arXiv:2611.33073v1 [math.NT] 24 Nov 2026

Sawin–Wood 测度模型的全局域非分歧伽罗瓦群的性质

Mark Shusterman Gonen Zimmerman

摘要

我们证明，对于 Sawin–Wood 测度 $\nu_{\Gamma,\,n,\,U}$，在 pro-$|\Gamma|'$ Γ-范畴中几乎必然有限生成且具有有限表示，其中 Γ 是一个非平凡有限群，n 与 $|\Gamma|$ 互素，U 是 Γ 的共轭类构成的非空多重集。随机群 X 的 Γ-生成元秩具有如下精确的尾部

$$\mathbf{P}(d_\Gamma(X) \geq r) = Ce^{-\kappa r^2-\zeta r}\big(1+O(e^{-\varepsilon r})\big),$$

其中，$C>0$、$\kappa>0$ 和 $\zeta\in\mathbb{R}$ 是取决于 n，Γ、U 和 $\varepsilon>0$ 的显式常数。几乎必然，X 具有一个使用最少数量 Γ 生成元的表示，并且其定义 Γ 关系的数量至多比生成元多 $|U|$ 个。我们还证明，在对于 Γ 的每个复表示，都存在 U 中的某个元素固定一个非零向量这一假设下，X 的每个开子群几乎必然具有有限交换化。最后，当 $n=1$、Γ 为循环群，且 U 仅包含 Γ 的一个生成元的共轭类（重数为一）时，我们证明 $H_2(X,\,\mathbb{Z})=0$ 几乎必然成立。

目录

1 引言与基本符号 2

1.1 ChatGPT 的使用.5 1.2 致谢.5

2 定义概率测度 5

2.1 可测性与平凡情形. . 6

3 尖锐尾定理的证明 7

3.1 尖锐尾部渐近中的常数.7 3.2 计算$\mathbf{P}(d_\Gamma(X^{\mathrm{ab}}) \geq r)$ 的渐近.9 3.3 为 $d_\Gamma(X)\geq r$ 构造有限商群.13 3.4 具有阿贝尔底的非阿贝尔见证的二次指数间隙 . . . . . 19 3.5 限定完整生成元秩尾部与阿贝尔生成元秩尾部之间的差异 . . . 21 3.6 尖尾证明的完成.24

4 几乎必然的有限表示与亏格 25

4.1 具有正概率的有限商群.25 4.2 一致有限层上同调界.26 4.3 过渡到有限剩余群.27 4.4 关系秩及其推论.27

5 在表示论假设下几乎必然 FAb 28
5.1 在固定素数处的界.31 5.2 跨素数界.36 5.3 FAb 定理的证明.38

6 二阶上同调的结构 39
6.1 增广模与结构定理.39 6.2 上同调界.40 6.3 结构定理的证明.41 6.4 消失推论.43

1 引言与基本记号

Sawin–Wood 测度 $\nu_{\Gamma,\,n,\,U}$ 对伽罗瓦扩张 $K/\mathbb{Q}$ 的最大非分歧 pro-$|\Gamma|'$扩张的伽罗瓦群进行建模，其中 Gal($K/\mathbb{Q}$) $\cong\Gamma$，并令 K 变化。这里 $n=\quad^{2\,\gcd(|\Gamma|,\,2)}$，而$U$ 由 Γ中的复共轭的共轭类组成（如果 K 是全实的，则为单位共轭类）。更多详情请参见 [8]。我们在 Pagano 和 Shusterman [7], 的工作基础上展开研究；他们运用冠理论，证明了 Sawin–Wood 模型及其他相关随机有限剩余群模型几乎必然有限生成。

这些有限生成与有限表示结果的动机，尤其源自 Shafarevich [2]长期以来提出的一个问题。对于数域 K 和由有限处组成的有限集 S，设 K_S/K 为在S之外的每个有限位置均非分歧的最大伽罗瓦扩张，并令$G_{K,\,S}$=Gal(K_S/K)。$G_{K,\,S}$ 是否拓扑有限生成? 其中，$S=\varnothing$ 这一情形，即不允许任何有限位置发生分歧，与本文尤为相关。

众所周知，Shafarevich 问题的函数域类比在非分歧情形下有肯定答案。结合 Shusterman [1] 和 Liu [5, 定理 1.2], 的结果可知，对于任意整体域 K，$G_{K,\,\varnothing}$ 的拓扑有限生成蕴含有限表示。因此，有限生成和有限表示正是我们的几乎必然结果为其提供概率类比的两个算术有限性问题。

固定一个有限群 Γ、一个满足 $(n,\ |\Gamma|)=1$ 的正整数 n，以及一个非空的由 Γ 的共轭类组成的有限多重集U。若 $\Gamma=1$，则测度 $\nu_{\Gamma,\,n,\,U}$ 集中在平凡群上（见第 2.1 节）。在这种情况下，有限性和同调消失的结论显然成立。以下我们假设 $\Gamma\neq 1$。

本文采用 Sawin 和 Wood 在 [8, 定理 1.8] 中提出的存在性假设：对每个素数 $p\mid n$，以及每个非零有限维 $\mathbb{F}_p[\Gamma]$-模 V，都存在$v\in V-\{0\}$ 和 $\gamma_E\in E\in U$，使得 $v^{\gamma_E}=v$。当 $n=1$时，这个不动向量条件是空泛的，但我们仍然假设 $U\neq\varnothing$。

Γ-群是带有 Γ 通过自同构作用的群；在有限剩余情形下，该作用是连续的。Sawin–Wood模型中出现的所有有限 Γ-群，其阶都与$|\Gamma|$互素；所考虑的所有有限剩余 Γ-群都是此类有限 Γ-群的逆极限。若一个有限剩余群的每个指数都只对应有限多个开子群，则称它为小群。若 $\gamma\in\Gamma$，记 G^{γ} 为不动点子群。为 U中出现的每个共轭类 E选取一个代表元 γ_E，并保留重数，然后定义不动点权重

$$w_U(G):=\frac{\prod_{E\in U}|G^{\gamma_E}|}{|G^{\Gamma}|}.$$

这是一个与所选代表元无关的正有理数；乘积在 U中计入重数。它是 [8, 定理 1.8]中的群因子。 G 上的 n-定向是 $H_3(G,\mathbb{Z}/n)^\Gamma$的一个元素。尽管下文陈述的结果涉及的是底层群，这一定向仍会出现在定义矩以及第二同调结果的证明中。

对于一个定向的有限剩余 Γ–群 $\boldsymbol{X}=(X,\ s_X)$ 和一个有限定向 Γ–群 $\boldsymbol{H}=(H,\ s_H)$，记 $\mathrm{Sur}_{\mathrm{or}}(\boldsymbol{X},\ \boldsymbol{H})$ 为满足条件 $f_*s_X=s_H$ 的连续 Γ–等变满同态 $f\colon X\twoheadrightarrow H$ 的集合。除非另有说明，Hom 和 Sur 分别表示有限生成范畴中的连续同态集和连续满同态集，包括其等变版本。Sawin–Wood 测度 $\nu_{\Gamma,\ n,\ U}$ 是定义在小型有限剩余 n–定向 pro-$|\Gamma|'$ Γ–群的同构类上的唯一概率测度，其矩由以下条件刻画：对于每个有限 n–定向 Γ–群 $\boldsymbol{H}=(H,\ s_H)$，若 $(|H|,\ |\Gamma|)=1$，

$$\mathbf{E}_{\boldsymbol{X}\sim\nu_{\Gamma,n,U}}\left|\mathrm{Sur}_{\mathrm{or}}(\boldsymbol{X},\boldsymbol{H})\right|=\begin{cases}\dfrac{|H^2(H\rtimes\Gamma,\mathbb{Z}/n)|}{|H^3(H\rtimes\Gamma,\mathbb{Z}/n)|\,w_U(H)}, & H_\Gamma=1,\\ 0, & H_\Gamma\neq 1.\end{cases}$$

这里 $\mathbb{Z}/n$ 具有平凡的 $H\rtimes\Gamma$–作用。在上述假设下，存在性与唯一性由 [8, 定理 1.8] 得出。在全文中，$\mathbf{E}$ 和$\mathbf{P}$ 分别表示关于该测度的期望和概率。

对于有限或 pro有限 Γ-群 G，令 $d_\Gamma(G)$ 为一个集合的最小基数，使得其 Γ-轨道生成 G（在概形有限情形下按拓扑意义生成）；若不存在这样的有限集合，则令 $d_\Gamma(G)=\infty$。除非明确提及定向，以下陈述中的随机变量均为样本 $\boldsymbol{X}=(X,\ s_X)$ 的底层 Γ-群。

以下所有表示秩均取自在 pro-$|\Gamma|'$ Γ-群范畴中。

令 $F'_m(\Gamma)$ 为由 m Γ 个生成元生成的自由 pro-$|\Gamma|'$ Γ-群。因此，它是由符号 $x_{i,\ \gamma}$ 生成的自由有限剩余群的最大 pro-$|\Gamma|'$ 商群，其中 $1\le i\le m$ 和 $\gamma\in\Gamma$，且 $\sigma(x_{i,\ \gamma})=x_{i,\ \sigma\gamma}$。对于一个由有限个 Γ 生成元生成的 pro-$|\Gamma|'$ 群 H 以及一个整数 $m\ge d_\Gamma(H)$，选取一个 Γ-等变满同态

$$\pi: F'_m(\Gamma)\twoheadrightarrow H,$$

并考察将核 π 作为$F'_m(\Gamma)$的闭正规 Γ子群生成所需的最少元素数。对于固定的 H 和 m，根据 [5, 命题 3.4] 中的关系模计算，以及在环境作用 $F'_m(\Gamma)\rtimes\Gamma$ 下应用的 [6, 定理 3.1],中的正规生成论证，该数与 π 的选取无关（平凡核的情形成立，因为有限生成 pro有限群的每个连续满自同态都是自同构）。记作$r_{\Gamma,m}(H)$。若 $H_\Gamma=1$，则$r_{\Gamma,m}(H)-m$ 与 $m\ge d_\Gamma(H)$无关。记

$$r_\Gamma(H):=r_{\Gamma,d_\Gamma(H)}(H).$$

采用生成元减关系约定，定义相对亏格如下：

$$\mathrm{def}_\Gamma(H):=d_\Gamma(H)-r_\Gamma(H).$$

对于 $H_\Gamma=1$，这也等于 $\sup_{m\ge d_\Gamma(H)}(m-r_{\Gamma,m}(H))$。

定理 1.1. 令 $\mathcal{I}$ 为非平凡不可约 $\mathbb{F}_p[\Gamma]$-模的同构类集合，其中 p 遍历不整除 $|\Gamma|$的素数。对于 $V\in\mathcal{I}$，令

$$q_V=|\operatorname{End}_\Gamma(V)|,\qquad \tau_V=\dim_{\operatorname{End}_\Gamma(V)}V,\qquad u_V=\sum_{E\in U}\dim_{\operatorname{End}_\Gamma(V)}V^{\gamma_E}.$$

将 $V^\vee = $同态集$\mathbb{F}_p(V, \mathbb{F}_p)$ 记作对偶 Γ-模，并令

$$\eta(q) = \prod_{j=1}^{\infty}(1 - q^{-j}).$$

对于 $p \nmid n$ 或 $V \not\simeq V^\vee$，设

$$a_V = 1, \qquad b_V = u_V, \qquad c_V = \eta(q_V)^{-1}.$$

对于 $p \mid n$ 和 $V \simeq V^\vee$，改设

$$\lambda_V = \log_{q_V}\left|\mathrm{Hom}_\Gamma\left(\bigwedge\nolimits^2_{\mathbb{F}_p} V, \mathbb{F}_p\right)\right|,$$

$$a_V = \tfrac{1}{2}, \qquad b_V = u_V + \tfrac{1}{2} - \lambda_V, \qquad c_V = \left[\eta(q_V)\prod_{j=0}^{\infty}(1 + q_V^{-j-u_V-1+\lambda_V})\right]^{-1}.$$

现在，在这两种情况下，定义

$$\kappa_V = a_V\tau_V^2\log q_V, \qquad \zeta_V = \tau_V\big(b_V - 2a_V(\tau_V - 1)\big)\log q_V,$$

并令

$$\kappa = \min_{V\in\mathcal{I}}\kappa_V, \qquad \mathcal{M} = \{V \in \mathcal{I} : \kappa_V = \kappa\}, \qquad \zeta = \min_{V\in\mathcal{M}}\zeta_V,$$

$$C = \sum_{\substack{V\in\mathcal{M}\\ \zeta_V=\zeta}} c_V q_V^{b_V(\tau_V-1)-a_V(\tau_V-1)^2}.$$

设 X 服从分布 $\nu_{\Gamma,n,U}$。则 $\kappa > 0$、 $\zeta \in \mathbb{R}$和 $C > 0$；此外，存在$\varepsilon > 0$，它仅取决于 Γ、 n、U，使得当整数 r趋于无穷时，

$$\mathbf{P}\big(d_\Gamma(X) \geq r\big) = Ce^{-\kappa r^2-\zeta r}\big(1 + O_{\Gamma,n,U}(e^{-\varepsilon r})\big). \tag{1.1}$$

对于 $\mathbf{P}(d_\Gamma(X) = r)$，同样的渐近关系也成立。特别地， X 以概率 *1* 是一个拓扑有限生成的 Γ-群。

定理 1.2. 令 X 服从分布 $\nu_{\Gamma,\ n,\ U}$。以概率 *1*， $d_\Gamma(X)$ 是有限的，并 d

$$r_\Gamma(X) \leq d_\Gamma(X) + |U|. \tag{1.2}$$

特别地， X 是有限表示的 *pro*-$|\Gamma|'$ Γ-群，并且

$$\mathrm{def}_\Gamma(X) \geq -|U|.$$

定理 1.2 的证明见第 4 节。有限表示的结果用到了 Liu 和 Lubotzky 在[5, 6]中证明的关于第二上同调的亏格界。

开子群的有限交换化这一动机源于以下事实：对于任意数域 K 和任意有限扩张 L/K，使得 $L \leq K^{ur}$，根据类域论和闵可夫斯基定理，$\mathrm{Gal}(K^{ur}/L)$ 的阿贝尔化是有限的。

定理 1.3。 设 X 具有分布 $\nu_{\Gamma,\, n,\, U}$。假设每个非平凡不可约复Γ-模 W 都满足

$$\sum_{E\in U} \dim_{\mathbb{C}} W^{\gamma_E} > 0.$$

那么，以概率 *1*，每个开子群 $H \leq X$ 都有有限交换化 .

^对于下一个结果， $H_2(X,\ \mathbb{Z})$ 表示具有紧系数和琐凡 X-作用的连续同调。

定理 1.4。 设 X 具有分布 $\nu_{\Gamma,\, n,\, U}$。假设 $n = 1$, Γ 是循环的，且 U 仅包含 Γ的一个生成元的共轭类（重数为一）。那么

$$\mathbf{P}\big(H_2(X, \widehat{\mathbb{Z}}) = 0\big) = 1. \tag{1.3}$$

定理 1.3 和定理 1.4 的证明分别见第 5 节和第 6 节。在数域情形中，定理 1.4 的假设迫使 Γ 为阶恰好等于 2 的循环群。事实上，由于 U 的代表元阶数至多为二（与阿基米德位置相关的上同调类便是如此），该假设特化为 $(\Gamma,\ n,\ U) = (C_2,\ 1,\ \{[\sigma]\})$，其中 $\sigma \neq 1$。

问题 1.5。 在定理 *1.3* 的假设下，以下结论是否成立？

$$\mathbf{P}_{\nu_{\Gamma,n,U}}\big(X\ \textit{has an open pronilpotent subgroup}\big) = 1\,?$$

受问题 1.5 的启发，也可以针对数域提出类似的问题。

问题 1.6. 设 $K/\mathbb{Q}$ 是一个实二次扩张，且 L/K 是其在每个有限位置均非分歧的最大奇数阶 *pro-* 伽罗瓦扩张。$\mathrm{Gal}(L/K)$ 是否必然包含一个原幂零开子群？

1.1 ChatGPT 的使用

GPT6 已用于协助构思陈述、猜想和证明。

1.2 致谢

Mark Shusterman 担任 A. Edward Friedmann 数学职业发展讲席教授。作者受到欧盟（欧洲研究委员会，函数域，101161909）的资助。

这项工作部分得到了通过 ChatGPT 学术研究者计划使用 OpenAI 模型的资助。

我们感谢 Carlo Pagano 与我们进行了富有帮助的交流。

2 定义概率测度

Sawin 和 Wood 在小的有限剩余 n-定向 Γ-群 $\boldsymbol{X} = (X, s_X)$ 上定义了 $\nu_{\Gamma,n,U}$。我们既使用这种定向概率律，也使用其到基础 Γ-群 X 的推前。我们先从定向矩公式推导出基础矩公式。

命题 2.1. 对于每个阶与 $|\Gamma|$ 互素的有限 Γ-群 H ，

$$\mathbf{E}\big|\mathrm{Sur}_\Gamma(X,H)\big| = \begin{cases} \dfrac{|H^2(H\rtimes\Gamma,\mathbb{Z}/n)|}{w_U(H)}, & H_\Gamma = 1, \\ 0, & H_\Gamma \neq 1. \end{cases} \tag{2.1}$$

因此， X 中商群Γ同构于 H 的开正规 Γ稳定子群的期望数量满足

$$\mathbf{E}\#\{N \trianglelefteq X : N \text{ open and } \Gamma\text{-stable}, X/N \simeq_\Gamma H\} = \frac{\mathbf{E}|\,\mathrm{Sur}_\Gamma(X,H)|}{|\,\mathrm{Aut}_\Gamma(H)|}. \tag{2.2}$$

这一期望也给出了存在此类商群的概率的上界。存在一个测度为一的集合，在该集合上，每个有限的 Γ商群 H 都满足 $H_\Gamma = 1$。在同一集合上， $X_\Gamma = 1$。

证明。令 $\boldsymbol{X} = (X, s_X)$。对于每个底层的 Γ满射 $f\colon\ X \twoheadrightarrow H$，在 H上恰有一个定向，即 $f_* s_X$，使得 f 保持定向。因此

$$|\,\mathrm{Sur}_\Gamma(X,H)| = \sum_{s\in H_3(H,\mathbb{Z}/n)^\Gamma} |\,\mathrm{Sur}_{\mathrm{or}}(\boldsymbol{X},(H,s))|.$$

由 [8, 定理 1.8],

$$\mathbf{E}\big|\mathrm{Sur}_{\mathrm{or}}(\boldsymbol{X},(H,s))\big| = \mathbf{1}_{H_\Gamma=1}\frac{|H^2(H\rtimes\Gamma,\mathbb{Z}/n)|}{|H^3(H\rtimes\Gamma,\mathbb{Z}/n)|\,w_U(H)}.$$

Thus

$$\mathbf{E}\big|\mathrm{Sur}_\Gamma(X,H)\big| = \mathbf{1}_{H_\Gamma=1}\frac{|H_3(H,\mathbb{Z}/n)^\Gamma|\,|H^2(H\rtimes\Gamma,\mathbb{Z}/n)|}{|H^3(H\rtimes\Gamma,\mathbb{Z}/n)|\,w_U(H)}.$$

由 [8, 引理 5.4 和 5.5] （参见 [8, 引理 4.7]的证明），

$$|H_3(H,\mathbb{Z}/n)^\Gamma| = |H^3(H\rtimes\Gamma,\mathbb{Z}/n)|.$$

这些因子相互抵消，从而证明了 (2.1)。

每个满足 $X/N \simeq_\Gamma H$ 的开正规 Γ-稳定子群 N 都恰好是Γ-等变满射 $X \to H$ 的核，其中 $|\mathrm{Aut}_\Gamma(H)|$: 这些满射对应于 Γ-同构 $X/N \to H$，而这些同构彼此相差一个唯一的 Γ-自同构的后复合，其中 H。按核对满射计数，再除以 $|\mathrm{Aut}_\Gamma(H)|$，并取期望，即得 (2.2)。

根据马尔可夫不等式，商群计数为正的概率至多等于其期望。

最后，有限 Γ-群在同构意义下至多可数。满足 $H_\Gamma \neq 1$ 的零矩商事件之并的测度为零。非平凡的有限剩余商群 X_Γ 必有一个非平凡的有限商群，其 Γ 作用平凡，这与上述结论矛盾。因此，在同一个满测度集上有 $X_\Gamma = 1$ 。

□

2.1 可测性与平凡情形

本文所讨论的有限商事件和生成元秩事件都是可测的。前者是 Sawin–Wood 空间中有限层商事件在各种定向下的有限并，下面的引理表明，后者是前者的可数并。

引理 2.2。 对于每个有限剩余 Γ-群 Y 以及每个非负整数 r,

$$d_\Gamma(Y) \le r \quad \Longleftrightarrow \quad d_\Gamma(Y/N) \le r \quad \textit{for every open normal } \Gamma\textit{-subgroup } N \textit{ of } Y.$$

证明。 只需证明逆向蕴含。假设每个有限 Γ-商群都由 r Γ-轨道生成。对于每个开正规 Γ-子群 N，令 $\mathcal{G}_N \subseteq Y^r$ 为那些像能够 Γ-生成 Y/N的元组所构成的集合。它是一个非空开闭子集。 $\mathcal{G}_N$的任意有限交中都包含一个元组，该元组能生成由相应 N 的交所确定的商群。由 Y^r 的紧致性可知， $\bigcap_N \mathcal{G}_N$中存在一个点，而该元组在拓扑意义下 Γ-生成 Y。 □

特别是，这些论证并未隐含任何有限生成假设。

为说明引言中的断言，假设 $\Gamma = 1$。那么，对于 X的每个有限商群 H，都有 $H_\Gamma = H$。由命题 2.1 可知，所有这类商群几乎必然都是平凡的，因此$X = 1$ 几乎必然成立。

3 尖锐尾部定理的证明

本节证明定理 1.1。我们先介绍论证中用到的常数和初等阿贝尔重数律。

3.1 尖锐尾部渐近中的常数

定理 1.1 中的常数由 Γ 的非平凡不可约表示决定。我们先计算它们的重数分布，然后结合它们的首要贡献，得到生成元秩尾部。

我们使用定理 1.1 中定义的集合 $\mathcal{I}$ 和参数 q_V， τ_V， u_V。与 w_U 的定义一样，定义 u_V 的求和保留了 U 中的重数，并且不依赖于所选的代表元 γ_E。对偶空间 $V^\vee$ 具有逆伴随作用。

3.1.1 计算 P（V 在 $X^{\mathrm{ab}}/pX^{\mathrm{ab}}$ 中的重数为 k）

本小节解释定理 1.1 中定义的常数从何而来。重数公式将在第 3.2 节中证明，定理将在第 3.6 节中证明。

设 m_V 为 V 在 $X^{\mathrm{ab}}/pX^{\mathrm{ab}}$ 中的重数，其中 $X^{\mathrm{ab}}/pX^{\mathrm{ab}}$ 是 X 的极大初等阿贝尔 p-商群。引理 3.3 中的求和论证给出

$$\mathbf{P}(m_V = k) = \sum_{t=k}^{\infty} (-1)^{t-k} q_V^{\binom{t-k}{2}} \begin{bmatrix} t \\ k \end{bmatrix}_{q_V} \frac{|H^2(V^t \rtimes \Gamma, \mathbb{Z}/n)|}{|\operatorname{Aut}_\Gamma(V^t)|\, w_U(V^t)}. \tag{3.1}$$

这里， $\begin{bmatrix} t \\ k \end{bmatrix}_q$ 是 $\mathbb{F}_q^t$的 k维子空间的数量。根据命题 2.1，该比值是 X 中商群与 V^t同构的开正规 Γ-稳定子群的期望数量。交错和提取出重数恰好为 k的概率。

对于 co 同调因子，如果 $p \mid n$ 和 $V \simeq V^\vee$，则使用定理 1.1中定义的 λ_V。那么

$$H^2(V^t \rtimes \Gamma, \mathbb{Z}/n) \simeq \operatorname{Hom}_\Gamma\left(\bigwedge\nolimits^2_{\mathbb{F}_p}(V^t), \mathbb{F}_p\right), \qquad |H^2(V^t \rtimes \Gamma, \mathbb{Z}/n)| = q_V^{\binom{t}{2}+\lambda_V t}.$$

如果 $p\nmid n$ 或 $V\not\simeq V^\vee$，那么

$$H^2(V^t\rtimes\Gamma,\mathbb{Z}/n)=0,\qquad |H^2(V^t\rtimes\Gamma,\mathbb{Z}/n)|=1.$$

该计算在引理 3.2 中得到了证明。

权重和自同构因子为

$$w_U(V^t)=q_V^{u_V t},\qquad |\operatorname{Aut}_\Gamma(V^t)|=|\operatorname{GL}_t(q_V)|=q_V^{t^2}\eta_{q_V}(t),$$

并且，对于素数幂 q，我们定义

$$\eta_q(k)=\prod_{j=1}^{k}(1-q^{-j}),\qquad \eta_q(0)=1. \tag{3.2}$$

计算 (3.1) 得到以下适用于每个 $k\geq 0$ 的公式，证明见引理 3.3。若 $p\nmid n$ 或$V\not\simeq V^\vee$，则

$$\mathbf{P}(m_V=k)=\frac{q_V^{-k^2-u_V k}}{\eta_{q_V}(k)}\prod_{j=1}^{\infty}(1-q_V^{-k-u_V-j}). \tag{3.3}$$

若 $p\mid n$ 且 $V\simeq V^\vee$，则

$$\mathbf{P}(m_V=k)=\frac{q_V^{-k^2/2-(u_V+1/2-\lambda_V)k}}{\eta_{q_V}(k)}\prod_{j=0}^{\infty}(1+q_V^{-j-u_V-1+\lambda_V})^{-1}. \tag{3.4}$$

定理 1.1 中定义的常数 a_V,b_V,c_V给出了重数尾部的二次指数、线性指数和首项因子。舒尔引理给出 $0\leq\lambda_V\leq 1$。当 $p\mid n$ 时，Sawin–Wood 不动向量假设给出 $u_V\geq 1$，因此所有参数都有定义，乘积均为正，且 $b_V\geq 0$。尾部与其首个质量具有相同的首项：由引理 3.3，当 $k\to\infty$ 时，

$$\mathbf{P}(m_V\geq k)=c_V q_V^{-a_V k^2-b_V k}\big(1+O_V(q_V^{-k})\big).$$

3.1.2 生成元秩尾部的主要项

对于 $V\in\mathcal{I}$ over $\mathbb{F}_p$，群 V^{m_V}是 $X^{\mathrm{ab}}/pX^{\mathrm{ab}}$的 V-等型商。由于 $d_\Gamma(V^{m_V})=\lceil m_V/\tau_V\rceil$，前述重数公式给出，当整数 $r\to\infty$时，

$$\begin{aligned}\mathbf{P}\big(d_\Gamma(V^{m_V})\geq r\big)&=\mathbf{P}\big(m_V\geq\tau_V(r-1)+1\big)\\&=c_V q_V^{b_V(\tau_V-1)-a_V(\tau_V-1)^2}e^{-\left(a_V\tau_V^2r^2+\tau_V(b_V-2a_V(\tau_V-1))r\right)\log q_V}\big(1+O_V(q_V^{-r})\big).\end{aligned}$$

衰减指数中的二次项系数和一次项系数分别为 κ_V 和 ζ_V，见定理 1.1。这里及下文中，log 表示自然对数。最小的二次项系数决定主导衰减，这体现在 κ 和 $\mathcal{M}$的定义中。集合 $\mathcal{I}$ 非空。最小值可以取到，$\kappa>0$，且 $\mathcal{M}$ 有限：由于 $a_V\geq\frac12$，对 κ_V的上界也会限制q_V和 τ_V，并且在给定特征下，不可约表示只有有限多个。在这些模中，一次项系数最小的那些模对首项常数 C 有贡献，该常数在定理 1.1 中定义。记

$$k_V(r)=\tau_V(r-1)+1. \tag{3.5}$$

证明给出了更精确的展开式

$$\mathbf{P}\big(d_\Gamma(X)\geq r\big)=\left(\sum_{V\in\mathcal{M}}c_V q_V^{-a_V k_V(r)^2-b_V k_V(r)}\right)\big(1+O_{\Gamma,n,U}(e^{-\varepsilon r})\big). \tag{3.6}$$

3.2 渐近计算 $\mathbf{P}(d_\Gamma(X^{\mathrm{ab}}) \geq r)$

第 3.3 节至第 3.5 节将说明，$\mathbf{P}(d_\Gamma(X) \geq r)$ 与 $\mathbf{P}(d_\Gamma(X^{\mathrm{ab}}) \geq r)$ 之间的差异，相对于此处计算的阿贝尔尾部可以忽略不计。

引理 3.1. 对于每个 $V \in \mathcal{I}$ 在 $\mathbb{F}_p$上的情形，令 m_V 为 V 在 $\mathbb{F}_p[\Gamma]$-模$X^{\mathrm{ab}}/pX^{\mathrm{ab}}$中的重数，其中 $X^{\mathrm{ab}}/pX^{\mathrm{ab}}$是 X的最大初等阿贝尔 p商群。几乎必然，

$$d_\Gamma(X^{\mathrm{ab}}) = \sup_{V \in \mathcal{I}} \left\lceil \frac{m_V}{\tau_V} \right\rceil. \tag{3.7}$$

特别地，$d_\Gamma(X^{\mathrm{ab}}) \geq r$ 当且仅当至少存在一个 V使得 $m_V \geq k_V(r)$ 。

证明。对于 $p \nmid |\Gamma|$，小型有限剩余群的最大初等阿贝尔 p商群是有限的。事实上，每个到 C_p 的非零连续映射都有一个指数为 p的开核，而每个这样的核只支持 $p-1$ 个此类映射。因此 $\mathrm{Hom}(X, C_p)$ 是一个有限维 $\mathbb{F}_p$-空间。在命题 2.1 的满测度集上，不存在平凡成分。

根据 $\mathbb{F}_p[\Gamma]$ 的韦德伯恩分解，其正则模包含 τ_V 个 V 的副本。一个重数为 m_V 的半单模由 k 个元素生成，当且仅当对所有 V 都有 $m_V \leq k\tau_V$。对于带有 Γ 作用的有限阿贝尔 p 群，一个元组生成该群，当且仅当它在模 p 下生成：如果它生成的子群 Γ 是 N 且 $G = N + pG$，迭代即可得到$G = N$。主分量可以同时生成。将这些事实应用于有限阿贝尔商群，并使用引理 2.2。 □

对于整数 m，$t \geq 0$，有

$$|\operatorname{Sur}_{\mathbb{F}_q}(\mathbb{F}_q^m, \mathbb{F}_q^t)| = \prod_{j=0}^{t-1}(q^m - q^j).$$

当 $t = 0$ 时计数为 1，当 $t > m$ 时计数为 0。

引理 3.2。固定 $V \in \mathcal{I}$。则

$$\mathbf{E}|\operatorname{Sur}_{\mathbb{F}_{q_V}}(\mathbb{F}_{q_V}^{m_V}, \mathbb{F}_{q_V}^t)| = \begin{cases} q_V^{-u_V t}, & p \nmid n \text{ or } V \not\simeq V^\vee, \\ q_V^{\binom{t}{2}+(\lambda_V - u_V)t}, & p \mid n,\ V \simeq V^\vee. \end{cases} \tag{3.8}$$

证明。从 X 到 V^t 的每个连续 Γ-等变映射都通过 V-等型商 V^{m_V} 分解，因此 |同态集$_\Gamma$(X, V^t)| = |同态集$^{\mathbb{F}_{q_V}}$($\mathbb{F}_{q_V}^{m_V}$, $\mathbb{F}_{q_V}^t$)|。将 (2.1) 应用于 $G = V^t$。其权为$q_V^{u_V t}$，且其余不变量消失。若 $p \nmid n$，则其以系数 $\mathbb{Z}/n$ 取值的正次数上同调消失。否则，只有系数的 p-主部分有贡献。对于 $p^e \| n$，万有系数序列为

$$0 \longrightarrow \operatorname{Ext}^1_{\mathbb{Z}}(V^t, \mathbb{Z}/p^e) \longrightarrow H^2(V^t, \mathbb{Z}/p^e) \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(\bigwedge^2 V^t, \mathbb{Z}/p^e) \longrightarrow 0.$$

左侧项是若干个 $V^\vee$ 的直和，不含 Γ-不变元。由于 $p \nmid |\Gamma|$，取不变元是正合的。该分解

$$\bigwedge^2 V^t \simeq \bigoplus_{i=1}^{t} \bigwedge^2 V \ \oplus \bigoplus_{i<j} (V \otimes_{\mathbb{F}_p} V)$$

对 $p=2$也成立。当 V是自对偶空间时，每个交叉被加数都有 q_V不变形式，否则只有零形式。自对偶情形下，对角被加数贡献 $q_V^{\lambda_V t}$；否则只有零不变形式。对 Γ 取平均，将此计算与 $V^t \rtimes \Gamma$的上同调对应起来。

□

3.2.1 不可约 Γ-模的重数尾部

引理 3.3。对于每个固定的 $V \in \mathcal{I}$,

$$\mathbf{P}(m_V \geq k) = c_V q_V^{-a_V k^2 - b_V k}\big(1 + O_V(q_V^{-k})\big). \tag{3.9}$$

隐含常数也可能依赖于 n、U。对于 V 和 $k \geq 0$ 一致地,

$$\mathbf{P}(m_V \geq k) \leq \rho^{-1} q_V^{-a_V k^2 - b_V k}, \qquad \rho = \eta(2) > 0. \tag{3.10}$$

证明。首先，当 $m_V \geq k$ 时，$|\operatorname{Sur}^{\mathbb{F}_{q_V}}(\mathbb{F}_{q_V}^{m_V}, \mathbb{F}_{q_V}^{k})| \geq |\mathrm{GL}_k(q_V)|$。由马尔可夫不等式和引理 3.2 得

$$\mathbf{P}(m_V \geq k) \leq \frac{\mathbf{E}|\operatorname{Sur}_{\mathbb{F}_{q_V}}(\mathbb{F}_{q_V}^{m_V}, \mathbb{F}_{q_V}^{k})|}{|\operatorname{GL}_k(q_V)|} = \frac{q_V^{-a_V k^2 - b_V k}}{\eta_{q_V}(k)} \leq \rho^{-1} q_V^{-a_V k^2 - b_V k},$$

因为 $\eta_{q_V}(k) \geq \eta(q_V) \geq \rho$。这就证明了一致上界。

要恢复各个单独的质量，使用

$$\begin{bmatrix} m \\ t \end{bmatrix}_{q_V} = \frac{|\operatorname{Sur}_{\mathbb{F}_{q_V}}(\mathbb{F}_{q_V}^{m}, \mathbb{F}_{q_V}^{t})|}{|\operatorname{GL}_t(q_V)|},$$

当 $t > m$ 时值为零。有限 q-二项式定理给出

$$\mathbf{1}_{\{m=k\}} = \sum_{e \geq 0} (-1)^e q_V^{\binom{e}{2}} \begin{bmatrix} m \\ k+e \end{bmatrix}_{q_V} \begin{bmatrix} k+e \\ k \end{bmatrix}_{q_V}.$$

事实上，对于 $m \geq k$，该和等于 $\begin{bmatrix} m \\ k \end{bmatrix}_{q_V} \prod_{j=0}^{m-k-1} (1 - q_V^j)$；当 $m = k$ 时它等于 1，否则为零。对于 $m < k$，所有项都为零。因此，交错和恰好分离出重数k。

取期望并应用 (2.1) 得到 (3.1)，现将其重述如下:

$$\mathbf{P}(m_V = k) = \sum_{t=k}^{\infty} (-1)^{t-k} q_V^{\binom{t-k}{2}} \begin{bmatrix} t \\ k \end{bmatrix}_{q_V} \frac{|H^2(V^t \rtimes \Gamma, \mathbb{Z}/n)|}{|\operatorname{Aut}_\Gamma(V^t)|\, w_U(V^t)}.$$

记 $t = k + e$，并使用高斯二项式系数的公式可得

$$\mathbf{P}(m_V = k) = \frac{1}{\eta_{q_V}(k)} \sum_{e \geq 0} \frac{(-1)^e q_V^{-k^2 - ke - e(e+1)/2}}{\eta_{q_V}(e)} \mathbf{E}|\operatorname{Sur}_{\mathbb{F}_{q_V}}(\mathbb{F}_{q_V}^{m_V}, \mathbb{F}_{q_V}^{k+e})|. \tag{3.11}$$

代入引理 3.2 中的矩，并将涉及 k 的项与涉及 e 的项分开，可得

$$\mathbf{P}(m_V = k) = \begin{cases} \dfrac{q_V^{-k^2 - u_V k}}{\eta_{q_V}(k)} \displaystyle\sum_{e \geq 0} \frac{(-1)^e q_V^{-(k+u_V)e - e(e+1)/2}}{\eta_{q_V}(e)}, & p \nmid n \text{ or } V \not\simeq V^\vee, \\ \dfrac{q_V^{-k^2/2 - (u_V + 1/2 - \lambda_V)k}}{\eta_{q_V}(k)} \displaystyle\sum_{e \geq 0} \frac{(-1)^e q_V^{-(u_V + 1 - \lambda_V)e}}{\eta_{q_V}(e)}, & p \mid n,\ V \simeq V^\vee. \end{cases}$$

这些表达式也说明了求和与期望可以交换次序：第一个级数因其关于 e 的二次指数为负而绝对收敛；第二个级数的各项绝对值则由一个几何级数所控制，因为 $u_V + 1 - \lambda_V \geq 1$ 和 $\eta_{q_V}(e) \geq \rho$。

欧拉乘积恒等式 [14, 推论 2.2，第 19] 页为

$$\sum_{e\geq 0} \frac{(-1)^e q_V^{-e(e+1)/2} z^e}{\eta_{q_V}(e)} = \prod_{j\geq 1}(1 - zq_V^{-j}), \quad z \in \mathbb{C}, \qquad \sum_{e\geq 0} \frac{z^e}{\eta_{q_V}(e)} = \prod_{j\geq 0}(1 - zq_V^{-j})^{-1}, \quad |z| < 1.$$

在第一种情形中，将 $z = q_V^{-k-u_V}$代入第一个恒等式；在第二种情形中，将$z = -q_V^{-u_V-1+\lambda_V}$代入第二个恒等式。方程 (3.11)随即恰好给出 (3.3) 和 (3.4)。

由于 $\eta_{q_V}(k) = \eta(q_V)(1 + O(q_V^{-k}))$ 且 $\prod_{j\geq 1}(1 - q_V^{-k-u_V-j}) = 1 + O(q_V^{-k})$，这些质量公式给出

$$\mathbf{P}(m_V = k) = c_V q_V^{-a_V k^2 - b_V k}\big(1 + O_V(q_V^{-k})\big).$$

最后，$k + 1$ 处的一致上界给出

$$0 \leq \mathbf{P}(m_V \geq k) - \mathbf{P}(m_V = k) = \mathbf{P}(m_V \geq k + 1) \leq \rho^{-1} q_V^{-a_V(k+1)^2 - b_V(k+1)}.$$

由于 $2a_V \geq 1$ 和 $b_V \geq 0$，这是一个相对 $O_V(q_V^{-k})$ 误差。这就证明了 (3.9)。 □

3.2.2 关于 $\mathbf{P}(d_\Gamma(X^{\mathrm{ab}}) \geq r)$ 的渐近式

命题 3.4。(3.6) 的右侧是$\mathbf{P}(d_\Gamma(X^{\mathrm{ab}}) \geq r)$的渐近式，具有相同类型的相对误差。

证明。 根据引理 3.1，

$$\mathbf{P}\big(d_\Gamma(X^{\mathrm{ab}}) \geq r\big) = \mathbf{P}\left(\bigcup_{V\in\mathcal{I}} \{m_V \geq k_V(r)\}\right).$$

由并集界和容斥原理的前两项可得

$$\begin{aligned}\left|\mathbf{P}\big(d_\Gamma(X^{\mathrm{ab}}) \geq r\big) - \sum_{V\in\mathcal{M}} \mathbf{P}\big(m_V \geq k_V(r)\big)\right| \leq \\ \sum_{\substack{\{V,W\}\subseteq\mathcal{M} \\ V\neq W}} \mathbf{P}\big(m_V \geq k_V(r),\ m_W \geq k_W(r)\big) + \sum_{V\in\mathcal{I}\setminus\mathcal{M}} \mathbf{P}\big(m_V \geq k_V(r)\big).\end{aligned} \tag{3.12}$$

右侧的第一项和限制了将各个概率相加时对 $V \in \mathcal{M}$ 的重复计数，而第二项和限制了来自 $\mathcal{M}$ 之外的模的贡献。下面所有的成对求和都取遍不同模的无序对。我们将第一项和拆分为

$$\begin{aligned}\sum_{\substack{\{V,W\}\subseteq\mathcal{M} \\ V\neq W}} \mathbf{P}\big(m_V \geq k_V(r),\ m_W \geq k_W(r)\big) = \\ \sum_{\substack{\{V,W\}\subseteq\mathcal{M},\ V\neq W \\ W\not\simeq V^\vee \text{ or } \gcd(|V|,n)=1}} \mathbf{P}\big(m_V \geq k_V(r),\ m_W \geq k_W(r)\big) + \sum_{\substack{\{V,W\}\subseteq\mathcal{M},\ V\neq W \\ W\simeq V^\vee,\ \gcd(|V|,n)>1}} \mathbf{P}\big(m_V \geq k_V(r),\ m_W \geq k_W(r)\big).\end{aligned}$$

根据引理 3.1，阈值为 $k_V(r) = \tau_V(r-1) + 1$。由于 $b_V \geq 0$ 和 $\kappa_V = a_V\tau_V^2 \log q_V$，我们将使用

$$q_V^{-a_V k_V(r)^2 - b_V k_V(r)} \leq q_V^{-a_V \tau_V^2 (r-1)^2} = e^{-\kappa_V (r-1)^2}.$$

作为比较，展开 $k_V(r) = \tau_V r - (\tau_V - 1)$ 得到主项

$$\begin{aligned}\sum_{V \in \mathcal{M}} c_V q_V^{-a_V k_V(r)^2 - b_V k_V(r)} &= e^{-\kappa r^2 - \zeta r} \sum_{V \in \mathcal{M}} c_V q_V^{b_V(\tau_V - 1) - a_V(\tau_V - 1)^2} e^{-(\zeta_V - \zeta) r} \\ &\asymp_{\Gamma, n, U} e^{-\kappa r^2 - \zeta r}.\end{aligned}$$

最后一个比较成立，因为 $\mathcal{M}$ 是有限的，每个系数都为正，且 $\zeta = \min_{V \in \mathcal{M}} \zeta_V$。

我们首先对满足 $W \neq V^\vee$ 或 $\gcd(|V|, n) = 1$的配对求和进行估计。对于这些配对，目标 $V^k \oplus W^l$的矩分解为各自矩的乘积。这与引理 3.2 中的外幂计算相同；对于不同素数，不存在交叉项。由马尔可夫不等式可得

$$\begin{aligned}\mathbf{P}(m_V \geq k, m_W \geq l) &\leq \frac{\mathbf{E}\big(|\operatorname{Sur}_{\mathbb{F}_{q_V}}(\mathbb{F}_{q_V}^{m_V}, \mathbb{F}_{q_V}^{k})| \, |\operatorname{Sur}_{\mathbb{F}_{q_W}}(\mathbb{F}_{q_W}^{m_W}, \mathbb{F}_{q_W}^{l})|\big)}{|\operatorname{GL}_k(q_V)| \, |\operatorname{GL}_l(q_W)|} \\ &= \frac{q_V^{-a_V k^2 - b_V k} q_W^{-a_W l^2 - b_W l}}{\eta_{q_V}(k) \eta_{q_W}(l)} \leq \rho^{-2} q_V^{-a_V k^2 - b_V k} q_W^{-a_W l^2 - b_W l}.\end{aligned} \tag{3.13}$$

将前面的指数界应用于两个因子，并利用 $\kappa_V = \kappa_W = \kappa$ for$V, W \in \mathcal{M}$，得到

$$\begin{aligned}&\sum_{\substack{\{V,W\} \subseteq \mathcal{M},\ V \neq W \\ W \not\simeq V^\vee \text{ or } \gcd(|V|,n)=1}} \mathbf{P}\big(m_V \geq k_V(r),\ m_W \geq k_W(r)\big) \\ &\quad \leq \rho^{-2} \sum_{\substack{\{V,W\} \subseteq \mathcal{M},\ V \neq W \\ W \not\simeq V^\vee \text{ or } \gcd(|V|,n)=1}} e^{-(\kappa_V + \kappa_W)(r-1)^2} \\ &\quad \leq \rho^{-2} \binom{|\mathcal{M}|}{2} e^{-2\kappa(r-1)^2}.\end{aligned}$$

个 $\binom{|\mathcal{M}|}{2}$ 配对。相对于主项，这个界的大小为 $O(e^{-\kappa r^2/2})$，因为 至多有 e

$$\frac{e^{-2\kappa(r-1)^2}}{e^{-\kappa r^2 - \zeta r}} = e^{-\kappa r^2 + (4\kappa + \zeta) r - 2\kappa} = O\big(e^{-\kappa r^2/2}\big).$$

无需随机变量之间相互独立。

现在我们对满足 $W \simeq V^\vee$ 且 $\gcd(|V|,\ n) > 1$ 的对求和。这些是在特征 $p \mid n$ 下的对偶对。这里 $q_W = q_V$、 $\tau_W = \tau_V$ 和 $u_W = u_V$，因此 $k_W(r) = k_V(r)$。混合矩为

$$\mathbf{E}\big(|\operatorname{Sur}_{\mathbb{F}_{q_V}}(\mathbb{F}_{q_V}^{m_V}, \mathbb{F}_{q_V}^{k})| \, |\operatorname{Sur}_{\mathbb{F}_{q_V}}(\mathbb{F}_{q_V}^{m_W}, \mathbb{F}_{q_V}^{l})|\big) = q_V^{kl - u_V(k+l)}.$$

Thus

$$\begin{aligned}\mathbf{P}\big(m_V \geq k_V(r),\ m_W \geq k_W(r)\big) &\leq \frac{\mathbf{E}\big(|\operatorname{Sur}_{\mathbb{F}_{q_V}}(\mathbb{F}_{q_V}^{m_V}, \mathbb{F}_{q_V}^{k_V(r)})| \, |\operatorname{Sur}_{\mathbb{F}_{q_V}}(\mathbb{F}_{q_V}^{m_W}, \mathbb{F}_{q_V}^{k_V(r)})|\big)}{|\operatorname{GL}_{k_V(r)}(q_V)|^2} \\ &= \frac{q_V^{-k_V(r)^2 - 2u_V k_V(r)}}{\eta_{q_V}(k_V(r))^2} \leq \rho^{-2} q_V^{-u_V k_V(r)} q_V^{-k_V(r)^2 - u_V k_V(r)}.\end{aligned} \tag{3.14}$$

这里 $u_V \geq 1$、 $a_V = 1$、 $b_V = u_V$ 和 $c_V = \eta(q_V)^{-1} \geq 1$。此外，

$$k_V(r) - r = (\tau_V - 1)(r-1) \geq 0, \qquad q_V^{-u_V k_V(r)} \leq 2^{-k_V(r)} \leq 2^{-r}.$$

每个对偶对都包含两个参数相同的成员。因此，将对偶对上的求和改为对其成员求和，可得

$$\begin{aligned}\sum_{\substack{\{V,W\}\subseteq\mathcal{M},\ V\neq W\\ W\simeq V^\vee,\ \gcd(|V|,n)>1}} \mathbf{P}\big(m_V \geq k_V(r),\ m_W \geq k_W(r)\big) &\leq \rho^{-2} \sum_{\substack{V\in\mathcal{M},\ V^\vee\in\mathcal{M}\\ V\not\simeq V^\vee,\ \gcd(|V|,n)>1}} q_V^{-u_V k_V(r)} q_V^{-k_V(r)^2 - u_V k_V(r)} \\ &\leq \rho^{-2} 2^{-r} \sum_{V\in\mathcal{M}} c_V q_V^{-a_V k_V(r)^2 - b_V k_V(r)}.\end{aligned}$$

因此，此误差至多为主项的 $\rho^{-2}2^{-r}$ 倍。特别地，主导求和中应包含对偶对的两个成员。

最后，我们对 (3.12) 中的 $V \notin \mathcal{M}$ 求和进行估计。二次衰减系数的集合 $\{\kappa_V : V \in \mathcal{I}\}$ 是局部有限的。令 $\kappa_2 > \kappa$ 为其中大于 κ 的最小值。这样的值存在，因为存在特征任意大的非平凡模。由 (3.10) 及上面的指数界，对于 $r \geq 3$，我们有

$$\begin{aligned}\sum_{V\notin\mathcal{M}} \mathbf{P}\big(m_V \geq k_V(r)\big) &\leq \rho^{-1} \sum_{V\notin\mathcal{M}} e^{-\kappa_V (r-1)^2} \\ &= \rho^{-1} \sum_{V\notin\mathcal{M}} e^{-\kappa_V((r-1)^2-4)} e^{-4\kappa_V} \\ &\leq \rho^{-1} e^{-\kappa_2((r-1)^2-4)} \sum_{V\in\mathcal{I}} e^{-4\kappa_V} \\ &\ll_{\Gamma,n} e^{-\kappa_2(r-1)^2}.\end{aligned}$$

在第三行中，我们对 $V \notin \mathcal{M}$ 使用了 $\kappa_V \geq \kappa_2$ 和 $(r-1)^2 - 4 \geq 0$。剩余的和是有限的：每个特征下至多有 $|\Gamma|$ 个单模，且 $\kappa_V \geq \frac{1}{2}\log p$，因此

$$\sum_{V\in\mathcal{I}} e^{-4\kappa_V} \leq |\Gamma| \sum_{p\nmid|\Gamma|} p^{-2} < \infty.$$

最后， $\kappa_2 > \kappa$ 使这一误差小于主项：

$$\frac{e^{-\kappa_2(r-1)^2}}{e^{-\kappa r^2 - \zeta r}} = e^{-(\kappa_2-\kappa)r^2 + (2\kappa_2+\zeta)r - \kappa_2} = O\big(e^{-(\kappa_2-\kappa)r^2/2}\big).$$

应用 (3.12) 和各自的渐近公式 (3.9)。由于 $\mathcal{M}$ 是有限的，且所有阈值都至少随 r 线性增长，因此所得的相对误差为某个 $\varepsilon > 0$ 的 $O(e^{-\varepsilon r})$。 □

3.3 为 $d_\Gamma(X) \geq r$ 生成有限商群

对于 $r \geq 4$，事件 $d_\Gamma(X) \geq r$ 迫使 X 到本小节构造的某个有限群 $\pi_J(G)$ 存在一个 Γ-等变满同态；这在命题 2.1 的满测度集上成立。根据引理 2.2，我们先选取一个有限 Γ-商群 G，使得 $d_\Gamma(G) \geq r$，然后进行冠约化并投影到指定重数。

投影群 $\pi_j(G)$ 未必满足 $d_\Gamma(\pi_j(G)) \geq r$。我们保留如下蕴含：若群 X 满足 $d_\Gamma(X) \geq r$，则它有一个这样的群作为商群。我们将利用命题 2.1 的商矩来界定这些商群出现的概率。

下面的有限群论和上同调论输入依赖于有限单群的分类。因此，我们对定理 1.1 和定理 1.2 的证明也依赖于该分类。

3.3.1 带 Γ作用的冠理论

我们将冠论论证相对于任意子群来陈述。对于有限群 E 和子群 $H \leq E$，令 $d_H(E) = \min\{k\colon E = \langle H,\ x_1,\ \ldots,\ x_k\rangle\}$。这样的元组称为相对生成元组。对于带有指定 $H = \Gamma$的 $E = G \rtimes \Gamma$，这等于 $d_\Gamma(G)$。以下结果不需要互素假设。

引理 3.5。若 $N \trianglelefteq E$ 且 $k \geq d_H(E)$，则 E/N 的每个相对生成 k元组都可提升为 E的一个元组。

证明。对于子群 $M \leq K \leq E$，令 $\mu_E(M,\ K)$表示 E的子群格的莫比乌斯函数，其特征为 $\mu_E(M,\ M) = 1$，并且当 $M < K$时，$\sum_{M\leq J\leq K} \mu_E(M,\ J) = 0$。对子群格应用莫比乌斯反演，可将其生成提升计数为

$$\sum_{\substack{M\leq E,\ H\leq M\\ MN=E}} \mu_E(M,E)|M\cap N|^k.$$

确实，包含 H 的子群只有在 $MN = E$ 时才能包含所有提升，此时每个元素在其中都有 $|M \cap N|$ 个提升。计数与元组无关，并且对于某个已有相对生成元组的像，该计数为正。 □

对于有限群 E，其 *Frattini* 子群 $\Phi(E)$ 是 E 的所有极大真子群的交（其中 $\Phi(1) = 1$）。如果有限群 L 有唯一的极小正规子群，则称其为 单右群，该极小正规子群称为其 单右。若此外 $\Phi(L) = 1$，则称 L 为 本原单右群，并用 A 表示其单右。其冠基幂为

$$L_t = \{(l_1,\ldots,l_t) \in L^t : l_1A = \cdots = l_tA\}. \tag{3.15}$$

它的底为 A^t，商群为 L/A。如果 A 是阿贝尔群，则 $L = A \rtimes (L/A)$，其中 A 是一个忠实不可约 $\mathbb{F}_p[L/A]$-模；令 $q_A = |\mathrm{End}^{L/A}(A)|$，且 $\tau_A = \dim_{\mathbb{F}_{q_A}} A$。否则，$A$ 是某个非阿贝尔单群的幂，共轭作用将 L 嵌入 $\mathrm{Aut}(A) \leq \mathrm{Sym}_{|A|}$。

引理 3.6。设 E 为有限群且 $H \leq E$。对于每个整数 $1 \leq r \leq d_H(E)$，存在一个满同态 $\pi\colon E \twoheadrightarrow L_t$ 到某个冠基幂，使得 $d_{\pi(H)}(L_t) \geq r$，而 L_t 的每个真商都可以由 $\pi(H)$ 的像及至多 $r-1$ 个额外元素生成。

证明。选择一个满同态 $\pi\colon E \twoheadrightarrow Q$，使 $|Q|$ 最小，并满足 $d_{\pi(H)}(Q) \geq r$。Q 的每个真商的相对生成元数至多为 $r-1$，因此只需证明 Q 是一个冠基幂。除去 $\Phi(Q)$ 不会改变相对生成元数：若 $J \leq Q$ 且 $J\Phi(Q) = Q$，则 $J = Q$。因此，由极小性可得 $\Phi(Q) = 1$。

冠分裂引理 [12, 引理 3 和 4] 给出正规子群 $R, D \trianglelefteq Q$，满足$D \neq 1$，其中 Q/R 为冠基幂，并且对每个 $J \leq Q$都具有以下性质：

$$JR = JD = Q \quad\Longrightarrow\quad J = Q.$$

假设 $R \neq 1$。由于 Q/R是真商，选择 $x_1, \ldots, x_{r-1} \in Q$（如果$r = 1$，则为空元组），使得

$$Q = \langle \pi(H), x_1, \ldots, x_{r-1} \rangle R.$$

它们的像与 $\pi(H)$ 的像一起生成 Q/RD。真商 Q/D 的相对生成元数也至多为 $r-1$。对 $Q/D \twoheadrightarrow Q/RD$ 应用引理 3.5：存在 y_1、……、 $y_{r-1} \in R$，使得

$$Q = \langle \pi(H), x_1 y_1, \ldots, x_{r-1} y_{r-1} \rangle D.$$

令 $J = \langle \pi(H)\ x_1 y_1$、……、 $x_{r-1} y_{r-1} \rangle$。用 R 中的元素乘以 x_i 不会改变它们在 Q/R 中的像，因此 $JR = Q$；最后一个展示式给出 $JD = Q$。于是 $J = Q$，这与 $d_{\pi(H)}(Q) \geq r$ 矛盾。因此 $R = 1$，且 Q 是一个冠基幂，证毕。 □

引理 3.7。设 L_t 是一个底为 A^t 的冠基幂，设 $H \leq L_t$，且设 $r \geq 4$ 为一个整数。假设 $d_H(L_t) \geq r$，而 L_t 的每个真商都可以由 H 的像以及至多 $r-1$ 个额外元素生成。那么

$$t > (r-3)\tau_A \quad (A\ abelian), \qquad t > |A|^{r-3} \quad (A\ nonabelian). \tag{3.16}$$

特别地，$t > 1$ 和 $d(L) \leq r - 1 + d(H)$，其中 $d(G)$ 表示取 $d_\Gamma(G)$，并将 Γ 取为平凡群。

证明。首先假设 A 是阿贝尔的。固定 $r-1$ 个 L/A 的元素，使其与 H的像一起生成该商群。在 $L_t = A^t \rtimes (L/A)$ 中，为每个固定元素选择一个提升 x_i，在其 $|A^t| = q_A^{\tau_A t}$ 个提升中独立且均匀地选择。下面所有概率均指该随机元组 $(x_1, \ldots, x_{r-1})$。

如果这些提升与 H一起不能生成 L_t，则它们包含于一个包含 H的极大子群 M中。由于它们的像与 H 的像一起生成 L_t/A^t，该子群满足 $MA^t = L_t$。于是 $M \cap A^t$ 是 A^t的一个极大 (L/A)-子模，其商群为 A，而 $M/(M \cap A^t)$ 是 $A \rtimes (L/A)$ 中 A 的补充子群。这样的子模共有 $(q_A^t - 1)/(q_A - 1) < q_A^t$ 个。对于每一个子模，补充子群的数量为

$$\frac{|A|}{|A^{L/A}|} \, |H^1(L/A, A)| \leq |A| \, |H^1(L/A, A)| < q_A^{2\tau_A},$$

根据 [3, 定理 A]；当 $L/A = 1$ 时，最后一个不等式显然成立。因此，出现的极大子群少于 $q_A^t q_A^{2\tau_A}$ 个。

对于每个这样的 M，A^t 的每个陪集都恰好包含 $|M \cap A^t|$ 个与 M 相交的元素。由于 $A^t/(M \cap A^t) \simeq A$，均匀性和独立性给出

$$\mathbf{P}(x_i \in M) = \frac{|M \cap A^t|}{|A^t|} = \frac{1}{|A|} = q_A^{-\tau_A}, \mathbf{P}(x_1, \ldots, x_{r-1} \in M) = q_A^{-\tau_A(r-1)}.$$

生成失败是上述刚刚计数的极大子群所对应事件的并。因此，如果 $t \leq (r-3)\tau_A$，并集界给出

$$\mathbf{P}\big(\langle H, x_1, \ldots, x_{r-1} \rangle \neq L_t\big) \leq \sum_M \mathbf{P}(x_1, \ldots, x_{r-1} \in M) < q_A^t q_A^{2\tau_A} q_A^{-\tau_A(r-1)} = q_A^{t-(r-3)\tau_A} \leq 1.$$

失败概率严格小于 1，因此存在某种提升的选择，使其与 L_t 一同生成 H，这与 $d_H(L_t) \geq r$ 矛盾。

现在假设 A 是非阿贝尔的，并选取一个坐标极小正规子群$N \simeq A$。关于 L_t/N 的假设给出

$$L_t = \langle H, x_1, \ldots, x_{r-1} \rangle N.$$

选取 H的生成元 $y_1, \ldots, y_{d(H)}$，并将它们添加进去，得到

$$(x_1, \ldots, x_{r-1}, y_1, \ldots, y_{d(H)}).$$

如果 $t \leq |A|^{r-3}$，那么

$$h := \left\lceil \frac{8}{5} + \log_{|A|} t \right\rceil \leq \left\lceil \frac{8}{5} + r - 3 \right\rceil = r - 1.$$

根据 [13, 命题 6],，存在 $n_1, \ldots, n_h \in N$，使得

$$L_t = \langle x_1 n_1, \ldots, x_h n_h, x_{h+1}, \ldots, x_{r-1}, y_1, \ldots, y_{d(H)} \rangle.$$

只有前 h 个元素 $x_1, \ldots, x_h$ 被修改了。因此，H的生成元保持不变，而另外 $r-1$ 个元素生成 L_t，再次导出矛盾。

由于 $r \geq 4$，两个界都意味着 $t > 1$。因此，L 是 L_t 的一个真坐标商，可由 H 的像以及至多另外 $r-1$ 个元素生成。这给出了 $d(L)$的界。

□

3.3.2 提取具有固定重数的商群

我们将相对冠引理应用于 $G \rtimes \Gamma$，然后投影到指定重数。由此得到的商群可以计数，且其概率可以一致地加以界定。该投影保留非阿贝尔性，这正是最终与阿贝尔化进行比较所需要的。

引理 3.8. 设 G 是一个有限 Γ-群，满足 $G_\Gamma = 1$、$(|G|, |\Gamma|) = 1$ 以及 $d_\Gamma(G) \geq r \geq 4$。存在一个满同态 $\pi\colon G \rtimes \Gamma \twoheadrightarrow L_t$，其像为一个冠基幂，使得

$$L_t = \pi(G) \rtimes \pi(\Gamma), \qquad A^t \leq \pi(G), \qquad d_{\pi(\Gamma)}(L_t) \geq r, \tag{3.17}$$

并且每个真商的相对秩至多为 $r-1$。此外，$(\pi(G))_\Gamma = 1$、L_t 和 L/A 都由 $\pi(\Gamma)$ 的像正规生成，并且

$$d(L/A) \leq r - 1 + d(\Gamma), \qquad t > (r-3)\tau_A \ \ (A \text{ abelian}), \qquad t > |A|^{r-3} \ \ (A \text{ nonabelian}). \tag{3.18}$$

特别地，$t > 1$ 和 $d(L) \leq r - 1 + d(\Gamma)$。

证明。将引理 3.6 应用于 $E = G \rtimes \Gamma$ 和 $H = \Gamma$，得到 $\pi\colon G \rtimes \Gamma \twoheadrightarrow L_t$。互素性给出 $\pi(G) \cap \pi(\Gamma) = 1$，因此 $L_t = \pi(G) \rtimes \pi(\Gamma)$。将引理 3.7 应用于 $H = \pi(\Gamma)$，得到重数界 $t > 1$，以及 $d(L/A) \leq d(L) \leq r - 1 + d(\Gamma)$。

令 $D = A^t \cap \pi(G)$。A^t 的半单结构给出 $D \simeq A^j$ 和 $A^t/D \simeq A^{t-j}$，其中某个 $0 \leq j \leq t$ 满足条件。由于后者嵌入 $L_t/\pi(G)$，互素性迫使 $j = t$ 或 $j = 0$。若 $j = 0$，则 $D = 1$，因此正规子群 $\pi(G)$ A^t 彼此中心化；而 $C_{L_t}(A^t) \leq A^t$ 随即推出 $\pi(G) = 1$，这不可能。因此 $j = t$ 且 $A^t \leq \pi(G)$。关系 $(\pi(G))_\Gamma = 1$ 由 G 下降而来，并等价于 L_t 由 $\pi(\Gamma)$ 正规生成。在阿贝尔情形 $L/A \neq 1$，因为否则 $\pi(\Gamma) = 1$ 且 $(\pi(G))_\Gamma = \pi(G) \neq 1$。 □

定义 3.9。 固定 $r \geq 4$。见证 是一个元组 $(G,\ L,\ A,\ \pi,\ r)$，满足引理 3.8 的假设和结论；特别地，$\pi\colon\ G \rtimes \Gamma \twoheadrightarrow L_t$。

要提取一个见证，令

$$j = \begin{cases} (r-3)\tau_A, & A \text{ abelian}, \\ |A|^{r-3}, & A \text{ nonabelian}. \end{cases} \tag{3.19}$$

由 (3.18)，$1 \leq j < t$。将 π 与投影 $L_t \twoheadrightarrow L_j$ 复合，投影到前 j 个坐标，得到 $\pi_j\colon G \rtimes \Gamma \twoheadrightarrow L_j$。元组 $(G,\ L,\ A,\ \pi_j,\ r)$ 是其提取见证。

若见证或提取见证 $(G,\ L,\ A,\ \varphi,\ r)$ 满足 $\varphi(G)$ 是非阿贝尔群，则该见证或提取见证是非阿贝尔的。其底类型是 A 的类型（阿贝尔或非阿贝尔）。

提取见证的见证商群是 Γ-群 $W = \pi_j(G)$，其中 $\gamma \cdot w = \pi_j(\gamma) w \pi_j(\gamma)^{-1}$。若 $\pi_j(\Gamma)$ 在 L_j 中是对角的，且当 A 是阿贝尔群时属于标准补 L/A，则该提取见证是规范化见证。

为了统计见证商群，将其归一化数据与每个规范化见证相关联：

- 若 A 是阿贝尔群，则取子群 $L/A \leq \mathrm{GL}_{\tau_A}(q_A)$ 以及由 $\pi_j(\Gamma)$ 诱导的同态 $\Gamma \to L/A$。
- 若 A 为非阿贝尔，则子群 $L \leq \mathrm{Sym}_{|A|}$（通过共轭作用于 A）以及由对角像 $\pi_j(\Gamma)$ 的一个坐标给出的同态 $\Gamma \to L$。

对于固定的 r，这些数据至多确定 $\pi_j(G)$ 的 Γ-同构类，正如引理 3.10 中所证明的；它们不记录源 G 或映射 π_j。

引理 3.10。 每个提取的见证 (G, L, A, π_j, r) 都可以通过用 A^j 中的一个元素对 π_j 进行共轭作用来规范化。如果原见证是非阿贝尔的，则其提取的见证也是非阿贝尔的。

对于阿贝尔情形中固定的 q_A、τ_A，或非阿贝尔情形中固定的 $|A|$，可能的归一化数据数量至多为

$$\begin{cases} q_A^{(r-1+2d(\Gamma))\tau_A^2}, & A \textit{ abelian}, \\ (|A|!)^{r-1+2d(\Gamma)}, & A \textit{ nonabelian}. \end{cases} \tag{3.20}$$

此外，对于每个规范化见证，

$$|\operatorname{Aut}_\Gamma(W)| \geq \begin{cases} |\operatorname{GL}_j(q_A)| \geq \rho q_A^{j^2}, & A \textit{ abelian}, \\ j!, & A \textit{ nonabelian}, \end{cases} \qquad \rho = \eta(2). \tag{3.21}$$

证明。 **1. 规范化 Γ的像**。

选择一个给出提取见证的原始见证（$G,\ L,\ A,\ \pi,\ r$），并令 $\pi_1\colon G \rtimes \Gamma \twoheadrightarrow L$为 π的第一坐标。映射 $\pi(\Gamma) \to L/A$ 是单射，因为 $A^t \leq \pi(G)$和$\pi(G) \cap \pi(\Gamma) = 1$。置

$$E := A\pi_1(\Gamma), \qquad E/A = A\pi_1(\Gamma)/A \simeq \pi(\Gamma).$$

因此（$|A|,\ |E/A|$）$= (|A|,\ |\pi(\Gamma)|) = 1$。$\pi(\Gamma)$在 L 中的坐标像是 E中A的补充子群。

阿贝尔情形。 在标准补 L/A 中，选择 E 内 A 的公共补群。

非阿贝尔情形。选择 $\pi_1(\Gamma)$ 作为 E 中 A 的公共补群。
在这两种情况下，根据 Schur–Zassenhaus [15, 定理 6.2.1 以及第 127],页，我们可以用 A 中的元素对每个坐标像进行共轭，使其落在所选的补充子群中。对于每个 $\gamma \in \Gamma$，共轭后的坐标都位于同一个补充子群中，并且投影到 E/A中的同一个元素。该投影在这个补充子群上是单射的，因此各坐标相等。因此，用所选 A元素组成的元组（视为 A^t中的元素）进行共轭后，$\pi(\Gamma)$ 变为对角的。其到 A^j 的投影将π_j 共轭为一个规范化的提取见证。

2. $\pi_j(G)$ 的性质。
子群G的一个 Γ-商群，其中 $(\pi_j(G))_\Gamma = 1$。它作为 L_j的子群被唯一确定：它是唯一的正规子群，其阶与 $|\Gamma|$ 互素，且其指数的所有素因子都属于 $|\Gamma|$的素因子。因此，它在 L_j的每个自同构下都保持不变。

阿贝尔情形。令 $N = \pi_j(G)/A^j \simeq \pi(G)/A^t \le L/A$。于是 $\pi_j(G) = A^j \rtimes N$。如果原始见证是非阿贝尔的，那么 $N \neq 1$，且它在 A 上的忠实作用使 $\pi_j(G)$成为非阿贝尔群。共轭作用保留这一性质。

非阿贝尔情形。子群 $A^j \le \pi_j(G)$已使 $\pi_j(G)$成为非阿贝尔群。

3. 可能的标准化数据计数。
阿贝尔情形。数据为 $L/A \le$ 一般线性群$\tau_A(q_A)$和一个映射 $\Gamma \to L/A$。根据 (3.18)，我们可以用一个生成$(r-1+d(\Gamma))$元组来指定该子群，并用 $d(\Gamma)$个生成元的像来指定该映射。因此，选择的数量至多为

$$|\operatorname{GL}_{\tau_A}(q_A)|^{r-1+2d(\Gamma)} \le q_A^{(r-1+2d(\Gamma))\tau_A^2}.$$

这些数据确定 L_j 及其 Γ-作用；任意元组只会导致重复计数。
非阿贝尔情形。通过在 A上的共轭作用将 $L \le$对称群$|A|$ 嵌入其中。界 $d(L) \le r-1+d(\Gamma)$ 使我们能够对 L 的生成元组以及标准化映射$\Gamma \to L$下 $d(\Gamma)$个生成元的像进行计数。至多有

$$(|A|!)^{r-1+d(\Gamma)}(|A|!)^{d(\Gamma)} = (|A|!)^{r-1+2d(\Gamma)}$$

选择。 L 的唯一极小正规子群和指定的 j 决定了 L_j 及其 Γ作用。在两种情形下，第 2 部分都将 W 确定为 L_j的特征子群，因此归一化数据在 Γ同构意义下确定了 W，但并未指定 G 或π_j。这就证明了 (3.20)。

4. 从下方界定 $|$自同构$_\Gamma(\pi_j(G))|$ 。
阿贝尔情形。 Aut L/A $A^j \simeq$ $\pi_j(\Gamma)$ q_A $L_j =$ ( ) GL ( ) 中 $A^j \rtimes L/A$ $\pi_j(G)$ 2, 的每个元素都可延拓为 ( ) 的一个自同构，且该自同构在 上的作用恒等。它逐点固定 ( )，并根据第 部分保持 ( )，因此其限制表示是 Γ等变的。由于 $A^j \le \pi_j(G)$，限制表示是忠实的，故有

$$|\operatorname{Aut}_\Gamma(\pi_j(G))| \ge |\operatorname{GL}_j(q_A)| \ge \rho q_A^{j^2}.$$

非阿贝尔情形。坐标置换作用于 L_j，并逐点固定对角的 $\pi_j(\Gamma)$。根据第 2 部分，它们保持 $\pi_j(G)$ 不变，并忠实地作用于 $A^j \le \pi_j(G)$。因此 $|\operatorname{Aut}_\Gamma(\pi_j(G))| \ge j!$ ，从而证明了 (3.21)。

□

3.4 阿贝尔底非阿贝尔见证的二次指数间隙

当 A 为非阿贝尔时，来自引理 3.10 的大重数和阶乘自同构群上界给出了第 3.5 节所需的概率估计。剩下的情形是一个具有阿贝尔底 A 的非阿贝尔归一化见证，因此其商群 $W = \pi_j(G)$ 是非阿贝尔的。为了证明此类商群出现的概率可以忽略不计，我们需要其二次衰减系数$\kappa(A)$（定义如下）严格大于首项系数 κ。

对于具有阿贝尔底的规范化见证，令

$$a(A) = \begin{cases} \frac{1}{2}, & p \mid n \text{ and } A \simeq A^\vee \text{ as } \mathbb{F}_p[L/A]\text{-modules}, \\ 1, & \text{otherwise}, \end{cases} \qquad \kappa(A) = a(A)\tau_A^2 \log q_A. \tag{3.22}$$

本小节中的所有对偶空间均取自素域。

引理 3.11。 我们有 $\kappa(A) \geq \kappa$。等号成立意味着

$$A|_\Gamma \simeq V \in \mathcal{M}, \qquad q_A = q_V, \quad \tau_A = \tau_V, \quad a(A) = a_V. \tag{3.23}$$

证明。 该限制表示含有一个非平凡成分：否则 $\pi_j(\Gamma)$ 作用平凡，而其正规生成性会使忠实群 $L/A \neq 1$ 变成平凡群。令 $\mathcal{R}$ 为由 Γ 在 A 上的作用所诱导的代数同态 $\mathbb{F}_p[\Gamma] \to \mathrm{End}^{\mathbb{F}_{q_A}}(A)$ 的像代数。对于一个 $\mathbb{F}_p[\Gamma]$-模 W，令 $\mathrm{Supp}(W)$ 表示其不可约成分的同构类集合，不计重数。于是

$$\mathcal{R} \simeq \prod_{V \in \mathrm{Supp}(A|_\Gamma)} M_{\tau_V}(q_V) \subseteq M_{\tau_A}(q_A), \qquad \sum_{V \in \mathrm{Supp}(A|_\Gamma)} \tau_V^2 \log q_V \leq \tau_A^2 \log q_A.$$

若存在平凡模，则 q_V，τ_V 具有相同的端同态域含义。若 $a(A) = 1$，则任一非平凡成分都给出该界。若 $a(A) = 1/2$，则在存在非平凡自对偶成分时使用它。否则，由自对偶性可得一个由不同成分组成的对偶对 V，$V^\vee$；像代数至少有两个因子，因此 $\mathcal{R} \subsetneq M_{\tau_A}(q_A)$，并且

$$\kappa(A) = \tfrac{1}{2}\log|M_{\tau_A}(q_A)| > \tfrac{1}{2}\log|\mathcal{R}| \geq \kappa_V \geq \kappa.$$

其他情形下的等号成立，意味着 $\mathcal{R} = M_{\tau_A}(q_A)$ 和 $a(A) = a_V$。因此，自然模在 $\mathbb{F}_p[\Gamma]$ 上不可约，且自同态域为 $\mathbb{F}_{q_A}$，从而证明了该断言。 □

命题 3.12。 对于具有阿贝尔底的规范化见证，若 $\kappa(A) = \kappa$，则 $\pi_j(G) = A^j$。因此，存在一个仅依赖于 Γ、n 的 $\kappa_+ > \kappa$，使得每个具有阿贝尔底的非阿贝尔归一化见证都满足 $\kappa(A) \geq \kappa_+$。

证明。 令 $Q = \pi_j(G)$ 和 $H = \pi_j(\Gamma) \leq L/A$。我们证明 $N := Q/A^j \leq L/A$ 是平凡的，由此得到 $Q = A^j$。我们分别讨论 $|\Gamma|$ 为偶数和奇数的情形。若一个不可约表示的表示空间不存在由群置换的两个或多个非零子空间的直和分解，则称该表示为本原表示。在偶数情形下，我们首先证明 $\left(A \otimes_{\mathbb{F}_{q_A}} \mathbb{F}_p\right)|_\Gamma$ 是 Γ 的本原表示。由于 N 的阶为奇数且其为可解群，克利福德理论和 Fong–Swan 定理便迫使 N 通过数量作用。在奇数情形下，H 是可解群，而一个循环商群会产生表示 W，使得 $\kappa_W < \kappa$，除非 $\tau_A = 1$。在两种情形下，由 H 正规生成便可推出 $N = 1$。

在两种情形下，我们都会用到整除关系 $\tau_A \mid |\Gamma|$。由引理 3.11， $A|_\Gamma \simeq V \in \mathcal{M}$，且 A 在 H 上的限制表示在 $\mathbb{F}_{q_A}$ 上绝对不可约：其像代数为 $M_{\tau_A}(q_A)$。令 $A = A \otimes_{\mathbb{F}_{q_A}} \mathbb{F}_p$。非模特征标理论给出 $\tau_A = \tau_V \mid |\Gamma|$；参见 [10]。还需回顾的是

$$L/A = N \rtimes H \leq \mathrm{GL}_{\tau_A}(q_A), \qquad (|N|, |\Gamma|) = 1,$$

并且 H 是 L/A的正规生成元。

$|\Gamma|$**为偶数的情形**。

等式 $\kappa(A) = \kappa$ 推出本原性。设 $A = B_1 \oplus \cdots \oplus B_k$是一个由非零子空间构成的分解，且这些子空间在 Γ的作用下彼此置换，其中 $k > 1$。不可约性使这一置换作用是传递的，因此 $2 \leq k \leq \tau_A$ 和 $k \mid |\Gamma|$。令 Γ通过置换B_i作用于 $\mathbb{F}_p^k$ ：若 $\gamma(B_i) = B_j$，则对标准基向量有 $\gamma(e_i) = e_j$ 。此作用保持增广模

$$M = \{(x_1, \ldots, x_k) \in \mathbb{F}_p^k : x_1 + \cdots + x_k = 0\}.$$

Γ-模 M 是半单的，因为 $p \nmid |\Gamma|$。传递性意味着 $\mathbb{F}_p^k$中每个被 Γ固定的向量都是常向量；这样的向量属于 M 当且仅当它为零，因为 $p \nmid k$。因此 M 没有平凡成分。

由于此作用置换坐标，点积是 Γ-不变的。它在M 上的限制是非退化的： M 中与 M 的所有向量正交的向量必须具有常数坐标，因此由于 $p \nmid k$，它只能为零。因此映射

$$M \longrightarrow M^\vee, \qquad x \longmapsto \left(y \longmapsto \sum_{i=1}^{k} x_i y_i \right)$$

是一个 Γ-等变同构，因此 M 作为 Γ-表示是自对偶的。

对于一个满足 $\dim_{\mathbb{F}_p} W = d$ 的成分 W，记作 $q_W = p^f$，则有 $d = f\tau_W$，从而$\tau_W^2 \log q_W \leq d^2 \log p$。如果 $a(A) = 1$，则任选 M 的一个成分。如果 $a(A) = 1/2$，则 $p \mid n$：若存在自对偶成分，就选择一个，使得 $a_W = 1/2$；否则选择一个不同对偶对中的成员，其维数至多为 $(k-1)/2$。在每种情况下，

$$\kappa \leq \kappa_W \leq a(A)(k-1)^2 \log p < a(A)\tau_A^2 \log q_A = \kappa,$$

矛盾。因此，A不允许存在这样的分解。

应用克利福德理论和丰–斯旺定理。群 N 的阶为奇数，因此根据 [9] 它是可解的。根据克利福德理论，$A|_N$ 是完全可约的，其同型分量由H置换。刚刚证明的本原性迫使其只有一个同型分量，因此

$$\overline{A}|_N \simeq V_0^{\oplus e}$$

对于一个不可约的 $\overline{\mathbb{F}}_p[N]$-模 V_0。令 $d = \dim_{\mathbb{F}_p} V_0$；则 $\tau_A = ed$。由于 N 是可解的，Fong–Swan 定理 [11, 定理 10.1]将 V_0 的布劳尔特征标提升为具有相同次数的普通不可约特征标。普通不可约特征标的次数整除群阶，因此 $d \mid |N|$。但同时 $d \mid \tau_A \mid |\Gamma|$，由互素性可得 $d = 1$。所有被加数都是同一个一维表示的副本，因此 N 中的每个元素都在 A上按数量作用。忠实性使得 N 在 L/A中是中心的，从而 $L/A = N \times H$。因此 H 是正规子群；由于它正规生成 L/A，我们得到 $L/A = H$ 和 $N = 1$。

情形 $|\Gamma|$ 为奇数。 我们断言 $\tau_A = 1$。否则 $\tau_A \mid |\Gamma|$ 给出 $\tau_A \geq 3$。非平凡像H 在一般线性群 $\mathrm{GL}_{\tau_A}(q_A)$ 中由 [9], 可解，因此它有一个商群 C_ℓ，其中 $\ell \neq p$为素数。由于 $\ell \mid |$一般线性群 $\mathrm{GL}_{\tau_A}(q_A)|$，对于某个 $i \leq \tau_A$，我们有 $\ell \mid q_A^i - 1$。拉回一个非平凡的简单 $\mathbb{F}_p[C_\ell]$-模，得到 $W \in \mathcal{I}$，满足 $\tau_W = 1$ 和 $q_W \leq q_A^i \leq q_A^{\tau_A}$。因此

$$\kappa \leq \kappa_W \leq \tau_A \log q_A < \tfrac{1}{2}\tau_A^2 \log q_A \leq \kappa(A) = \kappa,$$

矛盾。因此 $\tau_A = 1$，且 $L/A \leq \mathrm{GL}_1(q_A)$ 是阿贝尔的。由 H 对其进行正规生成，再次得到 $L/A = H$ 和 $N = 1$。

严格不等式 $\kappa(A) > \kappa_\circ$。 我们已经证明，只要 $\kappa(A) = \kappa$，就有 $\pi_J(G) = A^j$。因此，根据引理 3.11，每个具有阿贝尔底的非阿贝尔归一化见证都满足 $\kappa(A) > \kappa_\circ$ 数值集合

$$\{a\tau_A^2 \log q_A : q_A \text{ a prime power},\ \tau_A \geq 1,\ a \in \{1/2, 1\}\}$$

是局部有限的。其大于 κ 的最小元素可取为 κ_+。 □

3.5 Boun全体生成元秩尾部与阿贝尔生成元秩尾部之差 s

现在我们来界定$\mathbf{P}(d_\Gamma(X) \geq r)$ 与 $\mathbf{P}(d_\Gamma(X^{\mathrm{ab}}) \geq r)$ 之间的差。目标是证明，存在某个仅取决于 Γ, n 的 $\delta > 0$，使得

$$0 \leq \mathbf{P}(d_\Gamma(X) \geq r) - \mathbf{P}(d_\Gamma(X^{\mathrm{ab}}) \geq r) \ll_{\Gamma,n} e^{-(\kappa+\delta)r^2}.$$

若 $d_\Gamma(X) \geq r > d_\Gamma(X^{\mathrm{ab}})$，则第 3.3 节中的冠约化和投影会产生一个非阿贝尔归一化见证，其源群是 X 的有限 Γ-商群。因此，只需界定此类见证的概率。每个此类见证都给出 X 的一个非阿贝尔见证商群。

我们利用商矩将结构性结论转化为概率估计，并对参数化可能的非阿贝尔见证商群的归一化数据求和。对于阿贝尔底，不等式 $\kappa(A) \geq \kappa_+ > \kappa$ （见第 3.4 节）使得总和小于主要的初等阿贝尔尾概率。对于非阿贝尔底，指数重数和阶乘自同构群上界使得其贡献更小。

下文中的常数可以依赖于 Γ, n 并可适当增大。我们首先给出一个二阶上同调上界，用于两类冠的基底。

引理 3.13。 对于每个有限阿贝尔群 T，存在一个常数 θ_T，使得对于每个有限群 J及其在 T上的每个 J-作用，

$$|H^2(J, T)| \leq |J|^{\theta_T(d(J)+1)}. \tag{3.24}$$

证明。 $J = 1$ 的情形显然。否则，令 $C_{\mathrm{abs}} = 24/\log 2$。由 [4, 定理 13.9]及其后立即陈述的主因子界可知，存在一个自由有限剩余表示$1 \to R \to F \to J \to 1$，其中 R 可由至多

$$d(J) + 20 + (d(J) + 2)\log_2 |J| \leq C_{\mathrm{abs}} d(J) \log |J|$$

元素。不等式使用 $d(J) \geq 1$和 $\log_2 |J| \geq 1$。将 T上的作用提升到 F。由于 R作用平凡且 $H^2(F, T) = 0$，五项序列表明 $H^2(J, T)$ 是.....的商群

同态集$_{\mathrm{cont}}(R,\ T)^F$。这样的等变同态由其在所选正规生成元上的取值决定。因此

$$|H^2(J,T)| \le |T|^{C_{\mathrm{abs}} d(J)\log|J|} = |J|^{C_{\mathrm{abs}} d(J)\log|T|}.$$

因此我们可以取 $\theta_T = C_{\mathrm{abs}}\log\ |T|$。 □

对于 $T=\mathbb{Z}/n$，记 $\theta_n = \theta_{\mathbb{Z}/n}$。

引理 3.14. 对于规范化见证，取 (3.19) 中的 j，膨胀给出

$$H^2(\pi_j(G)\rtimes\Gamma,\mathbb{Z}/n) \simeq H^2(L_j,\mathbb{Z}/n).$$

若 A 是阿贝尔的，则

$$|H^2(L_j,\mathbb{Z}/n)| \le q_A^{(1-a(A))(j^2+j)+\tau_A j+\theta_n(r+d(\Gamma))\tau_A^2}. \tag{3.25}$$

若 A是非阿贝尔的，则

$$|H^2(L_j,\mathbb{Z}/n)| \le (|A|!)^{\theta_n(r+d(\Gamma))}|A|^{3\theta_n j}. \tag{3.26}$$

证明. $\pi_j(G)\rtimes\Gamma \to L_j = \pi_j(G)\rtimes\pi_j(\Gamma)$ 的核的阶整除 $|\Gamma|$，因此与 n 互素。膨胀将它们的上同调与系数 $\mathbb{Z}/n$ 识别。

阿贝尔底。令 A 具有特征 p。与 p 互素的系数只贡献基础上同调。对于 $p^e\|n$，Lyndon–Hochschild–Serre谱序列的二次项给出

$$|H^2(L_j,\mathbb{Z}/p^e)| \le |H^2(L/A,\mathbb{Z}/p^e)|\,|H^1(L/A,(A^\vee)^j)|\,|H^2(A^j,\mathbb{Z}/p^e)^{L/A}|.$$

根据 [3, 定理 A]，中间因子至多为 $q_A^{\tau_A j}$。万有系数序列的 Ext^1 项中没有（L/A）-不变元，因为 A 是非平凡不可约模。因此，它给出了最后一个群到 $\mathrm{Hom}(\bigwedge^2_{\mathbb{F}_p} A^j,\mathbb{F}_p)^{L/A}$的单射。由舒尔引理和外幂分解可知，当 A 自对偶时，该群至多为 $q^{\binom{j}{2}_A+j}$，否则至多为 1。应用 (3.24)，其中$|L/A| \le q_A^{\tau_A^2}$且 $d(L/A)+1 \le r+d(\Gamma)$，得到 (3.25)。

非阿贝尔底。设 $A = S^a$，其中 S 为简单的。由于 A^j 是完美的，同一谱序列没有中间的 H^1-项，并给出

$$|H^2(L_j,\mathbb{Z}/n)| \le |H^2(L/A,\mathbb{Z}/n)|\,|H^2(A^j,\mathbb{Z}/n)^{L/A}|.$$

每个非阿贝尔有限单群都由两个元素生成；参见 [4, p. 471]。因此，由 (3.24)、泛系数以及完美群的舒尔乘子的乘积公式可得

$$|H^2(A^j,\mathbb{Z}/n)^{L/A}| \le |H^2(S,\mathbb{Z}/n)|^{aj} \le |A|^{3\theta_n j}.$$

将 (3.24) 应用于 L/A，其中 $|L/A| \le |A|!$ 且 $d(L/A)+1 \le r+d(\Gamma)$，可得 (3.26)。 □

引理 3.15。令

$$C_0 = 3+(d(\Gamma)+3)\theta_n = 3+\frac{24}{\log 2}(d(\Gamma)+3)\log n.$$

对于规范化见证，令 j 如(3.19)中所示，具有商群 Γ-同构于 $\pi_j(G)$ 的开正规 Γ-稳定子群的期望数量满足

$$\mathbf{E}\#\{N\trianglelefteq X : N \text{ open and } \Gamma\text{-stable},\ X/N\simeq_\Gamma \pi_j(G)\} \le \begin{cases}\rho^{-1}q_A^{-a(A)j^2+C_0(\tau_A j+r\tau_A^2)}, & A \text{ abelian},\\ (|A|!)^{C_0 r}\,|A|^{C_0 j}/j!, & A \text{ nonabelian}.\end{cases}$$

证明。 根据 (2.1)、引理 3.14 以及 $w_U(\pi_j(G)) \ge 1$,

$$\frac{\mathbf{E}|\operatorname{Sur}_\Gamma(X,\pi_j(G))|}{|\operatorname{Aut}_\Gamma(\pi_j(G))|} \le \frac{|H^2(L_j,\mathbb{Z}/n)|}{|\operatorname{Aut}_\Gamma(\pi_j(G))|}.$$

*Ab*阿贝尔底。 使用 (3.25) 和 (3.21)。由于 $\tau_A \ge 1$ 和 $1-a(A) \le 1/2$, 我们得到

$$\frac{\mathbf{E}|\operatorname{Sur}_\Gamma(X,\pi_j(G))|}{|\operatorname{Aut}_\Gamma(\pi_j(G))|} \le \rho^{-1} q_A^{-a(A)j^2+3\tau_A j+[1+\theta_n(r+d(\Gamma))]\tau_A^2}.$$

不等式 $C_0 \ge 3$ 和 $1+\theta_n(r+d(\Gamma)) \le C_0 r$ 证明了阿贝尔情形。

非阿贝尔底。 使用 (3.26) 和 $|\mathrm{Aut}_\Gamma(\pi_j(G))| \ge j!$ 可得

$$\frac{\mathbf{E}|\operatorname{Sur}_\Gamma(X,\pi_j(G))|}{|\operatorname{Aut}_\Gamma(\pi_j(G))|} \le (|A|!)^{1+\theta_n(r+d(\Gamma))} \frac{|A|^{(1+3\theta_n)j}}{j!}.$$

由于 $1+\theta_n(r+d(\Gamma)) \le C_0 r$ 和 $1+3\theta_n \le C_0$, 这证明了非阿贝尔情形。 □

命题 3.16。 存在仅依赖于 Γ、n 的 $\delta>0$, 使得对于每个 $r \ge 4$, 某个有限 Γ-商群 G 是 X 的非阿贝尔归一化见证（G、L、A、π_j、r）的来源的概率为 $O_{\Gamma,\,n}(e^{-(\kappa+\delta)r^2})$。

证明。 对于每一种归一化数据, 令 W 为相应的见证商群。 X 以 W 为商群的概率至多为其商核的期望数。存在规范化见证意味着相应的 W 是一个商群, 因此对归一化数据应用并集界即可, 即使多个见证对应相同的 Γ-同构类型的 W 也不例外。

Set

$$C_1 = 8+4C_0+d(\Gamma), \qquad C_2 = C_0+1+2d(\Gamma),$$

其中 C_0 是引理 3.15 中的显式常数。

在阿贝尔底情形下, 将引理 3.15 中的不等式乘以计数式 (3.20), 并代入 $j=(r-3)\tau_A$。对于固定的 q_A, τ_A, a, 所得结果至多为

$$\rho^{-1} q_A^{\tau_A^2[-a(r-3)^2+C_0(2r-3)+r-1+2d(\Gamma)]} \le \rho^{-1}\exp\{-a\tau_A^2\log q_A[r^2-C_1 r]\}.$$

这里我们用到了 $r \ge 4$ 和 $a \ge 1/2$: 由此得到 $2d(\Gamma) \le d(\Gamma)r/2$, 以及 $2C_0+1+d(\Gamma)/2 \le a(4C_0+2+d(\Gamma))$。对于非阿贝尔见证商群为 W 且阿贝尔单底为 A 的见证, $\kappa(A) \ge \kappa_+ > \kappa$。对于 $r^2-C_1 r > 4$, 求和有如下上界:

$$\rho^{-1}e^{-\kappa_+[r^2-C_1 r-4]} \times \sum_{q_A\ge 2}\sum_{\tau_A\ge 1}\sum_{a\in\{1/2,1\}} q_A^{-4a\tau_A^2} \ll e^{-\kappa_+ r^2+O(r)}.$$

这里的和即使对所有整数 $q_A \ge 2$ 求和也收敛, 因为 $4a\tau_A^2 \ge 2\tau_A$。对于任意固定的 $0<\delta<\kappa_+-\kappa$, 这满足所需的界。

对于非阿贝尔底, 直接按 $|A|$ 计数。估计 (3.20) 和引理 3.15 中的不等式给出每个 $|A|$对应的总数上界:

$$(|A|!)^{C_2 r}\frac{|A|^{C_2 j}}{j!}, \qquad j=|A|^{r-3}.$$

事实上，这些界中的阶乘指数为 $(C_0+1)r-1+2d(\Gamma) \le C_2 r$，而 $|A|$ 的指数至多为 $C_2 j$。对于所有充分大的 r，一致地对 $|A| \ge 2$，由斯特林不等式可得：

$$\log\left((|A|!)^{C_2 r} \frac{|A|^{C_2 j}}{j!} \right) \le C_2 r |A| \log|A| - j\big((r-3-C_2)\log|A| - 1\big) \le -j \log|A|.$$

对于最后一个不等式，我们要求 r 足够大，使得

$$C_2 r|A| \le (r - C_2 - 6)|A|^{r-3},$$

一致地 地关于 $|A| \ge 2$成立。因此，对 $|A| \ge 2$ 的所有整数值求和可得

$$\sum_{|A|\ge 2} |A|^{-|A|^{r-3}} \le 2\, 2^{-2^{r-3}} = O(e^{-r^3}),$$

利用 $|A|^{r-3} \ge 2^{r-3} + |A| - 2$。对于每个固定的 $c>0$，这比 e^{-cr^2} 衰减得更快。所有并集都是可数的，并且这些界对于满足引言中所述不动向量条件的 U 均一致，因为只用到了 $w_U(\pi_j(G))^{-1} \le 1$。 □

3.6 尖尾证明的完备化

我们将精确的阿贝尔计算与可忽略见证估计结合起来。如果整个群至少需要 r 个生成元，而其阿贝尔化不需要，那么冠约化会产生一个非阿贝尔规范化见证；其存在性通过见证商群来界定。这就将阿贝尔渐近式转移到整个群上。接着，我们在 $\mathcal{M}$ 中的表示里选取最小的线性指数，以得到 C 和 ζ，并推出点质量渐近式。

定理 *1.1* 的证明。 在命题 2.1 的满测度集上进行讨论。
给 $\mathbf{P}(d_\Gamma(X) \ge r)$ 与 $\mathbf{P}(d_\Gamma(X^{\mathrm{ab}}) \ge r)$之间的差值设定上界。 若 $d_\Gamma(X) \ge r > d_\Gamma(X^{\mathrm{ab}})$，则由紧致性可得一个有限商群 G，使得 $d_\Gamma(G) \ge r$。应用引理 3.8，得到一个见证 (G, L, A, π, r)。其像 $\pi(G)$ 是非阿贝尔的，否则满同态$X \twoheadrightarrow_\Gamma \pi(G)$ 将经由 X^{ab} 分解。由引理 3.10，该见证具有非阿贝尔归一化提取。应用命题 3.16 得到

$$0 \le \mathbf{P}(d_\Gamma(X) \ge r) - \mathbf{P}(d_\Gamma(X^{\mathrm{ab}}) \ge r) \ll e^{-(\kappa+\delta)r^2}. \tag{3.27}$$

结合 (3.27)，命题 3.4 给出 (3.6)：有限和至少为 $e^{-\kappa r^2 - O_{(r)}}$，因此比较误差可并入其相对误差 $O(e^{-\varepsilon r})$。将 ε 减小，使得$\varepsilon \le 2\kappa$ 且对每个满足 $\zeta_V > \zeta$的 $V \in \mathcal{M}$ 都有 $\varepsilon \le \zeta_V - \zeta$后，展开 $k_V(r) = \tau_V r - (\tau_V - 1)$ 并利用 C和 ζ的定义，可将此和识别为 $Ce^{-\kappa r^2 - \zeta r}(1 + O(e^{-\varepsilon r}))$：含有$\zeta_V > \zeta$ 的项呈指数级小，其余项相加为 C。这就证明了 (1.1)。 $r+1$ 处尾部与 r 处尾部之比为 $O(e^{-2\kappa r})$，因此相减可得点质量具有相同的渐近式。

□

4 几乎必然有限表示与亏格

我们沿用引言中的记号，其中 $(n,|\Gamma|)=1$，且 U 满足其中陈述的不动向量条件。本节证明定理 1.2。所有上同调均为连续上同调。

额外的输入是 Sawin 和 Wood 关于以正概率出现的有限层商群所得到的不等式。这些不等式给出了第二上同调与第一上同调之差的界；随后，Liu 的关系公式将这一差值转化为估计式 (1.2)。

4.1 正概率出现的有限商群

一个层 是有限 Γ 群同构类的集合，由有限多个群在商群及有限次直积下生成 [8, 第 1 节1]。次直积是乘积中的一个 Γ-稳定子群，其到每个因子的投影都是满射。

记 $\mathcal{P}_{\Gamma,n}$ 为小型有限剩余 n-定向群的样本空间，并将一个定向样本记为 $\boldsymbol{X}=(X,s_X)$。对于一个层 $\mathcal{L}$，X 的最大 $\mathcal{L}$-商群是 $\mathcal{L}$ 中的商群，所有从 X 到 $\mathcal{L}$ 中某个群的连续 Γ-等变商映射都经由该商群分解。对于小型 X，它存在且是有限的；见 [8, 第 1 节1]。赋予其诱导定向后，将其记为 $\boldsymbol{X}^{\mathcal{L}}$。对于有限定向 Γ 群 $\boldsymbol{H}=(H,s_H)$，设

$$C(\mathcal{L},\boldsymbol{H}):=\{\boldsymbol{X}:\boldsymbol{X}^{\mathcal{L}}\simeq\boldsymbol{H}\}.$$

我们使用 $\nu_{\Gamma、n、U}$ 的完备化。

引理 4.1。存在一个测度为一的可测集 $\Omega_+\subseteq\mathcal{P}_{\Gamma,\,n}$ 使得每个包含 Ω_+ 中一点的 $C(\mathcal{L},\boldsymbol{H})$ 都具有正测度。如果 $\boldsymbol{X}\in\Omega_+$ 且 $\boldsymbol{H}=\boldsymbol{X}^{\mathcal{L}}$，那么 $H_\Gamma=1$。

证明。有限 Γ 群按同构计只有可数多个，因此层也只有可数多个。每个有限群只有有限多个 n 定向。因此，$C(\mathcal{L},\ \boldsymbol{H})$ 的集合是可数的。去掉其中零测度成员的并集，得到 Ω_+。最后一个断言由 [8, 定理 1.8], 得出；该定理指出，若 $C(\mathcal{L},\ \boldsymbol{H})$ 的商群具有 $H_\Gamma\neq1$，则其测度为零。 □

设 $\ell\nmid|\Gamma|$ 是素数，且 V 是有限维不可约 $\mathbb{F}_\ell[H\rtimes\Gamma]$-模。令 $V^\vee:=$同态集$_{\mathbb{F}_\ell}(V,\ \mathbb{F}_\ell)$。若 $V\rtimes H\in\mathcal{L}$，则称 V 在 $(\mathcal{L},\ \boldsymbol{H})$ 上合格，如 [8, 第 1 节6] 所述。该截面$H\to V\rtimes H$ 将 s_H 向前推送，得到一种定向，使得投影是一个定向态射。其核没有非平凡真子群同时满足正规于源对象且在 Γ 下稳定，因为 V 是不可约的。

根据定义 7.28]，记

$$H^2(H\rtimes\Gamma,V)^{\mathcal{L}}$$

为其关联的 Γ 到 H 的 V 扩张的底层群属于 $\mathcal{L}$ 的上同调类。对于合格的V，该集合非空，并且根据引理 5.9], 它是一个 $\mathbb{F}_\ell$ 子空间。定义模权重

$$w_{H,U}(V):=\frac{\prod_{E\in U}|V^{\gamma_E}|}{|V^{H\rtimes\Gamma}|}=\frac{|V^\Gamma|}{|V^{H\rtimes\Gamma}|}\,w_U(V).\tag{4.1}$$

这里，$w_U(V)$将前面定义的群权重应用于 V的加法 Γ-群。额外的下标 H 记录了分母中使用完整的 $H\rtimes\Gamma$-不动点空间。两个权重都是数，并且此公式中的所有不动点空间均按基数计数。

当 $\ell \mid n$时，我们希望定向 s_H 能够提升到扩张 $1 \to V \to E \xrightarrow{\pi} H \to 1$：也就是说，我们希望 $s_E \in H_3(E,\ \mathbb{Z}/n)^\Gamma$ 满足 $\pi_*(s_E) = s_H$。记 $H^2(H \rtimes \Gamma,\ V)^{\mathcal{L},\ s_H}$ 为能够如此提升的上同调类 $\alpha \in H^2(H \rtimes \Gamma,\ V)^{\mathcal{L}}$ 构成的子空间。根据 [8, 定义 7.28 和引理 7.29], ，这等价于

$$s_H(\alpha \smile \beta) = 0 \quad \text{for every } \beta \in H^1(H \rtimes \Gamma, V^\vee),$$
$$s_H\big(B(\varphi_*\alpha)\big) = 0 \quad \text{for every } \varphi \in \mathrm{Hom}_{H\rtimes\Gamma}(V, \mathbb{Z}/n).$$

这里，s_H 通过 [8, 引理 5.4–5.5], ，利用杯积计算 $H^3(H \rtimes \Gamma, \mathbb{Z}/n)$中的上同调类；杯积通过同态集 $\mathrm{Hom}(V, \mathbb{Z}/n) \simeq V^\vee$ 借助$(\mathbb{Z}/n)[\ell] \simeq \mathbb{F}_\ell$给出，而 B：$H^2(H \rtimes \Gamma, \mathbb{Z}/n) \to H^3(H \rtimes \Gamma, \mathbb{Z}/n)$是 $0 \to \mathbb{Z}/n \xrightarrow{\times n} \mathbb{Z}/n^2 \to \mathbb{Z}/n \to 0$的 Bockstein。对于非平凡不可约 V，第二个条件是空泛的；对于平凡模 $V = \mathbb{F}_\ell$，它至多增加一个 $\mathbb{F}_\ell$-线性条件。

如果 $H_\Gamma = 1$ 且 $C(\mathcal{L}, \boldsymbol{H})$具有正测度，[8, 命题 7.49] 就会针对每个合格的 V给出：

$$|H^2(H \rtimes \Gamma, V)^{\mathcal{L}}| \le |H^1(H \rtimes \Gamma, V)| w_{H,U}(V), \qquad \ell \nmid n, \tag{4.2}$$
$$|H^1(H \rtimes \Gamma, V^\vee)|\,|H^2(H \rtimes \Gamma, V)^{\mathcal{L}, s_H}| \le |H^1(H \rtimes \Gamma, V)| w_{H,U}(V), \qquad \ell \mid n. \tag{4.3}$$

4.2 一个一致的有限层上同调界

引理 4.2。设 $\boldsymbol{X} \in \Omega+$，设 $\boldsymbol{H} = \boldsymbol{X}^{\mathcal{L}}$，并设 V在$(\mathcal{L}, \boldsymbol{H})$处合格。那么

$$\dim_{\mathbb{F}_\ell} H^2(H \rtimes \Gamma, V)^{\mathcal{L}} \le \dim_{\mathbb{F}_\ell} H^1(H \rtimes \Gamma, V) + |U| \dim_{\mathbb{F}_\ell} V. \tag{4.4}$$

若 $\ell \nmid n$，则更精确的界为

$$\dim_{\mathbb{F}_\ell} H^2(H \rtimes \Gamma, V)^{\mathcal{L}} \le \dim_{\mathbb{F}_\ell} H^1(H \rtimes \Gamma, V) + \sum_{E \in U} \dim_{\mathbb{F}_\ell} V^{\gamma_E} - \dim_{\mathbb{F}_\ell} V^{H \rtimes \Gamma}. \tag{4.5}$$

证明。$C(\mathcal{L}, \boldsymbol{H})$由引理 4.1知具有正测度。在整个证明中，所有维数均取在 $\mathbb{F}_\ell$ 上。由于 V 不可约，

$$\dim V^{H \rtimes \Gamma} = \begin{cases} 0, & V \text{ is nontrivial}, \\ 1, & V = \mathbb{F}_\ell \text{ is trivial}. \end{cases}$$

由等式 (4.1) 得

$$\log_\ell w_{H,U}(V) = \sum_{E \in U} \dim V^{\gamma_E} - \dim V^{H \rtimes \Gamma} \le |U| \dim V - \dim V^{H \rtimes \Gamma}. \tag{4.6}$$

对于 $\ell \nmid n$，对 (4.2) 取对数。保留 (4.6) 中的等式即可得到 (4.5)；其上界则给出 (4.4)。

现在假设 $\ell \mid n$。定义 $H^2(H \rtimes \Gamma, V)^{\mathcal{L}, s_H}$ 的杯积条件给出了一个从 $H^2(H \rtimes \Gamma, V)^{\mathcal{L}}$ 到 $H^1(H \rtimes \Gamma, V^\vee)$ 对偶空间的线性映射。Bockstein 条件至多再贡献 $\dim V^{H \rtimes \Gamma}$ 个线性无关的线性泛函。因此，

$$\dim H^2(H \rtimes \Gamma, V)^{\mathcal{L}} - \dim H^2(H \rtimes \Gamma, V)^{\mathcal{L}, s_H} \le \dim H^1(H \rtimes \Gamma, V^\vee) + \dim V^{H \rtimes \Gamma}.$$

另一方面，由 (4.3) 得

$$\dim H^2(H \rtimes \Gamma, V)^{\mathcal{L}, s_H} \le \dim H^1(H \rtimes \Gamma, V) + \log_\ell w_{H,U}(V) - \dim H^1(H \rtimes \Gamma, V^\vee).$$

将这些不等式相加并利用（4.6），即可证明（4.4）。在平凡模的情形下，额外的 Bockstein 条件被（4.1）中的分母 $|V^{H \rtimes \Gamma}|$ 抵消。 □

4.3 过渡到 pro有限群

上述界仅涉及处于指定层中的扩张类。为了应用关系公式，我们需要对所有连续二阶上同调类得到同样的界。

命题 4.3。 设 $\boldsymbol{X} = (X, s_X) \in \Omega_+$，并设 V 是有限不可约连续 $\mathbb{F}_\ell[X \rtimes \Gamma]$-模，其中 $\ell \nmid |\Gamma|$。若 $H^1(X \rtimes \Gamma, V)$ 是有限维的，则

$$\dim_{\mathbb{F}_\ell} H^2(X \rtimes \Gamma, V) \le \dim_{\mathbb{F}_\ell} H^1(X \rtimes \Gamma, V) + |U| \dim_{\mathbb{F}_\ell} V. \tag{4.7}$$

若 $\ell \nmid n$，则此外

$$\dim_{\mathbb{F}_\ell} H^2(X \rtimes \Gamma, V) \le \dim_{\mathbb{F}_\ell} H^1(X \rtimes \Gamma, V) + \sum_{E \in U} \dim_{\mathbb{F}_\ell} V^{\gamma_E} - \dim_{\mathbb{F}_\ell} V^{X \rtimes \Gamma}. \tag{4.8}$$

证明。 设 $T \subseteq H^2(X \rtimes \Gamma, V)$ 是任意有限维子空间，其基为 $\alpha_1, \dots, \alpha_a$。由于取有限系数的连续上链可经有限商分解，因此存在一个开正规且 Γ-稳定的子群 N，它属于 X，并在 V 上平凡作用，使得这些上同调类是从 $H^2((X/N) \rtimes \Gamma, V)$ 膨胀而来。根据 $[8, \text{引理 } 5.8]$,，提升后的上同调类对应于有限 Γ-扩张$1 \to V \to E_i \to X/N \to 1$。

设 $\mathcal{L}$ 为由 $V \rtimes (X/N)$ 和 E_i 生成的层，并令 $\boldsymbol{H} = \boldsymbol{X}^{\mathcal{L}}$。商群$X/N$ 属于 $\mathcal{L}$，因此映射 $X \twoheadrightarrow X/N$ 可经由 H 分解。拉回

$$H \times_{X/N} E_i, \qquad H \times_{X/N} (V \rtimes (X/N)) \simeq V \rtimes H$$

是 $\mathcal{L}$ 中群的次直积，因此属于 $\mathcal{L}$。于是 V 在 $(\mathcal{L}, \boldsymbol{H})$ 处是合格的，膨胀到 $H \rtimes \Gamma$ 的上同调类属于 $H^2(H \rtimes \Gamma, V)^{\mathcal{L}}$。它们线性无关，因为进一步膨胀到 $X \rtimes \Gamma$ 后，它们构成 T 的所选基。应用引理 4.2 和膨胀–限制嵌入 $H^1(H \rtimes \Gamma, V) \hookrightarrow H^1(X \rtimes \Gamma, V)$ 可得

$$\dim T \le \dim H^2(H \rtimes \Gamma, V)^{\mathcal{L}} \le \dim H^1(X \rtimes \Gamma, V) + |U| \dim V.$$

这给出了每个有限维子空间 T 的上界，并证明了 (4.7)。若 $\ell \nmid n$，则用 (4.5) 代替粗略上界。不动点空间保持不变，并且 $V^{H \rtimes \Gamma} = V^{X \rtimes \Gamma}$，因为作用可经由 $H \rtimes \Gamma$ 分解。由此，同样的论证证明了 (4.8)。

□

4.4 关系秩及其推论

对于一个由有限个 Γ 生成的 pro-$|\Gamma|'$ 群 G，以及一个有限不可约 $\mathbb{F}_\ell[G \rtimes \Gamma]$-模 V，令

$$\xi_G(V) := \dim_{\mathbb{F}_\ell}\big(V^\Gamma / V^{G \rtimes \Gamma}\big) \ge 0.$$

令 $F = F'_{d_\Gamma(G)}(\Gamma)$，并令 R 为一个 Γ-等变满同态 $F \twoheadrightarrow G$的核。我们在条件 $R^{\mathrm{ab}} := R/[R,R] \neq 1$下使用相对关系公式。 $[5, \text{命题 } 3.4 \text{ 和 } 3.7]$ 中的关系模计算给出了 R^{ab} 作为有限剩余$G \rtimes \Gamma$-模的生成元秩。 $[6, \text{定理 } 3.1]$ （参见 $[6, \text{定理 } 5.1]$）的正规生成论证在环境作用 $F \rtimes \Gamma$下适用：非阿贝尔单因子总共至多需要一个正规生成元，而该生成元可由非零阿贝尔关系模吸收。因此，在此条件下，

$$r_\Gamma(G) = d_\Gamma(G) + \sup_{\substack{\ell \nmid |\Gamma| \\ V \text{ irreducible}}} \left\lceil \frac{\dim_{\mathbb{F}_\ell} H^2(G \rtimes \Gamma, V) - \dim_{\mathbb{F}_\ell} H^1(G \rtimes \Gamma, V) - \xi_G(V)}{\dim_{\mathbb{F}_\ell} V} \right\rceil. \tag{4.9}$$

此处 V 遍历有限连续模。只有在证明其中的所有上同调群都是有限维之后，我们才会应用该公式。

定理 *1.2* 的证明。将 Ω_+ 与可测集 $\{\boldsymbol{X}$ 取交：$d_\Gamma(X) < \infty\}$；根据定理 1.1，该集合的测度为一。固定取此交集中的一点。若 $d_\Gamma(X) = 0$，则 $X = 1$，结论立即成立。现假设 $d_\Gamma(X) > 0$。

X 的每个有限 Γ-商群都可经由有限层商群分解，因此由引理 4.1 可得$X_\Gamma = 1$。令 $F = F'_{d_\Gamma(X)}(\Gamma)$，且 $R = \ker(F \twoheadrightarrow X)$。对于素数 $\ell \nmid |\Gamma|$，由自由性和 $d_\Gamma(X) > 0$，存在非零的 Γ-等变同态 $f\colon F \to \mathbb{F}_\ell$，其目标上的 Γ-作用是平凡的。若$f(R) = 0$，则 f 会经由 $X_\Gamma = 1$ 分解，矛盾。因此 $R^{\mathrm{ab}} \neq 1$，验证了条件 (4.9)。

同样的论证适用于任意有限 Γ生成的 $H \neq 1$ with $H_\Gamma = 1$：对于每个$m \geq d_\Gamma(H)$，$F'_m(\Gamma)$的核 $\twoheadrightarrow H$ 具有非平凡的阿贝尔化。应用关系模公式 [5, 命题 3.7]以及前述的正规生成论证可得

$$r_{\Gamma,m}(H) - m = r_\Gamma(H) - d_\Gamma(H).$$

对于 $H = 1$，这同样成立，因为$r_{\Gamma,\ m}(1) = m$。这证明了引言中所声称的独立性。

设 V是一个有限不可约 $\mathbb{F}_\ell[X \rtimes \Gamma]$-模，满足 $\ell \nmid |\Gamma|$。由于 $H^1(\Gamma,\ V) = 0$，每个 1-余循环都与一个在 Γ上消失的 1-余循环上同调。这样的余循环由其在 X的任意 $d_\Gamma(X)$ Γ-生成元上的取值唯一决定。因此

$$\dim_{\mathbb{F}_\ell} H^1(X \rtimes \Gamma, V) \leq d_\Gamma(X) \dim_{\mathbb{F}_\ell} V < \infty.$$

根据命题 4.3,

$$\dim H^2(X \rtimes \Gamma, V) - \dim H^1(X \rtimes \Gamma, V) \leq |U| \dim V.$$

由于 $\xi_X(V) \geq 0$且 $|U|$是一个整数，(4.9) 中的每个上取整至多为 $|U|$。这证明了$r_\Gamma(X) \leq d_\Gamma(X) + |U|$，并且 $\mathrm{def}_\Gamma(X) \geq -|U|$在一个测度为一的集合上成立。 □

5 几乎必然 FAb：低于表示论假设

我们证明定理 1.3 中的充分条件。回忆一下，若每个开子群的阿贝尔化都是有限的，则称一个 pro 有限群为 FAb 群。本节中的所有阿贝尔化和正规闭包均指拓扑意义下的阿贝尔化和正规闭包。我们先将定理归结为两个概率估计，陈述这两个估计，然后在不同的小节中分别证明。

引理 5.1. 设 X 是一个 *pro*有限 Γ-群。若对 X 的每个开正规 Γ-稳定子群 H，H^{ab} 都是有限的，则 X 是 *FAb*。

证明。设 $J \leq X$ 是开子群。它在 $X \rtimes \Gamma$ 中的核为,

$$H = \bigcap_{g \in X \rtimes \Gamma} gJg^{-1},$$

是 X 中包含于 J 的开正规 Γ-稳定子群。事实上，J 在 $X \rtimes \Gamma$ 中的指数有限，因此交集中只会出现有限多个共轭。H 在 J^{ab} 中的像是有限群 H^{ab} 的商群。J^{ab} 对该像取商后，得到有限群 J/H 的一个商群。因此，J^{ab} 是有限的，符合要求。

□

在本节中， H 表示 X 的一个开正规 Γ-稳定子群；需要为商映射命名时，我们记作

$$f : X \twoheadrightarrow X/H.$$

共轭作用和 Γ-作用给出 $H^{\mathrm{ab}}(X/H) \rtimes \Gamma$ 的一个作用： H 的内自同构在其阿贝尔化上作用平凡，因此 $X \rtimes \Gamma$ 的作用可经由

$$(X \rtimes \Gamma)/H \simeq (X/H) \rtimes \Gamma.$$

记 $(H^{\mathrm{ab}})_p$ 为 H^{ab} 的 pro-p 主分量。

引理 5.2。 假设以下两个断言成立：

1. 对每个素数 p，以概率 1，$(H^{\mathrm{ab}})_p$ 对 X 的每个开正规 Γ-稳定子群 H 都是有限的。

2. 以概率 1，对每个这样的 H，都存在有限素数集 S_H，使得$(H^{\mathrm{ab}})_p = 0$ 对每个 $p \notin S_H$ 都成立。

那么 $\mathbf{P}(X$ 是 $FAb) = 1$。

证明。 对第一项断言中所有素数对应的概率为一事件取交集，再与第二项断言中的事件取交集。在所得事件上，对于每个开正规Γ-稳定 H，

$$H^{\mathrm{ab}} \simeq \prod_{p \in S_H} (H^{\mathrm{ab}})_p$$

都是有限群的有限直积。应用引理 5.1。 □

我们希望用有限扩张和上同调来表述引理 5.2 中的两个有限性条件。首先，我们需要一种遍历 X的所有开正规 Γ-稳定子群的方法。这些子群恰好是连续 Γ-等变满同态映射到有限 Γ-群的核。因此，我们固定一个有限 Γ-群 P，并考虑所有映射

$$f \in \mathrm{Sur}_\Gamma(X, P), \qquad H = \ker f, \qquad X/H \simeq_\Gamma P.$$

我们将对所有这些子群 H同时证明这两个条件。由于有限 Γ-群在同构意义下只有可数多个，我们随后可以对 P取所得概率为一事件的交集。

第一个条件：排除自由 $\mathbb{Z}_p$-商群。 固定一个素数 p。根据定理 1.1，几乎必然， X 作为普通的 pro有限群是拓扑有限生成的。由于 H 在 X中的指数有限，原有限 Schreier 定理表明，H以及因此的 H^{ab}都是拓扑有限生成的。因此，$(H^{\mathrm{ab}})_p$ 是一个有限生成的 $\mathbb{Z}_p$-模。除非它除以其有限挠子群后的商群是一个非零有限秩自由 $\mathbb{Z}_p$-模，否则它是有限的。挠子群在 $P \rtimes \Gamma$ 作用下保持不变，因此这个商群将是一个非零的 $\mathbb{Z}_p[P \rtimes \Gamma]$-模 Λ，且作为 $\mathbb{Z}_p$上的模是有限秩自由的。因此，只需排除 H^{ab} 的所有非零等变商群，只要它们作为 $\mathbb{Z}_p$-模是有限秩自由的。引理 5.7 中的转移论证表明，任何此类商群都满足 $\Lambda^{P \rtimes \Gamma} = 0$。

对于 $p\nmid|\Gamma|$，固定这样一个模 Λ，并令

$$\Lambda_t=\Lambda/p^t\Lambda,\qquad \upsilon_\Lambda=\sum_{E\in U}\operatorname{rank}_{\mathbb{Z}_p}\Lambda^{\gamma_E}.$$

一个等变商 $H^{\mathrm{ab}}\twoheadrightarrow\Lambda$ 会对每个 $t\geq 1$给出 X 在某个扩张中的有限 Γ-商群

$$1\longrightarrow\Lambda_t\longrightarrow\widetilde{X}_t\longrightarrow P\longrightarrow 1. \tag{5.1}$$

事实上，$H\twoheadrightarrow\Lambda_t$ 的核在 X 中是正规子群，且在 Γ作用下稳定。要排除这样的商群，只需证明随着 t增大，存在任何一个扩张 (5.1) 作为商群的概率趋于零。

这些扩张由群 $H^2(P\rtimes\Gamma,\Lambda_t)$ 分类；参见 [8, 引理 5.8]。对于每个 $\alpha\in H^2(P\rtimes\Gamma,\Lambda_t)$，取 $\widetilde{X}_{t,\alpha}$ 作为一个代表扩张。由并集界和命题 2.1 可得

$$\begin{aligned}\mathbf{P}\big(\exists\,\alpha\in H^2(P\rtimes\Gamma,\Lambda_t):X\twoheadrightarrow_\Gamma\widetilde{X}_{t,\alpha}\big)&\leq\sum_{\alpha\in H^2(P\rtimes\Gamma,\Lambda_t)}\mathbf{P}(X\twoheadrightarrow_\Gamma\widetilde{X}_{t,\alpha})\\&\leq\sum_{\alpha\in H^2(P\rtimes\Gamma,\Lambda_t)}\frac{|H^2(\widetilde{X}_{t,\alpha}\rtimes\Gamma,\mathbb{Z}/n)|}{w_U(\widetilde{X}_{t,\alpha})\,|\operatorname{Aut}_\Gamma(\widetilde{X}_{t,\alpha})|}.\end{aligned} \tag{5.2}$$

该求和可能会对某种商群类型重复计数，这只会增大上界。具有非平凡 Γ-余不变量的目标的商群概率为零，因此将其非负项纳入也不会有问题。至此，我们已用上同调项表示所需的概率上界。需要证明的估计如下。

引理 5.3。假设每个非平凡不可约复 Γ-模 W 都满足

$$\sum_{E\in U}\dim_{\mathbb{C}}W^{\gamma_E}>0.$$

固定一个如上所述的有限 Γ-群 P、一个素数 $p\nmid|\Gamma|$，以及一个非零 $\mathbb{Z}_p[P\rtimes\Gamma]$-模 Λ，它作为 $\mathbb{Z}_p$-模是有限秩自由的，并满足 $\Lambda^{P\rtimes\Gamma}=0$。则 $\upsilon_\Lambda>0$ 以及

$$\sum_{\alpha\in H^2(P\rtimes\Gamma,\Lambda_t)}\frac{|H^2(\widetilde{X}_{t,\alpha}\rtimes\Gamma,\mathbb{Z}/n)|}{w_U(\widetilde{X}_{t,\alpha})\,|\operatorname{Aut}_\Gamma(\widetilde{X}_{t,\alpha})|}\ll_{\Gamma,n,U,P,p,\Lambda}p^{-t\upsilon_\Lambda}\qquad(t\geq 1). \tag{5.3}$$

隐含常数与 t 及扩张类无关。因此，对于每个素数 p，以概率 *1*，$(H^{\mathrm{ab}})_p$ 对于 X 的每个开正规 Γ-稳定子群 H 都是有限的。

我们在第 5.1 节中通过估计 $H^2(P\rtimes\Gamma,\Lambda_t)$ 中扩张类的数量、每个被加数的上同调分子以及权重–自同构因子的倒数来证明 (5.3)。前两个界与 t 无关；第三个界提供了衰减 $p^{-t\upsilon_\Lambda}$。这排除了每个以有限秩自由 $\mathbb{Z}_p$-模为目标的固定等变商。由于这些目标的可能同构类是可数的，便可排除所有这类目标。

第二个条件：关于素数的可求和界。对于同一个固定的 P，我们需要用一个关于 p 可求和的量，来界定存在 $f\in$ 满同态集$_\Gamma(X,\ P)$ 且满足 $((\ker f)^{\mathrm{ab}})_p\neq 0$ 的概率。若存在这样的映射，记其核为 $H=\ker f$，则非零有限生成模 $(H^{\mathrm{ab}})_p$ 可模 p 有一个非零有限约化。该约化的一个不可约 $\mathbb{F}_p[P\rtimes\Gamma]$-商群 V

会产生一个 Γ-等变的 P 的扩张，其核为 V，且是 X 的商群。因此，与第一个条件一样，我们需要界定某个有限扩张族中的任意一个成为商群的概率。

只需处理 $p \nmid n|P|\,|\Gamma|$，因为仅排除了有限个素数。对于这些素数，$H^2(P \rtimes \Gamma,\ V) = 0$，因此每个这样的扩张都与 $V \rtimes P$ Γ-同构。此外，V不可能是平凡的 $P \rtimes \Gamma$-模：否则 $V \times P$ 将具有一个带平凡 Γ-作用的非平凡商群，这与 $X_\Gamma = 1$矛盾。

记 $\mathrm{Irr}_p^*(P \rtimes \Gamma)$ 为非平凡不可约 $\mathbb{F}_p[P \rtimes \Gamma]$-模的同构类。现在应用同一个商矩界可得

$$\begin{aligned}\mathbf{P}\big(\exists f \in \mathrm{Sur}_\Gamma(X,P) : ((\ker f)^{\mathrm{ab}})_p \neq 0\big) &\le \sum_{V \in \mathrm{Irr}_p^*(P\rtimes\Gamma)} \mathbf{P}(X \twoheadrightarrow_\Gamma (V \rtimes P)) \\ &\le \sum_{V \in \mathrm{Irr}_p^*(P\rtimes\Gamma)} \frac{|H^2((V \rtimes P) \rtimes \Gamma, \mathbb{Z}/n)|}{w_U(V \rtimes P)\,|\mathrm{Aut}_\Gamma(V \rtimes P)|}.\end{aligned} \tag{5.4}$$

因此，第二个条件将由以下上同调界推出 d.

Lemma 5.4. 假设每个非平凡不可约复 Γ-模 W 都满足

$$\sum_{E \in U} \dim_{\mathbb{C}} W^{\gamma_E} > 0.$$

对于每个固定的有限 Γ-群 P，满足 $P_\Gamma = 1$ 且对于每个素数 $p \nmid n|P|\,|\Gamma|$，

$$\sum_{V \in \mathrm{Irr}_p^*(P\rtimes\Gamma)} \frac{|H^2((V \rtimes P) \rtimes \Gamma, \mathbb{Z}/n)|}{w_U(V \rtimes P)\,|\mathrm{Aut}_\Gamma(V \rtimes P)|} \le \frac{|P|\,|\Gamma|}{p(p-1)} \frac{|H^2(P \rtimes \Gamma, \mathbb{Z}/n)|}{w_U(P)}. \tag{5.5}$$

因子 $|P|\,|\Gamma|\,|H^2(P \rtimes \Gamma, \mathbb{Z}/n)|/w_U(P)$ 是有限的，并且与 p无关。因此，对于这个固定的 P，几乎必然存在一个有限素数集，其中包含所有满足 $(H^{\mathrm{ab}})_p \neq 0$ 的 p，并且对所有满足 $H = \ker f$ 且 $f \in \mathrm{Sur}_\Gamma(X, P)$ 的情形同时成立。特别地，几乎必然每个开正规 Γ-稳定子群 H *of* X 在其阿贝尔化中都只有有限个非零主分量。

我们将在第 5.2 节证明这个界。它由三个因子构成：可能的不可约模的数量、固定上同调因子 $|H^2(P \rtimes \Gamma,\ \mathbb{Z}/n)|/w_U(P)$，以及一个权重–自同构比，其上界为 $1/[p(p-1)]$。将此界与 (5.4) 和 Borel–Cantelli 结合，即可得到对每个 P 的断言。对 P 取可数交，即可得到引理 5.2 所要求的同时成立的结论。

5.1 固定素数处的界

我们通过将商矩界分解为三个因子并分别估计，来证明引理 5.3。首先，我们记录这些估计及其在 H^{ab} 中应用所需的表示论事实和转移事实。

引理 5. **5.** 每个非平凡不可约复 Γ-模 W 都满足的断言 *s*

$$\sum_{E \in U} \dim_{\mathbb{C}} W^{\gamma_E} > 0$$

等价于 $u_V > 0$ 对每个 $V \in \mathcal{I}$都成立。如果这些等价断言成立，那么对于任意非零有限维 Γ-表示 D，在特征零或特征 $p \nmid |\Gamma|$下，

$$\sum_{E \in U} \dim D^{\gamma_E} > 0.$$

特别地，如果 $p \nmid |\Gamma|$ 且 Λ 是一个非零的 $\mathbb{Z}_p[\Gamma]$-模，它在 $\mathbb{Z}_p$ 上有限秩自由，那么

$$\upsilon_\Lambda > 0, \qquad \prod_{E \in U} |(\Lambda / p^t \Lambda)^{\gamma_E}| = p^{t\upsilon_\Lambda}. \tag{5.6}$$

如果 $n > 1$，*Sawin–Wood* 不动向量假设保证，对每个非平凡不可约复 Γ-模 W，都有 $\sum_{E \in U} \text{维数}_{\mathbb{C}}\, W^{\gamma_E} > 0$。

证明。 在特征为 $p \nmid |\Gamma|$的代数闭域上，普通不可约特征标与模不可约特征标一一对应，并且任意元素对应的特征值 1 的重数保持不变；参见 [10, 11]。等价地，将表示限制到其循环子群，并比较平凡特征标的重数。标量扩张不会改变不变子空间的维数。因此，将一个不可约模在 $\mathbb{F}_p$ 上分解为代数闭包上的模，即可证明其与 $u_V > 0$ 等价。特征零时，对 $\mathbb{Q}_p$ 上表示作相同比较即可。

所有相关表示都是半单的。根据所假设的不等式，它们的非平凡成分满足所需的正性；它们的平凡成分满足该条件，是因为 $U \neq \varnothing$。这就证明了 D 的断言。将其应用于 $\Lambda \otimes \mathbb{Q}_p$，得到 $\upsilon_\Lambda > 0$。每个 γ_E 的阶在 $\mathbb{Z}_p$中都是单位，因此取平均可使不变元函子正合，并得到

$$(\Lambda / p^t \Lambda)^{\gamma_E} = \Lambda^{\gamma_E} / p^t \Lambda^{\gamma_E}.$$

这就证明了 (5.6)。最后，若 $p \mid n$，Sawin–Wood 不动向量假设对每个不可约 $\mathbb{F}_p[\Gamma]$-模给出 $u_V > 0$；再通过特征标比较，便可得出对每个非平凡不可约复 Γ-模都成立的所述不等式。 □

引理 5.6. 对于有限群 J、素数 p 和整数 $d \geq 0$，自由秩为 d 的 $\mathbb{Z}_p[J]$-模（视为 $\mathbb{Z}_p$-模）只有有限多个同构类。

证明. 令 $c = v_p(|J|)$。设两个这样的模的模 p^{c+1} 约化同构，并将此同构提升为一个可逆的 $\mathbb{Z}_p$-线性映射 T。记它们的作用为 ρ_1, ρ_2。每个差 $\rho_2(g) T \rho_1(g)^{-1} - T$ 都能被 p^{c+1} 整除。因此

$$T_0 = \frac{1}{|J|} \sum_{g \in J} \rho_2(g) T \rho_1(g)^{-1}$$

它是整的、等变的，并且模 p 同余于 T。因此它是一个同构。对于固定的 d，$(\mathbb{Z}/p^{c+1})^d$ 上的作用只有有限多个，这就证明了所述结论。这里不需要假设 $p \nmid |J|$。 □

引理 5.7. 设 $X_\Gamma = 1$ 和 $p \nmid |\Gamma|$。若一个非零的 $\mathbb{Z}_p[(X/H) \rtimes \Gamma]$-模 Λ，作为 $\mathbb{Z}_p$ 上的有限秩自由模，是 H^{ab}的一个$(X/H) \rtimes \Gamma$-等变商群，则

$$(\Lambda \otimes \mathbb{Q}_p)^{(X/H) \rtimes \Gamma} = 0.$$

证明。令 $\Pi = X \rtimes \Gamma$，并设 $\varphi\colon H^{\mathrm{ab}} \twoheadrightarrow \Lambda$ 为给定的等变映射。我们使用连续转移同态

$$\mathrm{Ver}_{\Pi/H} : \Pi \longrightarrow H^{\mathrm{ab}}.$$

由于 H 是正规子群，转移在 H 上的限制就是范算子：

$$\mathrm{Ver}_{\Pi/H}(h) = \sum_{g \in (X/H)\rtimes\Gamma} g \cdot [h] \qquad (h \in H).$$

条件 $X_\Gamma = 1$ 给出 $\Pi^{\mathrm{ab}} \simeq \Gamma^{\mathrm{ab}}$。因此复合映射

$$\Pi \xrightarrow{\mathrm{Ver}_{\Pi/H}} H^{\mathrm{ab}} \xrightarrow{\varphi} \Lambda$$

为零：它经由有限群 Γ^{ab}分解，而 Λ 无挠。将其限制到 H 并利用 φ 的满射性，可得

$$\left(\sum_{g \in (X/H)\rtimes\Gamma} g\right)\Lambda = 0.$$

在 $\mathbb{Q}_p$上，算子

$$\frac{1}{|X/H|\,|\Gamma|}\sum_{g \in (X/H)\rtimes\Gamma} g$$

是投影到$(X/H)\rtimes\Gamma$-不变元上的投影。因此$(\Lambda\otimes\mathbb{Q}_p)^{(X/H)\rtimes\Gamma} = 0$，如所求。除法是在 $\mathbb{Q}_p$中进行的，所以即使 $p \mid |X/H|$，也是有效的。 □

引理 *5.3* 的证明。固定陈述中的 P、p和 Λ。我们先对(5.2)中扩张类的和作出界定，然后说明为何这排除了 H^{ab} 的每一个非零等变商，只要它在 $\mathbb{Z}_p$上是有限秩自由模。

1. 目标估计及需要界定的三个因子。由 (5.2) 可知，某个扩张是商群的概率有上界，该上界为其中出现的和。我们需要证明，随着 t 增大，这个和趋于零，且常数与 t 以及扩张类无关。P 被 Λ_t 扩张的扩张 $\widetilde{X}_{t,\alpha}$ 由 $\alpha \in H^2(P\rtimes\Gamma,\Lambda_t)$ 编号。对和中的各项分别取最大值，可得

$$\begin{aligned}&\sum_{\alpha\in H^2(P\rtimes\Gamma,\Lambda_t)} \frac{|H^2(\widetilde{X}_{t,\alpha}\rtimes\Gamma,\mathbb{Z}/n)|}{w_U(\widetilde{X}_{t,\alpha})\,|\operatorname{Aut}_\Gamma(\widetilde{X}_{t,\alpha})|} \le \\ &|H^2(P\rtimes\Gamma,\Lambda_t)| \max_{\alpha\in H^2(P\rtimes\Gamma,\Lambda_t)} |H^2(\widetilde{X}_{t,\alpha}\rtimes\Gamma,\mathbb{Z}/n)| \max_{\alpha\in H^2(P\rtimes\Gamma,\Lambda_t)} \frac{1}{w_U(\widetilde{X}_{t,\alpha})\,|\operatorname{Aut}_\Gamma(\widetilde{X}_{t,\alpha})|}.\end{aligned} \tag{5.7}$$

因此，只需证明右侧的前两个因子有与 t 无关的上界，而第三个因子为 $O(p^{-tv_\Lambda})$。我们依次证明这些界。

2. 扩张类数量的界。系数列

$$0 \longrightarrow \Lambda \xrightarrow{p^t} \Lambda \longrightarrow \Lambda_t \longrightarrow 0$$

给出一个正合序列

$$H^2(P \rtimes \Gamma, \Lambda) \longrightarrow H^2(P \rtimes \Gamma, \Lambda_t) \longrightarrow H^3(P \rtimes \Gamma, \Lambda).$$

因此，

$$|H^2(P \rtimes \Gamma, \Lambda_t)| \le |H^2(P \rtimes \Gamma, \Lambda)|\,|H^3(P \rtimes \Gamma, \Lambda)| = O(1).$$

右侧的群是有限的：有限群 $P \rtimes \Gamma$ 的正次数上同调取有限秩自由 $\mathbb{Z}_p$-模 Λ 为系数时，在 $\mathbb{Z}_p$ 上有限生成，并且被 $|P|\,|\Gamma|$湮灭。因此，扩张类的数量存在一个与 t无关的上界。

3. 对上同调分子进行界定。对于每个扩张，使用

$$1 \longrightarrow \Lambda_t \longrightarrow \widetilde{X}_{t,\alpha} \rtimes \Gamma \longrightarrow P \rtimes \Gamma \longrightarrow 1.$$

Lyndon–Hochschild–Serre谱序列的二次项给出

$$|H^2(\widetilde{X}_{t,\alpha} \rtimes \Gamma, \mathbb{Z}/n)| \le |H^2(P \rtimes \Gamma, \mathbb{Z}/n)|\,|H^1(P \rtimes \Gamma, H^1(\Lambda_t, \mathbb{Z}/n))| \times |H^2(\Lambda_t, \mathbb{Z}/n)|.$$

第一个因子是固定的。对于另外两个，令 $d_\Lambda = \operatorname{秩}_{\mathbb{Z}_p} \Lambda$ 以及 $v = v_p(n)$。尽管 Λ_t 的指数随 t 增长，但其循环生成元的数量始终为 d_Λ。因此，固定的系数$\mathbb{Z}/n$给出一致上界

$$|H^1(\Lambda_t, \mathbb{Z}/n)| \le p^{v d_\Lambda}, \quad |H^2(\Lambda_t, \mathbb{Z}/n)| \le p^{v\left(d_\Lambda + \binom{d_\Lambda}{2}\right)}.$$

第二个上界由有限阿贝尔群的万有系数序列得到。此外，对于任意有限 $P \rtimes \Gamma$-模 T，

$$|H^1(P \rtimes \Gamma, T)| \le |T|^{|P|\,|\Gamma|},$$

因为其上循环是从 $P \rtimes \Gamma$ 到 T 的函数。将此应用于 $T = H^1(\Lambda_t,\ \mathbb{Z}/n)$，可得谱序列中间因子有一个独立于 t 和 α 的界。因此，(5.7) 中的第二个因子一致有界。此论证也适用于 $p \mid n$ 和 $p \mid |P|$；固定素数估计并未排除其中任何一个。

4. 控制权重–自同构因子。省略 α，并记 $X_t = X_{t,\ \alpha}$。我们需要证明

$$\frac{1}{w_U(\widetilde{X}_t)\,|\operatorname{Aut}_\Gamma(\widetilde{X}_t)|} \ll p^{-t v_\Lambda}.$$

首先计算权重。互素不动点提升给出

$$w_U(\widetilde{X}_t) = w_U(P) \frac{\prod_{E \in U} |\Lambda_t^{\gamma_E}|}{|\Lambda_t^\Gamma|}. \tag{5.8}$$

例如，一个被 γ_E 固定的陪集有一个固定的提升，因为它的障碍属于 $H^1(\langle\gamma_E\rangle,\ \Lambda_t) = 0$；同样的论证也适用于整个子群 Γ。根据引理 5.5，

$$\prod_{E \in U} |\Lambda_t^{\gamma_E}| = p^{t v_\Lambda}, \qquad v_\Lambda > 0.$$

将其代入 (5.8)，恰好可以分离出我们仍需控制的比值：

$$\frac{1}{w_U(\widetilde{X}_t)\,|\operatorname{Aut}_\Gamma(\widetilde{X}_t)|} = \frac{p^{-tv_\Lambda}}{w_U(P)}\frac{|\Lambda_t^\Gamma|}{|\operatorname{Aut}_\Gamma(\widetilde{X}_t)|}. \tag{5.9}$$

因此 剩下的任务是证明，$|\Lambda_t^\Gamma|/|\operatorname{Aut}_\Gamma(\widetilde{X}_t)|$ 与无关地有界 t.

通过 Λ_t 中元素的共轭作用定义了 Γ 自同构 P 和 Γ固定的元素组成，即 $\Lambda_t^{P\rtimes\Gamma}$。因此

$$|\operatorname{Aut}_\Gamma(\widetilde{X}_t)| \geq \frac{|\Lambda_t^\Gamma|}{|\Lambda_t^{P\rtimes\Gamma}|}, \qquad \frac{|\Lambda_t^\Gamma|}{|\operatorname{Aut}_\Gamma(\widetilde{X}_t)|} \leq |\Lambda_t^{P\rtimes\Gamma}|.$$

假设 $\Lambda^{P\rtimes\Gamma}=0$ 现在控制了剩余项。步骤 2 中的同一系数列给出了一个注入

$$\Lambda_t^{P\rtimes\Gamma} \hookrightarrow H^1(P\rtimes\Gamma,\Lambda).$$

特别地，

$$|\Lambda_t^{P\rtimes\Gamma}| \leq |H^1(P\rtimes\Gamma,\Lambda)| = O(1). \tag{5.10}$$

将此与 (5.9) 结合可得

$$\frac{1}{w_U(\widetilde{X}_t)\,|\operatorname{Aut}_\Gamma(\widetilde{X}_t)|} \leq \frac{|H^1(P\rtimes\Gamma,\Lambda)|}{w_U(P)}p^{-tv_\Lambda}.$$

The 该界对于扩张类是一致的，因此 (5.7) 中的最后一个因子为 $O(p^{-tv_\Lambda})$.

5. 结合各个界并排除自由 $\mathbb{Z}_p$-商群。根据 (5.7) 以及上述三个估计，(5.2) 中的和为 $O(p^{-tv_\Lambda})$，由于 $v_\Lambda>0$，该值趋于零。这就证明了~(5.3)。特别地，对于某个$\alpha\in H^2(P\rtimes\Gamma,\ \Lambda_t)$，$X$ 具有同构于 X_t 的 Γ-商群的概率趋于零，其中α，当 $t\to\infty$ 时。

根据引理之前的约化，只需排除 H^{ab} 的非零 $P\rtimes\Gamma$-等变商群，且该商群作为 $\mathbb{Z}_p$-模是有限秩自由模。对于上文所述的任意固定 Λ，这样的商群将对每个 t产生一个上述形式的 Γ-商群 X。其概率为零，因为 t各个取值所对应的概率都趋于零。

最后，引理 5.6 表明，$\mathbb{Z}_p$ 上有限秩自由的 $\mathbb{Z}_p[P\rtimes\Gamma]$-模的同构类至多可数。取相应零测集的并集，即可同时排除所有形如 $H=\ker f$ with $f\in\operatorname{Sur}_\Gamma(X,P)$ 的非零商。有限 Γ-群的同构类也至多可数，而命题 2.1 排除了具有非平凡余不变量的群。因此，再取一次可数交集，便得到：对于几乎每个样本 X，对每个开正规 Γ-稳定子群 $H\leq X$，$(H^{\mathrm{ab}})_p$ 都是有限的。

□

关于 X 的无条件固定素数推论。对于第 6 节中的同调论证，我们还需要以下关于各个主分量的无条件陈述。它并不声称整个阿贝尔化是有限的。

引理 5.8。几乎必然，$(X^{\mathrm{ab}})_p$ 对每个素数 p 都是有限的。

证明。对于 $p\mid|\Gamma|$，主分量为零。否则，如引理 5.3 之前所述，如果 $(X^{\mathrm{ab}})_p$ 是无限的，那么它有一个非零的 Γ等变商群 Λ，且该商群在 $\mathbb{Z}_p$上是有限秩自由模。令

$$\Lambda_t=\Lambda/p^t\Lambda, \qquad d_\Lambda=\operatorname{rank}_{\mathbb{Z}_p}\Lambda>0.$$

引理 5.3 证明中的大部分固定素数论证在 $P = 1$下仍然适用。只有一个扩张类，因为 $H^2(\Gamma,\ \Lambda_t) = 0$，而相同的上同调界给出，取$v = v_p(n)$,

$$|H^2(\Lambda_t \rtimes \Gamma, \mathbb{Z}/n)| \le p^{v(d_\Lambda + \binom{d_\Lambda}{2})},$$

与 t 无关。区别在于权重–自同构估计。这里我们不要求

$$\sum_{E\in U} \dim_{\mathbb{C}} W^{\gamma_E} > 0$$

对每个非平凡的不可约复 Γ-模 W 都成立。相反，我们使用 $w_U(\Lambda_t) \ge 1$（因为$U \neq \varnothing$），以及 $(\mathbb{Z}/p^t)^\times$ 对 Λ_t 的忠实作用，其作用为数量 Γ-自同构。因此

$$\mathbf{P}(X \twoheadrightarrow_\Gamma \Lambda_t) \le \frac{|H^2(\Lambda_t \rtimes \Gamma, \mathbb{Z}/n)|}{w_U(\Lambda_t)\,|\operatorname{Aut}_\Gamma(\Lambda_t)|} \le \frac{p^{v(d_\Lambda + \binom{d_\Lambda}{2})}}{\varphi(p^t)} \longrightarrow 0.$$

商群 $X^{\mathrm{ab}} \twoheadrightarrow_\Gamma \Lambda$ 会为每个 t 导出这样的商群，因此其出现的概率为零。根据引理 5.6，只需排除可数多个具有 Γ-作用的有限秩自由$\mathbb{Z}_p$-模的同构类；对素数取可数交集，即完成证明。

□

5.2 跨素数界

现在我们证明引理 5.4。固定素数估计随 t 增大而趋于零；这里的估计则必须在 p 变化时可求和。我们再次分别考察目标的数量、它们的上同调因子以及权重–自同构因子。

引理 *5.4* 的证明。 固定 P，并令 $p \nmid n|P|\,|\Gamma|$。我们对 (5.4) 中不可约模的和进行估计；该和给出了存在某个 $f \in$满同态集$_\Gamma(X,\ P)$，使得 $((\ker f)^{\mathrm{ab}})_p \neq 0$ 的概率上界。与前一小节一样，我们先分离出三个因子，再分别对它们进行估计。这里p 会变化，因此所有常数都必须与 p无关。

1. 目标估计与需要估计的三个因子。 引理之前的归约说明了这些为何是相关商群：若存在 $f \in$满同态集$_\Gamma(X,\ P)$，其 $H = \ker f$ 满足 $(H^{\mathrm{ab}})_p \neq 0$，那么 $(H^{\mathrm{ab}})_p/p(H^{\mathrm{ab}})_p$ 的一个非平凡不可约商 V 会给出 X 的一个商群 $V \rtimes P$。消失 $H^2(P \rtimes \Gamma,\ V) = 0$ 确保每个这样的扩张都分裂，而平凡模则由 $X_\Gamma = 1$ 排除。因此，(5.4) 中的界适用。若 $\mathrm{Irr}_p^*(P \rtimes \Gamma)$ 为空，则和与概率都为零；以下假设它非空。

接下来，我们使用固定目标 P 的上同调来表示每个被加数。由于 $p \nmid n$，膨胀给出了一个同构

$$H^2(P \rtimes \Gamma, \mathbb{Z}/n) \simeq H^2((V \rtimes P) \rtimes \Gamma, \mathbb{Z}/n),$$

因为正规 p-群 V 的正次数上同调以系数 $\mathbb{Z}/n$ 计算时消失。因此，将 Λ_t 替换为 V 后，权重分解 (5.8) 给出精确恒等式

$$\frac{|H^2((V \rtimes P) \rtimes \Gamma, \mathbb{Z}/n)|}{w_U(V \rtimes P)\,|\operatorname{Aut}_\Gamma(V \rtimes P)|} = \frac{|H^2(P \rtimes \Gamma, \mathbb{Z}/n)|}{w_U(P)} \frac{|V^\Gamma|}{|\operatorname{Aut}_\Gamma(V \rtimes P)| \prod_{E\in U} |V^{\gamma_E}|}. \tag{5.11}$$

这个等式对求和中的每个模都成立，即使相应商事件的概率为零也是如此。对其求和便得到三因子估计

$$\begin{aligned}\sum_{V\in \mathrm{Irr}_p^*(P\rtimes\Gamma)} & \frac{|H^2((V\rtimes P)\rtimes\Gamma,\mathbb{Z}/n)|}{w_U(V\rtimes P)\,|\operatorname{Aut}_\Gamma(V\rtimes P)|}\\ &\le |\operatorname{Irr}_p^*(P\rtimes\Gamma)|\,\frac{|H^2(P\rtimes\Gamma,\mathbb{Z}/n)|}{w_U(P)}\\ &\quad\times \max_{V\in \mathrm{Irr}_p^*(P\rtimes\Gamma)}\frac{|V^\Gamma|}{|\operatorname{Aut}_\Gamma(V\rtimes P)|\prod_{E\in U}|V^{\gamma_E}|}.\end{aligned}\tag{5.12}$$

只需证明可能出现的不可约模数量至多为 $|P|\,|\Gamma|$，上同调因子有限且与 p 无关，并且最终的最大值至多为$1/[p(p-1)]$。前两个因子一致有界，第三个因子则提供可求和的衰减。

2. 不可约模数量的界。由于 $p\nmid|P|\,|\Gamma|$，马施克定理保证 $\mathbb{F}_p[P\rtimes\Gamma]$ 为半单代数。每个单模同构类都对应于该代数的一个简单分量，而每个分量的 $\mathbb{F}_p$-维数均为正。由于该代数的维数为 $|P|\,|\Gamma|$，

$$|\operatorname{Irr}_p^*(P\rtimes\Gamma)|\le |P|\,|\Gamma|.$$

特别 地，可能出现的模数量有一个与素数无关的上界 .

3. 固定商上同调因子的界。该因子

$$\frac{|H^2(P\rtimes\Gamma,\mathbb{Z}/n)|}{w_U(P)}=\mathbf{E}|\operatorname{Sur}_\Gamma(X,P)|<\infty$$

是固定的，其中与矩的等式用到了 $P_\Gamma=1$。这里的一切只取决于Γ， n， U， P，而与 p或 V 无关。因此，前两个因子一致有界。

4. 权重–自同构因子的界。固定 $V\in\operatorname{Irr}_p^*(P\rtimes\Gamma)$。我们必须证明

$$\frac{|V^\Gamma|}{|\operatorname{Aut}_\Gamma(V\rtimes P)|\prod_{E\in U}|V^{\gamma_E}|}\le\frac{1}{p(p-1)}.\tag{5.13}$$

我们分别得到两个分母因子：自同构给出 $p-1$，不变向量给出 p。

自同构因子给出 $p-1$。 在本证明中记 $q=|\operatorname{End}_{P\rtimes\Gamma}(V)|$。由舒尔引理以及 V 的有限性可知，这个自同态环是一个包含 $\mathbb{F}_p$的有限域，因此$q\ge p$。

对每个 $v\in V^\Gamma$，共轭作用 c_v是 $V\rtimes P$的一个 Γ-自同构，并固定其商群 P。作为从 V^Γ出发的映射，它的核是 $V^{P\rtimes\Gamma}=0$，因为 V是一个非平凡的不可约 $P\rtimes\Gamma$-模。因此，这些内自同构构成一个阶为 $|V^\Gamma|$的子群。

每个 $\lambda\in\operatorname{End}_{P\rtimes\Gamma}(V)^\times$ 也定义了一个 Γ-自同构

$$\mathrm{scal}_\lambda: V\rtimes P\longrightarrow V\rtimes P,\qquad \mathrm{scal}_\lambda(v,g)=(\lambda v,g)\quad(v\in V,\ g\in P).$$

这些构成一个阶为 $q-1$ 的子群。它与内子群的交是平凡的，因为通过 V 进行共轭作用在 V 上恒等，而 scal_λ 在其上的作用为 λ。因此，它们的乘积包含 $|V^\Gamma|(q-1)$ 个不同的 Γ-自同构。于是，

$$|\operatorname{Aut}_\Gamma(V \rtimes P)| \geq |V^\Gamma|(q-1) \geq |V^\Gamma|(p-1). \tag{5.14}$$

特别是，(5.13) 中的因子 $|V^\Gamma|$ 会抵消，因此自同构比至多留下 $1/(p-1)$。

不动点权重给出 p。由于 $V|_\Gamma \neq 0$，引理 5.5 给出

$$\prod_{E\in U} |V^{\gamma_E}| = p^{\sum_{E\in U} \dim_{\mathbb{F}_p} V^{\gamma_E}} \geq p. \tag{5.15}$$

合并这两个因子。由方程 (5.14) 和 (5.15) 得到

$$\frac{|V^\Gamma|}{|\operatorname{Aut}_\Gamma(V \rtimes P)| \prod_{E\in U} |V^{\gamma_E}|} \leq \frac{|V^\Gamma|}{|V^\Gamma|(p-1)p} = \frac{1}{p(p-1)}.$$

该界对每个 $V \in \mathrm{Irr}_p^*(P \rtimes \Gamma)$ 都成立，因此 (5.12) 中的最大值至多为 $1/[p(p-1)]$，如所需。

5. 合并各项界并对素数求和。回到 (5.12)，不可约模的个数、固定上同调因子以及权重与自同构之比的界给出 (5.5)。将其与 (5.4) 结合可知，存在一个 $f \in \mathrm{Sur}_\Gamma(X,\ P)$ 且满足 $((\ker f)^{\mathrm{ab}})_p \neq 0$ 的概率至多为

$$\frac{|P|\,|\Gamma|}{p(p-1)} \frac{|H^2(P \rtimes \Gamma, \mathbb{Z}/n)|}{w_U(P)}.$$

由于

$$\sum_{p\nmid n|P|\,|\Gamma|} \frac{1}{p(p-1)} < \infty,$$

第一 Borel–Cantelli 引理意味着，几乎必然只有有限多个素数 p 允许存在满足 $((\ker f)^{\mathrm{ab}})_p \neq 0$ 的任意 $f \in \mathrm{Sur}_\Gamma(X,\ P)$。这里不需要独立性。将整除 $n|P|\,|\Gamma|$ 的有限多个素数加入其中，便得到一个有限集，它同时包含所有满足 $(H^{\mathrm{ab}})_p \neq 0$ 的素数 p，对所有满足 $f \in \mathrm{Sur}_\Gamma(X,\ P)$ 的 $H = \ker f$ 均成立。最后，对有限 Γ-群 P（按同构分类）取可数交。由命题 2.1，几乎每个样本都没有余不变量非平凡的商群。因此，对于几乎每个 X，每个开正规 Γ-稳定子群 $H \leq X$ 的阿贝尔化 H^{ab} 只有有限多个非零主分量。

□

5.3 FAb 定理的证明

定理 1.3 的证明。 定理 1.3 的假设与引理 5.5 一起给出 $u_V > 0$对每个 $V \in \mathcal{I}$。对于每个素数 p，引理 5.3 几乎必然地给出 $(H^{\mathrm{ab}})_p$ 对每个开正规 Γ- 稳定的 $H \leq X$ 都是有限的。根据引理 5.4，几乎必然地，每个这样的 H 只有有限多个非零主分量。这正是引理 5.2 的两个假设，因此$\mathbf{P}(X \text{ 是 FAb}) = 1$。

□

6 第二上同调的结构

我们证明一个模满同态定理，并由此推导出定理 1.4。所有同调都是取紧系数的连续同调，且这些系数上的群作用是平凡的；上同调取离散系数。我们使用紧/离散对偶性以及 pro有限群的系数正合序列；见 [16]。第二同调群是紧阿贝尔群，并带有其自然的 Γ-作用，而

$$H_2(X,\widehat{\mathbb{Z}}) = \prod_{p\nmid|\Gamma|} H_2(X,\mathbb{Z}_p), \qquad H_2(X,\mathbb{Z}_p) = 0 \quad (p \mid |\Gamma|). \tag{6.1}$$

最后一个断言可通过在 X 的有限商群上取平均得到，也可通过与离散的 p-主上同调取对偶得到。

6.1 增广模与结构定理

Put

$$R_\Gamma = \prod_{p\nmid|\Gamma|} \mathbb{Z}_p$$

并定义紧 $R_\Gamma[\Gamma]$-模

$$\mathcal{K}_U = \ker\left(\bigoplus_{E\in U} R_\Gamma[\Gamma/\langle\gamma_E\rangle] \xrightarrow{\text{sum of augmentations}} R_\Gamma\right). \tag{6.2}$$

在 U 中，每次出现都贡献一个被加数。对于 $p\nmid|\Gamma|$，其 p-分量及其约化为

$$\mathcal{K}_{U,p} = \ker\left(\bigoplus_{E\in U} \mathbb{Z}_p[\Gamma/\langle\gamma_E\rangle] \xrightarrow{\text{sum of augmentations}} \mathbb{Z}_p\right), \quad \overline{\mathcal{K}}_{U,p} = \mathcal{K}_{U,p}/p\mathcal{K}_{U,p}. \tag{6.3}$$

增广映射是满射，因为 $U\neq\varnothing$，并且可通过取平均得到 Γ-等变分裂。因此$\mathcal{K}_{U,\,p}$ 是一个自由 $\mathbb{Z}_p$-模，其中

$$\operatorname{rank}_{\mathbb{Z}_p}\mathcal{K}_{U,p} = \sum_{E\in U}[\Gamma:\langle\gamma_E\rangle] - 1, \qquad \mathcal{K}_U = \prod_{p\nmid|\Gamma|}\mathcal{K}_{U,p}. \tag{6.4}$$

对于定向样本 $\boldsymbol{X}=(X,s_X)$，令

$$\omega_X = \partial_n(s_X) \in H_2(X,\widehat{\mathbb{Z}})^\Gamma[n], \tag{6.5}$$

其中 ∂_n 是与.....相关联的同调边界

$$0\longrightarrow\widehat{\mathbb{Z}}\xrightarrow{\times n}\widehat{\mathbb{Z}}\longrightarrow\mathbb{Z}/n\longrightarrow 0.$$

因此，$\langle\omega_X\rangle$ 是有限循环群，由 Γ逐点固定，且其阶整除 n。其 p-分量为$\langle\omega_{X,\,p}\rangle$，其中$\omega_{X,\,p}$是 ω_X的 p-分量。

定理 6.1。 在关于 Γ、 n、 U的既定假设下，存在一个$\nu_{\Gamma,\ n,\ U}$-测度为一的定向样本可测集，在该集合上存在一个连续的 $R_\Gamma[\Gamma]$-线性满同态

$$\phi_X : \mathcal{K}_U \twoheadrightarrow H_2(X, \widehat{\mathbb{Z}})/\langle \omega_X \rangle. \tag{6.6}$$

I $\widehat{\ }t$ 可以提升为一个连续的 $R_\Gamma[\Gamma]$-线性映射 ψ_X： $\mathcal{K}_U \to H_2(X,\mathbb{Z})$ 使得 t

$$\mathcal{K}_U \oplus \mathbb{Z}/n \twoheadrightarrow H_2(X, \widehat{\mathbb{Z}}), \quad (x, z) \longmapsto \psi_X(x) + z\omega_X \tag{6.7}$$

是一个满同态。 Γ 对 $\mathbb{Z}/n$ 的作用是平凡的，并且该被加数中的 1 映射到 ω_X。特别地，$\widehat{\ } H_2(X,\mathbb{Z})$ 作为恰紧阿贝尔群是拓扑有限生成的。这里不主张存在对这些满同态的规范或可测选择。

6.2 一个上同调界

我们首先给出消去定向边界的二阶上同调类的界。随后，利用万有系数定理得到定理 6.1 所需的重数界。对于一个定向的有限剩余 Γ-群 $(Y,\ s_Y)$，令 $\omega_Y = \partial_n(s_Y)$。若 $p \nmid |\Gamma|$ 和 V 是一个作用平凡的有限 $\mathbb{F}_p[\Gamma]$-模，则定义

$$H^2_{\omega_Y}(Y \rtimes \Gamma, V) := \{\alpha \in H^2(Y \rtimes \Gamma, V) : \langle \alpha|_Y, \omega_Y \bmod p \rangle = 0\}. \tag{6.8}$$

这里， ω_Y 模 p 是其在 $H_2(Y,\ \mathbb{F}_p)$ 中的像，且配对取值于 V^Γ。因此，当 $p \nmid n$ 或 $V^\Gamma = 0$ 时，这个子空间就是 $H^2(Y \rtimes \Gamma,\ V)$ 的全部。下面的恒等式将其与第 4.1 节中的 Bockstein 条件联系起来。

引理 6.2。 设 J 为一个 *pro*有限群，令 $s \in H_3(J,\mathbb{Z}/n)$，并设 $\omega = \partial_n(s).\eta \in H^2(J,\mathbb{Z}/n)$, *For*

$$\langle B\eta, s \rangle = \langle \eta, \omega \bmod n \rangle, \tag{6.9}$$

其中 B 是关于 $0 \to \mathbb{Z}/n \xrightarrow{\times n} \mathbb{Z}/n^2 \to \mathbb{Z}/n \to 0$ 的 ***Bockstein***，而 ω 模 n 表示其在 $H_2(J,\ \mathbb{Z}/n)$中的像。两个连接映射采用相容的符号约定。

证明。 在带恰紧整数系数的连续 bar 复形中，将表示s 的循环提升为链 c，并写作 $dc = nb$。于是 b 是表示 ω的循环。将表示 η的上循环提升为局部常值整数上链 $\widetilde{\eta}$。Bockstein 由模 n的 $d\widetilde{\eta}/n$ 表示，并且

$$\left\langle \frac{d\widetilde{\eta}}{n}, c \right\rangle = \left\langle \widetilde{\eta}, \frac{dc}{n} \right\rangle = \langle \widetilde{\eta}, b \rangle \pmod n.$$

这就是 (6.9)。 □

在公共满测度集 Ω_{hom} 上进行讨论；该集合由将引理 4.1 中的 Ω_+ 与命题 2.1 和引理 5.8 的满测度集取交得到。特别地， $X_\Gamma = 1$ 以及每个 $(X^{\mathrm{ab}})_p$都是有限的。对于从 Γ膨胀得到的 V，由其小性可知 $H^1(X \rtimes \Gamma,\ V)$ =同态集$_\Gamma(X,\ V)$ 是有限的；再由命题 4.3 得到有限维二阶上同调。

命题 6.3. 在Ω_{hom}上，对每个 $p \nmid |\Gamma|$ 以及每个具有平凡X作用的不可约 $\mathbb{F}_p[\Gamma]$-模 V，

$$\dim_{\mathbb{F}_p} H^2_{\omega_X}(X \rtimes \Gamma, V) - \dim_{\mathbb{F}_p} H^1(X \rtimes \Gamma, V) \le \sum_{E \in U} \dim_{\mathbb{F}_p} V^{\gamma_E} - \dim_{\mathbb{F}_p} V^\Gamma. \tag{6.10}$$

证明。固定 p 和 V；本证明中的所有维数均取自 $\mathbb{F}_p$。令 $\mathcal{T} \subseteq H^2_{\omega_X}(X \rtimes \Gamma, V)$ 为一个有限维子空间。如命题 4.3 的证明所示，选取一个包含相应扩张群和分裂扩张的有限层 $\mathcal{L}$，并令 $\boldsymbol{H} = \boldsymbol{X}^{\mathcal{L}}$。存在一个子空间

$$\mathcal{T}_H \subseteq H^2(H \rtimes \Gamma, V)^{\mathcal{L}}$$

其膨胀将其与 $\mathcal{T}$ 识别。模 V 是合格的，并且 $C(\mathcal{L},\ \boldsymbol{H})$ 具有正测度。对于商映射 $\pi\colon X \twoheadrightarrow H$，由自然性可得 $\omega_H = \pi_*\omega_X$，因此 $\mathcal{T}_H$ 中的每个上同调类都湮灭 ω_H。令

$$H^2_{\omega_H}(H \rtimes \Gamma, V)^{\mathcal{L}} = H^2(H \rtimes \Gamma, V)^{\mathcal{L}} \cap H^2_{\omega_H}(H \rtimes \Gamma, V).$$

因此 $\mathcal{T}_H \subseteq H^2_{\omega_H}(H \rtimes \Gamma,\ V)^{\mathcal{L}}$。

若 $p \nmid n$。则 $\omega_{H,\ p} = 0$ 且 $H^2_{\omega_H}(H \rtimes \Gamma,\ V)^{\mathcal{L}} = H^2(H \rtimes \Gamma,\ V)^{\mathcal{L}}$。对其中取对数可得 (4.2)

$$\dim H^2_{\omega_H}(H \rtimes \Gamma, V)^{\mathcal{L}} \leq \dim H^1(H \rtimes \Gamma, V) + \sum_{E \in U} \dim V^{\gamma_E} - \dim V^{\Gamma}. \tag{6.11}$$

若 $p \mid n$。对于 $\alpha \in H^2(H \rtimes \Gamma,\ V)^{\mathcal{L}}$ 和 $\varphi \in \mathrm{Hom}_{\Gamma}(V,\ \mathbb{Z}/n)$，将限制表示到 H 后应用引理 6.2，可得

$$s_H\big(B(\varphi_*\alpha)\big) = \varphi\big(\langle \alpha|_H, \omega_H \bmod p\rangle\big). \tag{6.12}$$

对于不可约 V，Bockstein 条件因而等价于 $\alpha \in H^2_{\omega_H}(H \rtimes \Gamma,\ V)^{\mathcal{L}}$：如果 V 非平凡，则两者都是自动成立的；而如果 $V = \mathbb{F}_p$ 平凡，则任意非零的 φ 都是单射。因此，$H^2(H \rtimes \Gamma,\ V)^{\mathcal{L},\ s_H}$ 是杯积映射的核

$$H^2_{\omega_H}(H \rtimes \Gamma, V)^{\mathcal{L}} \longrightarrow H^1(H \rtimes \Gamma, V^\vee)^*, \quad \alpha \longmapsto \big(\beta \longmapsto s_H(\alpha \smile \beta)\big),$$

其中 $(-)^* = $ 同态集$_{\mathbb{F}_p}(-,\ \mathbb{F}_p)$，且其取值按照第 4.1 节中的方式识别为 $\mathbb{F}_p$。因此，

$$\dim H^2_{\omega_H}(H \rtimes \Gamma, V)^{\mathcal{L}} \leq \dim H^2(H \rtimes \Gamma, V)^{\mathcal{L}, s_H} + \dim H^1(H \rtimes \Gamma, V^\vee).$$

对 (4.3) 取对数，右侧可由以下式子界定：

$$\dim H^1(H \rtimes \Gamma, V) + \sum_{E \in U} \dim V^{\gamma_E} - \dim V^{\Gamma},$$

从而在此情形下也证明了 (6.11)。

最后，$\dim\ \mathcal{T} = \dim\ \mathcal{T}_H \leq \dim\ H^2_{\omega_H}(H \rtimes \Gamma,\ V)^{\mathcal{L}}$，且膨胀映射为单射 $H^1(H \rtimes \Gamma,\ V)$ 到 $H^1(X \rtimes \Gamma,\ V)$ 中。应用 (6.11) 并改变 $\mathcal{T}$，即可证明 (6.10)。 □

6.3 结构定理的证明

定理 *6.1* 的证明。固定 Ω_{hom} 中的一个样本和一个素数 $p \nmid |\Gamma|$，并令

$$\mathcal{Q}_{X,p} = H_2(X, \mathbb{Z}_p)/\langle \omega_{X,p} \rangle.$$

1. 从上同调到重数。乘以 p 得到的系数列为

$$0 \longrightarrow H_2(X, \mathbb{Z}_p)/pH_2(X, \mathbb{Z}_p) \longrightarrow H_2(X, \mathbb{F}_p) \longrightarrow (X^{\mathrm{ab}})_p[p] \longrightarrow 0. \tag{6.13}$$

对于从 Γ膨胀得到的 V，评价对偶性和互素平均给出

$$H^i(X \rtimes \Gamma, V) \simeq \mathrm{Hom}_\Gamma(H_i(X, \mathbb{F}_p), V) \qquad (i = 1, 2).$$

对于每个不可约 V，这些上同调空间都是有限的。因此，将半单性应用于 $H_2(X, \mathbb{F}_p)$ 的连续对偶可知，$H_2(X, \mathbb{F}_p)$ 是有限的。

由于 $p \nmid |\Gamma|$，对 (6.13) 应用 $\mathrm{Hom}_\Gamma(-, V)$ 是正合的。将其限制到被 ω_X 消去的上同调类，可得短正合序列

$$0 \longrightarrow \mathrm{Hom}_\Gamma((X^{\mathrm{ab}})_p[p], V) \longrightarrow H^2_{\omega_X}(X \rtimes \Gamma, V) \longrightarrow \mathrm{Hom}_\Gamma(\mathcal{Q}_{X,p}/p\mathcal{Q}_{X,p}, V) \longrightarrow 0. \quad (6.14)$$

事实上，最后一项恰好由 $H_2(X, \mathbb{Z}_p)/pH_2(X, \mathbb{Z}_p)$ 上在 $\omega_{X,\,p}$ 的像上消失的泛函组成，因为

$$\mathcal{Q}_{X,p}/p\mathcal{Q}_{X,p} = H_2(X, \mathbb{Z}_p)/(pH_2(X, \mathbb{Z}_p) + \langle \omega_{X,p} \rangle).$$

第一项由在 $H_2(X, \mathbb{Z}_p)/pH_2(X, \mathbb{Z}_p)$ 的所有元素上消失的上同调类组成，因此它们自动消去 ω_X。

由引理 5.8，模 $(X^{\mathrm{ab}})_p$ 是有限的。其乘以 p 的序列表明，$(X^{\mathrm{ab}})_p[p]$ 与 $(X^{\mathrm{ab}})_p/p(X^{\mathrm{ab}})_p$ 具有相同的合成因子；由半单性，它们作为 $\mathbb{F}_p[\Gamma]$-模同构。因此，(6.14) 的第一项的维数为 $\dim H^1(X \rtimes \Gamma, V)$。取维数可得

$$\dim_{\mathbb{F}_p} \mathrm{Hom}_\Gamma(\mathcal{Q}_{X,p}/p\mathcal{Q}_{X,p}, V) = \dim_{\mathbb{F}_p} H^2_{\omega_X}(X \rtimes \Gamma, V) - \dim_{\mathbb{F}_p} H^1(X \rtimes \Gamma, V). \quad (6.15)$$

On 另一方面，分裂增广正合列和 Frobenius 互反律给出 e

$$\dim_{\mathbb{F}_p} \mathrm{Hom}_\Gamma(\overline{\mathcal{K}}_{U,p}, V) = \sum_{E \in U} \dim_{\mathbb{F}_p} V^{\gamma_E} - \dim_{\mathbb{F}_p} V^\Gamma. \quad (6.16)$$

由命题 6.3 可知，对于每个不可约V，(6.15) 中的同态集维数不超过 (6.16) 中的维数。除以 $\dim_{\mathbb{F}_p} \mathrm{End}_\Gamma(V)$ 后，即可比较它们的重数。因此，半单性给出一个满同态

$$\overline{\phi}_{X,p} : \overline{\mathcal{K}}_{U,p} \twoheadrightarrow_\Gamma \mathcal{Q}_{X,p}/p\mathcal{Q}_{X,p}.$$

2. 提升并合并主分量。 将 $\mathcal{K}_U$ 的一个 $\mathbb{Z}_p$-基的像直接经由 $H_2(X, \mathbb{Z}_p) \twoheadrightarrow \mathcal{Q}_{X,p}/p\mathcal{Q}_{X,p}$ 提升，再对 Γ 上的结果连续线性映射取平均。由此得到一个等变映射

$$\psi_{X,p} : \mathcal{K}_{U,p} \longrightarrow H_2(X, \mathbb{Z}_p).$$

其复合映射 $\phi_{X,p} : \mathcal{K}_{U,p} \to \mathcal{Q}_{X,p}$ 模 p 约化后仍为 $\overline{\phi_{X,p}}$，因为该映射本来就是等变的。其像是紧的，因而是闭的；其紧余核模 p 的约化为零。紧 Nakayama 引理使 $\phi_{X,p}$ 成为满射。特别地，

$$\psi_{X,p}(\mathcal{K}_{U,p}) + \langle \omega_{X,p} \rangle = H_2(X, \mathbb{Z}_p).$$

由中国剩余定理可得

$$\langle \omega_X \rangle = \prod_{p|n} \langle \omega_{X,p} \rangle, \qquad H_2(X, \widehat{\mathbb{Z}})/\langle \omega_X \rangle = \prod_{p \nmid |\Gamma|} \mathcal{Q}_{X,p}.$$

将 $\phi_{X,p}$ 相乘即可证明 (6.6)。将 $\psi_{X,p}$ 相乘，并附加映射 $\frown\mathbb{Z}/n \to H_2(X, \mathbb{Z})$，该映射将 1 映到 ω_X，即可证明 (6.7)。其源群是拓扑有限生成的：$\mathcal{K}_U$ 是 R_Γ 上的有限秩自由模，且额外的被加数是循环群。因此，其商群 $H_2(X, \mathbb{Z})$ 也具有相同性质。

□

6.4 消失的推论

定理 *1.4* 的证明。在定理的假设下，(6.2) 中的增广映射是 R_Γ 上的恒等映射，因此 $\mathcal{K}_U = 0$。此外， $n = 1$ 蕴含 $\omega_X = 0$。于是，(6.6) 中的满同态 $\widehat{\ }$ 几乎必然推出 $H_2(X, \mathbb{Z}) = 0$ 。 □

对于任意有限伽罗瓦扩张，相应的问题可表述如下。

问题 6.4. 设 $K/\mathbb{Q}$ 是一个有限伽罗瓦扩张，并令 $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$。设 $c \in \Gamma$ 为复共轭（因此若 K 是全实的，则 $c = 1$ ）。假设

对每个非平凡不可约复 Γ-模 W，都有 $\dim_{\mathbb{C}} W^c > 0$。

令 π 为不整除 $|\Gamma|$的素数集合，并令 L/K 为在每个有限位置均非分歧、且在每个实处均完全分裂的最大伽罗瓦 *pro-*π 扩张。$\mathrm{Gal}(L/K)$ 是否必然包含一个原幂零开子群?

对于一般的奇数阶 Γ，即使将“原幂零”替换为“可解幂零群”，我们也不知道类似问题是否有肯定答案。

参考文献

[1] M. Shusterman，有限域上曲线基本群的平衡表示，《数学研究快报》**29** （2022），第4期，1251–1259。doi:10.4310/MRL.2022.V29.N4.A13。[2] I. R. Shafarevich，代数数域，《国际数学家大会论文集》，斯德哥尔摩，1962年，Mittag-Leffler 研究所，于尔斯霍尔姆，1963年，第163–176页（俄文）。国际数学联盟论文集，第1卷。[3] M. Aschbacher 和 R. Guralnick，第一上同调群的一些应用，《代数杂志》**90** （1984），446–460。doi:10.1016/0021-8693(84)90183-2。[4] R. M. Guralnick、W. M. Kantor、M. Kassabov 和 A. Lubotzky，有限单群的表示：有限剩余与上同调方法，《群、几何与动力学》**1** （2007），469–523。doi:10.4171/GGD/22。[5] Y. Liu，具有受限分歧的极大扩张的伽罗瓦群表示，《代数与数论》**19**（2025），第5期，835–881。doi:10.2140/ant.2025.19.835。[6] A. Lubotzky，有限概形表示，《代数杂志》**242** （2001），第2期，672–690。doi:10.1006/jabr.2001.8805。[7] C. Pagano 和 M. Shusterman，随机与完美有限概形群中的高秩与重数，arXiv:2609.30200v1（2026）。[8] W. Sawin 和 M. Matchett Wood，全局域非分歧扩张的分布，arXiv:2602.21032v2（2026）。[9] W. Feit 和 J. G. Thompson，奇数阶群的可解性，《太平洋数学杂志》**13**（1963），第3期，775–1029。原期刊版本。[10] I. M. Isaacs，《有限群的特征标理论》，学术出版社，纽约，1976年。美国数学会修订重印本（2006年）。

[11]G. Navarro，有限群的特征标与区块，《伦敦数学学会讲义丛书》，第250卷，剑桥大学出版社，剑桥，1998年。doi:10.1017/CBO9780511526015。[12] A. Lucchini，有限群的切博塔廖夫不变量：*Kowalski* 和 *Zywina* 猜想，《美国数学会会刊》**146**（2018），第11期，4549–4562。doi:10.1090/proc/13805。arXiv:1509.05859v2（引用版本）。[13] A. Lucchini 和 D. Thakkar，最小生成集问题，《代数杂志》**640**（2024），117–128。doi:10.1016/j.jalgebra.2023.11.012。arXiv:2306.07633v1（引用版本）。[14] G. E. Andrews，分拆理论，剑桥大学出版社，1998年（1976年初版的重印本）。出版社记录。[15] H. Kurzweil 和 B. Stellmacher，有限群论：引言，Universitext，施普林格出版社，纽约，2004年。doi:10.1007/b97433。[16] L. Ribes 和 P. Zalesskii，赋 *profinite* 群，第二版，《数学及其边缘领域成果》，第3辑，第40卷，施普林格出版社，柏林，2010年。doi:10.1007/978-3-642-01642-4。