arXiv:2603.11833v1 [math.GR] 12 Mar 2026

数学中的扭子导论：着眼于密码学中的 Σ协议

Takao Inoué

日本大阪大和大学信息学部*

2026年3月12日

摘要

本文为扭子提供一篇预备性导论，旨在为作者后续工作中的应用做准备。本文并不追求全面综述，而是聚焦于对理解基于扭子的推理最为有用的那些方面：群作用、轨道、自由传递作用、不存在规范选定的原点，以及将群元素解释为点之间的输运。在展开基本定义和若干初等例子之后，我们强调一个核心主题：扭子不仅可由自由传递群作用抽象地刻画，也会自然地作为借助满足余循环条件的过渡数据粘合局部平凡片段而得到的对象出现。一个简短的可选章节指出了层与拓扑斯理论的视角。在最后一部分，我们说明这些思想如何为后续的概念性应用奠定基础，其中包括 Σ协议的若干方面。

关键词。 扭子、主齐性空间、仿射空间、群作用、局部平凡性、粘合数据、余循环、层扭子、拓扑斯理论、 Σ-协议

MSC2020。 20L05, 18F20, 94A60

目录

1 引言 3 2 群作用与轨道 5 3 自由且传递的作用 6 4 扭子的定义 8

4.1 作为未指定单位元之群的扭子.9 4.2 传输与相对位置.10 4.3 右托orsor.10 4.4 非空性的重要性.10 4.5 首次总结.11

*电子邮箱：inoue.takao@yamato-u.ac.jp；个人邮箱：takaoapple@gmail.com[通信时我更倾向于使用个人邮箱地址。
]

5 扭子的基本例子 **11**

5.1 仿射空间.11 5.2 线性方程组的解集.12 5.3 陪集.13 5.4 基与标架的集合.13 5.5 对这些例子的初步比较.14

6 基础理论习题 14

7 局部平凡性与粘合数据 15

7.1 初等意义下的局部平凡性.16 7.2 从一种平凡化到另一种.16 7.3 粘合观点.17 7.4 交叠处的相容性.18 7.5 整体平凡性为何可能失败.18 7.6 再论仿射空间.19 7.7 为下一节做准备.19

8 C余循环描述与重构 on 19

8.1 局部平凡化的过渡数据.20 8.2 余循环恒等式.20 8.3 从余循环到扭子.21 8.4 等价余循环.22 8.5 平凡余循环与整体平凡性.22 8.6 重构为何重要.22 8.7 总结.23

9 层扭子、局部截面与整体截面 23

9.1 群层.23 9.2 群层的作用.24 9.3 层扭子的定义.24 9.4 局部截面与局部平凡性.24 9.5 整体截面与整体平凡性.25 9.6 重新审视过渡数据.25 9.7 局部截面的重要性.26 9.8 初等情形作为特例.26 9.9 总结.26

10 层论与托扑理论视角概览 **27**

10.1 为什么层还不是全部内容.27 10.2 层的拓扑斯.28 10.3 拓扑斯中的群对象.28 10.4 拓扑斯中的作用与扭子.29 10.5 整体截面函子.29 10.6 内部存在性与局部存在性.29 10.7 下降与重构.30 10.8 为什么这与后续定理密切相关.30 10.9 启发式对照表.30 10.10总结.31

11 走向 Σ-协议的应用 **31**
11.1 从传输到协议结构.31 11.2 协议依赖层.32 11.3 局部平凡性与模拟.32 11.4 为什么层扭子是恰当的层次.33 11.5 迈向层拓扑斯中的扭子.33 11.6 启发式对照表.34 11.7 为后续定理做准备.34 11.8 总结.34

12 结论 **35**

A 第 7 节习题的解答 **36**

B 一份建议的讲座计划 4 **5**
B.1 一份九讲计划.45 B.2 可能的变体.46 B.3 教学说明.46 B.4 一种可能的延续：关于作者的后续论文的六讲.46 B.5 一份十五讲计划.46 B.6 十五讲制形式的教学价值.47 B.7 给授课教师的实用说明.47 B.8 最后的教学说明.47

C 基本术语词汇表 **48**

1 引言

扭子的概念出现在现代数学的许多领域，但人们往往是在已经学习了相当多的代数、几何或上同调知识之后，才初次接触到它。因此，这个概念看起来可能比实际更具技术性，也更令人费解。本讲义旨在以足够基础的方式介绍扭子，使读者可以独立阅读，同时强调那些在后续应用中至关重要的结构特征。

直观地说，扭子是一个具有对称性但没有选定原点的空间。群有一个特定的单位元，因此可以从绝对意义上看待它的元素。相比之下，扭子具有相同的对称模式，却不附带任何优选基点。有意义的是相对位置：给定扭子中的两个点，存在唯一的群元素将其中一点传输到另一点。因此，群自然适用于绝对性的表述，而扭子则由传输、比较和位移所支配。

仿射空间提供了基本的几何模型。仿射空间类似于向量空间，但没有典范选定的零向量。我们可以将两个点相减，得到一个向量，但不能以内在的方式将两个点相加。这已经体现了扭子的核心现象：差是有意义的，但绝对坐标则需要任意选取一个基准。这种仿射视角并非仅仅是几何上的便利。它凸显了一条结构性原理，而这条原理的重要性远远超出初等几何的范畴：在数学中，重要的对象往往不是孤立的点，而是差、位移和平移。从这个意义上说，仿射空间为扭子的一般理论提供了最清晰的初步模型。

这种视角在分析中尤其有用。许多基本的解析构造自然地用增量来表达，例如

$$f(x+h)-f(x),$$

此处的核心对象是位移 h，而非点 x 的绝对位置。从这一视角看，定义域自然可视为仿射空间，而增量则属于关联向量空间。因此，我们可以清楚地区分所在之处与移动方式。这种思维方式与 Schwartz [4] 所强调的分析中的仿射观点十分契合。就本文而言，这也解释了为何仿射空间是理解扭子的最自然切入点。

本文并非旨在全面综述扭子在数学中的所有应用，其目标更加专注。本文是为作者后续工作 [2], 中发展的层论和挠子论观点所撰写的数学背景预备材料，尤其针对那些基于扭子的推理以层论形式或从局部到整体的形式出现的情形。在这类情形中，主要问题往往不是是否存在一个全局指定的点，而是能否作出相容的局部选择，以及如何理解全局选择所面临的障碍。因此，本文特别强调局部平凡性、粘合数据、余循环描述，以及局部截面与整体截面之间的区别。

这一观点对于某些协议论构造的概念性解释尤为重要。在后续工作中，人们考虑与 Σ-协议相关联的层论对象，并研究这些对象在适当的群作用下表现得如同扭子的情形。从这个角度看，局部平凡性与模拟相关，而适当的整体选择的失败则反映了结构性安全约束。本文的目的并非建立那些后续结果，而是提供理解它们所需的数学语言。特别地，读者应当由此清楚地理解什么是扭子、扭子如何由粘合数据产生、层论的扭子与集合论的扭子有何不同，以及局部截面与整体截面之间的对比为何重要。

因此，本文的核心主题之一是：扭子不应仅仅通过自由且传递的群作用这一抽象定义来理解。该定义是根本性的，并将被仔细展开，但它只讲述了故事的一部分。同样重要的是，扭子自然地产生于由过渡数据粘合在一起的局部平凡片段。在局部，一个扭子可能看起来与作用群本身无法区分。然而在整体上，这些局部平凡化未必能组合成单一的、优先的整体平凡化。局部平凡化之间的不匹配由满足余循环条件的过渡函数来记录。这样一来，扭子便成为由相容的局部数据组装而成的数学对象中最简单、也最有启发性的例子之一。

这种粘合观点使扭子与几何、下降和上同调等更广泛的主题紧密相连。扭子之所以如此有用，原因之一在于它们处于群作用、局部到整体重构和初步上同调分类的交汇点。即使不深入探讨完整理论，也应认识到，扭子不只是属于初等群论，更属于关于相容性与重构的一般数学。因此，在论文的基础章节之后，我们还加入了一个简短的选读章节，介绍层论和拓扑斯论的视角。主要对初等理论感兴趣的读者初读时可以放心略过该章节。

本文的组织如下。第 2 节回顾群作用与轨道的语言。第 3 节研究自由且传递的作用，这两者共同直接引出扭子概念。第 4 节给出扭子的形式化定义。第 5 节阐述主要的基础示例，尤其强调仿射空间。第 6 节研究基点、差与传输子，突出说明与群的识别并非典范的。第 7 节包含关于基础理论的习题。第 8 节介绍局部平凡性

与粘合数据。第 9 节阐述余循环描述与重构。第 10 节转向层扭子，并阐明局部截面与整体截面的作用。第 11 节在逻辑上是可选的一节，介绍层论与拓扑斯论的视角概览，不过强烈建议有兴趣了解后续应用的读者阅读。第 12 节说明前述材料如何为之后应用于 Σ-协议做好准备。最后，我们在第 13 节以简短的总结作结。

附录提供了第 7 节习题的详细解答，着重强调基本定义的运用；还包括一份讲座计划，介绍如何在课堂上使用这些讲义，或将其作为研读作者后续论文课程的准备材料；此外，还附有一份基本术语词汇表，供快速查阅。

2 群作用与轨道

我们从群作用的基础语言开始。虽然扭子常被作为一种特殊的群作用来介绍，但分阶段讲解更为有益。轨道、稳定子以及点之间的传输等概念，已经包含了许多后来成为核心的结构。

定义 2.1。设 G 是一个群，X 是一个集合。G 在 X 上的左作用 是一个映射

$$G \times X \to X, \qquad (g, x) \mapsto g \cdot x,$$

使得

1. 对所有 $x \in X$，$e \cdot x = x$，其中 e 是 G的单位元，
2. $(gh) \cdot x = g \cdot (h \cdot x)$ 对所有 g、$h \in G$ 以及所有 $x \in X$均成立。

在这种情况下，我们称 G 作用于 X，或者称 X 是一个 G-集合。

备注 2.2. 类似地可以定义右作用。在本讲义中，我们主要讨论左作用，因为左作用足以支撑基础理论以及后续的概念性应用。

群作用使我们能够将 G 的元素视为集合 X上的变换。这样，群的抽象代数结构便通过 X 中点的移动显现出来。对于扭子理论而言，重要的不仅是点会移动，更在于它们彼此之间如何相对移动。

定义 2.3. 设 G 作用于集合 X，并设 $x \in X$。x 的轨道 是如下子集

$$G \cdot x := \{g \cdot x \mid g \in G\} \subseteq X.$$

因此，点的轨道由所有能够通过群的作用从该点到达的点组成。轨道将集合 X 分解为彼此可达的区域：当且仅当存在 G中的某个元素可将一个点传输到另一个点时，这两个点才属于同一轨道。

定义 2.4 定义。设 G 作用于集合 X，并设 $x \in X$。x 的稳定子是子群

$$G_x := \{g \in G \mid g \cdot x = x\}.$$

稳定子刻画了在点 x处仍不可见的对称性：其中的元素会作用，但会使 x 保持不变。从扭子的视角来看，稳定子最终会消失，因为我们最关注的作用不会有非平凡固定对称。

例 2.5。 设 V 是域 k上的向量空间。那么，加法群 $(V,+)$ 通过平移作用在 V 的底层集合上：

$$v \cdot x := v + x.$$

对任意 $x \in V$， x 的轨道是整个 V，因为每个点都可以通过平移从任意其他点到达。此外，x 的稳定子是平凡的，因为 $v + x = x$ 蕴含 $v = 0$。这个基本例子已经预示了扭子的情形。

例 2.6. 令 G 通过左乘作用于自身：

$$g \cdot x := gx.$$

于是任意点的轨道都是整个 G，且每个点的稳定子都是平凡的。这是自由传递作用的典范例子，我们将在下一节回到它。

轨道视角尤其有用，因为它把注意力从作为整体的集合 X 转移到其各点之间的关系上。若 $x, y \in X$ 位于同一轨道，则至少存在一个元素 $g \in G$ 使得

$$g \cdot x = y.$$

一般而言，这样的元素不必是唯一的。唯一性的失效由稳定子控制。事实上，若 $g \cdot x = y$ 且 $h \cdot x = y$，则

$$h^{-1}g \cdot x = x,$$

因此 $h^{-1}g \in G_x$。所以，传输的唯一性与稳定子的平凡性密切相关。

这一观察已经指向了扭子。粗略地说，扭子是这样一种空间：其中任意一个点都可以通过唯一的群元素从任意另一个点到达。换句话说，它提供了这样一种环境：群作用赋予了相对位置一个完全刚性的概念。不过，在对其进行精确定义之前，我们先将两个相关性质分别分离出来：自由性和传递性。

3 自由且传递的作用

现在我们讨论区分扭子所基于的作用的两个关键性质。每个性质都有一个简单直观的含义。传递性意味着该作用只有一个轨道：每个点都可以被移动到其他任意点。自由性意味着没有非平凡群元素会固定某个点：作用群不会在任何位置留下隐藏的对称性。当这两个条件同时成立时，该作用表现得尽可能刚性。

定义 3.1。 令 G 作用于集合 X。

1. 如果对于每一对 x、$y \in X$，都存在 $g \in G$ 使得……，则称该作用是传递的 。 t

$$g \cdot x = y.$$

等价地， X 由单个轨道组成。

2. 如果对于每个 $x \in X$ 和每个 $g \in G$，……，则称该作用是自由的 。

$$g \cdot x = x \quad \Longrightarrow \quad g = e.$$

等价地，每个点的稳定子都是平凡的。

注 3.2。 这两个条件在逻辑上彼此独立。一个作用可以是传递的但不是自由的，也可以是自由的但不是传递的。扭子恰好是在这两个条件同时成立时出现的。

例 3.3。 令 G 通过左乘作用于左陪集集合 G/H：

$$g \cdot (aH) := (ga)H.$$

这个作用是传递的，因为通过适当的群元素，可以将任意陪集移到另一个陪集。不过，除非 $H = \{e\}$，否则它不是自由的，因为陪集 H 的稳定子恰好是 H。

例 3.4. 令 $G = \mathbb{Z}$ 通过平移作用于 $X = \mathbb{Z}$：

$$n \cdot x := n + x.$$

这个作用是自由且传递的。因此，将 $\mathbb{Z}$ 视为由其自身作用的集合，它本身就提供了一个例子，展示了稍后将抽象为扭子概念的那种结构。

命题 3.5. 令 G 作用于集合 X。那么以下条件等价：

1. 该作用是自由且传递的；
2. 对于每个 x、$y \in X$，都存在唯一的 $g \in G$ 使得

$$g \cdot x = y.$$

证明。 首先假设该作用是自由且传递的。令 x，$y \in X$。由传递性，存在 $g \in G$ 使得 $g \cdot x = y$。再假设 $h \cdot x = y$。那么

$$h^{-1}g \cdot x = x.$$

由于该作用是自由的，我们必有 $h^{-1}g = e$，因此 $g = h$。所以所需的元素是唯一的。

反过来，假设对于每个 x，$y \in X$ 都存在唯一的 $g \in G$ 使得 $g \cdot x = y$。存在性立即意味着传递性。为证明自由性，取 $x \in X$ 并假设$g \cdot x = x$。但也有 $e \cdot x = x$。由唯一性可知，$g = e$。因此该作用是自由的。 □

这个命题至关重要。它表明，自由且传递的作用与这样一种系统完全等价：任意两点之间的每个相对位移，都由作用群中的一个唯一元素表示。为了后续讨论，明确写出这个群元素会很有帮助。

定义 3.6。 假设 G 在 X上自由且传递地作用。对于 x、$y \in X$，令

$$\mathrm{tr}(x, y) \in G$$

表示满足下述条件的唯一元素

$$\mathrm{tr}(x, y) \cdot x = y.$$

我们称 $\mathrm{tr}(x, y)$ 为从 x 到 y的传输子 。

图 1 展示了传输子的基本思想：两个点之间的关系由唯一的群元素来衡量。

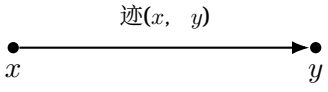


图 1：从 x 到 y 的传输子是将 x 映射到 y的唯一群元素 .

注 3.7. 输运子记号并非通用，但其背后的思想极为有用。在扭子中，群并非通过特选点来恢复，而是通过点之间的传输系统来恢复。之后，我们便可以自然地从相对位置而非绝对坐标的角度来思考。

传输子具有我们所预期的形式性质。对于任意 $x, y, z \in X$，有

$$\mathrm{tr}(x,x) = e, \qquad \mathrm{tr}(y,z)\,\mathrm{tr}(x,y) = \mathrm{tr}(x,z), \qquad \mathrm{tr}(x,y)^{-1} = \mathrm{tr}(y,x).$$

这些等式直接由唯一性得出。它们表明，尽管空间 X 本身未必带有群运算，但其点之间的比较受群 G支配。

图 2 展示了传输子的复合律。

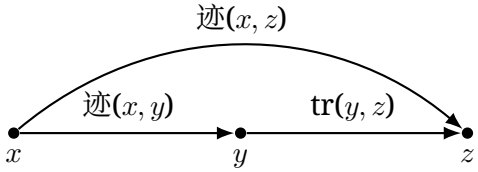


图 2：传递子的复合：$\mathrm{tr}(y,z)\,\mathrm{tr}(x,y) = \mathrm{tr}(x,z)$。

命题 3.8。 设群 G 在非空集合 X上自由且传递地作用，并选取一个点$x_0 \in X$。那么映射

$$\phi_{x_0} : G \to X, \qquad g \mapsto g \cdot x_0,$$

是一个双射。

证明。 由传递性可得满射性： X 中的每个点都具有 $g{\cdot}x_0$ 的形式，其中 $g \in G$。由自由性可得单射性：若 $g \cdot x_0 = h \cdot x_0$，则

$$h^{-1}g \cdot x_0 = x_0,$$

因此 $h^{-1}g = e$，所以 $g = h$。 □

这个命题说明，为什么可以非正式地将扭子描述为一个没有选定单位元的群。一旦选定一个点 x_0 ，集合 X 便与 G相对应。但这种对应取决于所选的 x_0，通常并没有典范的理由偏爱某个点。因此，群结构仅通过传输而存在，并没有内在指定的原点。

这种非典范的特征并非偶然的不便；它正是扭子思想的核心。扭子并不只是群的一个副本。更确切地说，它是一个在局部或关系层面表现得如同群、但在整体上缺乏特殊指定单位元的空间。这正是扭子会如此自然地出现在这样的语境中的原因：局部选择是可行的，但整体选择并不存在。

下一节将通过引入扭子的定义，把这些思想形式化。

4 扭子的定义

现在我们已经准备好明确这些笔记的核心概念。非正式地说，扭子是一个群在其上自由且传递地作用的空间。等价地说，在扭子中，每个点都可以通过唯一的群元素传输到任意其他点。这使得扭子看起来与群本身非常相似，只是没有预先特别指定任何单位元。

定义 4.1。 设 G 是一个群。左 G-扭子 是一个非空集合 X ，配备了 G 在 X 上的左作用，使得该作用自由且传递。

除非另有说明，扭子 一词均指集合论意义上的左托orsor。稍后我们会考虑层论版本，但集合的初等情形是首先需要牢记的模型。

根据命题 3.3，前面的定义可以等价地改写为一种非常有用的形式。

命题 4.2。 设 G 是作用在非空集合 X上的群。那么以下条件等价：

1. X 是一个 G-扭子；
2. 对任意 x、$y \in X$，都存在唯一的 $g \in G$ 使得

$$g \cdot x = y.$$

证明。 这正是用扭子的语言重述的命题 3.3。 □

因此，扭子的特征是唯一传递。这一概念如此灵活，原因之一就在于：我们不必把群看作由抽象对称性组成的集合，而可以把它看作扭子中各点之间所有相对位移构成的系统。

注 4.3. 扭子常被称为主齐性空间。“齐性”一词指的是，从作用的角度来看，每个点都相同；而“主”则体现了不存在非平凡稳定子。我们将在第 7 节重新讨论这一术语。

4.1 将扭子视为没有指定单位元的群

群通过左乘作用于自身，且该作用自由且传递。因此，每个群 G 都确定了一个典范的 G-扭子，即群 G自身的底层集合。一般扭子与群作用于自身的情形的区别在于，一般扭子并没有一个对应于单位元的首选点。

命题 4.4. 设 X 是一个 G-扭子，并选取一个点 $x_0 \in X$。那么映射

$$\phi_{x_0} : G \to X, \qquad g \mapsto g \cdot x_0,$$

是一个双射。

证明. 这已在命题 3.5 中证明。 □

这个双射的意义在于概念层面，而不仅仅是形式上的。它表明，一旦选定一个基点，每个扭子都将变得无法与该群区分。然而，基点的选择本身独立于扭子结构。不同的选择会导出不同的对应关系，而且通常不存在典范的对应关系。因此，扭子并非严格意义上的群，而是一个在作出选择后才呈现出类群性质的空间。

注 4.5. 这就是人们常听到这样一句口号的原因：扭子是“一个没有选定单位元的群”。这句口号是有用的，但前提是要记住，扭子本身并不配备乘法律。它所具有的不是内部群结构，而是一个群的外部单传递作用。

4.2 传输与相对位置

If X 是一个 G-扭子，则对每一对点 $x,\ y \in X$ 存在一个唯一传递 r

$$\mathrm{tr}(x,y) \in G$$

使得

$$\mathrm{tr}(x,y)\cdot x = y.$$

This pers这种视角使人可以将作用群视为编码 X 中所有相对位置的对象 .

图 3 强调了这一点：扭子由点与点之间的传输决定，而非由绝对坐标决定。

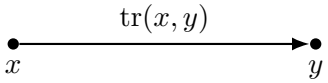


图 3：在扭子中，相对位置由两点之间唯一的传输子来度量。

恒等式

$$\mathrm{tr}(x,x) = e, \qquad \mathrm{tr}(y,z)\,\mathrm{tr}(x,y) = \mathrm{tr}(x,z), \qquad \mathrm{tr}(x,y)^{-1} = \mathrm{tr}(y,x)$$

说明传输子表现得像差运算。例如，在仿射空间中，两点之间的“差”是一个向量。扭子推广了这一现象：两点之间的差不是在向量空间中度量，而是在作用群中度量。

这一观点对后续章节尤为重要。当扭子源自局部平凡性与粘合数据，或是在层论背景下考察时，最重要的往往是对局部选择进行相对比较。因此，传输子形式体系不仅仅是一种方便的记号；它体现了这一主题的基本逻辑。

4.3 右扭子

为求完整，现记录这一概念的右作用版本。

定义 4.6。 设 G 是一个群。一个右 G-扭子是一个非空集合 X，配备右作用

$$X \times G \to X, \qquad (x,g) \mapsto x \cdot g,$$

使得该作用自由且传递。

上述内容显然都有相应的右手版本。在这些笔记中，默认采用左托orsor，因为这足以满足预期的应用需求。然而，在几何和下降理论中，左、右托orsor都会自然出现，因此必须注意所采用的约定。

4.4 非空性的重要性

扭子的定义中要求非空，这并非纯粹的技术细节。如果允许 X 为空，那么作用在形式上就会自动满足若干性质，但扭子的基本直觉也就荡然无存。扭子旨在刻画这样一种空间：其中的点可以通过唯一传递相互比较。没有点，也就无从传输。

此外，在后续的层论背景中，局部非空性与整体非空性之间的区别变得至关重要。一个层扭子可能在局部有点，却不允许存在任何整体截面。这种局部/整体张力正是这一概念在数学上变得强有力的主要原因之一。

4.5 首要总结

我们来总结一下基本图景。 G-扭子是一个非空集合 X，其上 G 自由且传递地作用。等价地，X 中的每一对点都确定了 G中的一个唯一传输子。选取一个基点，就能将 X 与 G对应起来，但这种对应并非典范的。因此，扭子具有类群的结构，却不带有首选的单位元。

这就是初等定义。然而，它的重要性不仅在于自由传递性的形式条件，也在于它为我们理解后续构造所作的铺垫。扭子是这样一种最简单的情形：其中存在协调一致的相对位置，却没有绝对原点。因此，扭子自然出现于仿射几何、粘合问题、下降理论情形，以及我们稍后将要指出的、针对 Σ-协议的层论方法中。

下一节将介绍若干基本例子，在本文余下部分中应始终牢记这些例子。

5 扭子的基本例子

只要先了解几个具体例子，扭子的抽象定义就会清晰得多。其中，仿射空间对建立直觉最为重要。它们以尽可能简单的方式表明，即使没有规范选定的原点，差仍然可以具有明确的含义。我们先讨论仿射空间，再考察几个进一步的例子，以说明代数情形中的同一模式。

5.1 仿射空间

仿射空间为扭子提供了基本的几何模型。非正式地说，仿射空间就像一个被遗忘了原点的向量空间。可以通过取差来比较各个点，但不能内在地把点与点相加。

定义 5.1. 设 V 是域 k上的向量空间。一个仿射空间，其模型为 V，是配备了映射的非空集合 A

$$A \times V \to A, \qquad (a, v) \mapsto a + v,$$

使得：

1. $a + 0 = a$ 对所有 $a \in A$，2. $(a + v) + w = a + (v + w)$ 对所有 $a \in A$ 与 v，$w \in V$，

3. 对每个 a、$b \in A$，存在唯一的 $v \in V$ 使得

$$a + v = b.$$

第三个条件恰好说明，V 的加法群在 A 上的作用是自由且传递的。因此，以 V 为模型的仿射空间，正是一个 V-扭子，其中 V 被视为加法群。

命题5.2. 设 V 是一个向量空间。以 V 为模型的仿射空间，与加法群$(V, +)$下的扭子是同一回事。

证明。 仿射空间的公理恰好表明，$(V, +)$ 对 A 的平移作用是有定义的、自由的且传递的。反过来，任何加法群 $(V, +)$ 上的扭子都可以写成 $a + v$ 的形式，并且满足仿射空间公理。

□

这个例子十分基础，因此可以将扭子视为仿射空间的直接推广。在仿射空间中，联系两个点的量是一个向量。在一般扭子中，联系两个点的量是作用群的一个元素。因此，仿射空间是一般理论的交换线性原型。

注 5.3. 仿射空间的观点并非只是术语上的差异。它真正的优势在于概念层面：从一开始便明确指出，我们关注的主要对象不是绝对位置，而是差、位移和平移。这正是后来在扭子的一般理论中再次出现的结构性思想。

若选定一个点 $a_0 \in A$，那么每个点 $a \in A$ 都可以唯一地写成

$$a = a_0 + v$$

其中 $v \in V$为某个元素。因此，选择 a_0 便可将 A 与 V等同起来。但这种等同取决于选定基点，而且没有典范的理由认为 A 中的某个点优于其他点。这正是扭子普遍具有的非典范平凡化现象。

注 5.4. 将分析所处的底层空间视为仿射空间，有一个实用的优点：这样可以避免把原点看作本质上具有特殊地位的点。在许多解析构造中，重要的并不是孤立地看待某个点，而是增量或位移。典型的表达式例如

$$f(x + h) - f(x)$$

已经清楚地表明：关键量是变化量 h，而不是定义域中存在一个优选原点。从这一视角看，定义域自然是一个仿射空间，而增量属于关联向量空间。这一区分了点与差，并明确指出，分析往往由相对位移而非绝对位置所支配。这与 *Schwartz*[4]所体现的分析中的仿射观点十分契合。

注 5.5. 可以这样概括这一要点：在分析的仿射方法中，点本身属于仿射空间，而增量属于关联向量空间。因此，我们不会混淆身处何处与如何移动。这种区分在初等分析中就很有概念上的价值；在几何中，它更为重要，因为流形和构形空间并非天然的向量空间，但在局部由位移数据所支配。就本讲义而言，这正是仿射空间构成扭子的最佳初始模型的主要原因之一。

5.2 线性方程的解集

第二个基本例子来自初等线性代数。线性方程的解集通常并非天然的向量空间，但选定一个特解后，它就成为向量空间。这是扭子在实践中出现的最简单方式之一。

例 5.6. 设 $T\colon V \to W$ 是向量空间之间的一个线性映射，并设 $w \in W$。考虑解集

$$S_w := \{v \in V \mid T(v) = w\}.$$

若 S_w 非空，则它自然是$\ker(T)$的加法群上的一个扭子。

证明。 设 $u \in \ker(T)$ 且 $v \in S_w$。 则

$$T(v + u) = T(v) + T(u) = w + 0 = w,$$

所以 $v+u \in S_w$。因此 $\ker(T)$ 通过平移作用于 S_w。

要看出该作用是传递的，令 $v_1, v_2 \in S_w$。那么

$$T(v_2 - v_1) = T(v_2) - T(v_1) = w - w = 0,$$

因此 $v_2 - v_1 \in \ker(T)$，从而

$$v_1 + (v_2 - v_1) = v_2.$$

要看出该作用是自由的，假设 $v+u=v$ 且 $u \in \ker(T)$。那么 $u=0$。因此，该作用是自由且传递的。

□

因此，只要一个线性方程至少有一个解，它的解集就不仅仅是一个集合：它是一个以核为模型的仿射空间。等价地，它是 $\ker(T)$ 作用下的一个扭子。这个例子特别有用，因为它表明，在研究仅由齐次修正确定的对象时，扭子会自然出现。

5.3 陪集

第三类基本例子直接来自群论本身。

例 5.7. 设 G 是一个群，$H \leq G$ 是一个子群。对于任意 $g \in G$，左陪集

$$gH = \{gh \mid h \in H\}$$

自然是一个右 H-扭子，其作用由右乘法给出：

$$(gh_1) \cdot h_2 := g(h_1 h_2).$$

类似地，采用相反约定后，也可以将其视为一个左 *torsor* .

证明。 H 在 gH 上的右作用是传递的，因为 gH 的每个元素都可写成 gh 的形式。该作用是自由的，因为

$$(gh) \cdot h' = gh$$

推出

$$ghh' = gh,$$

因此 $h' = e$。所以 gH 是一个右 H-扭子。 □

这个例子在概念上很重要。陪集与子群 H 相似，但它本身没有一个首选的单位元。同样，我们看到一种具有类群结构、却并非典范群的结构。

5.4 基的集合与标架

另一个很有启发性的例子是有限维向量空间的所有有序基构成的集合。

例 5.8。 设 V 是域 k 上的一个 n 维向量空间，并令 $B(V)$ 表示 V 的有序基集合。那么，$B(V)$ 是群 $\mathrm{GL}(V)$ 下的一个扭子。

证明。 群 $\mathrm{GL}(V)$ 在 $\mathcal{B}(V)$ 上的作用是将基 $(v_1, \ldots, v_n)$ 变为

$$(gv_1, \ldots, gv_n).$$

该作用是传递的，因为任一有序基都可通过唯一的可逆线性映射映到任一其他有序基。它是自由的，因为若 g 固定某个有序基，则它固定每个基向量，从而$g = \mathrm{id}_V$。因此该作用是自由且传递的。

□

这个例子表明，每当研究坐标系或标架的选择时，扭子都会自然出现。基是一种选择，但所有这类选择构成的集合，往往比其中任何一个单独选择都更自然。在几何中，这一思想尤为重要：标架丛正是由这种扭子结构构造而成的。

5.5 示例的首次比较

尽管前面的例子来自不同领域，但它们都具有相同的形式模式。具体来说，每种情况下：

1. 存在一个对象或选项的集合，
2. 存在一个允许的变换群，
3. 每个对象都可以通过唯一的变换从任何其他对象到达。

这正是扭子的条件。

不同示例之间的差异在于对作用群的诠释。对于仿射空间，作用群是通过平移作用的向量空间。对于解空间，作用群是线性映射的核。对于陪集，作用群是通过乘法作用的子群。对于基，作用群是一般线性群。因此，扭子概念提炼出了一个共同的结构模式，揭示了表面上不同的数学情形背后的共性。

注记 5.9. 就本讲义而言，仿射空间的例子应始终置于核心位置。它最清楚地说明了一个事实：扭子具有有意义的差，却没有一个指定的原点。后续理论的大部分内容，都可以理解为对这一简单几何思想的广泛推广。

下一节将通过一般性地研究基点、差和传递子，进一步探讨这一点。

6 基础理论习题

本节收录了一小组习题，旨在巩固扭子的初等理论。其中大多数都很直接，但仍值得仔细推导，因为后续各节将会用到这些思想。

1. 设 G 作用于集合 X。证明，当且仅当每个点的稳定子都是平凡的时，该作用才是自由的。

2. 设 G 作用于集合 X。证明，当且仅当 X 由单个轨道组成时，该作用才是传递的。

3. 举出一个传递但不自由的作用的例子。

4. 举出一个自由但不传递的作用的例子。

5. 设 G 在非空集合 X 上自由且传递地作用。直接证明，对于每个 $x, y \in X$，存在唯一的 $g \in G$ 使得
$$g \cdot x = y.$$

6. 设 X 是一个 G-扭子，并设 $x_0 \in X$。证明映射
$$\phi_{x_0} : G \to X, \qquad g \mapsto g \cdot x_0$$
是一个双射。

7. 设 X 是一个 G-扭子，并设 $x_0, x_1 \in X$。若 $h \in G$ 是满足以下条件的唯一元素
$$h \cdot x_0 = x_1,$$
证明
$$\phi_{x_1}(g) = \phi_{x_0}(gh)$$
对所有 $g \in G$。

8. 设 X 是一个 G-扭子。证明传递子恒等式

$$\begin{aligned}\operatorname{tr}(x,x) &= e,\\ \operatorname{tr}(x,y)^{-1} &= \operatorname{tr}(y,x),\\ \operatorname{tr}(y,z)\operatorname{tr}(x,y) &= \operatorname{tr}(x,z).\end{aligned}$$

9. 设 A 是以向量空间 V 为模型的仿射空间。证明 A 是加法群 $(V,+)$ 上的扭子。

10. 设 $T\colon V \to W$ 是向量空间之间的线性映射，并设

$$S_w = \{v \in V \mid T(v) = w\}.$$

假设 S_w 非空。证明 S_w 是以 $\ker(T)$ 为模型的仿射空间。

11. 设 G 是一个群，$H \le G$ 是其子群。证明每个左陪集 gH 都是一个右 H-扭子。

12. 设 V 是一个有限维向量空间。证明 V 的有序基集合是 $\mathrm{GL}(V)$ 上的扭子。

13. 设 X 是一个 G-扭子。固定一个点 $x_0 \in X$，并通过沿双射传输群运算，在 X 上定义一个二元运算

$$G \to X, \qquad g \mapsto g \cdot x_0.$$

证明这使得 X 成为一个群。然后证明所得的群结构取决于对 x_0的选择。

14. 解释为什么前一个练习并不与“扭子不带有典范群结构”这一陈述相矛盾。

15. 设 X 是一个 G-扭子。对于固定的 $x \in X$，定义

$$d_x(y) := \operatorname{tr}(x,y).$$

证明 $d_x\colon X \to G$ 是一个双射。将其解释为由基点 x所确定的坐标系。

16. 用你自己的话解释以下两种陈述之间的区别：

（a）选定一个基点后，扭子就可以与一个群等同起来；（b）扭子典范地就是一个群。

17. 为什么扭子的定义中要包含非空性？如果允许空集，会在概念上导致什么问题？

18. 写一段简短的文字，说明为什么仿射空间是扭子一般理论的最佳入门模型。

7 局部平凡性与粘合数据

到目前为止，扭子一直以其初等形式呈现：扭子是一个非空集合，配备了自由且传递的群作用。这个定义至关重要，后文所述内容都不会取代它。不过，如果止步于此，我们仍未看到扭子为何会如此自然地出现在几何、下降理论和局部到整体构造中这一更深层的原因。

因此，本节在概念上十分重要。本节旨在凸显另一种同样对后续理论至关重要的观点：扭子不仅是由自由且传递的作用定义的对象，也是一个局部平凡、但仍可能整体非平凡的对象，因为它是通过粘合数据由局部片段拼合而成的。从这个意义上说，缺少一个首选基点并不只是一个否定性的表述，而是一个明显的迹象，表明局部平凡化可能存在，却无法拼合成单一的整体平凡化。

注 7.1。 这种视角的转变是本文的主要结构要点之一。扭子不应仅被看作“带有自由且传递作用的集合”，也应被看作“一个局部平凡的对象，其整体形式由局部平凡化如何粘合在一起决定”。后续层论的和拓扑斯论的应用都高度依赖这一第二种视角。

本节旨在从直观层面阐明这一思想。形式化的层论和拓扑斯论版本将在后文讨论。现在，核心要点是：扭子虽然整体上没有一个指定的原点，但局部上可能存在这样的选择，而不同局部选择之间的变化由群值过渡数据来衡量。

7.1 初等意义下的局部平凡性

设 X 是一个 G-扭子。若选取一个基点 $x_0 \in X$，则映射

$$\phi_{x_0} : G \to X, \qquad g \mapsto g \cdot x_0$$

是一个双射。因此，选定一个点后，扭子便与作用群相识别。从这个意义上说，扭子总能借助基点实现平凡化 。

乍看之下，这似乎将扭子归结为群的一个副本。但这并不是正确的结论。关键在于，平凡化依赖于一种选择，而这种选择通常并非典范的。这正是粘合观点的起点：我们可以有平凡化，却没有一个优先的选择。

注 7.2。 局部平凡性的重要之处在于，它说明扭子如何能够“类似于群”，却又不能典范地成为一个群。局部而言，选定基点后，它看起来与作用群完全一样。然而在整体上，缺少优先选择这一点依然存在。因此，典范原点的不存在并非偶然的缺失，而是扭子必须通过粘合来描述的结构性原因。

后续理论之所以有趣，在于许多情境下，这样的选择只能在局部进行，而无法在整体上进行。扭子的局部平凡性意味着，在每个足够小的区域上，都可以选取一个局部原点，或者等价地，将扭子与作用群等同起来。但这些局部等同在交叠区域上未必一致。它们之间的差异，正是粘合数据的来源。

即使在初等的集合论情形中，这一点也已经显现出来。一个基点可以使扭子平凡化，但换一个基点就会得到不同的平凡化。从一种平凡化过渡到另一种平凡化，由作用群中的唯一一个元素所控制。后续理论只是将这一现象系统地组织起来，并推广到一族局部区域上。

7.2 从一种平凡化到另一种平凡化

再次假设 X 是一个 G-扭子，并令 x_0，$x_1 \in X$。如前所见，存在唯一的元素 $h \in G$ 使得

$$h \cdot x_0 = x_1.$$

相应的平凡化

$$\phi_{x_0}, \phi_{x_1} : G \to X$$

相关

$$\phi_{x_1}(g) = \phi_{x_0}(gh).$$

这个公式很初等，却是过渡函数的原型。它说明，改变选定的原点并不会破坏对扭子的描述，而是通过群中的平移来改变这种描述。因此，扭子并不自带首选坐标系，但所有坐标系构成的集合本身受作用群控制。

注 7.3. 这里很适合再次阐明核心思想。每个选定基点都将扭子与作用群等同起来，因此扭子是局部平凡的。但扭子并非以任何典范方式整体平凡，因为不同的平凡化相差非平凡的过渡元。因此，缺少基点应当被积极地理解：它正是粘合现象在初等形式下的体现。

在几何情形中，这种现象反复出现。人们在重叠区域上选取局部平凡化，并在每个交叠处比较这两种选择。这种比较由一个取值于作用群的元素，或更一般地说，一个取值于作用群的函数来编码。这些就是扭子的过渡数据。

7.3 粘合观点

粘合观点始于以下观察：扭子不必一开始就作为一个整体平凡的对象给出。相反，它可以由若干部分构造而成，每个部分单独来看都是平凡的；只需指定这些部分在交叠区域上如何相互识别即可。

非正式地说，假设一个环境空间被若干区域覆盖

$$U_i.$$

在每个 U_i 上，假设我们的扭子看起来都与群 G 本身完全一样。换句话说，在每个区域上，我们都选定了一个局部平凡化。那么在交叠区域 $U_i \cap U_j$ 上，这两个局部平凡化未必一致。

图 4 展示了基本的粘合情形：通过过渡数据在交叠区域上比较局部平凡化。

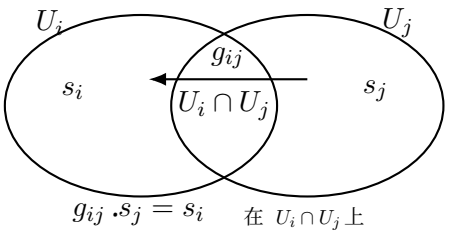


图 4：通过过渡数据 g_{ij} 比较交叠部分上的两个局部平凡化。

它们的差异由一个变换来衡量

$$g_{ij}$$

其取值在 G 中。这些变换描述了如何从第 j 个局部图景过渡到第 i 个局部图景。

核心思想是，扭子并非由任何单个平凡化恢复出来，而是由整个相容的局部平凡化族及其相互关联的过渡数据共同恢复出来。这正是扭子作为粘合对象的含义。

注 7.4. 这里应当把概念图景阐述得十分明确：扭子是局部平凡的，因为在每个区域上，它都可以与群等同。它在整体上是一个粘合对象，因为这些局部等同在交叠区域上彼此不同。因此，不存在整体上特定的基点，这与局部平凡化无法合并为一个典范的整体平凡化，是同一种结构性现象。

7.4 交叠处的相容性

在一个区域族上选定局部平凡化后，过渡数据便不能任意取值，而必须满足相容条件。

最基本的一点是，将某个平凡化与其自身比较时，不应有任何变化。因此，预期有

$$g_{ii} = e.$$

如果从第 i 个平凡化切换到第 j 个平凡化，再切换回来，结果应当仍然没有变化。因此，预期有

$$g_{ji} = g_{ij}^{-1}.$$

更重要的是，在三重交叠区域上

$$U_i \cap U_j \cap U_k,$$

可以用两种不同方式比较平凡化。可以直接从第 k 个平凡化切换到第 i 个，也可以先从 k 切换到 j，再从 j 切换到 i。为保持一致，这两种过程必须相同。因此，预期有如下关系

$$g_{ij}g_{jk} = g_{ik}.$$

这就是余循环条件。它表达了一个简单但至关重要的事实：局部坐标变换若要定义一个相干的全局对象，就必须彼此相容。

注记 7.5. 余循环条件应被理解为整体相干性的代数形式。它保证扭子不只是群的若干局部副本的集合，而是由它们组装而成的单一全局对象。若没有这种相容性，就根本得不到一个定义良好的粘合对象。

7.5 整体平凡性为何可能失效

如果所有局部平凡化都能在整体上达成一致，那么就会得到扭子的一个单一的优先平凡化。等价地，就会得到一个整体选定基点，或与作用群的一个整体等同。但在许多情形中，这是不可能的。

正是这种失效赋予了扭子大部分趣味。扭子在局部上与作用群无法区分，但在整体上仍可能保持扭曲。这一障碍在任何一个局部片段内部都不可见；它只在人们试图同时比较所有局部片段时才会显现。

注 7.6。 后续理论应当牢记这一点：缺少全局原点并非只是有所缺失，而是一种结构性障碍。扭子具有足够的局部对称性，因此在邻近区域看起来是平凡的；但它缺乏足够的整体相干性，无法确定一个单一的全局基点。因此，研究扭子时，自然要借助粘合与余循环。

应牢记这种局部/整体张力。这是扭子自然出现于几何、上同调和下降理论中的主要原因之一。扭子形式体系记录了这样一个事实：局部选择可能处处存在，却无法汇集成单一的整体选择。

7.6 重新审视仿射空间

仿射空间的例子也可以再次作为指引。选定一个点后，仿射空间便是整体平凡的，但没有哪个点是优先的。因此，它已经以尽可能简单的形式体现了这样一条原则：局部或辅助选择可能存在，却不一定是典范的。

在更复杂的情形中，可能不仅有多个可选的基点，还有定义在相互交叠的定义域上的多个局部坐标系。这些坐标系之间的过渡由作用群来度量，正如在仿射情形中，选择一个原点而非另一个原点，会使坐标描述发生平移。

因此，仿射空间不仅是扭子的第一个例子，也是扭子背后粘合思想的第一个例子。

注 7.7。 仿射空间尤其清楚地展现了这一核心主张：采用局部原点或选定的原点完全可行，但几何本身并未指定其中任何一个。一般的扭子形式体系正是对这一思想的推广：局部平凡化可能存在，但对象本身是由这些平凡化之间的关系所定义，而非由典范的全局基点的存在所定义。

7.7 为下一节做准备

本节的目的在于阐明概念，而非讨论技术细节。我们尚未定义层上的扭子，也尚未阐述完整的重构理论。相反，我们提炼出了以下基本模式：

1. 扭子局部平凡；
2. 不同的局部平凡化由群值过渡数据联系起来；
3. 这些过渡的相容性由余循环恒等式表达；
4. 整体平凡化的缺失是扭曲的根本来源。

让我们最后再强调一次关键点。扭子不仅仅是一个带有自由且传递作用的集合。这个定义只是形式上的出发点。但扭子的更深层几何意义在于，它是一个局部上与作用群无法区分、整体上通过粘合组装而成的对象。因此，缺少首选基点，最好理解为局部平凡化无法合并为单一典范整体平凡化。

下一节将通过阐述余循环描述，并解释如何根据这类数据重构扭子，使这一点更加精确。

8 余循环描述与重构

在上一节中，我们强调了一种对后续理论至关重要的观点转变：扭子不仅是由自由且传递的作用定义的对象，也是一个局部平凡、并通过粘合数据在整体上组装而成的对象。现在，我们将这一思想阐述得更加精确。

基本原理很简单。假设一个对象在覆盖的每个成员上都是平凡的。那么，全局对象便由这些局部平凡片段在交叠区域上的识别方式决定。对于扭子而言，这些识别由取值于作用群的元素，或更一般地说，由取值于作用群的函数来刻画。这些识别之间的相容性则由余循环条件表达。

注记 8.1。 本节应被视为第 *8* 节所阐述的概念图景的形式化对应部分。核心思想仍然相同：扭子在局部上是作用群的一个副本，但在整体上可能发生扭曲。记录这种扭曲的是余循环数据。

8.1 局部平凡化的过渡数据

让我们先从区域族的非正式描述开始

$$U_i$$

覆盖某个环境空间。假设在每个 U_i 上，我们的扭子都已被平凡化。也就是说，在每个 U_i 上，它都被识别为作用群 G。

现在考虑一个交叠

$$U_i \cap U_j.$$

在这个交叠上，我们有两个平凡化：一个来自 U_i，另一个来自 U_j。由于二者描述的是交叠上的同一个扭子，它们必然相差一个群变换。因此得到一个过渡函数

$$g_{ij} : U_i \cap U_j \to G.$$

g_{ij} 的含义是，它告诉我们如何从第 j 个局部平凡化转到第 i 个局部平凡化。换句话说，族 $\{g_{ij}\}$ 记录了局部平凡化无法直接彼此一致这一事实。

注 8.2。 这是“缺少全局基点”这一思想首次以精确形式出现：它被编码在局部平凡化之间的不匹配中。如果存在单一的整体平凡化，那么所有局部平凡化都可以相容地选取，过渡数据也就会变得平凡。

8.2 余循环恒等式

过渡函数 $\{g_{ij}\}$ 不能是任意的。它们必须满足第 8 节中非正式讨论过的相同一致性要求。

首先，在每个区域 U_i 上，将平凡化与其自身比较不会产生变化，因此预期有

$$g_{ii} = e.$$

其次，在每个交叠 $U_i \cap U_j$ 上，从第 j 个平凡化变换到第 i 个平凡化，再变回去，应该不会产生任何变化，因此预期有

$$g_{ji} = g_{ij}^{-1}.$$

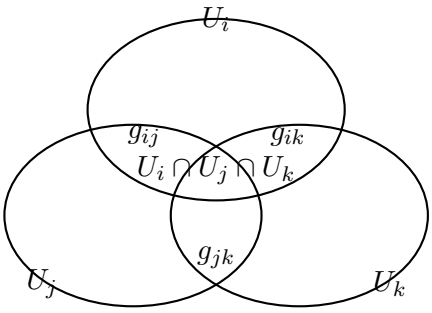
第三，也是最重要的一点，在一个三重交叠上

$$U_i \cap U_j \cap U_k,$$

比较第 k 个平凡化与第 i 个平凡化有两种方式：可以直接比较，也可以通过 U_j 上的中间平凡化来比较。这两种方式必须一致。因此得到

$$g_{ij} g_{jk} = g_{ik}.$$

图 5 说明了余循环条件，即在三重交叠上沿两条不同的比较路径所得的结果必须相同。



$g_{ij}g_{jk} = g_{ik}$ 关于 $U_i \cap U_j \cap U_k$

图 5：在三重交叠区域上，两种在局部平凡化之间转换的方式必须一致；这就是余循环条件。

这就是余循环条件。

定义 8.3. 一族过渡函数

$$g_{ij} : U_i \cap U_j \to G$$

称为一个以 G 为值的 1-余循环，若它在所有相关交叠区域上都满足

$$\begin{aligned} g_{ii} &= e, \\ g_{ji} &= g_{ij}^{-1}, \\ g_{ij}g_{jk} &= g_{ik}. \end{aligned}$$

注 8.4. 此时，“余循环”一词无需让人望而生畏。它只表示一个相容的过渡数据系统。余循环条件是这样一个事实的代数表述：局部坐标变换的复合是一致的。

8.3 从余循环到扭子

反过来，也可以从余循环数据出发重构一个扭子。

假设我们给定了局部平凡片段，每个片段都以群 G 为模型，定义在区域 U_i 上，并配有过渡函数

$$g_{ij} : U_i \cap U_j \to G$$

这些过渡函数满足余循环条件。接着，我们通过规定在交叠区域上，将 j 次平凡化中描述的点与应用过渡函数 g_{ij} 后在 i 次平凡化中对应的点视为同一点，从而将 G 的局部副本粘合起来。

余循环条件恰好保证了这一识别过程在三重交叠区域上是一致的。没有这一条件，就无法得到定义良好的全局对象。有了这一条件，便可得到一个全局定义的扭子，它在局部上与 G 相识别。

因此，余循环不仅记录扭子，也能生成扭子。

注记 8.5. 这种重构视角至关重要。扭子并非只是一个已经存在、碰巧具有局部平凡化的对象。它实际上可以由这些平凡化以及比较它们的余循环构造出来。从这个意义上说，余循环并非次要的记录工具；它们正是扭子的粘合指令。

8.4 等价余循环

不同的局部平凡化选择可能产生不同的余循环，但仍描述同一个整体扭子。因此，理解何时应将两个余循环视为等价十分重要。

假设我们在每个区域 U_i 上，使用一个函数改变所选的平凡化

$$h_i : U_i \to G.$$

那么，旧的过渡函数 g_{ij} 将替换为新的过渡函数g'_{ij}，二者满足公式

$$g'_{ij} = h_i \, g_{ij} \, h_j^{-1}.$$

这只是局部坐标变换的代数表达。整体扭子并未改变；改变的只是用于描述它的局部平凡化。

定义 8.6. 若存在定义在区域 U_i 上的函数 h_i，使得等价 余循环 $\{g_{ij}\}$ 和 $\{g'_{ij}\}$ 满足

$$g'_{ij} = h_i \, g_{ij} \, h_j^{-1}$$

在每个交叠 $U_i \cap U_j$ 上。

等价余循环描述同一个扭子。因此，扭子并非由单个余循环决定，而是由一个余循环等价类决定。

备注 8.7。 这里也应当凸显这一核心主题。扭子并不依附于某个特定的平凡化，因此也不依附于某个特定的余循环。真正具有内在意义的是整体粘合对象本身，而不是它的任何一种局部坐标描述。

8.5 平凡余循环与整体平凡性

最简单的余循环是平凡余循环，此时

$$g_{ij} = e$$

在每个交叠上都成立。在这种情况下，所有局部平凡化都直接一致，因此 G 的局部副本可以在没有任何扭曲的情况下粘合在一起。由此得到的扭子是整体平凡的。

反过来，如果一个扭子存在整体平凡化，那么就可以选取与之相容的局部平凡化，而相应的余循环便是平凡的。

因此，平凡余循环恰好对应于扭子具有全局原点的情形，或者等价地，扭子与作用群之间存在全局识别。

注 8.8。 这一点值得明确指出。扭子的扭曲程度由其余循环偏离平凡的程度来衡量。因此，缺少全局基点这一事实，在代数上体现为非平凡的过渡数据。这是最清晰的方式之一，可以看出缺少典范原点并非只是少了一种装饰，而是一种真正的结构特征。

8.6 为什么重构很重要

乍一看，余循环描述似乎只是对已有认识的一种技术性改述。但它远不止于此。这正是扭子自然进入上同调、下降理论和层论的形式。

余循环观点之所以强大，在于它将两个不同的要素区分开来：

1. 局部平凡性，使对象在局部上易于处理；
2. 过渡数据的相容性，它决定了其全局结构。

这种区分正是研究局部简单但全局扭曲的对象时所需要的。

对于本文而言，这一点很重要，因为后面的层论章节将以这种局部到整体的方式重新诠释扭子。在那里，局部截面和过渡数据将发挥与此处局部平凡化和余循环相同的作用。

8.7 总结

我们来总结本节的主要内容。

1. 局部平凡的扭子决定了交叠区域上的过渡函数。2. 这些过渡函数满足余循环恒等式。3. 可以利用相容的余循环通过粘合重构扭子。4. 不同的局部平凡化选择会产生等价的余循环。5. 扭子整体平凡，当且仅当其余循环是平凡的。

这具体体现了第8节和第9节的指导思想：扭子是一种对象，它局部上是作用群的一个副本，但整体上由粘合组装而成。它的扭曲由余循环数据衡量。

下一节将把这一图景从初等情形扩展到群层下的扭子；在这种情形中，局部截面与整体截面之间的区别尤为重要。

9 层扭子、局部截面与整体截面

前几节以刻意浅显的形式阐述了扭子的概念。首先，扭子被定义为带有自由且传递的群作用的集合，随后又被重新诠释为一个局部平凡的对象，由相容的粘合数据拼合而成。现在，我们转向与局部到整体数学最为相关的版本：群层上的扭子。

这一步在概念上十分重要。在集合论情形中，扭子要么可由选定的一个点平凡化，要么不可平凡化。而在层论情形中，即使不存在整体截面，也可能存在局部截面和局部平凡化。局部存在性与整体存在性之间的这种区别，正是层扭子如此有用的原因，也是它们日后与预期应用相关的主要原因之一。

注9.1。 此处应牢记本文的核心主题。扭子不仅是一个带有自由且传递的作用的对象，也是一个局部平凡的对象，其全局结构由粘合所决定。在层论背景下，局部与整体之间的对比尤为鲜明，因为截面可能局部存在，却并不存在于整体上。

9.1 群层

设 X 为一个拓扑空间。 X 上的群层 是一个层$\mathcal{G}$ ，使得对每个开集$U \subseteq X$，集合$\mathcal{G}(U)$是一个群，且限制映射是群同态。

因此，群层为每个开集指定一个局部对称性群，其方式与到更小开集上的限制以及局部截面的粘合相容。当作用对称性本身局部变化时，这是适当的设定。

注9.2。 在初等理论中，只有一个在所有地方都作用的全局群 G 。对于层扭子，在开集 U 上相关的对称性是群层在 U上的截面所构成的群 $\mathcal{G}(U)$ 。因此，作用对称性本身现在具有局部性质。

9.2 群层的作用

设 $\mathcal{F}$ 是 X上的集合层，且$\mathcal{G}$ 是 X上的群层。$\mathcal{G}$ 对$\mathcal{F}$的左作用 是指，对于每个开集 $U \subseteq X$，群 $\mathcal{G}(U)$ 都作用于集合 $\mathcal{F}(U)$，并且这些作用与限制映射相容。

具体来说，这意味着如果

$$g \in \mathcal{G}(U), \qquad s \in \mathcal{F}(U),$$

那么就有一个元素

$$g \cdot s \in \mathcal{F}(U),$$

并且如果 $V \subseteq U$ 是开集，那么先限制再作用，所得结果与先作用再限制相同。

因此，层作用就是在所有开集上统一定义且与局部化相容的作用。

9.3 层扭子的定义

现在我们来到了这一基本概念的层论类比。

定义 9.3。 设 G 是拓扑空间 X上的群层。G-扭子是 X 上的一个集合层 F，配备了 G 的一个作用，并满足：

1. F 是局部非空的，也就是说，存在 X 的一个开覆盖 $\{U_i\}$，使得对所有 i，都有 $F(U_i) \neq \varnothing$；

2. 对每个开集 $U \subseteq X$ 以及任意两个截面

$$s, t \in \mathcal{F}(U),$$

存在 U 的一个开覆盖 $\{V_\alpha\}$，使得在每个 V_α 上都存在唯一的元素

$$g_\alpha \in \mathcal{G}(V_\alpha)$$

with

$$g_\alpha \cdot s|_{V_\alpha} = t|_{V_\alpha}.$$

这个定义表达的扭子概念与之前完全相同，只不过现在采用了局部形式。截面未必能通过单个全局群元素在全局范围内进行比较；相反，它们可以在局部以唯一的方式进行比较。

注 9.4。 这就是“扭子局部平凡”这一原则的层论形式。两个截面的比较未必能在全局上进行，但必须能够在局部上唯一地进行。因此，自由传递性现在以局部化的方式表达。

9.4 局部截面与局部平凡性

设 $\mathcal{F}$ 是一个$\mathcal{G}$-扭子。根据定义，$\mathcal{F}$ 是局部非空的。因此，对于 X中的每个点，都存在一个邻域 U，在其上可以选取一个截面

$$s \in \mathcal{F}(U).$$

这样的局部截面扮演局部基点的角色。一旦选定它，在同一个开集上的每个其他局部截面，都可以唯一地表示为利用群层的一个截面作用于 s 的结果。

更准确地说，如果固定了 $s \in \mathcal{F}(U)$，那么映射

$$\mathcal{G}(U) \to \mathcal{F}(U), \qquad g \mapsto g \cdot s,$$

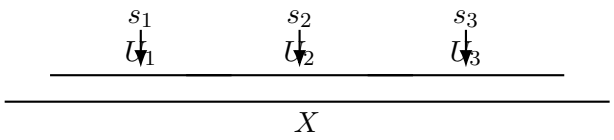
beh的作用类似于局部平凡化：它在局部将扭子与群层相识别 s.

注 9.5. 这正是选择普通扭子中的一个基点所对应的层论类比。局部截面使扭子在局部平凡化。但一般而言，未必存在一个能在所有地方同时将其平凡化的整体截面。这正是粘合问题出现之处。

因此，层扭子按照定义就是一个局部平凡的对象。关键不只是存在局部截面，而是一旦选定这样的截面，该区域上的整个扭子便与作用于其上的群层无法区分。

9.5 整体截面与整体平凡性

图 6 展示了基本的局部/整体区分：层扭子可能在某个覆盖上有局部截面，却不存在任何单一的整体截面。



存在局部截面，但没有选定单一的整体截面

图 6：层扭子可能在某个覆盖上有局部截面，却没有单一的整体截面。

整体截面的作用现在已十分清楚。如果层扭子 $\mathcal{F}$ 有一个整体截面

$$s \in \mathcal{F}(X),$$

那么，这个截面就充当全局基点。在这种情况下，$\mathcal{G}(X)$ 对 s 的作用给出了该扭子的整体平凡化。

因此，整体截面的存在意味着该扭子是整体平凡的。反过来，整体截面的缺失则表明该扭子仍然存在整体扭曲，尽管它处处局部平凡。

注 9.6. 这是本文最重要的概念要点之一。对于层扭子，局部截面与整体截面之间的区别，就是局部平凡性与整体平凡性之间的区别。因此，整体截面的缺失并非仅仅是一种遗漏；它准确地表达了局部选择无法粘合成一个整体选择这一数学事实。

这是最清晰地呈现局部与整体对比的形式。层扭子在覆盖的每个成员上都可能是平凡的，却无法在整体上平凡。因此，它的扭曲在局部不可见；只有在尝试将所有局部平凡化粘合在一起时，扭曲才会显现。

9.6 再论过渡数据

现在假设 $\mathcal{F}$ 是一个$\mathcal{G}$-扭子，并且我们在一个开覆盖上选取了局部截面

$$s_i \in \mathcal{F}(U_i)$$

，该开覆盖为$\{U_i\}$，覆盖 X。

在交叠 $U_i \cap U_j$ 上，截面 s_i 和 s_j 都属于

$$\mathcal{F}(U_i \cap U_j).$$

由于 $\mathcal{F}$ 是一个扭子，局部存在唯一一个$\mathcal{G}$ 的元素，能将其中一个变换为另一个。因此可得到过渡数据

$$g_{ij} \in \mathcal{G}(U_i \cap U_j)$$

使得

$$g_{ij} \cdot s_j = s_i$$

在交叠区域上。

这些转移截面满足与上一节相同的余循环条件。事实上，在三重交叠上，传输的唯一性意味着

$$g_{ij} g_{jk} = g_{ik}.$$

因此，整个余循环图景在层论背景中自然地重新出现。唯一的区别在于，过渡数据现在存在于一个群层中，而不是存在于某个固定的全局群中。

注 9.7。 此时，一般性的思想变得尤为清晰。层扭子之所以是局部平凡的，是因为局部截面存在。它之所以能够整体粘合，是因为这些局部截面之间通过过渡数据相互关联。整体截面的障碍，恰恰在于这些局部平凡化无法以一种平凡的方式在整体上相容。

9.7 局部截面为何重要

值得强调的是，局部截面的作用不只是见证层扭子的非空性。它们是描述扭子所依据的局部原点。没有它们，就不会有局部平凡化，也不会有转移上闭链。

因此，在层论的语境中，截面不只是集合中的一个元素，而是对参考点的局部选择。正是这类局部选择的存在使挠子理论成为可能，而正是这些选择无法整体化，使挠子理论变得有趣。

这一观察是通向预期应用的主要桥梁之一。在后文中，某些依赖于协议的对象将以一种特殊方式加以诠释，使得局部可实现性对应于局部截面，而整体相干性则成为一个更为微妙的问题。因此，读者应当充分熟悉这样一个观念：局部截面就是局部基点，而整体截面则是整体平凡化。

9.8 初等情形作为特例

了解集合的普通挠子理论如何自然地融入这一图景是很有帮助的。如果将底层空间取为单点，那么群层就是一个群，集合层就是一个集合，而层扭子恰好就是普通挠子。

因此，层论的概念并非另一种不同的概念，而是对初等概念的真正扩展。普通理论是这样一种特殊情形：局部数据与全局数据之间不存在非平凡的区别。

注 9.8. 这就是层论版本如此自然的原因。它并未取代扭子的初等概念，而是阐明了当我们进入真正的局部到整体环境时，这一概念会变成什么。

9.9 总结

我们来总结一下本节的要点。

1. 群层提供局部变化的对称性。

2. 层扭子是带有局部自由且传递作用的集合层。 3. 局部截面发挥局部基点的作用。 4. 局部截面产生局部平凡化。 5. 整体截面产生整体平凡化。 6. 缺少整体截面表明局部选择无法拼接成一个整体选择。 7. 局部截面之间的过渡数据满足余循环恒等式。

这就是与后续应用最直接相关的扭子理论形式。下一节将简要、可选地概览这一图景如何在更具概念性的层面上自然融入层论与拓扑斯理论。

10 层论与拓扑斯论的视角概览

对于以最基础的方式阅读本文而言，本节在逻辑上是可选的；但对于希望全面理解后续层论应用的读者，强烈建议阅读本节。本节的目的并非系统地发展拓扑斯理论，而是解释为什么层的拓扑斯为促成本笔记中扭子构造的那些对象提供了自然的背景宇宙。

核心信息很简单。一旦理解扭子是由相容的局部数据组装而成的局部平凡对象，自然就会提出这样的问题：能否找到一个数学环境，使局部数据、限制、粘合以及内部对称性都得到统一处理。层论已经指向这一方向，而格罗滕迪克拓扑斯可以被视为这样一种自然环境：在其中，这种局部到整体逻辑得以内化。

注记 10.1。对于后续预期的应用，拓扑斯并非只是一种方便的语言。它是这样一个数学宇宙：局部协议数据、内部对称性和整体相干性都在同一层面上表达。因此，“拓扑斯中的扭子”这一说法不应被理解为抽象的修饰，而应视为层论观点的自然延续。

10.1 为什么层还不是全部

在前面的各节中，我们反复使用了同一种模式：在一个覆盖上有局部平凡化，在交叠区域上比较它们，并考察它们是否能够粘合成一个全局对象。这已经体现了层论的基本逻辑。

层通过限制与粘合来组织局部数据。但当我们开始研究的不只是集合层，还包括内部代数结构、作用和扭子时，从单个层转向这些对象所处的整个范畴会很有帮助。这个范畴就是拓扑斯。

因此，拓扑斯视角并非背离层论，而是当人们决定将层论的局部到整体数学视为一个独立的背景宇宙时所得到的结果。

备注 10.2. 从层到拓扑斯的转变，类似于从单个集合到整个集合范畴的转变。一旦我们不仅想讨论特定对象，还想讨论群、作用、商、扭子以及它们之间的内部构造，那么在整个环境范畴中进行研究便是自然而然的选择。

10.2 层的拓扑斯

设 (C, J) 是一个景。该范畴

$$\mathbf{Sh}(C, J)$$

(C, J) 上的层构成一个格罗滕迪克拓扑斯。就本笔记的目的而言，读者可以将其视为一个由变化的局部数据构成的广义空间。它的对象是层，态射是层态射，其内部逻辑适用于限制与粘合。

应当牢记，景 (C, J) 编码了哪些态射族被视为覆盖，因此也决定了哪些局部性与相容性概念适用。因此，层的拓扑斯并非只是一个被动的容器，它编码了问题的局部几何。

在后续应用中，所处理的并非普通拓扑空间上的层，而是定义在与某个协议自然关联的景上的层。由此得到的拓扑斯便是背景宇宙，用于组织局部记录数据、模拟结构和扭子类似行为。

注记 10.3。 这正是明确提及拓扑斯的关键原因之一。拓扑斯$\mathbf{Sh}(C, J)$ 告诉我们，对于当前问题，“局部”和“相容”意味着什么。因此，当后续定理提到(C_{Π}, J_{Π})上的层的拓扑斯时，这个景并非无关紧要：它规定了协议 Π 所适用的局部性概念。

图 7 示意了预期的环境：在拓扑斯 $\mathbf{Sh}(C, J)$ 中，考虑一个作用于对象 F 的群对象 G，并探讨 F 是否存在整体截面。

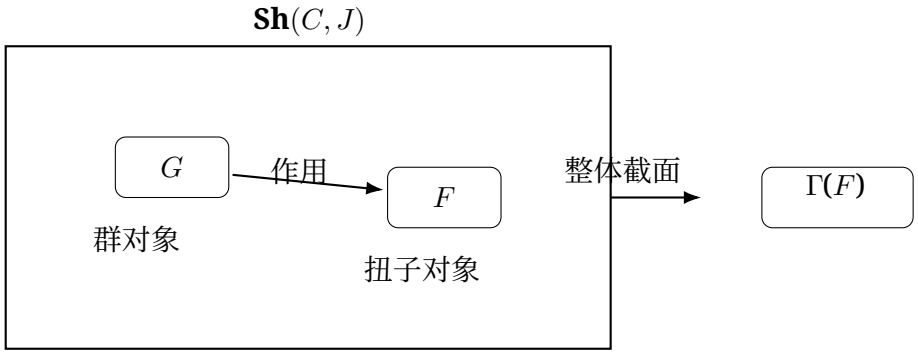


图 7：在拓扑斯 $\mathbf{Sh}(C, J)$ 中，可以考虑一个群对象 G、一个对象 F，G作用于其上，以及 F 是否有整体截面这一问题。

10.3 拓扑斯中的群对象

在普通的集合范畴中，群是一个集合，带有乘法、单位元和逆元，并满足通常的公理。在拓扑斯中，也可以用完全相同的形式方式定义一个群对象：一个对象 G，以及乘法、单位元和逆元态射，它们在内部满足群公理。

关键在于，定义相同，但其含义是拓扑斯内在的。因此，我们应当把群对象看作存在于层宇宙中的对称对象。

在层拓扑斯这一特殊情形下，群对象对应于群层。因此，上一节的层论讨论已经是内在概念的具体形式。

注记 10.4. 这是一个重要的概念简化。拓扑斯中的群对象并不是一种奇特的新型群，而是同一思想自然的内在版本。对于层拓扑斯，这种内在概念与熟悉的外在概念——群层——相一致。

10.4 拓扑斯中的作用与扭子

有了群对象之后，我们也可以讨论拓扑斯内部的作用。若 G 是一个群对象，且 F 是另一个对象，那么 G 对 F 的作用可在内部以与集合范畴中完全相同的形式定义。

这引出了扭子对象的概念。通俗地说，拓扑斯中的扭子是一个局部非空的对象，群对象以局部自由且传递的方式作用于其上。从外部来看，当该拓扑斯是一个层拓扑斯时，这便还原为群层下扭子的概念。

因此，短语“F是拓扑斯 $\mathbf{Sh}(C,J)$ 中 G 下的扭子”应当这样理解：在 (C,J) 上的层所构成的宇宙中，对象 F表现得像一个具有对称性但没有选定原点的空间，并且在局部上与对称对象 G无法区分。

注 10.5. 这是本节的主要阐释目标之一。关于拓扑斯中扭子的陈述，应当听起来像是对初等理论的自然内化，而不是一种毫不相干的抽象构造。形式框架有所变化，但结构思想依然相同：局部平凡性、传输，以及整体平凡化可能无法实现。

10.5 整体截面函子

为了理解后续的应用，还有一个概念尤为重要：整体截面函子。

若$\mathcal{E}$ 是一个拓扑斯，我们可以考察对象 F 的整体点或整体截面所构成的集合。在层拓扑斯$\mathbf{Sh}(C,J)$中，这相当于在终对象上取截面，也就是作出一个整体定义且相容的选择。

因此，说一个扭子对象有整体截面，意思是存在一个整体相容的基点，在整个层宇宙中都有定义。这样的截面会将扭子整体平凡化。

反过来，没有整体截面意味着不存在单一的整体相容选择，即使在某个覆盖上可能存在局部截面。这正是前文强调的局部/整体区分在拓扑斯论中的体现。

注 10.6. 对于后续定理而言，这一点至关重要。整体截面并非仅仅是“某处的一个元素”，而是贯穿整个景的相容整体选择。因此，局部截面与整体截面之间的区别，恰恰就是局部可实现性与整体相容平凡化之间的区别。

10.6 内部存在性与局部存在性

拓扑斯观点最有用的教益之一是，存在性会对局部性变得敏感。在通常的集合论中，说一个对象非空，不过是说它有一个元素。在层论的或拓扑斯论的设定中，一个对象可以在局部被占据，却不具有任何整体点。

对于扭子而言，这一点是决定性的。拓扑斯中的扭子可以是局部平凡的，因为它在某个覆盖上具有局部截面，却仍然缺少整体截面。因此该扭子并非整体平凡，尽管每一局部片段看起来都是平凡的。

这正是前文各节用粘合与余循环所描述的那种结构现象。拓扑斯观点并不改变这一现象。它通过把该现象置于一个局部存在性与整体存在性被形式地区分开来的宇宙之中，从而澄清了它。

注释 10.7。 这是拓扑斯语言在此处发挥作用的最深刻的概念性原因之一。它使我们能够将“存在相容的局部实现”与“存在一个单一的全局相干实现”视为数学上不同的陈述。这一区别将在后文发挥关键作用。

10.7 下降与重构

拓扑斯理论视角也解释了为什么扭子自然属于下降数学。

下降原理指出，全局对象可以由局部对象及与之相容的粘合数据重构而成。但这正是本讲义中对扭子的描述方式：作用群的局部副本通过过渡数据在交叠区域上相互比较，并满足余循环条件。

因此，扭子是基本的下降对象之一。它们的余循环描述就是下降数据，而根据相容余循环重构扭子，则是一种下降构造。拓扑斯是这一逻辑的自然背景，因为它旨在系统地处理局部数据与粘合。

备注 10.8. 因此，可以将情况概括如下：扭子不仅在群论中自然而然，也属于下降数学的范畴。它们的局部平凡性、过渡函数以及可能存在的整体扭曲，都是这样一个一般原理的具体体现：全局结构可以由相容的局部数据编码。

10.8 为什么这与后续定理密切相关

现在，我们可以更清楚地说明，为什么本节对于全面理解后续定理密切相关。

后续定理所讨论的并非仅仅是一个带有群作用的集合，而是关乎 t:

1. 与协议 Π 相关的景 (C_Π， J_Π)；2. 该景上的层拓扑斯 **Sh**(C_Π， J_Π)；3. 该拓扑斯中的群对象或群层 G_Π ； 4. 带有 G_Π 作用下的扭子结构的对象 F_Π ； 5. 局部平凡性以及整体截面可能不存在的情况。

若没有当前的视角，这样的陈述在形式上可能显得繁复。有了当前的视角，它便应显现为此前所探讨的所有主题的自然综合：局部性、粘合、传输、余循环、局部截面以及整体障碍。

注 10.9。 这就是为什么本节虽然在逻辑上并非必需，但对于希望深入理解后续应用的读者而言，在数学上几乎不可或缺。它提供了一种背景诠释，使后续定理的每个部分在概念上都显得自然而然。

10.9 启发式词典

对于 方便读者，我们再一次记录下主要的概念对应关系 e.

普通群 $\longrightarrow$拓扑斯中的群对象，普通扭子 $\longrightarrow$拓扑斯中的扭子对象，选定基点 $\longrightarrow$整体截面，局部基点 $\longrightarrow$局部截面，平凡化变换 $\longrightarrow$ 转移上闭链，整体平凡性 $\longrightarrow$存在整体截面，整体扭曲 $\longrightarrow$尽管局部平凡，却不存在整体截面。

这 ictionary并不能替代形式定义，但它是恰当的概念性指导 e.

10.10 总结

让我们总结一下本截面的主要内容。

1. 层拓扑斯 $\mathbf{Sh}(C, J)$ 是局部数据与粘合的自然宇宙。2. 群对象和扭子对象可以在该宇宙中以内在方式定义。3. 在层拓扑斯中，群层和层扭子是这些内在概念的具体外在形式。4. 整体截面表示整体一致的选择。5. 即使不存在任何整体截面，局部截面仍可能存在。6. 正是这种局部/整体区分，使扭子在后续应用中发挥作用。7. 因此，关于拓扑斯中扭子的论述，应理解为先前发展的初等扭子理论的自然内在版本。

下一节将回到本文的主线，更直接地说明这种扭子语言如何为后续关于密码学中 Σ-协议的概念性应用铺路。

11 面向 Σ-协议的应用

现在，我们从概念层面说明，前几节所发展的扭子观点为何与后续关于 Σ-协议的研究相关。本节的目的并非用扭子语言对协议理论进行完整的形式化，而是解释这种形式化为何自然而然，以及先前发展的数学思想为何为理解它提供了恰当的准备。

注记 11.1. 读者应谨记，本节主要旨在阐释动机。我们的目的是说明，如何运用扭子、局部平凡性、余循环以及局部截面与整体截面的语言，来梳理某些协议理论现象。完整的技术细节将在后续工作中展开。

11.1 从传输到协议结构

从最基本的层面来看，扭子是一个空间，其中相对位置具有意义，尽管并未选定优先原点。这自然让人联想到协议理论中的情形：给定某种结构化数据，可以在局部进行比较、变换或传输，但未必能将其归约为一个全局固定的标准形。

在 Σ-协议中，人们关注的是交互记录、见证、模拟行为，以及局部数据各部分之间的相容条件。扭子观点提示我们，有时不应将这类数据视为彼此孤立的代数令牌，而应视为某个空间中的点，并由适当作用下的传输来组织。从这一视角看，相关的数学问题不仅在于底层代数对象是什么，还在于其点是否存在局部参考选择、这些选择如何相互比较，以及它们能否在整体上粘合起来。

注 11.2. 这是前文强调传输首次发挥作用的地方。在扭子理论中，重要的从来不只是点的存在，更在于一个点与另一个点之间受控的关联方式。在协议情境中研究局部实现之间的结构化关系时，同样的逻辑便显得颇有启发性。

11.2 协议依赖层

层论观点启示了以下一般模式。对于协议 Π，可以尝试为其关联一个类层对象，使其在某个上下文区域上的截面表示局部可实现的记录数据，或局部相容的协议行为。“区域”的确切含义取决于具体应用：在后续研究中，它们通过适配该协议的景或格罗滕迪克拓扑来编码。

从概念上说，重要的是，人们不再仅仅通过单一的全局交互记录集合来研究协议。相反，人们研究的是一族变化的局部交互记录空间，连同限制映射与粘合条件。这样一来，协议结构便以层论的方式被组织起来，人们便可以开始追问：所得对象是否表现得像某个适当群层作用下的扭子。

备注 11.3. 这是通向后续定理的主要概念桥梁之一。这一转变是从“一个协议具有某些交互记录”转向“一个协议决定了一个局部记录数据的层”。一旦完成这一转变，挠子语言便可供使用。

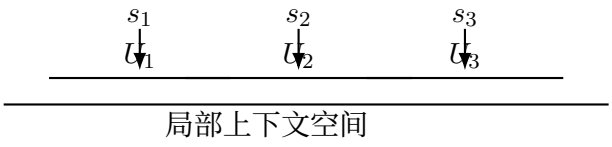
11.3 局部平凡性与模拟

该框架所提示的最自然的对应之一涉及局部平凡性。在挠子理论中，局部平凡性意味着，在每个足够小的区域上，该对象都容许一个局部截面，因而有一个局部基点，从而与作用群等同起来。

在协议理论的语境中，模拟数据发挥着类似的作用。粗略地说，模拟器在适当的局部上下文上提供一种特殊的记录数据表示方式，而无需经过某个全局固定的见证。这使得将模拟视为提供局部平凡化的对应物变得很自然。

更明确地说，可以将模拟器看作针对每个可接受的局部上下文生成一个局部一致的记录描述。这样的描述不必等同于一次性对所有记录数据进行基于全局见证的参数化。但它确实提供了一个局部参考表示，相关结构相对于该表示变得清晰起来。从这个意义上说，模拟器发挥着局部平凡化的作用：它为依赖于协议的对象提供一个局部坐标系，即使不存在单一的全局坐标选择。

图 8 以示意方式说明了这一类比。每个局部上下文 U_i 都携带一个局部模拟描述 s_i；这些局部描述发挥着局部截面或局部平凡化的作用。重要的并不是已经选择了一个单一的、基于全局见证的原点，而是拥有局部一致的参考数据。



局部模拟记录数据的作用类似于局部平凡化

图 8：这一类比的示意图：模拟器提供局部参考描述，发挥局部平凡化的作用。

从这个角度看，诚实验证者零知识体现了局部平凡性：该协议允许存在局部相容的模拟实现，它们充当相关类层对象的局部坐标系。扭子图景则表明，这些局部坐标系不必源自一个全局选定的参考点；它们可能只在局部存在。

注 11.4. 应从结构层面而非字面层面理解这种类比。模拟器并非以任何简单的集合论意义而言，本身就是层的一个截面。相反，它提供了这样一种

局部参照机制，使局部平凡性在概念上显得合理。扭子语言所捕捉的是局部参照数据、局部传输，以及整体相容平凡化可能失效的模式。

注释 11.5。 这正是前文如此着重强调局部截面的原因。局部截面不只是一个局部元素，它还是一个局部原点。在预期的应用中，模拟发挥着类似的作用：它提供局部参照数据，使相关的转录结构变得可理解，即使不存在基于全局见证的平凡化也是如此。

11.4 为什么层扭子恰到好处

此时，普通的集合论扭子为何不够，应该已经很清楚了。相关的协议理论现象并非纯粹是全局性的。它们涉及局部可实现性、对子上下文的限制、交叠处的相容性，以及整体相干性可能失效的情况。层扭子正是为处理这些特征而设计的。

层扭子可以用来表达：

1. 截面的局部存在性，
2. 在局部变化的对称性下唯一的局部传输，
3. 交叠区域上的过渡数据，
4. 整体截面可能不存在。

当在局部到整体框架中比较模拟与安全性时，人们恰恰会预期出现这种模式。

注释 11.6. 因此，从普通挠子转向层扭子并非出于技术上的奢求，而是预期应用的结构所必然要求的。一旦以层论的方式组织协议，自然的扭子概念便自动成为层论的扭子概念。

11.5 迈向层的拓扑斯中的扭子

加入可选的拓扑斯论部分，正是为了让下一步显得顺理成章。如果某个协议确定了一个景 (C_Π, J_Π)，那么我们便可以不只研究孤立的层，而是在整个拓扑斯中

$$\mathbf{Sh}(C_\Pi, J_\Pi).$$

在该拓扑斯中，接下来可以考虑：

- 一个与该协议相关的对象 F_Π ，
- 一个作用于 F_Π 的群对象或群层 G_Π ，
- F_Π 是 G_Π 下的扭子这一可能性。

到这时，诸如“F_Π 是 $(C_\Pi,\ J_\Pi)$ 上的层拓扑斯中的 G_Π 下的扭子”这样的表述就不再显得突兀了。这不过是本文所阐述的初等理论在层论和拓扑斯论中的延续：局部平凡性、传输、粘合，以及可能存在的整体障碍。

注 11.7。 这是本文主要的教学目标之一。读者若已读过前面的各节，此时应当能够将“层拓扑斯中的扭子”理解为“没有选定原点的群作用”的自然推广，而不是一种毫不相干的抽象构造。

11.6 启发式对照表

为便于后文使用，将扭子观点所揭示的概念对应关系概述如下：

普通挠子理论 协议论启发式 选定基点 选定的局部引用数据 局部截面 局部可实现性/局部模拟数据 整体截面 整体相容平凡化 局部描述之间的转移上闭链相容性数据 非平凡挠子 全局扭曲但局部平凡的结构

这份对照表有意采用启发式表述，但它揭示了托ors形式体系何以有用。它以一种普通的逐点语言无法做到的方式，组织起局部可实现性与整体相干性之间的关系。

11.7 后续定理的准备

为这些笔记提供动机的后续定理，可概略表述如下：在适当假设下，依赖协议的层状对象 F_{Π} 带有相应对称对象 G_{Π}下的扭子结构。其局部平凡性与模拟行为有关，而适当整体截面的缺失则反映了结构性安全约束。

本文并不证明该定理。本文旨在使这类定理变得容易理解。读完本文后，读者应当明白该陈述的各个部分为何顺理成章：

1. 为什么要将类层对象与局部协议数据联系起来；
2. 为什么局部传输意味着扭子结构；
3. 为什么局部平凡性对应着类似模拟的行为；
4. 为什么整体截面的存在与否很重要。

如果这一概念性铺垫已成功，那么后续定理看起来就不会像是任意的形式技巧，而会呈现为扭子、局部平凡性、余循环、层以及拓扑斯论粘合等基础数学内容的自然综合。

11.8 总结

让我们总结一下本节的目的。

1. 扭子语言有助于整理依赖协议的局部数据。2. 层论协议对象可能存在由模拟所暗示的局部平凡化。3. 整体截面对应于整体相干的平凡化。4. 这种整体相干性的缺失可能反映结构性安全约束。5. 因此，层拓扑斯中的扭子是后续研究 Σ-协议的自然语言。

下一节将总结本文所走过的数学路径，为全文作结：从群作用和仿射空间，到粘合、层扭子，以及为之后密码学中的应用所做的概念准备。

12 结论

这些笔记的主要目的，是为扭子提供预备性介绍，并着眼于其后续在密码学 Σ-协议中的应用。我们并未试图全面综述扭子在数学中的所有出现形式，而是聚焦于一条更具体的概念路径：从群作用和仿射空间，到局部平凡性、粘合数据、层扭子，以及局部截面与整体截面之间的对比。

最初的基本出发点很简单：扭子是一个非空集合，配备了自由且传递的群作用。等价地说，它是一个空间，其中每个点都可以通过唯一的群元素传输到其他任意一点。从这个角度看，扭子可以视为具有对称性但没有选定原点的空间。这也解释了为何仿射空间是基本模型：差是有意义的，而绝对位置则需要额外的选择。

随后我们强调，尽管这个基本定义至关重要，但它并未穷尽这一概念的含义。扭子不仅仅是由自由且传递的作用所定义的对象；它还是一种局部平凡、但可能在整体上非平凡的对象，因为它是通过粘合数据由局部片段拼合而成的。第二种观点至关重要。它解释了扭子为何自然地出现在几何、下降和局部到整体数学中，也表明，对于缺少优选基点这一点，应当作积极的理解：这反映了局部平凡化无法组合成一个典范的整体平凡化。

由此，余循环描述使粘合图景更加精确。扭子确定了交叠区域上的过渡数据，这些数据满足余循环恒等式；反过来，也可以利用相容的余循环重构扭子。这样，扭子便成为由局部比较数据编码的最简单、最清晰的全局对象范例之一。

接着，层论章节将这一图景拓展到与后续研究最相关的语境中。群层上的扭子由局部截面局部平凡，但未必存在任何整体截面。因此，局部存在性与整体存在性之间的区别——这一点在粘合观点中已隐约显现——由此在数学上得到了明确体现。可选的拓扑斯论部分旨在说明，这并非层所独有的偶然特征，而是拓扑斯内部更一般的局部到整体逻辑的一部分。

最后，我们概述了这种语言为何有助于思考 Σ-协议。重点并非取代此类协议通常采用的代数理论，而是构建一个概念框架，以便以层论的方式组织依赖于协议的对象，将局部平凡性与类似模拟的行为联系起来，并将适当整体截面的缺失视为结构性安全约束的体现。在这一语境下，某个依赖于协议的对象是层拓扑斯中的扭子这一说法，就不再显得突兀；它正是这些笔记中所发展的数学思想的自然延续。

如果本论述达到了预期目的，读者现在应该能够从两种互补的角度理解扭子。一方面，扭子是在群作用下具有唯一传递的空间。另一方面，它是一个局部平凡的对象，其整体形式由粘合所决定。这两种观点共同构成了后文层论的和密码学的应用所依据的数学背景，而这些应用正是本著作的动机所在。

参考文献

[1] J. Giraud，《非阿贝尔上同调》，数学科学基础丛书，第179卷，Springer-Verlag，柏林—纽约，1971。

[2] T. Inoué，格罗滕迪克拓扑与密码安全的层论基础：攻击者模型与作为第一步的 Σ-协议，arXiv:2602.17301 [cs.CR], 2026。

[3] J. S. Milne，平展上同调，《普林斯顿数学丛书》第 33 卷，普林斯顿大学出版社，新泽西州普林斯顿，1980。

[4] L. Schwartz，《分析学教程》第1卷，Hermann，巴黎，1981。

[5] Stacks项目作者，《Stacks项目》， `https://stacks.math.columbia.edu`。

[6] T. Szamuely，《伽罗瓦群与基本群》，剑桥高等数学研究丛书，第117卷，剑桥大学出版社，剑桥，2009。

[7] W.C. Waterhouse，《仿射群概形导论》，数学研究生教材，第66卷，Springer-Verlag，纽约–柏林，1979。

Takao Inoué
大和大学信息学部 日本 吹田市片山町2-5-1，大阪，
564-0082 inoue.takao@yamato-u.ac.jp（个人）
takaoapple@gmail.com（我更喜欢使用个人邮箱）

A 第 7 节习题的解答

本附录包含第 7 节习题的详细解答。目的不仅是记录正确答案，更是展示如何实际运用基本定义。读者尤其应注意自由作用、传递作用、扭子和传输子的定义反复发挥的作用。这些概念很简单，却支配着后续的一切。

1. **练习**。设 G 作用于一个集合 X。证明：当且仅当每个点的稳定子都是平凡的，该作用才是自由作用。

   解答。回顾定义。

   如果对每个 $x \in X$ 和每个 $g \in G$，该作用都是自由的，那么

   $$g \cdot x = x \Longrightarrow g = e.$$

   另外，点 $x \in X$ 的稳定子是

   $$G_x := \{g \in G \mid g \cdot x = x\}.$$

   首先假设该作用是自由的。固定 $x \in X$。若 $g \in G_x$，则由定义有 $g \cdot x = x$。由于该作用是自由的，这蕴含 $g = e$。因此 $G_x = \{e\}$。
   反之，假设对每个 $x \in X$都有 $G_x = \{e\}$。设对某些 $g \in G$和 $x \in X$有 $g \cdot x = x$。则 $g \in G_x$，故 $g = e$。因此该作用是自由的。
   因此，该作用是自由的当且仅当每个稳定子都是平凡的。

   评论。这是一个基础示例，展示了如何展开两个定义，并验证它们只是用不同的语言表达了同一件事。实际中，自由性通常通过计算稳定子来验证。

2. **练习**。 设 G 作用于集合 X。证明该作用是传递的，当且仅当 X由单个轨道组成。

解答。 回顾一下，如果对于每个 $x,\ y \in X$，都存在 $g \in G$使得该作用是传递的

$$g \cdot x = y.$$

此外， x 的轨道是

$$G \cdot x = \{g \cdot x \mid g \in G\}.$$

首先假设该作用是传递的。任取 $x \in X$。对于每个 $y \in X$，由传递性可知，存在某个 $g \in G$ 使得

$$g \cdot x = y.$$

因此 $y \in G\cdot\ x$。所以 X 中的每个点都属于 x的轨道，因此

$$X = G \cdot x.$$

因此 X 由单个轨道组成。
反过来，假设 X 由单个轨道组成。那么存在某个 $x \in X$ 使得

$$X = G \cdot x.$$

现在令 $y,\ z \in X$。由于 y和 z属于同一个轨道，因此存在元素 $g,\ h \in G$ 使得

$$y = g \cdot x, \qquad z = h \cdot x.$$

Then

$$z = h \cdot x = hg^{-1} \cdot (g \cdot x) = hg^{-1} \cdot y.$$

So z 可由 G中的某个元素作用于 y 得到。因此该作用是传递的 .

评论。 同样，这只是将同一个思想在两种表述之间进行转换：传递性意味着所有点彼此相通，而“一个轨道”恰好表达了这一点。

3. **练习**。 举出一个传递但不自由的作用的例子。

解答。 令群 G 作用于左陪集的集合 G/H，其中 $H \leq G$ 是一个非平凡子群。该作用由左乘给出：

$$g \cdot (aH) := (ga)H.$$

Thi该作用是传递的：给定任意两个陪集 aH 和 bH，满足条件的元素 $ba^{-1} \in G$ s

$$(ba^{-1}) \cdot (aH) = bH.$$

然而，如果 $H \neq\{e\}$，该作用就不是自由的。事实上，陪集 H 的稳定子恰好就是 H 。由于 H 是非平凡的，稳定子也非平凡，因此该作用不是自由的。

评论。 这个例子很重要，因为陪集作用是观察传递性而非自由性的标准方法之一。

4. 练习。 举出一个自由但不传递的作用的例子。

解答。 令 $G = \mathbb{Z}$ 通过在每个副本中平移，作用于由两个 $\mathbb{Z}$ 的副本构成的不交并 $X = \mathbb{Z} \sqcup \mathbb{Z}$ 上:

$$n \cdot (m, \varepsilon) := (n + m, \varepsilon),$$

其中 $\varepsilon \in \{0, 1\}$ 表示我们所在的副本。

这个作用是自由的：若

$$n \cdot (m, \varepsilon) = (m, \varepsilon),$$

then

$$(n + m, \varepsilon) = (m, \varepsilon),$$

那么 $n = 0$。

但它不是传递的，因为一个副本中的点无法移动到另一个副本中。因此至少存在两个不同的轨道。

评论。 这个例子表明，自由性是每个点处的局部条件，而传递性则是关于整个集合如何联结在一起的整体条件。

5. 练习。 设 G 在非空集合 X 上自由且传递地作用。直接证明，对于每个 $x,\ y \in X$ 都存在唯一的 $g \in G$ 使得

$$g \cdot x = y.$$

解答。 我们将用到假设的两个部分。

由于该作用是传递的，对于任意给定的 $x,\ y \in X$ 至少存在一个 $g \in G$ 使得

$$g \cdot x = y.$$

为证明唯一性，假设 $g,\ h \in G$ 都满足

$$g \cdot x = y, \qquad h \cdot x = y.$$

Then

$$h^{-1}g \cdot x = h^{-1} \cdot (g \cdot x) = h^{-1} \cdot y = x.$$

由于该作用是自由的，固定 x 的唯一元素是单位元。因此

$$h^{-1}g = e,$$

因此 $g = h$。

因此存在唯一这样的 g。

评论。 这道练习是挠子理论背后的关键计算。传递性保证传输的存在性，而自由性保证传输的唯一性。

6. 练习。 设 X 是一个 G-扭子，且设 $x_0 \in X$。证明该映射

$$\phi_{x_0} : G \to X, \qquad g \mapsto g \cdot x_0$$

是一个双射。

解答。由于 X 是一个扭子，该作用是自由且传递的。

为了证明满射性，设 $x \in X$。根据传递性，存在 $g \in G$ 使得

$$g \cdot x_0 = x.$$

因此， X 的每个点都属于 ϕ_{x_0}的像。

为了证明单射性，假设

$$\phi_{x_0}(g) = \phi_{x_0}(h).$$

Then

$$g \cdot x_0 = h \cdot x_0.$$

将 h^{-1} 作用于等式两边，

$$h^{-1}g \cdot x_0 = x_0.$$

由于该作用是自由的， $h^{-1}g = e$，因此 $g = h$。

因此， ϕ_{x_0} 是一个双射。

评论。这正是“选定一个基点后，扭子就变成群的一个副本”这一口号的精确数学内涵。

7. 练习。 设 X 是一个 G-扭子，且 x_0， $x_1 \in X$。若 $h \in G$ 是满足下式的唯一元素

$$h \cdot x_0 = x_1,$$

证明

$$\phi_{x_1}(g) = \phi_{x_0}(gh)$$

对所有 $g \in G$ 均成立。

解答。 根据定义，

$$\phi_{x_1}(g) = g \cdot x_1.$$

由于 $x_1 = h \cdot x_0$，这就变为

$$\phi_{x_1}(g) = g \cdot (h \cdot x_0) = (gh) \cdot x_0.$$

但右侧恰好是

$$\phi_{x_0}(gh).$$

So

$$\phi_{x_1}(g) = \phi_{x_0}(gh)$$

对所有 $g \in G$。

评论。 这明确展示了改变基点如何改变坐标描述：这两个识别相差一个群中的平移。

8. 练习。 设 X 是一个 G-扭子。证明传输子恒等式

$$\begin{aligned} \operatorname{tr}(x, x) &= e, \\ \operatorname{tr}(x, y)^{-1} &= \operatorname{tr}(y, x), \\ \operatorname{tr}(y, z)\operatorname{tr}(x, y) &= \operatorname{tr}(x, z). \end{aligned}$$

解答。 根据定义，$\mathbf{tr}(x, y)$ 是 G 中满足以下条件的唯一元素：

$$\operatorname{tr}(x, y) \cdot x = y.$$

对于第一个单位元， e 和 $\mathrm{tr}(x,x)$ 都将 x 映射到 x。根据唯一性，

$$\mathrm{tr}(x,x)=e.$$

对于第二个单位元，令

$$g=\mathrm{tr}(x,y).$$

于是 $g\cdot x=y$，所以

$$x=g^{-1}\cdot y.$$

因此 g^{-1} 将 y 映射到 x。根据唯一性，

$$g^{-1}=\mathrm{tr}(y,x).$$

So

$$\mathrm{tr}(x,y)^{-1}=\mathrm{tr}(y,x).$$

对于第三个单位元，令

$$g=\mathrm{tr}(x,y),\qquad h=\mathrm{tr}(y,z).$$

Then

$$g\cdot x=y,\qquad h\cdot y=z.$$

因此

$$(hg)\cdot x=h\cdot(g\cdot x)=h\cdot y=z.$$

所以 hg 将 x 映射到 z。根据唯一性，

$$hg=\mathrm{tr}(x,z).$$

也就是说，

$$\mathrm{tr}(y,z)\,\mathrm{tr}(x,y)=\mathrm{tr}(x,z).$$

评论。这些恒等式表明，传输子表现得像广义差：恒等元表示没有位移，逆元表示反向，乘法表示依次组合位移。

9. **练习**。设 A 是一个以向量空间 V为模型的仿射空间。证明 A 是加法群 $(V,+)$ 下的扭子。

解答。根据仿射空间的定义，存在一个作用

$$A\times V\to A,\qquad (a,v)\mapsto a+v,$$

满足：

(a) $a+0=a$，(b) $(a+v)+w=a+(v+w)$，(c) 对每个 a，$b\in A$，都存在唯一的 $v\in V$使得

$$a+v=b.$$

前两个性质说明 $(V,+)$ 作用于 A。第三个性质准确地说，对于每个a，$b\in A$，都存在唯一一个 $v\in V$，将 a 映射到 b。这恰好就是该作用自由且传递的条件。

因此，A 是加法群 $(V,+)$ 作用下的扭子。

评论。这是整篇笔记中最重要的例子。它是后续所有扭子思想的基本几何模型。

10. 练习。 设 $T: V \to W$ 是一个向量空间之间的线性映射，并设

$$S_w = \{v \in V \mid T(v) = w\}.$$

假设 S_w 非空。证明 S_w 是一个以 $\ker(T)$ 为模型的仿射空间 .

解答。 我们定义 $\ker(T)$ 在 S_w 上的平移作用：对于 $u \in \in \ker(T)$ 和 $v \in S_w$，令

$$v + u.$$

首先检查这样定义的结果仍属于 S_w。由于 $v \in S_w$，我们有 $T(v) = w$。又由于 $u \in \in \ker(T)$，我们有 $T(u) = 0$。因此

$$T(v+u) = T(v) + T(u) = w + 0 = w.$$

所以 $v + u \in S_w$。
现在验证仿射空间公理。显然

$$v + 0 = v, \qquad (v + u_1) + u_2 = v + (u_1 + u_2).$$

最后，设 v_1，$v_2 \in S_w$。那么

$$T(v_2 - v_1) = T(v_2) - T(v_1) = w - w = 0,$$

因此 $v_2 - v_1 \in \ker(T)$。此外，

$$v_1 + (v_2 - v_1) = v_2.$$

$\ker(T)$ 中的这个元素是唯一的，因为如果

$$v_1 + u = v_2,$$

则必然

$$u = v_2 - v_1.$$

因此 S_w 是以 $\ker(T)$ 为模型的仿射空间。

评论。 本练习很好地体现了一般原则：“解答相差齐次解。”

11. 练习。 设 G 是一个群，$H \leq G$ 是一个子群。证明每个左陪集 gH 是一个右 H-扭子。

解答。 在 gH 上定义 H 的右作用如下：

$$(gh_1) \cdot h_2 := g(h_1 h_2).$$

首先，这一定义是良定的，因为 gH 中的每个元素都具有 gh_1 的形式，而右乘 H 中的元素后仍属于 gH。
作用公理很容易验证：

$$(gh) \cdot e = gh, \qquad ((gh) \cdot h_1) \cdot h_2 = (gh) \cdot (h_1 h_2).$$

要证明传递性，任取两个元素 gh_1，$gh_2 \in gH$。于是

$$(gh_1) \cdot (h_1^{-1} h_2) = gh_2.$$

因此，任意一点都可以变换到其他任意一点。

为证明自由性，假设

$$(gh) \cdot h' = gh.$$

Then

$$ghh' = gh.$$

在左侧乘以 $(gh)^{-1}$，得到

$$h' = e.$$

因此，该作用是自由的。

因此， gH 是一个右 H-扭子。

评论。 陪集看起来像子群，但它没有指定的单位元。这就是为什么它是一个扭子，而不是典范意义上的群。

12. **练习。** 设 V 是一个有限维向量空间。证明， V 的有序基集合在 $\mathrm{GL}(V)$ 的作用下是一个扭子。

解答。 令$\mathcal{B}(V)$为 V的有序基集合。定义 $\mathrm{GL}(V)$ 在$\mathcal{B}(V)$上的作用如下:

$$g \cdot (v_1, \ldots, v_n) := (gv_1, \ldots, gv_n).$$

这确实是一个作用，因为单位映射固定每个基，而线性映射的复合对应于作用的复合。

为证明传递性，令

$$(v_1, \ldots, v_n), \qquad (w_1, \ldots, w_n)$$

为两个有序基。存在唯一的线性自同构 $g \in \mathrm{GL}(V)$，使得

$$g(v_i) = w_i$$

对所有 i 均成立。因此

$$g \cdot (v_1, \ldots, v_n) = (w_1, \ldots, w_n).$$

为证明自由性，假设

$$g \cdot (v_1, \ldots, v_n) = (v_1, \ldots, v_n).$$

于是，对于每个基向量 v_i，都有 $g(v_i) = v_i$。由于线性映射由其在一组基上的取值唯一确定，我们得出 $g = \mathrm{id}_V$。
因此，该作用是自由且传递的，所以 $\mathcal{B}(V)$ 是一个 $\mathrm{GL}(V)$-扭子。

评论。 这是几何中标架丛的原型。

13. **练习。** 设 X 是一个 G-扭子。固定一个点 $x_0 \in X$，并通过沿双射传输群运算，在 X 上定义一个二元运算

$$G \to X, \qquad g \mapsto g \cdot x_0.$$

证明这使得 X 成为一个群。然后证明所得的群结构取决于 x_0 的选择。

解答。 由于 X 是一个 G-扭子，映射

$$\phi_{x_0} : G \to X, \qquad g \mapsto g \cdot x_0$$

是一个双射。

在 X 上定义乘法，方式为

$$x * y := \phi_{x_0}\big(\phi_{x_0}^{-1}(x)\,\phi_{x_0}^{-1}(y)\big).$$

这是沿双射的标准结构传递。

因为 ϕ_{x_0} 是双射且 G 是群，立即可知 $(X, *)$ 是一个群：结合律、单位元和逆元均由 G 传递而来。

该群结构的单位元是

$$\phi_{x_0}(e) = x_0.$$

因此，选定基点成为单位元。

现在选择另一个基点 $x_1 \in X$。使用 x_1 重复同样的构造，会在 X 上产生另一种群运算，其单位元为 x_1。除非 $x_1 = x_0$，否则这两个单位元不同，因此这两种群结构也不同。

因此，群结构取决于基点的选择。

评论。 这是本笔记中最重要的概念性练习之一。它表明，扭子可以构成一个群，但这必须先进行非规范选择。

14. **练习。** 解释为什么前一个练习并不与“扭子不具有典范群结构”这一陈述相矛盾。

解答。 前一个练习仅表明，选定基点之后，可以将 G 的群结构传输到 X 上。但所得的群运算取决于该选择。

典范群结构应当由 X 自身内在地决定，而不需要任何额外选择。这正是扭子所缺少的。扭子具有足够的结构，可以通过传输比较各个点，但其结构不足以以一种优先的方式选出某个点作为单位元。

因此不存在矛盾：扭子可以具有许多种群结构，每个选定基点对应一种，但它并不携带典范群结构。

15. **练习。** 设 X 是一个 G-扭子。固定 $x \in X$，定义

$$d_x(y) := \mathrm{tr}(x, y).$$

证明 $d_x : X \to G$ 是一个双射。将其解释为由基点 x 确定的坐标系。

解答。 固定 $x \in X$。对于每个 $y \in X$，传输子 $\mathrm{tr}(x,\ y)$ 是将 x 发送到 y 的 G 中唯一元素。因此，映射

$$d_x : X \to G, \qquad y \mapsto \mathrm{tr}(x, y)$$

将每个点对应到其相对于基点 x 的位移。

为证明满射性，令 $g \in G$。由于作用定义在 X 上，点

$$y := g \cdot x$$

属于 X。根据传输子的定义，

$$\mathrm{tr}(x, y) = g.$$

因此， d_x 是满射。

为证明单射性，假设

$$d_x(y_1) = d_x(y_2).$$

Then

$$\mathrm{tr}(x, y_1) = \mathrm{tr}(x, y_2).$$

将两边作用于 x，得到

$$y_1 = y_2.$$

因此 d_x 是单射。

因此， d_x 是一个双射。

这是由基点 x确定的坐标系：每个点都由它相对于 x的唯一位移来描述。

评论。 这是映射 $\phi_x : G \to X$的传输子版本。一个映射从群元素到点，另一个则从点到群元素。

16. **练习**。 请用自己的话解释以下两个说法之间的区别：

(a) 选定一个基点后，扭子就能与一个群相识别；(b) 扭子典范地就是一个群。

解答。 第一个说法的意思是，一旦选定扭子中的一个点，就可以将该点用作原点，从而把扭子与作用群相识别。这种识别完全有效，但取决于所选的点。

第二个说法则意味着，扭子无需任何额外选择就具有内在的群结构，并且有一个点以自然的方式被指定为单位元。

因此，区别在于经过选择后的非典范识别与无需选择的内在结构之间的区别。扭子具有前一种性质，但一般不具有后一种性质。

17. **练习**。 为什么扭子的定义中包含非空性？如果允许空集，概念上会有什么问题？

解答。 扭子是这样一种空间，其中任意两个点都可以通过唯一传递进行比较。如果一个点也没有，这种基本直觉便不复存在。

形式上，若允许空集存在，某些条件可能会因空真而成立，但由此得到的对象便不再配称为这里所说的扭子。它没有基点、没有传输子、没有局部坐标，也无法比较点。

在后续的层论中，这一点尤为重要，因为我们会仔细区分截面的局部存在性与截面的整体存在性。扭子的通常定义以一个确实含有元素的空间为起点。

18. **练习**。 写一小段文字，说明为什么仿射空间是扭子一般理论的最佳入门模型。

解答。 仿射空间是理解扭子的最佳入门模型，因为它们在最熟悉的情境中体现了核心思想：我们可以通过差来比较点，却没有典范指定的原点。作用群就是底层向量空间的加法群，因此扭子结构很容易通过平移来直观理解。

与此同时，仿射空间已经展现了扭子的关键非典范特征：选定一个点，就能将仿射空间与向量空间等同起来，但这种选择并非内在的。因此，仿射空间为「没有选定原点的对称性」这一一般概念提供了具体的几何原型。

B 建议的讲座计划

本附录提出一种可能的方案，说明如何将这些讲义用于一门短期讲座课程。该计划面向每次约 90 分钟的课程。这仅仅是一项建议：视听众情况而定，可以将材料压缩到更少的课次，也可以放慢进度，安排更多习题。

一种自然的标准安排是九讲课程。前半部分讲解扭子的初等理论，后半部分则转向局部平凡性、粘合、层扭子，以及通往后续应用的概念桥梁，其中涉及 Σ-协议。

B.1 九讲计划

1. **引言；群作用与轨道**。介绍这些讲义的总体目标。回顾群作用、轨道和稳定子，重点说明点与点之间传输的思想。2. **自由且传递的作用；扭子的定义**。

解释自由且传递的作用为何是关键结构。正式引入扭子，并讨论“没有选定单位元的群”这一说法。

3. **基础例子 I：仿射空间**。
将仿射空间作为贯穿始终的例子来展开。强调点与差之间的区别，并解释这一视角为何对几何和分析有用。

4. **基础例子 II：基点、差与传递子**。讨论线性方程组的解集、陪集和基的集合。然后解释基点、非典范的识别以及传递子恒等式。5. **基础理论习题**。

完成第 7 节中的精选习题。在这一阶段，特别有必要强调定义在实践中的用法。附录中的解答可作为辅助材料。

6. **局部平凡性与粘合数据**。介绍扭子的第二个主要视角：它们是局部平凡但整体上可能并不平凡的对象。解释过渡数据和基本的粘合思想。7. **余循环描述与重构**。阐述过渡函数、余循环恒等式、余循环的等价性，以及如何根据余循环数据重构扭子。8. **层扭子、局部截面与整体截面**。

转向群层下的扭子。强调局部截面与整体截面之间的区别，并说明为什么整体平凡性比局部平凡性要求更强。

9. **托扑理论视角概览；迈向 Σ-协议**。
介绍可选的拓扑斯论视角，尤其适合基础较强的学生。接着解释扭子观点如何为后续将其应用于密码学中的 Σ-协议奠定基础。最后总结整门课程。

B.2 可能的变体

对于较短的课程，可以合并第3讲和第4讲，并精简可选的拓扑斯理论材料。这样便形成压缩的七讲制形式。

对于进度较慢或程度较高的课程，可以将第5讲扩展为完整的习题课，并对层论和拓扑斯论的部分进行更深入的讲解。如此一来，这些材料完全可以支撑十讲或更多讲。

B.3 教学说明

本讲义的一个核心教学目标，不只是让读者掌握定义，还要让读者了解这些定义如何应用。因此，习题及其详细解答是课程设计中不可或缺的一部分。它们旨在帮助学生从对定义的形式化熟悉，逐步迈向真正理解并能实际运用。

B.4 一种可能的延续：关于作者后续论文的六讲

本讲义的编写不仅是为了提供一份自成一体的入门材料，也是为了给作者后续的研究工作提供预备背景。因此，一种自然的使用方式是采用以下十五讲制形式：前九讲以本讲义为基础，随后六讲专门讲授后续论文 [2]。

在这种安排下，前九讲将介绍后续理论所需的数学语言：群作用、扭子、仿射空间、局部平凡性、粘合数据、余循环、层扭子，以及基本的拓扑斯理论视角。接下来的六讲则将阐释这些思想如何用于 Σ-协议的层论解释。

B.5 十五讲计划

第1–9讲。 这就是上文所述的九讲预备课程。

第10讲：动机及后续论文的整体概述。 说明后续工作的总体目的。为什么要以层论的方式组织协议论数据？为什么局部性很重要？从普通转录集合转向景上的层，有何裨益？本讲应帮助学生认识到，后续论文并非与此前内容无关的抽象理论，而是前九讲所学内容的自然延续。

第11讲：与协议关联的景。 介绍附属于协议 Π的景(C_Π, J_Π)。说明其对象和态射的含义，尤其是覆盖的作用。教学的主要目的是阐明“局部性”在协议论背景下的含义，以及为什么格罗滕迪克拓扑是对其进行编码的恰当形式化工具。

第12讲：依赖协议的层。 阐述类层对象 F_Π 的构造。解释其截面所表示的内容、限制映射如何解释，以及层论粘合为何相关。本讲应阐明，人们不再研究孤立的交互记录，而是研究一个按相容性组织的局部协议数据系统。

第13讲：对称对象及其作用。 引入相应的群对象或群层 G_Π，并解释其如何作用于 F_Π。此时，应鼓励学生将这一形式体系与此前关于普通挠子和层扭子的理论联系起来。主要目标是让挠子断言在结构上显得自然而非出人意料。

第14讲：扭子定理与证明策略。 陈述并解释后续论文中的主要扭子定理。讨论局部平凡性所起的作用、它与模拟的关系，以及缺乏适当整体截面的重要意义。如果证明对于单次讲课而言过长，可以给出证明概要，并提炼出关键思想：将局部截面视为局部平凡化、在对称对象作用下进行传输，以及将整体障碍视为一种结构性特征。

第15讲：结构性诠释与进一步方向。 解释由此得到的安全性质诠释，包括局部平凡性与诚实验证者零知识之间的关系，以及整体障碍与可靠性类型现象之间的关系。最后讨论可能的扩展方向，例如更一般的协议、更丰富的拓扑，或层论与拓扑斯论方法在密码学中的更广泛应用。

B.6 十五讲制形式的教学价值

这种十五讲制形式具有明显的概念优势。前九讲提供了纯粹的数学基础，使学生逐步熟悉扭子这一概念的更复杂形式：从仿射空间和群作用，到粘合数据、余循环、层扭子和拓扑斯。随后六讲则展示，这些概念并非只是形式上的一般性概念，而是能够切实组织密码学结构的工具。

这样一来，后续论文便不必作为一篇孤立的高深文本来讲授，而可以被视为扎实数学背景的自然应用。这使后续定理的概念内容更容易理解。

B.7 给授课教师的一个实用说明

对于数学素养较高的听众，这门十五讲的课程几乎可以完全按照此处的写法讲授。对于经验较少的听众，放慢第8—11讲的进度可能会有所帮助，因为从初等扭子过渡到层扭子，再过渡到景上的层，正是抽象程度提升最为显著的阶段。

在课程的后半部分，明确回顾前半部分的内容也很有帮助。例如：

- 后文中的局部截面应与层扭子中的局部基点进行比较；
- 协议相关的转移数据应与第8节和第9节中的余循环进行比较；
- 缺少合适的整体截面，应与扭子的整体平凡性失效进行比较。

这类提示有助于学生看到，后续理论确实是建立在先前理论之上的。

B.8 最终教学说明

因此，本课程背后的整体教学策略是循序渐进的。前九讲训练读者将扭子理解为空间中的传输、局部平凡对象以及全局粘合结构。最后六讲则展示如何在层论的和拓扑斯论的框架中，运用这种数学语言重新诠释协议论概念。事实上，这正是本讲义预期的主要用途之一。

C 基本术语词汇表

本术语表仅旨在作为本讲义通篇所用主要术语的快速指南。其中的解释较为非正式，意在帮助读者回顾每个概念在本文论述中的作用。

仿射空间。 一个以向量空间为模型的非空集合，其中可以将向量加到点上，也可以将两点相减得到向量，但没有典范选定的原点。在这些讲义中，仿射空间是扭子的典型例子。

基点。 扭子中选定的一个点。选定基点后，扭子便与作用群相认同，但这种认同不是典范的。**余循环**。 交叠区域上的一套相容过渡数据。对于扭子，余循环记录了局部平凡化之间的差异，以及它们如何粘合成一个全局对象。**下降**。 一种一般原理：可以从局部对象及其相容的粘合数据重建全局对象。扭子是下降对象的基本例子之一。**自由作用**。 一种群作用，其中没有非单位元群元素会固定任何点。等价地说，每个稳定子都是平凡的。

整体截面。 层或类层对象的一个全局定义的截面。对于层扭子，整体截面给出一个整体平凡化。

粘合数据。 用于规定如何在交叠区域上识别局部平凡片段的数据。对于扭子，这通过过渡元素或余循环来表达。

群作用。 群 G 对集合或对象 X的作用，描述 G中的元素如何移动 X中的点。

群对象。 群在拓扑斯等范畴中的内部版本。在层拓扑斯中，群对象对应于群层。

局部截面。 仅在局部区域上定义的截面。对于层扭子，局部截面起到局部基点的作用。

局部平凡性。 对象在限制到足够小的区域后变为平凡的性质。对于扭子，这意味着它们在局部看起来像作用群。

Orb轨道。 在群作用下，从给定点可到达的点的集合。

主齐性空间。 扭子的另一种称呼。这一术语强调，在该作用下每个点看起来都一样，并且没有首选原点。

群层。 一种层，其在每个开集上的截面构成一个群，且限制映射由群同态给出。

层扭子。 群层下的扭子。它局部非空，且局部自由且传递，但可能没有整体截面。

稳定子。 对于群作用下的点 x ，由所有固定 x 的元素构成的子群。

拓扑斯。 一种广义空间或局部数据构成的数学宇宙，例如景上的层范畴。在这些笔记中，拓扑斯为层扭子及后续应用提供了自然的背景。

扭子。 一个非空对象，其上有群的自由且传递的作用；更一般地，也可以是群层的自由且传递的作用。扭子可以理解为一个具有对称性却没有选定原点的空间。

传递作用。 一种群作用，其中每个点都可以被移动到其他任意点。等价地说，该作用只有一个轨道。

传输子。 对于扭子中的两个点 x，y，将 x 映射到 y 的唯一群元素。它起到广义差的作用。