in \mathrm{Aut}(X, +)$。由此可得 $\mu_x \mu_y = \mu_{x \oplus y}$。结合这一结果和（i），我们有$\mu_x \mu_{-x} = \mu_{x \oplus (-x)} = \mu_0 = \mathrm{id}_X$。

（vi）回忆一下（iv）中的 $x + y = x \oplus \mu_x(y)$。于是 $x \oplus \mu_x(y \oplus \mu_y(z)) = x \oplus \mu_x(y + z) = x + ($ $y + z) = (x + y) + z = (x + y) \oplus \mu_{x+y}(z) = x \oplus \mu_x(y) \oplus \mu_{x+y}(z)$，因此 $\mu_x(y \oplus \mu_y(z)) = \mu_x(y) \oplus \mu_{x+y}(z)$ 总是成立。注意， $\mu_x \in \mathrm{Aut}(X, \oplus)$ 当且仅当 $\mu_x(y \oplus \mu_y(z)) = \mu_x(y) \oplus \mu_x \mu_y(z)$。假设 $\mu_x \in \mathrm{Aut}(X, \oplus)$，那么 $\mu_x(y)$ $\oplus \mu_x \mu_y(z) = \mu_x(y \oplus \mu_y(z)) = \mu_x(y) \oplus \mu_{x+y}(z)$，这意味着 $\mu_x \mu_y = \mu_{x+y}$。反过来，若 $\mu_x \mu_y = \mu_{x+y}$，则 μ_x $(y) \oplus \mu_x \mu_y(z) = \mu_x(y) \oplus \mu_{x+y}(z) = \mu_x(y \oplus \mu_y(z))$，并且可得 $\mu_x \in$ 自同构群$(X, \oplus)$。□

推论 8.2。 在命题 8.1 的假设下，若 $\mu : x \mapsto \mu_x$ 是$(X, +)$ 在 X 上的作用，则 $\mu_y(x) - x \in \mathrm{Ker}(\mu)$ 对所有 $x, y \in X$。

证明。 若 μ 是 $(X, +)$ 在 X 上的作用，则 $\mu_{x+y} = \mu_x \mu_y = \mu_{x \oplus y}$ 由命题 8.1 可知。因此，id $_X = \mu_{x \oplus y} \mu_{x+y}^{-1} = \mu_{(x \oplus y) - (x+y)}$。 由命题 8.1(ii), $(x \oplus y) - (x + y) = \mu_y(x) + y - x - y = \mu_y(x) - x$ 于是属于 μ 的核。□

下一个陈述同时使用 L_x 和 R_x，以强调其与引理 7.6 的联系。当然， $L_x = R_x$ 对每个 $x \in X$ 都成立，因为假设 $(X, +)$ 是交换的。

引理 8.3. 在命题 8.1 的假设下，若对每个 $x \in X$ 都有 $L_{f^3}^{-1}{}_{(x)} f L_{f^2(x)} f^{-1} = f^{-1} R_{f(x)} f R_x^{-1}$，则 $f^{-1} \mu_x f = \mu_{f^2(x)}$，且对每个 $x \in X$， $\mu_x \in \mathrm{Aut}(X, \oplus)$。

证明。由命题 8.1(iii)，可得 $L_{f^3}^{-1}(x)fL_{f^2}(x)f^{-1} = f^{-1}R_{f(x)}fR_x^{-1} = \mu_{x_0}$。由 (2.4)，$L_{f^3}^{-1}(x)fL_{f^2}(x)f^{-1} = R_{f^3}(x)fR_{f^2}^{-1}(x)f^{-1}$。根据命题 8.1(iii)，右端等于 $f\mu_{f^2}(x)f^{-1}$。综上，对每个 $x \in X$，都有 $\mu_x = f\mu_{f^2}(x)f^{-1}$。由于 f 是 $(X,\oplus)$ 到 $(X,+)$ 的同构，且 $\mu_x \in \mathrm{Aut}(X,+)$，因此 $\mu_{f^2}(x) = f^{-1}\mu_x f \in \mathrm{Aut}(X,\oplus)$。□

命题 8.4. 设 $(X,+)$ 是穆芳环路 $(Q,\cdot)$ 的正规阿贝尔子群。设$a \in Q$，且令 f 为 T_a 在 X 上的限制。那么对每个 $x \in X$，由 (7.1) 定义的置换$\mu_{f,x} = \mu_x$ 都是 $(X,+)$ 的自同构，并且 $\mu : x \mapsto \mu_x$ 是 $(X,+)$ 在 X 上的作用。此外，f 是 $(X,+)$ 上的 Moufang 置换，参见定义 1.2。

证明。映射 μ_x 是X，$+$）的自同构，这由推论 7.4得出。因此，命题 8.1 的所有假设均已满足。由命题 7.7，引理 8.3 的所有假设也均已满足。因此，根据引理 μ 是 $(X,+)$ 在 X 上的作用，这由引理 8.3 和命题 8.1（vi）得出。

令 β 如（P1）中所定义，即 $\beta(x,y) = f^{-1}(f(x)+f(y))-x-y$。显然，$\beta$ 是对称的。令 $x\oplus y = f^{-1}(f(x)+f(y))$ 如命题 8.1 中所述，并回忆 $x\oplus y = \mu_x(y)+x$，从而 $\beta(x,y) = x\oplus y - x - y = \mu_x(y) - y$。由于 $\mu_x \in \mathrm{Aut}(X,+)$，$\beta$ 是双加性的。最后，命题 8.1(iii) 中的 $\mu_x(x) = x$ 表明 β 是交错的。

我们有 $\beta(\beta(x,y)\ z) = \mu_{\beta(x,y)}(z) - z = \mu_{\mu_x(y)-y}(z) - z$。根据推论 8.2，$\mu_x(y) - y$ 属于 μ 的核，因此 $\beta(\beta(x,y)\ z) = 0$，这就是（P2）。

根据定义，将 $\beta(\beta(x,y)\ z) = 0$重写后得到 $f(\beta(x,y)+z) = f(\beta(x,y))+f(z)$。由引理 8.3，$\mu_x f = f\mu_{f^2}(x)$ 对所有 $x \in X$ 都成立。因此 $\beta(x,f(y))+f(y) = \mu_x f(y) = f\mu_{f^2}(x)(y) = f(\beta(f^2(x)\ y)+y) = f(\beta(f^2(x)\ y))+f(y)$。将 $f(x)$ 代入 x，得到$\beta(f(x)\ f(y)) = f(\beta(f^3(x)\ y))$，即 (P3)。我们已证明，$f$ 是 $(X,+)$ 上的 Moufang 置换。□

9. Moufang permutations and their properties

本节首先考察阿贝尔群（X，$+$）上的穆芳置换的性质。接着，我们证明穆芳置换的幂仍是穆芳置换，并计算其关联的双加性映射，参见命题 9.6。本节中的若干陈述和证明与第 3 节中的类似，但由于两节都不是另一节的特例，因此我们完整给出论证。

从定义 1.2 容易看出，X 上的恒等映射是一个 Moufang 置换。另请注意，若 (f,β) 是 $(X,+)$ 上的 Moufang 对，则 $\beta = 0$ 当且仅当 f是 $(X,+)$ 的一个自同构。

引理 9 .1. 设 (f,β) 是 $(X,+)$ 上的 Moufang 对，且 i 是一个整数。那么 :
（i） $f(0) = 0$, $f(2x) = 2f(x)$ and $f(-x) = -f(x)$ 对所有 $x \in X$ 均成立，（ii）像(β) $\subseteq$ 根(β)，$2X \subseteq$ 根(β) and 2像(β) $= 0$,
（iii） f^i 同时置换根(β)和像(β)，（iv）当 $\{x,y\} \cap$根(β) $\neq \emptyset$ 时，$f^i(x+y) = f^i(x)+f^i(y)$，（v） f^i 在根(β)上的限制是一个自同构。

证明。（i）回想第 2.1 小节中关于映射 $X\times X \to X$ 的基本性质。由于 β 是交错的，我们有 $0 = \beta(x,x) = f^{-1}(f(x)+f(x))-x-x = f^{-1}(2f(x))-2x$，因此 $2f(x) = f(2x)$。特别地，$2f(0) = f(2\cdot 0) = f(0)$，于是 $f(0) = 0$。由双加性可得 $f^{-1}(0) = 0 = -\beta(x,x) = \beta(x,-x) = f^{-1}(f(x)+f(-x))$，所以 $f(x)+f(-x) = 0$。

（ii）像(β) $\subseteq$ 根(β) 是对（P2）的另一种表述。正如第2.1小节中所指出的，$\beta(2x, y) = 2\beta(x, y) = 0$。

（iii）对于 $y \in X$，以下条件等价：$y \in$ Rad(β)，$\beta(x, y) = 0$ 对所有$x \in X$, $\beta(f^3x, y) = 0$对所有 $x \in X$, $f^{-1}\beta(fx, fy) = 0$对所有 $x \in X$（由 (P3)），$\beta(fx, fy) = 0$对所有 $x \in X$（因为 $f(0) = 0$由（i）），$\beta(x, fy) = 0$对所有 $x \in X$, $f(y) \in$Rad(β)。类似地，$z \in$Img(β) 当且仅当 $z = \beta(f^3x, y)$ 对某个 $x, y \in X$当且仅当 $z = f^{-1}\beta(fx, fy)$ 对某个 $x, y \in X$当且仅当$f(z) \in$ Img(β)。

（iv）定义条件 (P1) 可改写为 $f(x + y + \beta(x, y)) = f(x) + f(y)$。不妨设 $x \in$Rad(β)。于是 $\beta(x, y) = 0$且 $f(x + y) =$$f(x) + f(y)$ 成立。由（iii），对任意整数 i，$f^i(x) \in$ Rad(β)。由归纳法可得$f^{i+1}(x+y) = f^i(f(x+y)) = f^i(f(x)+f(y)) = f^i(f(x))+f^i(f(y)) = f^{i+1}(x)+f^{i+1}(y)$，对任意$i > 0$均成立。继续考虑 $i > 0$，可得 $f^i(f^{-i}(x) + f^{-i}(y)) = f^i(f^{-i}(x)) + f^i(f^{-i}(y)) = x + y$，因此 $f^{-i}(x + y) = f^{-i}(x) + f^{-i}(y)$。第（v）部分由（iii）和（iv）推出。□

引理 9.2. 设 f 是 $(X, +)$ 上的一个 Moufang 对。那么

$$\beta(f^ix, f^iy) = f^i\beta(f^{3i}x, y), \tag{9.1}$$

$$\beta(f^{3i}x, f^{3j}y) = f^{-3(i+j)}\beta(x, y) \tag{9.2}$$

对所有整数 i, j 均成立。

证明。我们先用9.1对所有非负整数 i 成立这一点，按照 i归纳证明（ $i = 0$的情形显然成立。对于 $i = 1$，9.1即为定义条件P3。假设9.1对某个 $i \geq 0$成立。那么

$$\begin{aligned}\beta(f^{i+1}x, f^{i+1}y) &= \beta(f^ifx, f^ify) = f^i\beta(f^{3i}fx, fy)\\ &= f^i\beta(ff^{3i}x, fy) \overset{(P3)}{=} f^if\beta(f^3f^{3i}x, y) = f^{i+1}\beta(f^{3(i+1)}x, y).\end{aligned}$$

仍取非负整数 i，于是还有

$$f^i\beta(f^{-i}x, f^{-i}y) = f^i\beta(f^{3i}f^{-4i}x, f^{-i}y) \overset{(9.1)}{=} \beta(f^if^{-4i}x, y) = \beta(f^{-3i}x, y),$$

这意味着 $\beta(f^{-i}x, f^{-i}y) = f^{-i}\beta(f^{-3i}x, y)$，从而完成了对9.1的证明。

由 β 的对称性，对于任意整数 i，我们有

$$f^i\beta(f^{3i}x, y) \overset{(9.1)}{=} \beta(f^ix, f^iy) = \beta(f^iy, f^ix) \overset{(9.1)}{=} f^i\beta(f^{3i}y, x) = f^i\beta(x, f^{3i}y).$$

将 f^{-i} 应用于两边，得到

$$\beta(f^{3i}x, y) = \beta(x, f^{3i}y). \tag{9.3}$$

对于（9.2），首先注意到

$$f^{-3i}\beta(x, y) = f^{-3i}\beta(f^{3(-3i)}f^{9i}x, y) \overset{(9.1)}{=} \beta(f^{-3i}f^{9i}x, f^{-3i}y) = \beta(f^{6i}x, f^{-3i}y) \overset{(9.3)}{=} \beta(f^{3i}x, y),$$

这就是（9.2）在 $j = 0$ 这一特殊情形下的结果。对于任意 j，于是有

$$\beta(f^{3i}x, f^{3j}y) \overset{(9.3)}{=} \beta(f^{3(i+j)}x, y) = f^{-3(i+j)}\beta(x, y),$$

证明完毕。□

接下来证明，若 f 是 $(X, +)$ 上的 Moufang置换，则 f^i 也是 $(X, +)$ 上的 Moufang置换。

引理 9.3。设 (f,β) 是 $(X,+)$ 上的 Moufang 对。那么对每个整数 i，映射$f^i\beta$: $X\times X\to X$ 是对称、交错且双加性的，并且满足 Img($f^i\beta$) =Img(β) $\subseteq$ Rad(β) = Rad($f^i\beta$)。

证明。由引理 9.1， f^i是 Rad(β)的自同构，Img(β) $\subseteq$Rad(β)，且 f^i置换 Img(β)。因此，Img($f^i\beta$) = Img(β)， $f^i\beta$是对称且双加性的（因为 β是对称且双加性的），并且也是交错的（因为 β 是交错的，且 f(0) = 0）。再次利用 f(0) = 0，可知 $f^i\beta(x,y)=0$当且仅当 $\beta(x,y)=0$。因此 Rad($f^i\beta$) =Rad(β)。□

引理 9.4。若(f,β)是$(X,+)$上的 Moufang 对，则$(f^{-1},f^3\beta)$也是$(X,+)$上的 Moufang 对。

证明。回顾一下，由引理 9.1， $f(-x)=-f(x)$且 2Img(β) = 0。由 (P1) 和引理 9.1，我们有 $f(x)+f(y)=f(x+y+\beta(x,y))=f(x+y)+f\beta(x,y)=f(x+y)-f\beta(x,y)$，因此对任意 x, $y\in X$， $f\beta(x,y)=f(x+y)-f(x)-f(y)$。在下面计算的最后一步使用这一点，可知

$$f^3\beta(x,y)\overset{(9.2)}{=}\beta(f^{-3}x,y)\overset{(9.1)}{=}f\beta(f^{-1}x,f^{-1}y)=f(f^{-1}x+f^{-1}y)-x-y,$$

这是（P1）关于（f^{-1}， $f^3\beta$）的对应形式。此外，

$$f^3\beta(f^{-1}x,f^{-1}y)\overset{(9.1)}{=}f^3f^{-1}\beta(f^{-3}x,y)=f^2\beta(f^{-3}x,y)=f^{-1}f^3\beta((f^{-1})^3x,y),$$

这是（P3）的对应形式。由引理 9.3， $f^3\beta$ 是交错且双加性的。由于 f将像(β) $\subseteq$根(β)，且 $f(0)=0$由引理 9.1，我们有 $f^3\beta(f^3\beta(x,\ y)\ z)$ =$f^3(0)=0$，这是（P2）的对应形式。□

回顾（ $I(i,\ j)$）中的区间（1.1）。

命题 9.5。设 (f,β) 是 $(X,+)$ 上的一个 Moufang 对。那么对于每个整数 i，我们有

$$f^{-i}(f^i(x)+f^i(y))=x+y+\sum_{k\in I(0,i)}f^{-3k}\beta(x,y) \tag{9.4}$$

对于每个 $x,y\in X$。

证明。 我们先证明，对所有 9.4）成立的情形 $i\geq 0$，此时 $I(0,i)=\{0,1,\dots,i-1\}$。情形 $i=0$ 显然，因为 $I(0,0)=\emptyset$，而情形 $i=1$ 是（P1）。如果（9.4）对某个$i\geq 0$ 成立，那么

$$f^{-i-1}(f^{i+1}x+f^{i+1}y)=f^{-1}f^{-i}(f^ifx+f^ify)=f^{-1}\Big(fx+fy+\sum_{k\in I(0,i)}f^{-3k}\beta(fx,fy)\Big).$$

根据引理 9.1，像(β) $\subseteq$ 根(β) 和 f 对根(β) 进行置换，这意味着 $\sum f^{-3k}\beta(fx,fy)$ 的每个加数以及它们的和都属于根(β)。根据引理9.1（iv），我们可以继续进行上述计算：

$$f^{-1}(fx+fy)+f^{-1}\sum_{k\in I(0,i)}f^{-3k}\beta(fx,fy)=f^{-1}(fx+fy)+\sum_{k\in I(0,i)}f^{-3k-1}\beta(fx,fy).$$

现在， $f^{-1}(fx+fy)=x+y+\beta(x,\ y)$ 由 (P1)。此外， $\beta(fx,\ fy)=f\beta(f^3x,\ y)=f^{-2}\beta($ $x,\ y)$ 由 (P3) 和 (9.2)，因此

$$\sum_{k\in I(0,i)}f^{-3k-1}\beta(fx,fy)=\sum_{k\in I(0,i)}f^{-3k-1}f^{-2}\beta(x,y)=\sum_{k\in I(0,i)}f^{-3(k+1)}\beta(x,y)=\sum_{k=1}^{i}f^{-3k}\beta(x,y).$$

总之，

$$f^{-i-1}(f^{i+1}x+f^{i+1}y)=x+y+\beta(x,y)+\sum_{k=1}^{i}f^{-3k}\beta(x,y)=x+y+\sum_{k=0}^{i}f^{-3k}\beta(x,y),$$

即（9.4）对于 $i+1$。

现在令 $i<0$，使得 $I(0,i)=\{-i,-i+1,\ldots,-1\}$。根据引理 9.4，$(f^{-1},f^3\beta)$ 是一个 Moufang 对。对于 $i=-1$，(9.4) 化简为 $f(f^{-1}(x)+f^{-1}(y))=x+y+f^3\beta(x,y)$，这就是 (P1) 对 $(f^{-1},f^3\beta)$ 的对应形式。如果对于某个 $i<0$，(9.4) 成立，那么

$$f^{-i+1}(f^{i-1}x+f^{i-1}y)=ff^{-i}(f^if^{-1}x+f^if^{-1}y)=f\Big(f^{-1}x+f^{-1}y+\sum_{k\in I(0,i)}f^{-3k}\beta(f^{-1}x,f^{-1}y)\Big),$$

根据引理 9.1 可进一步写为

$$f(f^{-1}x+f^{-1}y)+f\sum_{k\in I(0,i)}f^{-3k}\beta(f^{-1}x,f^{-1}y)=f(f^{-1}x+f^{-1}y)+\sum_{k\in I(0,i)}f^{-3k+1}\beta(f^{-1}x,f^{-1}y).$$

现在，$f(f^{-1}x+f^{-1}y)=x+y+f^3\beta(x,\ y)$ 根据（P1），对于 Moufang 对（f^{-1}，$f^3\beta$）。此外，$\beta(f^{-1}x,\ f^{-1}y)=f^{-1}\beta(f^{-3}x,\ y)=f^2\beta(x,\ y)$ 根据（9.1）和（9.2），因此

$$\sum_{k\in I(0,i)}f^{-3k+1}\beta(f^{-1}x,f^{-1}y)=\sum_{k\in I(0,i)}f^{-3k+1}f^2\beta(x,y)=\sum_{k\in I(0,i)}f^{-3(k-1)}\beta(x,y)=\sum_{k=-(i-1)}^{-2}f^{-3k}\beta(x,y).$$

总之，

$$f^{-i+1}(f^{i-1}x+f^{i-1}y)=x+y+f^3\beta(x,y)+\sum_{k=-(i-1)}^{-2}f^{-3k}\beta(x,y)=x+y+\sum_{k=-(i-1)}^{-1}f^{-3k}\beta(x,y),$$

这就是（9.4）对于 $i-1$。 □

命题 9.6。设 (f,β) 是 $(X,+)$ 上关于 $i\in\mathbb{Z}$ 的 Moufang 对。令

$$\beta_i=\sum_{k\in I(0,i)}f^{-3k}\beta.$$

则 (f^i,β_i) 是 $(X,+)$ 上的 Moufang 对。此外，$\mathrm{Img}(\beta_i)\subseteq\mathrm{Img}(\beta)\subseteq\mathrm{Rad}(\beta)\subseteq\mathrm{Rad}(\beta_i)$。

证明。由引理 9.3，β_i 是一个对称交替双加映射，满足 $\mathrm{Img}(\beta_i)\subseteq\mathrm{Img}(\beta)\subseteq\mathrm{Rad}(\beta)\subseteq\mathrm{Rad}(\beta_i)$。由命题 9.5，$(f^i,\beta_i)$ 满足（P1）的对应形式。由（9.1）和引理 9.1，可得

$$\beta_i(f^ix,f^iy)=\sum_{k\in I(0,i)}f^{-3k}\beta(f^ix,f^iy)=f^i\sum_{k\in I(0,i)}f^{-3k}\beta(f^{3i}x,y)=f^i\beta_i(f^{3i}x,y),$$

这就是（P3）的对应形式。（P2）的对应形式可通过与引理 9.4的证明类似的论证得到。□

推论 9.7. 设 $(f,\ \beta)$ 是作用在 $(X,\ +)$ 上的 Moufang 对，并设 β_i 如命题9.6. 中所定义。则

$$f^{-i}(x+y)=f^{-i}(x)+f^{-i}(y)+f^{2i}\beta_i(x,y).\tag{9.5}$$

对每个 x、$y\in X$ 和 $i\in\mathbb{Z}$。

证明。 由（P1）对于 Moufang 对（f^i， β_i），我们有

$$f^{-i}(x+y)=f^{-i}(f^if^{-i}(x)+f^if^{-i}(y))=f^{-i}(x)+f^{-i}(y)+\beta_i(f^{-i}x,f^{-i}y).$$

根据（P3）和（9.2）对于（f^i， β_i，我们有

$$\beta_i(f^{-i}x,f^{-i}y)=f^{-i}\beta_i(f^{-3i}x,y)=f^{-i}f^{3i}\beta_i(x,y)=f^{2i}\beta(x,y).$$ □

最后，下面给出导论中提到的 Moufang 对与构造对之间的关系。

命题 9.8. 设 (f,β) 是 $(X,+)$ 上的 Moufang 对。那么 (f^3,β) 是 $(X,+)$ 上的构造对。

证明. 根据定义， β 是交错且双加性的。由（P1）可明显看出， β 也是对称的。令 (g,γ) $=(f^3,$ $\beta)$。那么（P2）变为（C2）。由（9.2）， $g^{-1}\gamma(x,y)=f^{-3}\beta(x,y)$ $=\beta(f^3x,y)=\gamma(gx,y)$，这就是（C3）。最后，由（9.4）对于 $i=3$，我们有 $g^{-1}(gx+gy)$ $=f^{-3}(f^3x+f^3y)$ $=x+y+\sum_{k=0}^{2}f^{-3k}\beta(x,y)=x+y+\gamma(x,y)+g^{-1}\gamma(x,y)+g^{-2}\gamma(x,y)$，这就是（C1）。□

10. Moufang loops constructed from Moufang permutations

本节讨论由 Moufang置换构造的穆芳环路，并证明大部分主要结果。

定理 10.1. 设 $(X,+)$ 是穆芳环路 $(Q,\cdot)$ 的一个阿贝尔正规子群，并设$a\in Q$。记 f 为 T_a 在 X上的限制。则 f 是 $(X,+)$上的 Moufang置换，其关联的双加性映射 β 定义如下：(P1)。此外，

$$a^{3i}x\cdot ya^{3j}=a^{3(i+j)}\Big(f^{-3j}(x)+f^{-3j}(y)+\sum_{k\in I(-2j,i)}f^{-3k}\beta(x,y)\Big),\tag{10.1}$$

$$a^{3i}x\cdot a^{3j}y=a^{3(i+j)}\Big(f^{-3j}(x)+y+\sum_{k\in I(i+j,-j)}f^{-3k}\beta(x,y)\Big)\tag{10.2}$$

对所有整数 i、j 以及所有 x、$y\in Q$，均成立。

证明。 由命题 8.4， f 是 $(X,+)$ 上的 Moufang置换，其关联的双加性映射为 β。设 $\delta=i-j$ 且 $b=a^3$。由 (2.10)，可得

$$b^ix\cdot yb^j=b^{i+j}f^{-i-2j}(f^{i-j}x+f^{i-j}y)=b^{i+j}f^{-3j}f^{-\delta}(f^\delta x+f^\delta y).$$

由于 (f^δ,β_δ) 根据命题 9.6是一个 Moufang 对，因此可得

$$b^ix\cdot yb^j=b^{i+j}f^{-3j}f^{-\delta}(f^\delta x+f^\delta y)=b^{i+j}f^{-3j}(x+y+\beta_\delta(x,y)).$$

根据引理 9.1和（9.5）， f^{-3j}（$x+y+\beta_\delta$（x， y））等于

$$f^{-3j}(x+y)+f^{-3j}\beta_\delta(x,y)=f^{-3j}x+f^{-3j}y+f^{6j}\beta_{3j}(x,y)+f^{-3j}\beta_\delta(x,y).$$

根据引理 9.1和引理 3.4（ii），我们有

$$f^{6j}\beta_{3j}=f^{6j}\sum_{k\in I(0,3j)}f^{-3k}\beta=\sum_{k\in I(0,3j)}f^{-3(k-2j)}\beta=\sum_{k\in I(0,3j)-2j}f^{-3k}\beta=\sum_{k\in I(-2j,j)}f^{-3k}\beta$$

and

$$f^{-3j}\beta_\delta = f^{-3j}\sum_{k\in I(0,\delta)} f^{-3k}\beta = \sum_{k\in I(0,i-j)} f^{-3(k+j)}\beta = \sum_{k\in I(0,i-j)+j} f^{-3k}\beta = \sum_{k\in I(j,i)} f^{-3k}\beta.$$

由于 2像$(\beta)=0$ 根据引理 9.1，引理 3.4 表明

$$f^{6j}\beta_{3j} + f^{-3j}\beta_\delta = \sum_{k\in I(-2j,j)} f^{-3k}\beta + \sum_{k\in I(j,i)} f^{-3k}\beta = \sum_{k\in I(-2j,j)\oplus I(j,i)} f^{-3k}\beta = \sum_{k\in I(-2j,i)} f^{-3k}\beta,$$

完成对（10.1）的证明。

对于（10.2），注意到 因为 $T_b = f^3$，所以 $b^i x\cdot b^j y = b^i x\cdot b^j y b^{-j} b^j = b^i x\cdot f^{3j}$（$y$）$b^j$。现在由（10.1）可得

$$b^i x\cdot b^j y = b^{i+j}\Big(f^{-3j}(x) + y + \sum_{k\in I(-2j,i)} f^{-3k}\beta(x, f^{3j}y)\Big).$$

由（9.2）和引理 3.4，上述公式中的和等于

$$\sum_{k\in I(-2j,i)} f^{-3(k+j)}\beta(x,y) = \sum_{k\in I(-2j,i)+j} f^{-3k}\beta(x,y) = \sum_{k\in I(-j,i+j)} f^{-3k}\beta(x,y) = \sum_{k\in I(i+j,-j)} f^{-3k}\beta(x,y),$$

完成证明。 □

推论 10.2。 在定理 10.1的假设下，若 $Q = \langle a^3\rangle X$，则公式 （10.1）、（10.2）均完整描述了 Q 中的乘法。

回顾定义 $C \ltimes_{(g,\gamma)} X$ 4.6 中的环路，根据定理 4.7，它们是 Moufang 的。按照我们的约定，每当我们写出 $C \ltimes_{(g,\gamma)} X$时，都假设定义 4.6的所有假设均成立。还要回顾定义 $r(g,\ \gamma)$ 中的参数（4.1），它出现在定义 4.6中。

引理 10.3. 设 $(X,+)$ 是一个 3-可除阿贝尔群，C 是一个有限循环群。设 f 是 $(X,+)$ 上的一个 Moufang置换，其关联的双加性映射为 β，且 $|f^3|$ 整除$|C|$。那么 $(g,\gamma) = (f^3,\beta)$ 是一个构造对，满足定义 4.6 的所有假设。

证明。根据命题 9.8，$(g,\gamma) = (f^3,\beta)$ 是 $(X,+)$ 上的一个构造对。令 $n = |C|$。根据我们的假设，$|g|$ 整除 n。令 $r = r(g,\gamma)$。由于 X 是 3-可除的，因此不含任何 3 阶元素。那么显然，根(γ) 不含任何 3 阶元素。由于 $|g| < \infty$，引理 4.5 蕴含 r 整除 $|g|$。因此 r 整除 n，且定义 4.6 的所有假设均成立。□

定理 10.4. 设 $Q = CX$ 是一个 3-可除穆芳环路，其中 $(X,+)$ 是 Q 的正规阿贝尔子群，且 Q 和 $C = \langle a^3\rangle$ 对某个 $a\in C$ 成立。设 f 是 T_a 在 X 上的限制，且 β 是关联的双加性映射。则：

（i）$(g,\ \gamma) = (f^3,\ \beta)$是一个满足定义 4.6 所有假设的构造对，且穆芳环路 $M = \langle a^3\rangle \ltimes_{(g,\gamma)} X$ 定义良好，（ii）$\varphi:\ M\to Q$ 由 $\varphi(a^{3i},\ x)\mapsto a^{3i}x$ 定义的映射是一个满同态，（iii）的核 φ 与 $C\times 0$ 和 $1\times X$ 的交集均为平凡子群。

证明。（i）由于 C 是 3-可除的，因此它是有限的，设其阶为 n。根据定理 10.1，T_a 在 X 上的限制f 是定义于（X，$+$）上的一个 Moufang置换，而 Q 中的乘法完全由（10.2）确定。根据命题 9.8，（g，γ）$=$（f^3，β）是一个构造对。对于 X，我们有 $f^{3n} = (T_a)^{3n} = (T_{a^{3n}}) = T_1 = \mathrm{id}_X$，因此 $|f^3|$整除 n。根据引理 10.3，所有假设

定义4.6的条件均满足。根据定理4.7，$M = \langle a^3 \rangle \ltimes_{(f^3,\beta)} X$是一个定义良好的穆芳环路，其乘法为（1.4）。

（ii）和（iii）：由（10.2）和（1.4），可得

$$\varphi(a^{3i}, x)\varphi(a^{3j}, y) = a^{3i}x \cdot a^{3j}y = a^{3(i+j)}(f^{-3j}(x) + y + \sum_{k\in I(i+j,-j)} f^{-3k}\beta(x, y))$$

$$= \varphi(a^{3(i+j)}, f^{-3j}(x) + y + \sum_{k\in I(i+j,-j)} f^{-3k}(\beta(x, y))) = \varphi((a^{3i}, x)(a^{3j}, y)),$$

因此 φ 是一个同态，显然是满射。φ 的核由所有满足 $0 \le i < n$ 的 $(a^{3i}, x) \in M$ 组成，其中 $a^{3i}x = 1$。若 $x = 1$，则得到 $a^{3i} = 1$，进而得到 $a^3 = 1$, $a = 1$。若 $a^{3i} = 1$，则得到 $x = 1$。□

命题 10.5. 设 S 是 $Q = C \ltimes_{(g,\gamma)} X = \langle b \rangle \ltimes_{(g,\gamma)} X$ 的一个非空子集。那么，S 是 Q 的一个正规子圈，且与 $1 \times X$ 和 $C \times 0$ 的交均为平凡子圈，当且仅当存在 $k \in \mathbb{Z}$ 和 $z \in X$，使得 $S = \langle (b^k, z) \rangle = \{(b^{ki}, iz)$: $i \in \mathbb{Z}\}$, $|b^k| = |z|$ 且 $(b^k, z) \in Z$({v20)。

证明。若（b^k，z）$\in Z$（Q），则 g（z）$= z \in$是γ的根，这由命题 5.5 得出，因此对所有 b^k，z）^{i} =（b^{ki}，iz）成立。反向蕴含显然，因为每个中心子圈都是正规子环，而条件 $i \in \mathbb{Z}$保证 $|b^k| = |z|$ 与 S 及 $1 \times X$ 都仅有平凡交。$C \times 0$

证明直接蕴含。假设 $S \trianglelefteq Q$ 与 $1 \times X$ 及$C \times 0$ 都仅有平凡交。我们声称，对于每个 $c \in C$，至多存在一个 $x \in X$ 使得（c，x）$\in S$。假设对于某些 x、$y \in X$，有（c，x）、（c，y）$\in S$。那么（c，x）（c，y）$^{-1} \in S$，且（c，x）（c，y）$^{-1} =$（1，u），其中 $u \in X$。由于 S与 $1 \times X$ 仅有平凡交，因此有 $u = 0$ 且$x = y$。

因此，存在 $k \in \mathbb{Z}$ 和 $z \in X$，使得 $S = \langle (b^k, z) \rangle$。我们有 $(b^k, z) \in S$，并且还有 $T_{(b^i,x)}(b^k, z) \in S$，因为 $S \trianglelefteq Q$。但是，$T_{(b^i,x)}(b^k, z) = (b^i, x)(b^k, z) \cdot (b^i, z)^{-1} = (b^k, u)$，其中某个 $u \in X$，由此可得 $T_{(b^i,x)}(b^k, z) = (b^k, z)$。类似地，$L_{(b^i,x),(b^j,y)}(b^k, z) = (b^k, z) = R_{(b^i,x),(b^j,y)}(b^k, z)$。因此，$(b^k, z) \in Z(Q)$。

我们还声称，对每个 $x \in X$，至多存在一个 $c \in C$，使得 $(c, x) \in S$。假设对于某些 $c, d \in C$，有 (c, x)、$(d, x) \in S$。我们有 $(c, x) = (c, 0)(1, x)$，以及 $(d, x) = (d, 0)(1, x)$。因此，$(cd^{-1}, 0) = (c, 0)(d, 0)^{-1} \in S$。由于 S与 $C \times 0$的交平凡，我们有 $c = d$。由此可得 $|b^k| = |z|$。□

定理 10.6（分裂的三可除阿贝尔群扩张循环群型穆芳群环）。假设 $(X, +)$ 是一个 3-可除阿贝尔群，且 C 是一个 3-可除循环群。以下条件等价:

（i） Q 是一个穆芳环路，$X \trianglelefteq Q$、$Q = CX$ 和 $C \cap X = 1$。（ii） Q 同构于 $C \ltimes_{(f^3,\beta)} X$，其中存在一个作用于 $(X, +)$ 的 Moufang置换 f，其关联的双加性映射为 β。

证明。由定理 4.7可知，逆向蕴含（ii）$\Rightarrow$（i）显然。对于正向蕴含，定理 10.4表明，Q 是同态 $\varphi : M = \langle a^3 \rangle \ltimes_{(f^3,\beta)} X \to Q$, $\varphi(a^{3i}, x) = a^{3i}x$的像，其中 f是 T_a 在 X上的限制。假设（a^{3i}, x）属于 φ的核。那么 $a^{3i}x = 1$ 意味着 $x \in C \cap X = 1$ 且 $a^{3i} = 1$。因此，φ是单射。□

References

[1] Michael Aschbacher, 《散在群》, 剑桥数学论丛第104卷, 剑桥大学出版社, 剑桥, 1994年。[2] John C. Baez, 《八元数》, 《美国数学会通报》（新辑）39（2002年）, 第2期, 145–205页。[3] Mariah Barnes, 《关于环的交换子、四元数自同构环及相关主题》, 博士论文, 丹佛大学数学系, 2022年5月。[4] Gerrit Bol, 《几何结构与群》, 《数学年刊》114（1937年）, 第1期, 414–431页。[5] Richard Hubert Bruck, 《对环论的贡献》, 《美国数学会汇刊》60（1946年）, 245–354页。[6] Wing Loon Chee 和 Andrew Rajah, 《奇数阶穆芳环路 pq^4》, 《马来西亚数学科学学会通报》（第2辑）37（2014年）, 第2期, 425–436页。[7] Orin Chein, 《小阶穆芳环路 I》, 《美国数学会汇刊》188（1974年）, 31–51页。[8] Orin Chein, 《小阶穆芳环路》, 《美国数学会回忆录》13（1978年）, 第197号。[9] Orin Chein 和 Edgar G. Goodaire, 《具有唯一非单位交换子（结合子、平方）的穆芳环路》, 《代数杂志》130（1990年）, 第2期, 369–384页。[10] Orin Chein 和 D.A,. Robinson, 《刻画穆芳环路的一条“额外”定律》, 《美国数学会会刊》33（1972年）, 29–32页。[11] John H. Conway 和 Derek A. Smith, 《关于四元数与八元数：其几何、算术与对称性》, A K Peters, Ltd., 马萨诸塞州纳蒂克, 2003年。[12] Ale˘s Dr´apal, 《穆芳定理的一个简化证明》, 《美国数学会会刊》139（2011年）, 第1期, 93–98页。[13] Ale˘s Dr´apal, 《关于以与3互素的循环因子扩张穆芳环路》, 《代数通讯》45（2017年）, 第6期, 2350–2376页。[14] Ale˘s Dr´apal, 《素数幂阶穆芳环路中心幂零性的一个简短证明》, 已投稿。[15] Ale˘s Dr´apal 和 Petr Vojt˘echovsk´y, 《穆芳环路中的阿贝尔同余与可解性》, 已投稿。[16] Ferenc Fenyves, 《额外环 I》, 《德布勒森数学刊》15（1968年）, 235–238页。[17] Ralph Freese 和 Ralph McKenzie, 《同余模簇的交换子理论》, 伦敦数学会讲义丛书第125卷, 剑桥大学出版社, 剑桥, 1987年。[18] Stephen M. Gagola, III, 《产生穆芳环路的阿贝尔群的循环扩张》, 《群论杂志》15（2012年）, 第1期, 1–7页。[19] Stephen M. Gagola, III, 《由半自同构诱导的穆芳环路循环扩张》, 《代数与应用杂志》13（2014年）, 第4期, 1350128, 7页。[20] George Glauberman, 《奇数阶环路 II》, 《代数杂志》8（1968年）, 393–414页。[21] George Glauberman 和 C.R.B. Wright, 《有限穆芳 2-环的幂零性》, 《代数杂志》8（1968年）, 415–417页。[22] Edgar G. Goodaire、Sean May 和 Maitreyi Raman, 《阶小于64的穆芳环路》, Nova Science Publishers, Inc., 纽约州科马克, 1999年。[23] Mark Greer 和 Lee Raney, 《环与群的穆芳半直积及逆性质扩张》, 《查理大学数学评论》55（2014年）, 第3期, 411–420页。[24] Robert L. Griess, Jr., 《码环》, 《代数杂志》100（1986年）, 第1期, 224–234页。[25] Tom´a˘s Kepka 和 Petr N˘emec, 《交换穆芳环与小阶分配群胚》, 《捷克斯洛伐克数学杂志》31(106)（1981年）, 第4期, 633–669页。[26] Michael K. Kinyon 和 Kenneth Kunen, 《额外环的结构》, 《拟群及相关系统》12（2004年）, 39–60页。[27] G´abor P. Nagy 和 Maurizio Valsecchi, 《关于具有中心结合子的幂零穆芳环》, 《代数杂志》307（2007年）, 第2期, 547–564页。[28] Fook Leong 和 Andrew Rajah, 《奇数阶穆芳环路 $p^\alpha q_1^2 \cdots q_n^2 r_1 \cdots r_m$》, 《代数杂志》190（1997年）, 第2期, 474–486页。[29] Fook Leong 和 Andrew Rajah, 《穆芳环路中的分裂扩张》, 《德布勒森数学刊》52（1998年）, 第1–2期, 33–42页。[30] Martin W. Liebeck, 《有限单穆芳环的分类》, 《剑桥哲学会数学会刊》102（1987年）, 第1期, 33–47页。

[31] Ruth Moufang, 《Alternativk ¨orper und der Satz vom vollst ¨andigen Vierseit》（D9），《汉堡大学数学研讨班论文集》9（1933），第1期，207–222页。[32] Ruth Moufang, 《Zur Struktur von Alternativk ¨orpern》，《数学年刊》110（1935），第1期，416–430页。[33] G´abor P. Nagy 和 Petr Vojtˇechovsk´y, 《LOOPS：在 GAP 中计算拟群和环路》，2.2.0 版。[34] G´abor P. Nagy 和 Petr Vojtˇechovsk´y, 《阶为 64 和 81 的穆芳环路》，《符号计算杂志》42（2007），第9期，871–883页。[35] E.A. O'Brien 和 Petr Vojtˇechovsk´y, 《维数至多为 8 的码环》，《代数杂志》473（2017），607–626页。[36] Lowell J. Paige, 《一类单穆芳环路》，《美国数学会会刊》7（1956），471–482页。[37] H.O. Pflugfelder, 《拟群与环路：导论》，Heldermann，柏林（1990）。[38] J.D. Phillips 和 Petr Vojtˇechovsk´y, 《从群中汲取灵感：环路的等式基础》，Loops '07 会议论文集，布拉格，发表于《查理大学数学评论》49（2008），第2期，279–290页。[39] Andrew Rajah, 《奇数阶穆芳环路》 pq^3, 《代数杂志》235（2001），第1期，66–93页。[40] Michael C. Slattery 和 Ashley L. Zenisek, 《阶为 243 的穆芳环路》，《查理大学数学评论》53（2012），第3期，423–428页。[41] Tonny A. Springer 和 Ferdinand D. Veldkamp, 《八元数、Jordan 代数与例外群》，Springer 数学专著，Springer 出版社，柏林，2000年。[42] David Stanovsk´y 和 Petr Vojtˇechovsk´y, 《环路的交换子理论》，《代数杂志》399（2014），290–322页。[43] David Stanovsk´y 和 Petr Vojtˇechovsk´y, 《阿贝尔扩张与可解环路》，《数学新进展》66（2014），367–384页。[44] Max Zorn, 《Alternativk ¨orper und quadratische Systeme》，《汉堡大学数学研讨班论文集》9（1933），395–402页。（Dr´apal）

Department of Mathematics, Charles University, Sokolovská 83, 18675 Praha 8, Czech Republic电子邮箱，Dr´apal：drapal@karlin.mff.cuni.cz（Vojtˇechovsk´y）

Dept. of Mathematics, University of Denver, 2390 S. York St., Denver, CO80208, USA电子邮箱，Vojtˇechovsk´y：petr@math.du.edu