arXiv:2304.01323v1 [math.NT] 3 Apr 2023

具有局部数据的随机群：实现数域计数的启发式方法

BRANDON ALBERTS

ABSTRACT. 我们将数域 K 上的带局部数据的群定义为一个群 G，并附有从分解群 Gal $(\overline{K}_p/K_p) \to G$ 出发的同态。这类群类似于伽罗瓦群，只是缺少全局信息。受随机群在类群统计研究中的应用启发，我们使用 Sawin–Wood 提供的工具，构造一个定义在 K 上的带局部数据的随机群，作为绝对伽罗瓦群 Gal$(\overline{K}/K)$ 的模型；在该模型中，Frobenius 元的代表元按 Haar 测度随机分布，正如 Chebotarev 密度定理所预示的那样。我们利用作者证明的范畴大数定律结果，表明这是 Malle-Bhargava 原理的随机群版本。具体而言，在某些概率收敛概念下，包括期望收敛、依概率收敛和几乎处处收敛，该模型满足数域计数猜想，例如 Malle 猜想。这些结果为数域计数猜想提供了新的启发式依据，并开始弥合数域计数启发式与类群统计之间的理论鸿沟。

1. INTRODUCTION

数域族中的类群和数域非分歧扩张的伽罗瓦群，按预测将依照某些随机群呈现分布；也就是说，在拟有限群空间上存在一个概率测度 $\mu_{\mathcal{F},\,\mathscr{C}}$ 使得按猜想

$$\lim_{X\to\infty} \frac{\#\{K \in \mathcal{F} : \mathscr{C}(K) \cong G,\ \mathrm{disc}(K) \leqslant X\}}{\#\{K \in \mathcal{F} : \mathrm{disc}(K) \leqslant X\}} = \mu_{\mathcal{F},\mathscr{C}}(G), \tag{1}$$

其中 $\mathcal{F}$ 是一个数域族，而 $\mathscr{C}$ 可以是类群、Gal(K^{un}/K), ，或类似的构造，例如 K [FW89,BBH17,LWZB19] 的最大非分歧且次数与 2| 互素的伽罗瓦扩张的伽罗瓦群。该原理的经典版本是 Cohen–Lenstra 启发式 [CL84], ； Friedman–Washington 已证明，它等价于预测二次数域类群的 p 部分按某些随机 p 进矩阵的余核分布 [FW89]。这些启发式加深了我们对非分歧扩张结构的理解，并凸显了绝对伽罗瓦群中有趣的等分布性质。

Malle 猜想及其关于数域分布的推广与非分歧扩张的分布密切相关，因为它们对如下函数的增长率提出了更为一般的问题：

$$\#\{K \in \mathcal{F} : \text{other conditions},\ \mathrm{disc}(K) \leqslant X\} \tag{2}$$

如 $X \to \infty$。Malle [Mal02,Mal04] 研究的经典例子是

$$N(K, G; X) := \#\{L/K : [L : K] = n,\ \mathrm{Gal}(L/K) \cong G,\ \mathrm{Nm}_{L/K}\mathrm{disc}(L/K) \leqslant X\}.$$

对于 $G \subset S_n$ 一个传递子群，以及 $\mathrm{Gal}(L/K) \subset S_n$ 伽罗瓦群的伽罗瓦闭包 L/K ，并考虑其在 n 嵌入 $L \hookrightarrow L$上的作用。通过诉诸局部信息并假设存在一种“平均局部到整体原理”，可以推测这些计数函数的增长率。尽管 Malle 计数函数与类群统计中出现的计数函数明显相似，但目前文献中尚未建立 Malle 猜想与随机群之间的联系。本文旨在通过为绝对伽罗瓦群 $G_K := \mathrm{Gal}(\overline{K}/K)$, 构造一个“随机对象模型”，弥合非分歧扩张分布理论与其他数域族分布理论之间的差距；该模型可用于验证 Malle 猜想。

为此，我们定义两个范畴，并将在其上构建一个对绝对伽罗瓦群进行建模的随机对象。令 $G_{K_p} :=\mathrm{Gal}(\overline{K}_p/K_p)$ 为赋值 p 处的分解群。

(1) 带局部数据的群范畴 $\mathbf{proGrp}(K)$，其对象为一对 (G, ϕ) ，由一个拟有限群和一个连续同态元组 $\phi = (\phi_p)$ 构成；对于 K 的每个赋值 p ，都有一个同态 $\phi_p \colon G_{K_p} \to G$。完整定义（包括态射）见定义 2.1。(2) 具有有限局部数据的有限群范畴 $\mathbf{Grp}(K)$ ，其对象为三元组(G, S, ϕ) ，由一个有限群 G、 K 的有限个赋值 S以及一族连续同态 $\phi = (\phi_p)_{p\in S}$构成；对于 $p \in S$ 的每个赋值，都有一个同态 $\phi_p \colon G_{K_p} \to G$ 。完整定义（包括态射）见定义 2.2。

我们将证明，$\mathbf{proGrp}(K)$ （除去一个零测集）同构于 $\mathbf{Grp}(K)$的原对象范畴。近年来，Sawin–Wood [SW22] 的工作解决了广泛情形下原对象范畴上的矩问题，适用于非常一般的有限矩序列，但需满足一些温和条件。我们将证明 $\mathbf{Grp}(K)$ 满足这些条件，并给出一族符合 Sawin–Wood 所定义的良态有限矩序列，见命题 2.4。

特别地，利用 [SW22] 的主要结果，我们证明如下：

定理 1.1. 设 K 为一个数域。则在 $\mathbf{proGrp}(K)$ 的同构类上存在唯一的概率测度 μ_K^{MB}，使得

$$\int_{\mathrm{proGrp}(K)} \#\mathrm{Epi}(\mathscr{G}, (G, S, \phi))\ d\mu_K^{\mathrm{MB}}(\mathscr{G}) = |G^{\mathrm{ab}}[|\mu(K)|]|^{-1}|G|^{-|S\cup P_\infty|+1}$$

对于每个 $(G、\ S、\ \phi) \in \mathbf{Grp}(K)$。这里， $\mu(K)$是 K中单位根构成的群，而 P_∞是 K的无限位点集合。

上标“MB”代表“Malle-Bhargava”，因为我们将证明， μ_K^{MB}在某种意义上是与 Malle-Bhargava 原理 [Bha07, Woo19]相对应的随机群类比。 μ_K^{MB}的有限矩是根据切博塔廖夫密度定理和对类群统计的启发式预测构造的。我们将在引理 5.4 中证明，这些有限矩与 Malle-Bhargava 局部级数所预测的结果一致。

Malle 计数函数在伽罗瓦对应的意义下，计算的是从绝对伽罗瓦群到 G 的、判别式有界的满射。给定一个带局部数据的群$\mathscr{G}$，我们可以通过局部判别式 $\mathrm{disc}(\pi|_{G_{K_p}})$ 定义满射 π 的判别式： $\mathscr{G} \to G$ 。因此，Malle 计数函数可以推广到带局部数据的群。作者最近证明了一个关于范畴 [Alb22], 中随机对象的计数函数的大数定律版本，表明这些函数往往以概率 1 具有特定的

增长率。我们将数域的判别式排序转换到这一背景中，并利用 [Alb22] 的主要结果证明，在 n¨aively expected 的情形下， μ_K^{MB}以概率 1 满足 Malle 猜想，其首项常数可表示为一个收敛的欧拉乘积。

定理 1.2. 设 K 为一个数域， $G \subset S_n$ 为一个传递群， μ_K^{MB} 为构造得到的具有局部数据的群的分布。若 $\mathscr{G}$ 按照 μ_K^{MB} 分布，则

(i) 对任意 $\epsilon > 0$,

$$\frac{\#\{\pi \in \mathrm{Surj}(\mathscr{G}, G) : |\mathrm{disc}(\pi)| \leqslant X\}}{X^{1/a(G)+\epsilon}} \xrightarrow{a.s.} 0$$

当 $X \to \infty$ 时，其中“几乎处处收敛”表示“几乎必然收敛”。

(ii) 若 $G = \langle g \in G : \mathrm{ind}(g) = a(G) \rangle$ 由最小指标元素生成，则

$$\frac{\#\{\pi \in \mathrm{Surj}(\mathscr{G}, G) : |\mathrm{disc}(\pi)| \leqslant X\}}{c(K,G)X^{1/a(G)}(\log X)^{b(K,G)-1}} \xrightarrow{p.} 1$$

如 $X \to \infty$，其中“p.”表示“依概率收敛”。

(iii) 如果每个真正规子群 $N \trianglelefteqslant G$ 满足以下条件之一

(a) N 不含最小指标元素，或

(b) $G \backslash N$ 至少包含两个 K-共轭类的最小指标元素，

then

$$\frac{\#\{\pi \in \mathrm{Surj}(\mathscr{G}, G) : |\mathrm{disc}(\pi)| \leqslant X\}}{c(K,G)X^{1/a(G)}(\log X)^{b(K,G)-1}} \xrightarrow{a.s.} 1$$

如 $X \to \infty$，其中“a.s.”表示“几乎必然收敛”。

这里 $a(G)$、 $b(K$、$G)$ 和 K-共轭类的定义与 Malle 猜想（猜想 1.3）中的定义相同，并且

$$c(K,G) = \frac{(\mathrm{Res}_{s=1}\zeta_K(s))^{b(K,G)}}{a(G)^{b(K,G)-1}(b(K,G)-1)!|G^{\mathrm{ab}}[|\mu(K)|]| \cdot |G|^{u_K}} \prod_{p|\infty} \left(\sum_{f \in \mathrm{Hom}(G_{K_p}, G)} 1 \right)$$
$$\cdot \prod_{p \nmid \infty} \left[\left(1 - p^{-1}\right)^{b(K,G)} \left(\frac{1}{|G|} \sum_{f \in \mathrm{Hom}(G_{K_p}, G)} p^{-\frac{\nu_p \mathrm{disc}(f)}{a(G)}} \right) \right]$$

对于 $u_K = \mathrm{rk}\mathcal{O}_K^\times$， K 的单位秩。

这些方法非常稳健，可应用于 Malle 计数函数的多种推广。为使表述清晰，我们将此陈述最一般的版本（例如，在无限多个赋值处限制局部条件）留待未来的论文讨论。不过，在证明过程中，我们需要定理 1.2 的一个更一般的版本。这是因为判别式排序与非判别式排序之间存在自然关系，而我们在证明中利用了这些关系。这个更一般的结果在定理 6.1 中陈述，其中尤其包括分歧素数乘积排序。

定理 1.2 还强调了这样一个事实： μ_K^{MB}是 Malle-Bhargava 原理和 Malle 最初猜想的随机群类比，因为即使在 Malle 猜想不成立的情况下，它仍与 Malle 猜想一致。将这些预测构建为随机群，有助于我们揭示 Malle-Bhargava 原理的问题所在，并寻找修正方法。在第 7 节中，我们讨论 Malle 猜想已知的障碍，以及

这些障碍如何与带局部数据的随机群 μ_K^{MB}相互作用。我们不提出猜想，而是着重说明，将 Malle 猜想的预测表述为带局部数据的随机群，如何使这些障碍更加清晰，并为如何得出改进后的预测提供线索。

1.1. 历史背景与动机。对于 K 一个数域和 $G \subseteq S_n$ 一个传递子群，Malle 猜想可通过伽罗瓦对应改述为：计数从绝对伽罗瓦群出发的满射

$$\mathrm{Surj}(G_K, G; X) = \{\pi : G_K \twoheadrightarrow G : \mathrm{Nm}_{K/\mathbb{Q}}\mathrm{disc}(\pi) \leqslant X\},$$

其中 G_K 表示 K 的绝对伽罗瓦群，而 $\mathrm{disc}(\pi)$ 是由 $\pi^{-1}(\mathrm{Stab}_G(1))$固定的域的判别式。伽罗瓦对应蕴含 $\#\mathrm{Surj}(G_K, G;\ X) = |\text{自同构群}(G)| \cdot N(K, G;\ X)$，因此确定该函数的增长率是一个等价的问题。

猜想 1.3（Malle [Mal02,Mal04]）。设 $G \subset S_n$ 为一个有限传递群。设 $a(G) = \min_{g \neq 1}\mathrm{ind}(g)$，其中元素的指标定义为 $\mathrm{ind}(g) = n - \#\{\text{个 } g\}$的轨道。则

(i)（强形式）设 $\chi : G_K \to \hat{\mathbb{Z}}^\times$ 通过 $x.g = g^{\chi(x)}$ 作用于 G，并设 $b(K、G)$ 是在共轭类 $c \subset G$ 上的圆分作用下，$(c) = a(G)$ 的 ind 取最小值时的轨道数。那么存在一个正常数 $c(K$，使得 $G)$

$$\#\mathrm{Surj}(G_K, G; X) \sim c(K, G) X^{1/a(G)} (\log X)^{b(K,G)-1}$$

当 $X \to \infty$ 时。

(ii)（弱形式）

$$X^{1/a(G)} \ll \#\mathrm{Surj}(G_K, G; X) \ll_\epsilon X^{1/a(G)+\epsilon}$$

当 $X \to \infty$ 时。

已知强形式在某些情况下不成立，尤其是 $C_3 \wr C_2 \subseteq S_6$，正如 Kl¨uners [Kl¨u05a] 所示。然而，在许多其他情况下，强形式已知成立，包括

- 阿贝尔群 [M¨ak85、Wri89],
- S_3 在次数 3 [中的情形 DH71、DW88]，以及次数 6 [BW07],
- S_4 和 S_5 在次数 4 和 5 中的情形，分别见 [Bha14、BSW15],
- D_4；次数 4 [CYDO02],
- ；广义四元数群 [Kl¨u05b],
- ；大多数缠绕积 $C_2 \wr H$ [Kl¨u12],
- $A \times S_n$，其中 $n = 3$ 为 4、5，且 A 是不含某些小素数因子的阿贝尔群[Wan21、MTTW20], ；以及
- Heis$_3 \subseteq S_9$，其中 $K = \mathbb{Q}$ [FK21]。

常数 $c(K, G)$ 的取值也是研究的主题，但对于这里应当预期什么取值，我们所知甚少。Bhargava 最初提出 Malle-Bhargava 原理，部分目的就是预测当 $G = S_n$ 为对称群 [Bha07] 时这个常数的取值。关于 G 为阿贝尔群的情形，广泛的研究见 [Woo09] 。

定理 1.2 表明，按照 μ_K^{MB} 分布的带局部数据的群 $\mathscr{G}$ 以概率 1 满足关于 G-扩张的 Malle 猜想（在关于 G 的一些温和条件下）。带局部数据的群范畴旨在模拟绝对伽罗瓦群 G_K，即带有分解子群的拟有限群。事实上，μ_K^{MB}正是根据绝对伽罗瓦群的性质（如切博塔廖夫密度）构建的。尽管 G_K 是一个确定性对象，但我们有理由认为，可以根据 μ_K^{MB}中概率为 1 的事件来启发式地推断有关 G_K 的信息。

将随机模型用于确定性对象有先例，尤其是用于素数集合的 Cramér 随机模型 [Cra94,Gra95]。在这类模型中，100% 的情况下都会出现的行为，被认为可以作为证据，表明我们应当预期相应的确定性对象也具有相同的行为。对于素数而言，这类随机模型被用于论证 Hardy–Littlewood 猜想、哥德巴赫猜想，以及许多其他涉及素数间隔的猜想。

沿着这一思路，定理 1.2 给出了带局部数据的群以概率 1 呈现的行为，这可以视为有力证据，表明 G_K 也具有这些性质。这种形式的论证在 [Alb22 的广义计数启发式 1.7], 中有所阐述：如果我们预期 G_K 在按 μ_K^{MB}分布的带局部数据的群中是“典型的”，就可以据此作出预测。当然，众所周知，Malle 猜想按其原本表述并不成立——Klüners 在 $C_3 \wr C_2 \subseteq S_6$ 中给出了第一个反例，其中 Malle 预测的 b-不变量过小 [Klü05a]。Klüners 的反例展示了 $G_{\mathbb{Q}}$ 在按 μ_K^{MB}分布的带局部数据的群中某种非典型行为，具体而言，就是 $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$ 是 $G_{\mathbb{Q}}$的一个商。

因此，本文不尝试提出任何猜想。我们的目的是以随机对象为工具，按照 Malle 猜想的思路对计数函数建模，从而为这项工作开个头；但我们也认识到，已知绝对伽罗瓦群具有一些非典型行为。在论文末尾，我们讨论定理 1.2 与 Malle 猜想的已知成立情形（以及反例）的比较。本文不试图解决这些问题，而是着重说明如何在带局部数据的随机群这一框架下理解这些问题。未来工作的目标之一，是利用这一框架更好地刻画绝对伽罗瓦群的行为，并提出比 Malle-Bhargava 原理更准确的具体预测。

1.2. 论文结构。第 2 节中，我们构造带局部数据的群范畴，并证明它是 [SW22] 意义下某个菱形范畴的原对象范畴。此外，我们证明命题 2.4，给出一族 [SW22] 中定义的“良态序列”。这些结果为在该范畴中解决矩问题奠定基础，以便利用 [SW22] 中的主要结果，根据给定的有限矩构造概率测度。具体而言，第 3 节针对一列模拟绝对伽罗瓦群的特定有限矩，构造测度μ_K^{MB}，从而证明定理 1.1。

在第 5 节中，我们将数域的判别式排序转化为 [Alb22], 的语言，即底层有限对象范畴上的一列 L^1-函数 f_n。随后，我们确定该排序的矩，它们与 Malle-Bhargava 局部级数的系数和一致。接着，我们运用 [Alb22] 的主要结果，在第 6 节中证明定理 1.2，并证明若干恰当的推广，包括分歧素数乘积排序。

在第 7 节中，我们用带局部数据的群这一语言来阐释 Malle-Bhargava 原理中已知的问题。在某些情况下，我们证明这些问题在 μ_K^{MB} 中发生的概率为 0，这表明在这些情况下，G_K “不够典型”，因而不能以此为依据使用广义计数启发式来预测增长率。本节不提出任何猜想，但我们会利用这些信息指出，对随机模型可能需要作出哪些调整，才能得到更准确的预测。

1.3. 记号。

$$
\begin{aligned}
G_K &= \mathrm{Gal}(\overline{K}/K) \text{ the absolute Galois group of } K \\
P_K &= \{\text{places of } K\} \\
P_\infty &= \{p \in P_K | p \mid \infty\} \\
G_{K_p} &= \mathrm{Gal}(\overline{K}_p/K_p) \text{ the absolute Galois group of } K_p, \text{ where } p \text{ is a place of } K \\
I_p &= \text{the inertia group of } \overline{K}_p/K_p, \text{ where } p \text{ is a place of } K \\
\mathrm{Fr}_p &= \text{a representative of the Frobenius element in } G_{K_p} \\
I_K &= \text{the group of fractional ideals of } K \\
|\mathfrak{a}| &= \text{the norm down to } \mathbb{Q} \text{ of a fractional ideal } \mathfrak{a} \in I_K \\
\mathrm{disc}(\pi) &= \prod_p p^{\mathrm{ind}(g_p)} \text{ where } g_p \text{ generates } \pi(I_p) \\
\mathrm{ind}(g) &= n - \#\{\text{orbits of } g\}, \text{ where } g \in G \subseteq S_n \\
\mathrm{inv} &= \text{called an invariant, is some map } \prod_p \mathrm{Hom}(G_{K_p}, G) \to I_K
\end{aligned}
$$

$\mathsf{MB}_{\mathrm{inv}}(K, \Sigma, s) =$ Malle-Bhargava 局部级数，见引理 5.4 $\mathsf{Grp}(K) =$ 具有有限 K局部数据的有限群范畴，见定义 2.2(G, S, ϕ) 表示 Grp 中的一个对象$(K)\mathsf{proGrp}(K) =$ 具有 K 局部数据的群范畴，见定义 2.1$\mathscr{G}$ 表示 proGrp 中具有由 $\phi_{\mathscr{G}}$隐式给定局部数据的对象(K) $N(\mathscr{G}, f_n) = \sum_{(G,S,\phi)\in\mathsf{Grp}(K)} f_n(G, S, \phi)\#\mathsf{Epi}(\mathscr{G}, (G, S, \phi))$，见 [Alb22，定义 1.1] $M =$由有限矩序列$M(\{(G$给定的 Grp 上的离散测度(K) $, S, \phi)\}) = M_{(G,S,\phi)}\mu_K^{\mathrm{MB}} =$由定理 1.1 确定的唯一测度$M^{(j)} =$ 由 μ诱导的混合矩，见第 6.3 小节$\xrightarrow{p.}$ 依概率收敛$\xrightarrow{a.s.}$ 几乎必然收敛，即在测度为 1 的集合上收敛$f(X) \ll g(X)$ 存在常数 C，使得对所有 X，$f(X) \leqslant Cg(X) f(X) = O(g(X))$ 存在常数 C，使得对所有 X，$f(X) \leqslant Cg(X)$ $f(X) = o(g(X))$ 表示当 $X \to \infty$时 $\dfrac{f(X)}{g(X)} \to 0$

Acknowledgments

作者谨此感谢 Melanie Matchett Wood 多年来就本文主题与方向进行的诸多讨论。作者也感谢 Nigel Boston、Yuan Liu、Peter Koymans 和 Frank Thorne 提供的宝贵交流与反馈。

2. The category of groups with local data

本节定义带局部数据的群范畴，并用 [SW22] 的语言将其实现为原对象范畴。借助 [SW22], 中证明的若干工具，我们证明该范畴满足应用 Sawin–Wood 主要结果所需的假设。为解决第 3 节中的矩问题，我们在命题 2.4 中给出一族良态序列。

2.1. 带局部数据的群范畴。我们对带局部数据的群作如下精确定义：

定义 2.1. 我们用 $\mathsf{proGrp}(K)$ 表示带有 K-局部数据的拟有限群范畴。

(a) 该范畴的对象是由一个拟有限群 G 与一族连续同态 $\phi_p\colon G_{K_p}\to G$ （ K 的每个赋值 p 各有一个）组成的对 (G,ϕ) 。(b) 态射 $\pi\colon (G,\phi)\to(H,\psi)$ 是一个连续同态 $\pi\colon G\to H$，满足对 K 的每个赋值 p，均有 $\pi\phi_p=\psi_p$ 。

当上下文足以明确指出 K 时，我们常将这些对象简称为“带局部数据的群”，并省略拟有限性这一条件。

K 的任何伽罗瓦扩张不仅带有一个伽罗瓦群，还带有一个配备局部数据的伽罗瓦群，该局部数据由 $(\mathrm{Gal}(L/K),\phi_{L/K})$ 给出，其中 $\phi_{L/K}|_{G_{K_p}}$ 由相应的局部扩张 $G_{K_p}\to\mathrm{Gal}(L_p/K_p)\hookrightarrow\mathrm{Gal}(L/K)$ 给出。

备注：严格来说，带局部数据的伽罗瓦群仅在对每个 $\phi_{L/K,p}$ 的像取共轭后才是良定义的。我们始终为 K 的每个赋值 p 固定一个嵌入 $G_{K_p}\hookrightarrow G_K$，以便明确指定带局部数据的伽罗瓦群。这主要是为了方便——只要所有排序和局部条件都是共轭不变的，即使不作此选择，本文的结果仍然成立。不过，如果不必额外处理一个悬而未决的共轭关系，读者会更容易理解本文。

我们希望将 [SW22] 的结果应用于 $\mathsf{proGrp}(K)$，然而这个范畴有不可数多个同构类。因此，我们考虑 [SW22 中的原对象情形，即定理 1.7 和 1.8], ；由于我们允许 $\mathsf{proGrp}(K)$ 中包含拟有限群，这种情形是有意义的。为了应用这些结果，我们需要找到一个有限对象范畴，使得 $\mathsf{proGrp}(K)$ 是相应的原对象范畴。

仅仅将对限制为 $(G$、$\phi)$ 且 G 有限还不够，因为这样仍会有不可数多个对象。我们还需要限制具有局部数据的赋值。

定义 2.2。我们用 $\mathsf{Grp}(K)$ 表示带有有限 K-局部数据的有限群范畴。

(a) 该范畴的对象是由有限群 G、其上的有限个素位 S 以及一族连续同态 $\phi_p\colon G_{K,S}\to G$ （每个赋值 $p\in S$ 对应一个）组成的对 (G,S,ϕ)。(b) 态射 $\pi\colon (G,S,\phi)\to(H,S',\psi)$ 是连续同态 $\pi\colon G\to H$，满足• $S'\subseteq S$,• （对每个赋值 $p\in S\cap S'$），以及• （对每个赋值 $p\in S\backslash S'$）。

当 K 的含义可从上下文中明确时，我们通常会将这些对象简称为“具有有限局部数据的有限群”。

显然，$\mathbf{Grp}(K)$ 只有可数多个同构类，因为有限群 G有可数多个，有限位点集 S有可数多个，并且对于每个 G 和 $p \in S$，$\mathbf{Hom}(G_{K_p}, G)$ 都是有限集。我们对态射的定义体现了我们对这个范畴的期望：态射只能从具有更多赋值局部数据的对象指向具有较少赋值局部数据的对象，这反映了我们希望在逆极限中获得所有赋值处的局部数据。我们要求 $\pi\phi$ 在任意赋值 $p \notin S'$ 处非分歧，这一点则稍微微妙一些。原因有二：

- 我们希望保留分歧数据，使这些有限对象能够与判别式相容。特别是，我们希望任何满态射 $(G, S, \phi) \to (G, S', \psi)$在 G上限制为恒等映射时，都不会遗忘惯性数据。这将意味着，只要存在这样的满态射，就有 $\mathbf{disc}(G, S, \phi) = \mathbf{disc}(G, S', \psi)$。• 为什么不要求 $\pi\phi(G_{K_p}) = 1$? 那样限制会过于严格。在具有这一性质的逆极限中，只有除有限多个赋值外处处完全分裂的带局部数据的群会作为原对象出现。根据切博塔廖夫密度定理，这会排除所有带局部数据的伽罗瓦群，从而遗漏我们试图建模的核心结构。

我们简要概述 [SW22] 中定义的层概念以及这些范畴上的拓扑。在大多数情况下，我们可以直接引用 [SW22], 的结果，不过有时也需要深入探究这种拓扑的具体细节。层的概念尤其对处理原对象很重要。

$\mathbf{Grp}(K)$ 的一个层是 $\mathbf{Grp}(K)$, $\mathcal{C}$ 的同构类的一个子集，它是包含某个有限同构类集合的最小子集，并且向下封闭且并封闭，其中

- 向下封闭是指，如果 $(G, S, \phi) \in \mathcal{C}$ 且 $\mathbf{Epi}((G, S, \phi), (H, S', \varphi)) \neq \varnothing$，那么$(H, S', \varphi) \in \mathcal{C}$；而• 并封闭是指，对于任意有限对象 (G, S, ϕ)，如果 (H_1, S_1, ϕ_1) 和 (H_2, S_2, ϕ_2) 都是 (G, S, ϕ) 的商（即存在到它们的满态射），并且都属于 $\mathcal{C}$，那么它们的并 $(H_1, S_1, \phi_1) \vee (H_2, S_2, \phi_2)$ 也属于该集合；此并取为 (G, S, ϕ) 的商对象格中的并。

层级 t opology 在 $\mathbf{proGrp}(K)$ 或 $\mathbf{Grp}(K)$ 上定义为取基本开集

$$U_{\mathcal{C},\mathscr{H}} = \{\mathscr{G} : \mathscr{G}^{\mathcal{C}} = \mathscr{H}\},$$

其中 $\mathcal{C}$ 是一个层级，$\mathscr{H} \in \mathcal{C}$，而 $\mathscr{G}^{\mathcal{C}}$ 是属于 $\mathcal{C}$ 的 $\mathscr{G}$ 的最大商群，或者等价地，是 $\mathscr{G}$ 的商对象格中所有低于 $\mathscr{G}$ 的 $\mathcal{C}$ 元素的并。

现在我们证明，这些范畴满足应用 [SW22] 中工具所需的精确条件。

命题 2.3。设 K 是一个数域。那么

(a) $\mathbf{Grp}(K)$ 是一个菱形范畴 *[SW22，定义 1.3];* 并且 (b) $\mathbf{proGrp}(K)$ 同构于 $\mathbf{Grp}(K)$ 的原对象子范畴，其中每个赋值 p 都在某个有限商群 *[* 的局部数据中定义 K SW22，第 1.*2]* 节。

$\mathbf{Grp}(K)$ 的原对象范畴可以通过与下文相同的证明，证明其同构于对象 $(G$、S、$\phi)$ 的范畴，其中 G 是一个拟有限群，S 是任意素位集

属于 K，以及 $\phi=(\phi_p)_{p\in S}$ 一族连续同态 $\phi_p:\ G_{K_p}\to G$。我们定义的概率测度将支撑在子范畴 $\mathbf{proGrp}(K)$ 上，因此没有必要考虑完整的原对象范畴。

证明。Sawin–Wood 为识别菱形范畴证明了极其一般的工具。此处我们将使用他们的三个结果。

Sawin–Wood 在 [SW22，引理 6.19] 中证明，有限群范畴 $\mathbf{Grp}$ 是一个菱形范畴。给定 K 的赋值集合 P_K，令 $\mathcal{P}_K$ 为如下单射范畴的对偶范畴：其对象为 P_K 的有限子集，态射为包含映射。在此范畴中，$\mathbf{Hom}(S,S')$ 要么为空，要么只包含嵌入 $S\hookleftarrow S'$。此范畴显然满足菱形范畴的性质。

因此，由 [SW22，引理 6.16] 可知积范畴 $\mathbf{Grp}\times\mathcal{P}_K$ 是一个菱形范畴。局部数据 ϕ 可视为此范畴中的某种“有限数据”。令 $\mathcal{G}:\mathbf{Grp}\times\mathcal{P}_K\to\mathbf{FinSet}$ 为如下函子：它将

$$(G,S)\mapsto\prod_{p\in S}\mathrm{Hom}(G_{K_p},G).$$

那么，范畴 $(\mathbf{Grp}\times\mathcal{P}_K,\mathcal{G})$ 的对象为对 (G,S,ϕ)，其中 $(G,S)\in\mathbf{Grp}\times\mathcal{P}_K$，并配备 $\phi\in\mathcal{G}(G,S)$；由 [SW22，引理 6.21] 可知，该范畴是一个菱形范畴。这恰好就是 $\mathbf{Grp}(K)$。

$\mathbf{Grp}(K)$ 的原对象在 [SW22 第 1.2] 小节中定义为一个序列 $X=(X^{\mathcal{C}})$，该序列由层级 $\mathcal{C}$ 索引，并满足：对于任意 $\mathcal{C}\subset\mathcal{C}'$，都有 $(X^{\mathcal{C}'})^{\mathcal{C}}=X^{\mathcal{C}}$。令 $\mathcal{P}(\mathbf{Grp}(K))$ 表示 $\mathbf{Grp}(K)$的原对象范畴。

显然存在一个函子 $F:\mathbf{proGrp}(K)\to\mathcal{P}(\mathbf{Grp}(K))$，定义如下：

$$(G,\phi)\mapsto((G,S,\phi)^{\mathcal{C}})$$

and

$$\pi\mapsto\pi^{\mathcal{C}}.$$

这本质上是从 $\mathbf{proGrp}(K)$ 到每个层级 $\mathcal{C}$ 的一族遗忘函子。这个函子的像恰好是那些在所有赋值处都包含局部数据的原对象。令 $\mathcal{D}$ 表示这个范畴。

逆函子 $F^{-1}:\ \mathcal{D}\to\mathbf{proGrp}(K)$ 由逆极限给出。若将 $X^{\mathcal{C}}$写作 $(G_{\mathcal{C}},S_{\mathcal{C}},\phi_{\mathcal{C}})$，则

$$X\mapsto\left(\varprojlim_{\mathcal{C}}G_{\mathcal{C}},\bigcup_{\mathcal{C}}S_{\mathcal{C}},\varprojlim_{\mathcal{C}}\phi_{\mathcal{C}}\right)$$

and

$$(\pi^{\mathcal{C}})\mapsto\varprojlim_{\mathcal{C}}\pi^{\mathcal{C}}$$

显然，$F^{-1}\circ F$是恒等函子。由于 $\mathcal{D}$是 $\mathcal{P}(\mathbf{Grp}(K))$的子范畴，恰由满足 $\bigcup S_{\mathcal{C}}$为所有赋值的集合的那些对象构成，因此可知 $F\circ F^{-1}$也是恒等函子。□

2.2. 良态序列。Sawin–Wood [SW22] 的结果适用于“良态”的矩序列，即它们不会增长得太快。更明确地说，Sawin– Wood 将有限矩序列 $M_{(G,S,\phi)}$ 称为“良态”，如果级数

$$\sum_{(G,S,\phi)\in\mathcal{C}}\ \sum_{\pi\in\mathrm{Surj}((G,S,\phi),(F,S',\psi))}\frac{|\mu((F,S',\psi),(G,S,\phi))|}{|\mathrm{Aut}(G,S,\phi)|}Z(\pi)^3M_{(G,S,\phi)}.$$

绝对收敛，其中 $\mu(A,B)$ 是商对象格上的 M¨obius 函数，$Z(\pi)$ 是满足格分配律的 (G,S,ϕ) 与 (F,S',ψ) 之间元素的数量，而 $M_{(G,S,\phi)}$ 是所讨论的矩。

命题 2.4. 设 $M_{(G,\ S,\ \phi)}$ 是定义在 $\mathbf{Grp}(K)$ 的同构类上的有限矩序列。假设存在仅依赖于 S 的实常数 $f(S)$ 和 $e(S)$，使得$M_{(G,\ S,\ \phi)} = O(f(S)|G|^{e(S)})$。那么，序列 $M_{(G,\ S,\ \phi)}$ 按照 *[SW22]* 的意义是良态的。

命题 2.4 可视为群对应结果的类比：Sawin– Wood 在 [SW22, 推论 6.13] 中证明，若 $M_G = O(|G|^n)$ 对某个实数 n成立，则M_G 在有限群范畴中是良态的。命题 2.4 的力度基本相同：只需对 S 变化时进行很少的控制，而对 ϕ 变化时无需进行控制。

证明. 实际上，检验良态性可能有些繁琐。Sawin–Wood 为我们证明了一些有用的工具，可以缩短这一过程。回顾一下，范畴 $\mathbf{Grp}(K)$ 由 $(\mathbf{Grp}\ \times \mathcal{P}_K, \mathcal{G})$ 给出，其中函子有限数据 $\mathcal{G}(G,S) = \prod_p \mathbf{Hom}(G_{K_p}, G)$。Sawin–Wood 已在 [SW22, 引理 6.22]中研究了具有有限数据的范畴中的良态性。序列 $M_{(G,\ S,\ \phi)} = O(f(S)|G|^{e(S)})$ 是良态的，当且仅当序列

$$\sum_{\phi \in \prod_p \mathrm{Hom}(G_{K_p},G)} M_{(G,S,\phi)} = O\left(f(S)\prod_{p\in S}|\mathrm{Hom}(G_{K_p},G)||G|^{e(S)}\right)$$

在 $\mathbf{Grp}\ \times \mathcal{P}_K$ 中具有良态性。

Sawin–Wood 并未讨论积范畴中的良态性，但良态性总和的许多特征在积下都可以分解。注意，在积范畴中，我们必然有

$$\begin{aligned}\mathrm{Aut}(G,G') &= \mathrm{Aut}(G)\times\mathrm{Aut}(G'),\\ \mu((F,F'),(G,G')) &= \mu(F,G)\mu(F',G'),\\ Z(\pi_1,\pi_2) &= Z(\pi_1)Z(\pi_2).\end{aligned}$$

此外，积范畴中的每一层都包含在由各个范畴中的层 $\mathcal{C}_1 \times \mathcal{C}_2$ 构成的积中。由此可立即证明以下结果：

引理 2.5. 设 C_1 和 C_2 是两个菱形范畴。若序列 $(M_G)_{G\in C_1}$ 和$(M_{G'})_{G'\in C_2}$在各自的范畴中具有良态性，则序列$(M_G M_{G'})_{(G,\ G')\in C_1\times C_2}$在积范畴中具有良态性。

我们将证明的细节留给感兴趣的读者，因为我们实际上无法使用这一结果。我们并未假设我们的矩序列在积下可分解；事实上，上界 $f(S)|G|^{e(S)}$ 并不能在积下分解。幸运的是，事实证明，范畴 $\mathcal{P}_K$ 对于良态性而言特别理想。

引理 2.6. 设 C 是一个菱形范畴， $\mathcal{N}$ 是由有限子集 $\mathbb{N}$ 在包含关系下构成的对偶范畴。若对于每个固定对象 $S \in \mathcal{N}$，序列 $M_{(G,\ S)}$ 在 C中表现良好，则序列 $M_{(G,\ S)}$ 在范畴 $C \times \mathcal{N}$中表现良好。

这里我们指出，无论如何选择基域 K， $\mathcal{P}_K$ 和 $\mathcal{N}$ 作为范畴都是同构的。这个同构来自从可数集 P_K到 $\mathbb{N}$的一个双射。

证明。$\mathcal{N}$ 的任意层 $\mathcal{C}$ 都仅由某个有限集 $S \subseteq \mathbb{N}$的有限多个子集组成。在范畴 $\mathcal{N}$中，每个态射都是满态射；对于任意对象 S，满态射恰好对应于 S的有限多个子集。因此，对于任意乘积层级 $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2$，我们将良态性求和拆分为

$$\sum_{(G,S)\in\mathcal{C}} \sum_{\pi\in\mathrm{Surj}((G,S),(F,S'))} \frac{|\mu((F,S'),(G,S))|}{|\mathrm{Aut}(G,S)|} Z(\pi)^3 M_{(G,S)}$$

$$= \sum_{S\in\mathcal{C}_2} \sum_{\pi_2\in\mathrm{Surj}(S,S')} \frac{|\mu(S',S)|}{|\mathrm{Aut}(S)|} Z(\pi_2) \left(\sum_{G\in\mathcal{C}_1} \sum_{\pi_1\in\mathrm{Surj}(G,F)} \frac{|\mu(F,G)|}{|\mathrm{Aut}(G)|} Z(\pi_1)^3 M_{(G,S)} \right).$$

前两个求和是有限的，而根据$M_{(G,\ S)}$ 中每个对象 S的良态性，后两个内层求和绝对收敛。因此，整个求和收敛。□

根据 [SW22，推论 6.13], ，对于某个实数 n 的任意序列 $M_G = O(|G|^n)$ 在 Grp 上都是良态的。已知分解群 G_{K_p} 对于每个赋值 p都具有有限秩，该秩取决于 K 和 p。因此

$$\begin{aligned} M_{(G,S)} &= \sum_{\phi\in\prod_p \mathrm{Hom}(G_{K_p},G)} M_{(G,S,\phi)} \\ &= O\left(f(S) \prod_p |\mathrm{Hom}(G_{K_p},G)||G|^{e(S)} \right) \\ &= O_S\left(|G|^{e(S)+O_{K,S}(1)} \right), \end{aligned}$$

对于每个固定的 $S \in \mathcal{P}_K$ （其中 K 始终固定），该对象在 Grp 中必然是良态的。因此，根据引理 2.6，它在 $\mathsf{Grp}\times\mathcal{P}_K$中是良态的，从而证明了序列 $M_{(G,\ S,\ \phi)}$的良态性。□

3. Constructing the Malle-Bhargava measure

本节中，我们证明定理 1.1，该定理给出了一个 μ_K^{MB}概率测度的存在性与唯一性，用于刻画绝对伽罗瓦群。具体而言，我们利用切博塔廖夫密度定理构造有限矩序列 M_G，然后应用 [SW22，定理 1.8]。该结果表明：给定原对象同构类上的任意测度序列，若其有限矩收敛到一个良态序列，则这些测度本身弱收敛到原对象同构类上的唯一测度。

3.1. 逼近绝对伽罗瓦群的测度序列。记 $P_\infty = \{p \mid \infty\}$ 为无限位点的集合。对于包含所有无限位点的有限处集合 S，我们定义前自由积

$$F_{K,S} = \mathop{\ast}_{p\in S} G_{K_p}.$$

这不是一个带局部数据的群，因为在S之外的赋值处没有任何局部数据。受切博塔廖夫密度定理和类域论的启发，对于任意一组 (r_x)元素$r_x \in F_{K,\ S}$对于 $x \in \{0, ..., |S|-1\} \cup (P_K \backslash S)$ 我们定义商

$$\mathscr{F}_{K,S}(r) = F_{K,S}/\langle r_0, ..., r_{|S|-1}\rangle.$$

$r_1, ..., r_{|S|-1}$ 来自类域论，由 S-单位群$\mathcal{O}_K^\times$的秩给出。这些 $|S|-1 = |S\backslash P_\infty| + (|P_\infty|-1)$ 关系对应于 [LW20, LWZB19] 中针对 n 的 $n+u$ 关系，其中 $|S\backslash P_\infty|$对应于 S中有限处的数量，而 u 对应于单位秩 $u_K = \mathrm{rk}\mathcal{O}_K^\times = |P_\infty| - 1$。

关系 r_0 描述了类域论中由基域 $\mu(K)$ 的单位根产生的关系。由于 [LWZB19] 只考虑阶与 $|\mu(K)|$ 互素的非分歧扩张，因此其中并未出现这一关系。

元组中用于 $p \notin S$ 的元素 r_p 不会对底层群产生关系，而是用于指定局部数据。这通过以下方式给出了 $\mathscr{F}_{K,\ S}(r)$ 典范的局部数据 $\phi = (\phi_p)$

- ϕ_p is the composition $G_{K_p} \hookrightarrow F_{K,S} \to \mathscr{F}_{K,S}(r)$ if $p \in S$, and
- $\phi_p|_{I_p} = 1$ and $\phi_p(\mathrm{Fr}_p) = r_p$ if $p \notin S$.

受切博塔廖夫密度（该密度指出，弗罗贝尼乌斯元素在绝对伽罗瓦群中按 Haar 测度随机变化）和类群启发式（该启发式预测单位群按 Haar 测度随机嵌入幺元）的启发，我们定义以下概率测度。

定义 3.1。设 S 为一个包含所有无限赋值的有限赋值集。定义

$$\mu_{K,S}^{\mathrm{MB}}(A) = \mathrm{Prob}\left(\mathscr{F}_{K,S}(r) \in A\right)$$

对于 $\mathsf{proGrp}(K)$ 的 Borel σ-代数中的任意集合 A，其中每个 r_x 均从以下空间中独立地按 Haar 测度随机取值：

(a) r_0 在 $F_{K,\ S}^{\mathrm{ab}}[|\mu(K)|]$ 中 $F_{K,\ S}$ 在阿贝尔化映射下的原像中按 Haar 测度随机取值；(b) 对于 $p \notin S$，r_1、r_2、...、$r_{|S|-1}$ 和 r_p 在 $F_{K,\ S}$中相互独立地按 Haar 测度随机取值。

令 $\mathsf{ab}\colon F_{K,\ S} \to F_{K,\ S}^{\mathrm{ab}}$。$r_0$ 的不同行为旨在确保存在一个满射同态 $\mathcal{O}_{K,\ S}^\times \to \mathsf{ab}(\langle r_0, r_1, ..., r_{|S|-1}\rangle)$，它从 S的单位元映到 K，其中 $\mu(K)$ 的一个生成元被映到 r_0，而 $\mathcal{O}_{K,\ S}^\times$ 自由部分的一组基被映到 r_1、...、$r_{|S|-1}$。根据狄利克雷单位定理，并注意到 $P_\infty \subset S$，秩相等。根据局部类域论，阿贝尔化为

$$F_{K,S}^{\mathrm{ab}} \cong \prod_{p \in S} K_p^\times,$$

按 Haar 测度随机改变关系 $r_0, ..., r_{|S|-1}$，对应于选择一个 Haar随机同态 $\mathcal{O}_{K,\ S}^\times \to \prod_{p\in S} K_p^\times$，从而随机选择 S-单位元的一个像。

这一构造旨在配合 Malle 猜想。给定实数 X，判别式不超过 X 的扩张 L/K 只有有限多个。令 L_X 为所有此类扩张的复合域。那么，带局部数据 $(\mathrm{Gal}(L_X/K), \phi_{L_X/K})$ 的伽罗瓦群是 $\mathscr{F}_{K,\ S}(r)$ 的一个商，至少对应于一个非平凡元组 r；其中 $S = S_X$ 选得足够大，以生成 $\mathrm{Gal}(L_X \cap K^{ur}/K)$，而 r 是某个与 G_K 兼容、用于定义关系的元组。

类群统计中的这一理念——单位群在 S理想群中的像是 Haar随机的——启发了模型中让 $r_0, r_1, ..., r_{|S|-1}$ 随机变化的选择。切博塔廖夫密度定理则启发了模型中允许 r_p 随 $p \notin S$ 按 Haar 测度随机变化的选择。综合起来，这种启发式推理与 $\mu_{K,\ S}^{\mathrm{MB}}$一致。当 $X \to \infty$趋于极限时，我们需要越来越大的赋值集合 S_X，因此，用 $\mu_{K,\ S}^{\mathrm{MB}}$ 的极限来建模 G_K 是合理的，其中 S 趋向于全体赋值的集合 P_K。

3.2. 定理 1.1 的证明。构造测度 μ_K^{MB}，使其为 $\mu_K^{\mathrm{MB},\ s}$ 的极限，这正是 [SW22，定理 1.8] 的目的。只需计算 $\mu_K^{\mathrm{MB},\ s}$ 的有限矩在 S 趋向于全体赋值集合时的极限；我们将验证其性质良好，并利用命题 2.4 及 [SW22，定理 1.8]证明它对应于唯一的测度。

命题 3.2. 设 K 是一个数域，且 $(G、\ S、\ \phi) \in \mathbf{Grp}(K)$。那么对于任意素位集 $S' \supseteq S$

$$\int \#\mathrm{Epi}(\mathscr{G}, (G, S, \phi))\ d\mu_{K,S'}^{\mathrm{MB}} = |G^{\mathrm{ab}}[|\mu(K)|]|^{-1}|G|^{-|S\cup P_\infty|+1}.$$

这个命题是定理 1.1 中有限矩的来源。我们指出，该结果比计算有限矩的极限更强。$S' \supseteq S$ 最终会在极限中成立，因此

$$\lim_{S'\to P_K} \int \#\mathrm{Epi}(\mathscr{G}, (G, S, \phi))\ d\mu_{K,S'}^{\mathrm{MB}} = |G^{\mathrm{ab}}[|\mu(K)|]|^{-1}|G|^{-|S\cup P_\infty|+1}$$

因为该序列最终为常数。

证明. 对于固定的 $(G、\ S、\ \phi) \in \mathbf{Grp}(K)$，我们考虑若 $S \subseteq S'$，则

$$\int \#\mathrm{Epi}(\mathscr{G}, (G, S, \phi))\ d\mu_{K,S'}^{\mathrm{MB}} = \sum_{\substack{\varphi\in \mathrm{Hom}(F_{K,S'}, G)\\ \varphi|_{F_{K,S}}=\phi\\ \varphi(I_p)=1 \text{ if } p\in S'\setminus S}} \int \#\mathrm{Epi}(\mathscr{G}, (G, S', \varphi))\ d\mu_{K,S'}^{\mathrm{MB}}.$$

每个 ϕ 都可以理解为一个同态 $F_{K,\ S} \to G$。集合 $\mathbf{Epi}(\mathscr{F}_{K,\ S'}(r)、\ (G、\ S'、\ \varphi))$ 至多包含一个元素；若 φ 经由商 $F_{K,\ S'} \to \mathscr{F}_{K,\ S'}(r)$ 分解，则该元素由 φ 给出。当且仅当每个关系都属于核时，这种情况才会发生。这些关系按 Haar 测度相互独立地随机变化，因此可得

$$\begin{aligned}\int \#\mathrm{Epi}(\mathscr{G}, ((G, S', \varphi), \pi))\ d\mu_{K,S'}^{\mathrm{MB}} &= \prod_{i=0}^{|S'|-1} \mu_{Haar}\left(\ker q_*\varphi\right)\\ &= |G^{\mathrm{ab}}[|\mu(K)|]|^{-1}|G|^{-|S'|+1}.\end{aligned}$$

对于有限处，恰有 $|G|$ 个非分歧连续同态 $G_{K_p} \to G$，因此求和中每个 $p \in S'\setminus(S \cup P_\infty)$ 都要额外乘上一个因子 $|G|$。于是积分为

$$\begin{aligned}\int \#\mathrm{Epi}(\mathscr{G}, (G, S, \phi))\ d\mu_{K,S'}^{\mathrm{MB}} &= |G^{\mathrm{ab}}[|\mu(K)|]|^{-1}|G|^{|S'\setminus(S\cup P_\infty)|-|S'|+1}\\ &= |G^{\mathrm{ab}}[|\mu(K)|]|^{-1}|G|^{-|S\cup P_\infty|+1}.\end{aligned}$$

□

现在我们可以证明定理 1.1 了。

定理 1.1 的证明。矩序列

$$M_{(G,S,\phi)} = |G^{\mathrm{ab}}[|\mu(K)|]|^{-1}|G|^{-|S\cup P_\infty|+1} = O(|G|^0)$$

满足命题 2.4 的假设，因此按照 [SW22] 的意义，它表现良好。因此，命题 3.2 与 [SW22, Theorem 1.8] 共同蕴含了某个测度的存在

μ_K^{MB}定义在 $\mathsf{Grp}(K)$ 的原对象范畴上，使得 $\mu_{K,S}^{\mathrm{MB}} \to \mu_K^{\mathrm{MB}}$弱收敛为$S \to P_K$，且 μ_K^{MB}具有给定的有限矩。由于 $\mu_{K,S}^{\mathrm{MB}}$ 的总测度为 1，μ_K^{MB}的总测度也为 1，因此它是一个概率测度。因此，只需证明 μ_K 支撑在 $\mathsf{proGrp}(K)$ 上。

由构造可知，μ_K^{MB}, S 支撑在 $\mathsf{proGrp}(K)$ 上，因此很容易想到，由于弱收敛， μ_K^{MB}也支撑在其上。然而，这并非弱收敛测度序列普遍具有的性质。 P_K 是可数的这一事实在此帮了我们。对于 K的每个赋值 p，令 f_p 为定义在 $\mathsf{Grp}(K)$ 的原对象上的函数，其定义为

$$f_p(G,S,\phi) = \begin{cases} 1 & p \notin S \\ 0 & p \in S, \end{cases}$$

这里提醒一下，原对象可以在任意赋值集 S上带有局部数据。此函数是连续的，因为

$$f_p^{-1}(0) = \bigcup_{\mathcal{C}} \bigcup_{\substack{(G,S,\phi)\in\mathcal{C} \\ p\in S}} U_{\mathcal{C},(G,S,\phi)}$$

是基本开集的并集，并且

$$f_p^{-1}(1) = \bigcup_{\mathcal{C},\ p\in S(\mathcal{C})} \bigcup_{\substack{(G,S,\phi)\in\mathcal{C} \\ p\notin S}} \left(U_{\mathcal{C},(G,S,\phi)} \setminus \bigcup_{\substack{(G,S\cup\{p\},\psi)\in\mathcal{C} \\ \psi|_S=\phi}} U_{\mathcal{C},(G,S\cup\{p\},\psi)} \right),$$

其中， $S(\mathcal{C})$ 是至少出现在层 $\mathcal{C}$的一个同构类中的素数集。最内层的并集是有限个基本开集的并集；事实上，这些基本开集在由 [SW22]定义的层拓扑中既开又闭。因此，集合差是开集，而这个原像又是开集的并集。因此， f_p 可提升为定义在原对象上的连续函数。有界连续函数的期望值沿弱收敛测度序列收敛。μ_K^{MB}, S 支撑在 $\mathsf{proGrp}(K)$ 上这一事实意味着

$$\int f_p \, d\mu_K^{\mathrm{MB}} = \lim_{S\to P_K} \int f_p \, d\mu_{K,S}^{\mathrm{MB}} = 0.$$

因此，在 p 处没有局部数据的原对象集合是一个零测集。赋值 p 只有可列多个，因此由可列可加性可知，$\mathsf{proGrp}(K)$ 的补集是一个零测集，即 μ_K^{MB} 支持在 $\mathsf{proGrp}(K)$ 上。□

4. Outlining the Proof of Theorem 1.2

传递子群 $G \subseteq S_n$ 的 Malle 经典计数函数是通过排序 disc_X^G： $\mathsf{Grp}(K) \to \mathbb{R}$ 定义的

$$\mathrm{disc}_X^G(H,S,\phi) = \begin{cases} 1 & H \cong G,\ |\mathrm{disc}(\phi)| \leqslant X, \text{ and } S = \{|p| \leqslant X\} \\ 0 & \text{else.} \end{cases}$$

作者在 [Alb22] 中定义了相应范畴上的计数函数：

$$N(\mathscr{G}, \mathrm{disc}_X^G) := \sum_{(G,S,\phi)\in \mathrm{Grp}(K)} \mathrm{disc}_X^G(G,S,\phi) \# \mathrm{Epi}(\mathscr{G}, (G,S,\phi)).$$

定理 1.2 将利用 [Alb22] 的结果予以证明。这大致分为三个重要步骤:

(I) 我们首先证明，Malle 计数函数与 $N(\mathscr{G}、\mathrm{disc}_X^G)$ 的计数函数一致，也就是说

$$N(\mathscr{G}, \mathrm{disc}_X^G) = \#\{\pi \in \mathrm{Surj}(\mathscr{G}, G) : |\mathrm{disc}(\pi)| \leqslant X\}.$$

这将由第 5 节中证明的引理 5.2 推出。

(II) [Alb22，定理 1.3]指出，在适当条件下，计数函数$N(\mathscr{G}、\mathrm{disc}_X^G)$渐近等于

$$\int_{\mathrm{Grp}(K)} \mathrm{disc}_X^G \; dM := \sum_{(G,S,\phi)\in \mathrm{Grp}(K)} \mathrm{disc}_X^G(G,S,\phi) M_G$$

当 X 趋于无穷时。这个积分在引理 5.4 中计算，结果表明它等于 Malle-Bhargava 局部级数的系数之和。这正是 Malle 预测的渐近增长率的来源。

备注：严格来说， [Alb22]要求 X 为正整数，而非实数。这对我们的目的没有影响，因为判别式的范数总是取正整数值。为符合 Malle 猜想的标准记号，全文中我们将约定 X 为正整数。

(III) 为了验证 [Alb22, Theorem 1.3], 的条件，我们将借助 [Alb22, Theorem 1.4] 和 [Alb22, Corollary 1.5]。只需对以下形式的积分给出上界

$$\int_A \mathrm{disc}_X^G \; dM^{(j)} (dM)^{2k-j} := \sum_{(G_i,S_i,\phi_i)\in A} \prod_{i=1}^{2k} \left(\mathrm{disc}_X^G(G_i,S_i,\phi_i)\right) M^{(j)}_{(G_i,S_i,\phi_i)_{i=1}^j} \prod_{i=j+1}^{2k} M_{(G_i,S_i,\phi_i)}$$

对于特定的子范畴 $A \subseteq \mathbf{Grp}(K)^{2k}$。这里，由 μ_K^{MB} 诱导的混合矩 $M^{(j)}\colon \mathbf{Grp}(K)^j/\cong \to [0,\infty]$ 定义为

$$M^{(j)}_{((G_1,S_1,\phi_1),\ldots,(G_j,S_j,\phi_j))} := \int_{\mathrm{proGrp}(K)} \left(\prod_{i=1}^{j} \#\mathrm{Epi}(\mathscr{G}, (G_i,S_i,\phi_i)) \right) \; d\mu_K^{\mathrm{MB}}(\mathscr{G}).$$

先验地，这些矩未必有限，不过我们将证明，在我们关注的情形中它们是有限的。这将是第 6 节的重点，我们将在引理 6.4 中给出混合矩的上界。随后即可推出定理 1.2。

用于最后一步的引理 6.4 是本文中技术性最强的结果。事实证明，disc_X^G 的混合矩与按其他非判别式不变量排序、且具有受限分歧行为的满射计数自然相关。因此，自然（事实上也是必要的）要在比定理 1.2 更一般的框架下开展研究。

因此，我们将第 5 节围绕可容许不变量和任意受限局部条件来组织，而判别式排序将是后者的一个特例。特别是，引理 5.2 对可容许不变量和容许局部条件作了完全一般的表述。这就完全推广了步骤 (I) 和 (II)。

我们在第 6 节证明定理 1.2。该节几乎完全专注于证明引理 6.4，以完成步骤 (6)。这些方法本质上具有一般性，读者有理由认为，在我们于引理 5.4 中呈现的一般性层次上，类似的结果也成立。然而，在更一般的情形下，分析会变得技术上复杂，而且有时需要对排序和/或局部条件作出额外假设。尽管

引理 6.4 是全文技术性最强的部分，但它也是关键所在，正是它使我们能够应用 [Alb22] 的结果。为了不掩盖引理 6.4 背后的思路，我们仅讨论可行的最简单情形。

5. Multiplicative orderings and the Malle-Bhargava local series

本节的目标是以完全一般的形式完成步骤 (I) 和 (II)。我们将定义可容许不变量和可容许局部条件族，以便在此框架下开展研究，并证明引理 5.4，给出排序与 Malle-Bhargava 局部级数之间的明确对应关系。

5.1. 按可容许不变量排序。我们将研究更一般的排序以及更一般的局部限制。在 Malle 猜想的研究中，这一扩展框架已得到广泛考察。

定义 5.1。固定一个有限群 G、一个有限个素位的集合 S、一个不变量 $\mathrm{inv} : \prod_p \mathrm{Hom}(G_{K_p}, G) \to I_K$，以及 $\Sigma = (\Sigma_p)$ 一个局部条件族 $\Sigma_p \subseteq \mathrm{Hom}(G_{K_p}, G)$。于是，我们定义相应的排序 $\mathrm{inv}_X^{G\,S\,\Sigma}{}_{,,}$：$\mathrm{Grp}(K)/\cong \to \{0,1\}$ to，即由满足以下条件的集合 $(H, S', \phi) \in \mathrm{Grp}(K)$ 的示性函数构成的序列：

(a) $H \cong G$，(b) $S' = S \cup \{|p| \leqslant X\}$，(c) $\phi \in \prod_{p \in S'} \Sigma_p$，以及 (d) $|\mathrm{inv}(\phi)| \leqslant X$。

如果对所有赋值 p，$\Sigma_p = \mathrm{Hom}(G_{K_p}, G)$ 都是平凡的，我们可以在记号中省略 Σ。如果 $S = \varnothing$，我们可以在记号中省略 S。

判别式排序 disc_X^G 是一个特例，其中 $S = \varnothing$ 和 Σ 是平凡族。我们以尽可能一般的形式定义了 $\mathrm{inv}_X^{G\,S\,\Sigma}{}_{,,}$，尽管并非每一种 G、S、inv 和 Σ 的选择都对应于一个数域计数函数。例如，即使考虑计数函数 $\#\{\pi \in \mathrm{Surj}(G_K, G) : |\mathrm{inv}(\pi)| \leqslant X\}$，我们也需要 inv 具有 Northcott 性质，才能保证该计数是有限的。

如果 $\mathrm{inv} : \prod \mathrm{Hom}(G_{K_p}, G) \to I_K$ 满足 [Alb20], 中所述的条件，即满足

- $\mathrm{inv} = \prod_p \mathrm{inv}_p$ 是乘法性的，
- $\mathrm{inv}_p(\pi)$ 由 $\pi|_{I_p}$ 确定，当且仅当 $\pi|_{I_p} = 1$时等于 1，并且

引理 5.2. 设 G 是一个有限群，S 是有限个赋值，Σ 是一个局部条件族，且 inv 是一个可容许不变量。则

$$N(\mathscr{G}, \mathrm{inv}_X^{G,S,\Sigma}) = \#\left\{\pi \in \mathrm{Surj}(\mathscr{G}, G) : (\pi|_{G_{K_p}}) \in \prod \Sigma_p \ \textit{and}\ |\mathrm{inv}(\pi)| \leqslant X\right\}.$$

特别地，计数函数与 S无关。

计数函数与 S 无关，这一点对我们的证明至关重要。S 所起的作用基本上纯粹是记账——在额外位置施加局部条件，有助于表述范畴论结果。正如我们在此处看到的，并且将在引理 5.4 中再次看到，额外位置的选择完全不会影响计数函数。

证明。固定 S 和 X，考虑一个满射 $\pi : \mathscr{G} \to G$。显然，这会特化为 $\mathbf{Epi}(\mathscr{G}, (G, S \cup \{|p| \leqslant X\}, \pi\phi_{\mathscr{G}}))$中的一个满态射，因此可得

$$\mathrm{Surj}(\mathscr{G}, G) = \bigcup_{\phi} \mathrm{Epi}(\mathscr{G}, (G, S \cup \{|p| \leqslant X\}, \phi)).$$

此外，假设存在两个满态射 $\pi_i \in \mathbf{Epi}(\mathscr{G}, (G, S \cup \{|p| \leqslant X\}, \phi_i))$ for $i = 1$，2，其底层群同态等价于 π。那么

$$\pi_1\phi_{\mathscr{G}} = \pi\phi_{\mathscr{G}} = \pi_2\phi_{\mathscr{G}},$$

这意味着在每个赋值 $p \in S \cup \{|p| \leqslant X\}$处都有 $\phi_{1,\ p} = \phi_{2,\ p}$。特别地，群层面的恒等映射诱导出一个同构 $(G, S \cup \{|p| \leqslant X\}, \phi_1) \cong (G, S \cup \{|p| \leqslant X\}, \phi_2)$。因此，该并集实际上是不交并

$$\mathrm{Surj}(\mathscr{G}, G) = \coprod_{\phi} \mathrm{Epi}(\mathscr{G}, (G, S \cup \{|p| \leqslant X\}, \phi)).$$

注意到可容许性意味着 $|\mathbf{inv}(\pi)| = |\mathbf{inv}(\pi\phi_{\mathscr{G}})|$，即可得到该结果，因此不变量不超过 X 的元素之和在两边相同。□

$\mathbf{inv}_X^{G\,S\,\Sigma}(A)$，，、$\mathbf{inv}_X^{G\,S\,\Sigma}(B) \neq 0$，，这一事实意味着 $\#\mathbf{Epi}(A, B) = 0$，对于证明计数函数独立于 S 的选择至关重要，也是对上述证明部分内容的重新表述。我们的目标是利用 [Alb22], 的结果研究这些计数函数；该结果使我们能够通过研究离散测度 M （由 μ_K^{MB} 的有限矩诱导）下 $\mathbf{inv}_X^{G\,S\,\Sigma}$，，的矩来证明概率为 1 的结论。计数函数独立于 S 这一事实，使我们能够让 inv 和 Σ 在有限多个赋值处取任意行为。

在证明渐近结果时，人们常要求 inv 具有 [Alb21], 中的 Frobenian 性质，这保证关于 Malle-Bhargava 局部级数的陶伯定理能够给出良好的渐近增长率。这涵盖了所有判别式排序，尤其包括分歧素数乘积排序。我们将在第 6 节采用更严格的要求。

5.2. 受限局部条件的类型。所选局部条件族 $\Sigma =(\Sigma_p)$ 的类型可能影响增长率。特别是，可以对每个赋值 p 都选择 $|\Sigma_p| = 1$。这种选择方式有不可数多种，但数域 K 上的 G-扩张只有可数多个，因此我们预计没有 G-扩张能够满足如此严格的局部限制选择。

这种行为归结为我们能够通过 Σ 控制多少种分解类型。为刻画这一区别，我们作如下定义：

定义 5.3。若 $\mathrm{Hom}_{ur}(G_{K_p}$ 对除有限多个赋值外的所有赋值均成立，我们称 $\Sigma = (\Sigma_p)$ 为可容 $G)$ 许局部条件族 $\Sigma_p \subset \mathrm{Hom}(G_{K_p}$。

引理 5.4 将在这一一般性层面上证明。与不变量的情形一样，人们也常要求 Σ 按照 [Alb21] 中定义的意义是 Frobenian。在第 6 节中，我们将采用比这更严格的要求

5.3. $\mathrm{inv}_X^{G\,S\,\Sigma}{}_{,,}$的一阶矩。我们证明，$\mathrm{inv}_X^{G\,S\,\Sigma}{}_{,,}$的 L^1-范数与 Malle-Bhargava 局部级数的系数一致。即使我们只假设可容许性，证明也相同，因此我们以这一一般性层面陈述结果：

引理 5.4. 设 $M_{(G,\ S,\ \phi)} = |G^{\mathrm{ab}}[|\mu(K)|]| \cdot |G|^{-|S\cup P_\infty|+1}$ 为 μ_K^{MB}的有限矩。固定一个有限群 G、有限个素位 S、一个可容许不变量 inv，以及一个局部条件族 Σ。令 (a_n) 表示 Malle-Bhargava 局部级数的狄利克雷系数

$$\mathrm{MB}_{\mathrm{inv}}(K,\Sigma,s) = \prod_p \left(\frac{1}{|G|} \sum_{f_p \in \Sigma_p} |\mathrm{inv}(f_p)|^{-s} \right) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

Then

(a) 若 Σ 可容许，则

$$\int_{\mathrm{Grp}(K)} \mathrm{inv}_X^{G,S,\Sigma} dM = \frac{|G|}{|G^{\mathrm{ab}}[|\mu(K)|]|} \sum_{n \leqslant X} a_n,$$

(b) 若 Σ 不可容许，则对所有 n 都有 $a_n = 0$，并且存在一个仅依赖于 K 的常数 $r > 1$，使得

$$\int_{\mathrm{Grp}(K)} \mathrm{inv}_X^{G,S,\Sigma} dM = O(r^{-X/\log X}).$$

引理 5.4 的一个重要推论是，$\mathrm{inv}_X^{G\,S\,\Sigma}{}_{,\ ,}$是 [Alb22，定义 1.2]意义下的一个 L^1-排序。因此，[Alb22，引理 3.1] 指出，$N(\mathscr{G}，\ \mathrm{inv}_X^{G\,S\,\Sigma})_{,\ ,}$关于 μ_K^{MB}几乎处处良定义且有限。

证明。按惯例取 $P_\infty \subseteq \{|p| \leqslant X\}$，并为简便起见设 $S(X) = S \cup \{|p| \leqslant X\}$。该矩等于一个有限和

$$\begin{aligned}\int_{\mathrm{Grp}(K)} \mathrm{inv}_X^{G,S,\Sigma}\, dM &= \sum_{\substack{(G,S(X),\phi)\\ |\mathrm{inv}(\phi)|\leqslant X\\ \phi\in\prod\Sigma_p}} |G^{\mathrm{ab}}[|\mu(K)|]|^{-1} |G|^{-|S(X)|+1} \\ &= \frac{|G|}{|G^{\mathrm{ab}}[|\mu(K)|]|} \sum_{\substack{(G,S(X),\phi)\\ |\mathrm{inv}(\phi)|\leqslant X\\ \phi\in\prod\Sigma_p}} \prod_{p\in S\cup\{|p|\leqslant X\}} |G|^{-1}\end{aligned}$$

对于任意映射 $f\colon I_p \to G$，设 $\Sigma_p(f) = \{\psi \in \Sigma_p\colon \psi|_{I_p} = f\}$。于是可得

$$\int_{\mathrm{Grp}(K)} \mathrm{inv}_X^{G,S,\Sigma}\, dM = \frac{|G|}{|G^{\mathrm{ab}}[|\mu(K)|]|} \sum_{\substack{\phi:*_p I_p\to G\\ |\mathrm{inv}(\phi)|\leqslant X\\ \phi\in\mathrm{res}_{*_p I_p}(\prod\Sigma_p)}} \prod_{p\in S(X)} \frac{|\Sigma_p(\phi_p|_{I_p})|}{|G|},$$

其中 $*_p I_p$ 是惯性群的前自由积。

首先，假设 Σ 可容许，以证明 (a) 部分。取足够大的 S，使其包含所有满足 $\Sigma_p \not\ni \mathrm{Hom}_{ur}(G_{K_p}, G)$ 的赋值；根据可容许性，这些赋值只有有限个。鉴于

对于任意 $p \notin S$，$|\Sigma_p(1)| = |G|$ 我们可以写成

$$\int_{\mathrm{Grp}(K)} \mathrm{inv}_X^{G,S,\Sigma}\, dM = \frac{|G|}{|G^{\mathrm{ab}}[|\mu(K)|]|} \sum_{\substack{\phi:*_p I_p \to G \\ |\mathrm{inv}(\phi)| \leqslant X \\ \phi \in \mathrm{res}_{*_p I_p}(\prod \Sigma_p)}} \prod_p \frac{|\Sigma_p(\phi_p|_{I_p})|}{|G|}.$$

我们考虑相应的狄利克雷级数

$$\frac{|G|}{|G^{\mathrm{ab}}[|\mu(K)|]|} \sum_{\substack{\phi:*_p I_p \to G \\ \phi \in \mathrm{res}_{*_p I_p}(\prod \Sigma_p)}} \prod_p \frac{|\Sigma_p(\phi_p|_{I_p})|}{|G|} \mathrm{inv}(\phi)^{-s}.$$

这是积性函数之和，因此可分解为

$$\begin{aligned} &\frac{|G|}{|G^{\mathrm{ab}}[|\mu(K)|]|} \prod_p \left(\frac{|\Sigma_p(1)|}{|G|} + \frac{1}{|G|} \sum_{\substack{f_p \in \mathrm{Hom}(I_p, G) \\ f_p(I_p) \neq 1}} |\Sigma_p(f)| |\mathrm{inv}_p(f_p)|^{-s} \right) \\ &= \frac{|G|}{|G^{\mathrm{ab}}[|\mu(K)|]|} \mathrm{MB}_{\mathrm{inv}}(K, \Sigma, s), \end{aligned}$$

注意，对除有限多个 p 之外的所有赋值，均有 $|\Sigma_p(1)|/|G| = 1$，从而确保该乘积在某个右半平面内收敛。比较系数即完成 (a) 部分的证明。

现在，假设 Σ 不可容许。此时有无穷多个常数项小于 1，因此显然 Malle-Bhargava 局部级数发散至 0。令A 为满足 $\Sigma_p \ni \mathrm{Hom}_{ur}(G_{K_p}、 G)$的无限素位集。则

$$\int_{\mathrm{Grp}(K)} \mathrm{inv}_X^{G,S,\Sigma}\, dM = \frac{|G|}{|G^{\mathrm{ab}}[|\mu(K)|]|} \sum_{\substack{\phi:*_p I_p \to G \\ |\mathrm{inv}(\phi)| \leqslant X}} \prod_{\substack{p \in A \\ \phi|_{I_p} = 1 \\ |p| \leqslant X}} \frac{|G| - 1}{|G|} \prod_{p \notin A \text{ or } \phi|_{I_p} \neq 1} \frac{|\Sigma_p(\phi|_{I_p})|}{|G|}.$$

每次至多有一个满足 $|p| \in [X/2, X]$ 的赋值在 ϕ 中分歧，因此由 K 上的素数定理给出的下界，存在仅依赖于 K 的正常数 a，使得

$$\int \mathrm{inv}_X^{G,S,\Sigma}\, dM \leqslant \frac{|G|}{|G^{\mathrm{ab}}[|\mu(K)|]|} \left(\frac{|G| - 1}{|G|} \right)^{\frac{aX}{\log X}} \sum_{\substack{\phi:*_p I_p \to G \\ |\mathrm{inv}(\phi)| \leqslant X}} \prod_{p \notin A \text{ or } \phi|_{I_p} \neq 1} \frac{|\Sigma_p(\phi|_{I_p})|}{|G|}.$$

剩余的和具有乘法性，其生成狄利克雷级数为

$$\prod_p \left(1 + \frac{1}{|G|} \sum_{\substack{f_p \in \mathrm{Hom}(I_p, G) \\ f_p(I_p) \neq 1}} |\Sigma_p(f)| |\mathrm{inv}_p(f_p)|^{-s} \right).$$

一个陶伯定理将此和的大小上界约束为 $O(X^{1+\epsilon})$（例如，参见 [Alb21，推论 2.4]）。因此

$$\int_{\mathrm{Grp}(K)} \mathrm{inv}_X^{G,S,\Sigma}\, dM \ll X^{1+\epsilon} \left(\frac{|G| - 1}{|G|} \right)^{\frac{aX}{\log X}}$$

$$\ll r^{-\frac{X}{\log X}}$$

对某个常数 $r > 1$。 □

5.4. 陶伯定理。引理 5.4 的适用范围极其广泛。再假设 inv 和 Σ 是 Frobenian，则可将陶伯定理应用于引理 5.4，以得到当 $X \to \infty$ 时 $\int \mathrm{inv}_X^{G\,S\,\Sigma} dM$,, 的渐近增长率。 [Alb21 第 2] 节对这一过程作了一般性处理。

为使引理 6.4 的证明尽可能易于理解，我们将讨论范围限定在以下情形:

推论 5.5。设 $\mathrm{inv} : \prod_p \mathrm{Hom}(G_{K_p}, G) \to I_K$ 是一个不变量，存在权函数 $w : G \to \mathbb{Z}_{\geqslant 0}$，使得

- $w(1) = 0$,• w 在 K-共轭类上为常数，且对于除有限多个赋值 p 以外的所有赋值，$\mathrm{inv}_p(\pi) = w(g)$ 当且仅当 $\pi(I_p) = \langle g \rangle$。

以及一个局部条件族，使得在 K 的除有限多个赋值外， $\Sigma_p = \mathrm{Hom}(G_{K_p}, G)$ 。若 (a_n) 是 Malle-Bhargava 局部级数 $\mathrm{MB}_{\mathrm{inv}}(K, \Sigma, s)$ 的狄利克雷系数，那么

$$\frac{|G|}{|G^{\mathrm{ab}}[|\mu(K)|]|} \sum_{n \leqslant X} a_n \sim c_{\mathrm{inv}}(K, \Sigma) X^{1/a_{\mathrm{inv}}(G)} (\log X)^{b_{\mathrm{inv}}(K,G)-1},$$

其中
(a) G 中元素的最小权重由下式给出

$$a_{\mathrm{inv}}(G) = \min_{g \in G \setminus \{1\}} w(g),$$

推广了 Malle 猜想 1.3 中的 $a(G)$ 。
(b) a 在 G 中以最小权重发生分歧的方式数的平均值由 b 给出 y

$$b_{\mathrm{inv}}(K, G) = \#\{K\text{-}conjugacy\ classes\ \kappa \subseteq G\ of\ minimal\ weight\ w(\kappa) = a_{\mathrm{inv}}(G)\},$$

推广了 Malle 猜想 1.3 中的 $b(K、G)$ 。
（c）首项系数由一个收敛的欧拉乘积给出，其中各因子考虑了单位元

$$c_{\mathrm{inv}}(K, \Sigma) = \frac{\left(\operatorname*{Res}_{s=1} \zeta_K(s)\right)^{b_{\mathrm{inv}}(K,G)-1}}{a_{\mathrm{inv}}(G)^{b_{\mathrm{inv}}(K,G)-1}(b_{\mathrm{inv}}(K,G)-1)!|G^{\mathrm{ab}}[|\mu(K)|]| \cdot |G|^{u_K}} \prod_{p|\infty} |\Sigma_p|$$
$$\cdot \prod_{p \nmid \infty} \left[(1-p^{-1})^{b_{\mathrm{inv}}(K,C)} \left(\frac{1}{|G|} \sum_{f \in \Sigma_p} p^{-\frac{\nu_p \mathrm{inv}(f)}{a_{\mathrm{inv}}(G)}} \right) \right],$$

其中 $u_K = \mathrm{rk}\mathcal{O}_K^\times = r_1(K) + r_2(K) - 1 = |P_\infty| - 1$。

该证明是陶伯定理 [Alb21、推论 2.4] 的推论。判别式是推论 5.5 所涵盖的一个此类不变量，其权函数由指标函数 $\mathrm{ind}(g) = n - \#\{\text{orbits of } g\}$ 给出。另一个重要例子是分歧素数乘积排序，它对应的权函数在所有非恒等元素上都等于 1。满足推论 5.5 条件的局部条件族 Σ，是指仅在有限多个赋值处施加限制的局部条件族。

6. Applying the Law of Large Numbers

本节证明定理 6.1，这是对定理 1.2 的略微推广，纳入了分歧素数乘积排序等其他排序，以及仅在有限多个赋值处受限的局部条件。

这将通过 [Alb22]的主要结果来完成。我们将证明 $\mathsf{Grp}(K)$ 中关于满态射乘积的一些事实，这些事实将使我们能够对$\mathrm{inv}_X^{G,S,\Sigma}$,的混合矩给出上界；这些混合矩出现在 [Alb22, 定理 1.4] 中，以便完成步骤 ()。结合 [Alb22, 定理 1.3],，这些结果将用于证明定理 6.1。

6.1. 按可容许不变量排序的计数函数。定理 1.2 的证明稍作工作即可推广为以下结果。由于在这种一般性下进行研究是自然的，我们将证明：

定理 6.1. 设 K 为一个数域， S 为有限个素位， G 为一个有限群，inv 为一个可容许不变量，且存在权函数 $w\colon G\to\mathbb{Z}_{\geqslant 0}$ 使得

- $w(1)=0$在 K-共轭类上为常数，并且对除有限多个赋值 p之外的所有• ，

$\mathrm{inv}_p(\pi)=w(g)$ 当且仅当 $\pi(I_p)=\langle g\rangle$,

以及一个局部条件族，使得对于除 K的有限多个赋值之外的所有赋值， $\Sigma_p=\mathsf{Hom}(G_{K_p},G)$ 。那么

（i）对于任意 $\epsilon>0$,

$$\frac{N(\mathscr{G},\mathrm{inv}_X^{G,S,\Sigma})}{X^{1/a_{\mathrm{inv}}(G)+\epsilon}}\xrightarrow{a.s.}0$$

当 $X\to\infty$时，其中“a.s.”表示“几乎必然收敛”。

（ii）若 $G=\langle g\in G:\ w(g)=a_{\mathrm{inv}}(G)\rangle$ 由最小权元素生成，则

$$\frac{N(\mathscr{G},\mathrm{inv}_X^{G,S,})}{c_{\mathrm{inv}}(K,\Sigma)X^{1/a_{\mathrm{inv}}(G)}(\log X)^{b_{\mathrm{inv}}(K,G)-1}}\xrightarrow{p.}1$$

当 $X\to\infty$时，其中“p.”表示“依概率收敛”。

(iii) 假设每个真正规子群 $N\trianglelefteq G$ 都满足以下条件之一：

(a) N 不包含最小权重的元素，或者

(b) $G\backslash N$ 至少包含两个最小权重的 K-共轭类。

Then

$$\frac{N(\mathscr{G},\mathrm{inv}_X^{G,S,\Sigma})}{c_{\mathrm{inv}}(K,\Sigma)X^{1/a_{\mathrm{inv}}(G)}(\log X)^{b_{\mathrm{inv}}(K,G)-1}}\xrightarrow{a.s.}1$$

如 $X\to\infty$，其中“a.s.”表示“几乎必然收敛”。

不变量 $a_{\mathrm{inv}}(G)$、 $b_{\mathrm{inv}}(K$、 $G)$ 和 $c_{\mathrm{inv}}(K$、 $\Sigma)$ 的定义与推论 5.5 中相同。

当然，判别式排序满足这些条件，因此显然定理 1.2 是定理 6.1 的特例。尤其值得关注的是分歧素数乘积排序，它同样满足这些条件。本节余下部分将着重证明定理 6.1。

6.2. $\mathbf{Grp}(K)$ 中的满态射积。 [Alb22] 的范畴论结果完全取决于是否存在被有限矩 M 保持的满态射积。对象 G_1 和 G_2 的满积在 [Alb22，定义 3.1] 中被定义为满足以下泛性质的对象 $G_1 \times_{\mathrm{epi}} G_2$

$$\begin{array}{ccc} H & \twoheadrightarrow & G_2 \\ \downarrow & \searrow & \uparrow \\ G_1 & \twoheadleftarrow & G_1 \times_{\mathrm{epi}} G_2 \end{array}$$

其中图中的所有态射（包括泛态射）都要求是满态射。满态射积的存在性是范畴的一种性质，并不取决于所考虑的排序，因此我们将单独证明 $\mathbf{Grp}(K)$ 中满态射积的分类。

范畴 $\mathbf{Grp}(K)$ 中，在相同赋值处具有局部数据的对象之间存在有限积，其形式为

$$(G_1, S, \phi_1) \times (G_2, S, \phi_2) = (G_1 \times G_2, S, \phi_1 \times \phi_2),$$

这继承自 Grp 上的积结构。若满积存在，则它必然通过泛态射与通常的积同构。

引理 6.2。 对象 $(G_1、 S、 \phi_1)$ 与 $(G_2、 S、 \phi_2)$ 在 $\mathbf{Grp}(K)$ 中有一个满积 *if*

$$G_1 \times G_2 = \langle (\phi_1 \times \phi_2)(G_{K_p}) : p \in S \rangle.$$

满态射积的存在与 $\#\mathbf{Epi}(\mathscr{G}, (G_1, S, \phi_1))$ 和 $\#\mathbf{Epi}(\mathscr{G}, (G_2, S, \phi_2))$的相关性密切相关。这些对象的构造方式使得元素 $\pi_i \in \mathbf{Epi}(\mathscr{G}, (G_i, S, \phi_i))$ 分别模拟具有伽罗瓦群 G_1 和 G_2 、且局部条件由 ϕ_1 和 ϕ_2给定的数域 L_1/K 和 L_2/K 。条件

$$G_1 \times G_2 = \langle (\phi_1 \times \phi_2)(G_{K_p}) : p \in S \rangle$$

可转化为 $L_1 \cap L_2 = K$，也就是说， L_1 和 L_2 的交为平凡交。根据切博塔廖夫密度定理，这等价于 $\mathbf{Gal}(L_1/K)$ 和 $\mathbf{Gal}(L_2/K)$中 Frobenius 的分布相互独立。由于 μ_K^{MB}和 $\mu_K^{\mathrm{MB}},\ s$ 是根据切博塔廖夫密度给出的弗罗贝尼乌斯元素分布构造的，直观而言，这些分布的独立性理应对应于某种适当意义下 π_1 和 π_2 的独立性。

作者在更一般的情形下证明了：当满积存在（且 M 尊重积结构）时，$\#\mathbf{Epi}(\mathscr{G}, (G_1, S, \phi_1))$ 与 $\#\mathbf{Epi}(\mathscr{G}, (G_2, S, \phi_2))$ 不相关，见 [Alb22，引理 5.2]。这里的证明更为直接，但作者提出这些结果的主要灵感恰恰来自这一对应关系。

证明。设有如下交换图

$$\begin{array}{ccc} (H, S', \psi) & \twoheadrightarrow & (G_2, S, \phi_2) \\ \downarrow & \overset{\pi}{\searrow} & \uparrow \\ (G_1, S, \phi_1) & \twoheadleftarrow & (G_1 \times G_2, S, \phi_1 \times \phi_2), \end{array}$$

其中 π 是泛态射，并假设 $\langle (\phi_1 \times \phi_2)(G_{K_p}) \rangle = G$。该 n

$$G_1 \times G_2 = \langle \pi\psi(G_{K_p}) \rangle \leqslant \mathrm{im}\ \pi \leqslant G_1 \times G_2,$$

这意味着 π 作为群同态是满射，因此是一个满态射。这与 $(H、\ S'、\ \psi)$ 的选择无关，因此证明了满积的存在性。□

如 [Alb22 定理 1.4 和 1.5], 所述，证明计数函数的大数定律，只取决于那些不存在满积的元素元组。通过证明这些对象在该排序下具有零密度， [Alb22 定理 1.3] 将以概率 1 给出渐近增长率。我们可以利用引理 6.2 来描述这些对象。

与 [Alb22 定理 1.4], 一样，我们定义 $E(2,M)$ 为对象的集合 $((G_1,S_1,\phi_1),(G_2,S_2,\phi_2)) \in \mathbf{Grp}(K)^2$ ，其中

- The epi-product $(G_1,S_1,\phi_1)\times_{\mathrm{epi}}(G_2,S_2,\phi_2)$ exists, and
- $M_{(G_1,S_1,\phi_1)\times_{\mathrm{epi}}(G_2,S_2,\phi_2)} = M_{(G_1,S_1,\phi_1)}M_{(G_2,S_2,\phi_2)}$.

引理 6.3。设 M 为 $\mathbf{Grp}(K)/\cong$ 上由 $M(G,S,\phi)=M_{(G,\ S,\ \phi)}=|G^{\mathrm{ab}}[|\mu(K)|]|^{-1}|G|^{-|S\cup S_\infty|+1}$ 给出的离散测度，并设

$$((G_1,S,\phi_1),(G_2,S,\phi_2))\in \mathrm{Grp}(K)^2\backslash E(2,M)$$

其中，每个坐标上的素位集 S 都相同。于是，群

$$D=\langle(\phi_{1,p}\times\phi_{2,p})(G_{K_p}) : p\in S\rangle$$

是一个 p roper 子群 $G_1\times G_2$ ，且以下条件至少有一个成立：

(a) 对至少一个 $i\in\{1,\ \rho_i(D)\neq G_i\ 2\}$，其中 $\rho_i:\ G_1\times G_2\to G_i$ 是到 i^{th} 坐标的投影；或者 (b) 对所有 $j\in\{1,\ \iota_j(G_j)\nsubseteq D\ 2\}$，其中 $\iota_j:\ G_j\to G_1\times G_2$ 是到 j^{th} 坐标的包含态射。

证明。我们用逆否命题证明此结果，因此假设对每个 $m\in\{1,\ \rho_m(D)=G_m\ 2\}$，且存在一个坐标 j，使得 $\iota_j(G_j)\subseteq D$。不失一般性，假设 $j=1$。那么 $G_1\times 1\subseteq D$ ，而 $\rho_2(D)=G_2$ 蕴含 $G_1\times G_2\subseteq D$。根据引理 6.2，这意味着 $(G_1、\ S、\ \phi_1)$ 和 $(G_2、\ S、\ \phi_2)$ 具有一个满积，而该满积必然同构于直积 $(G_1、\ S、\ \phi_1)\times(G_2、\ S、\ \phi_2)$。

此外，

$$\begin{aligned}M_{(G_1,S,\phi_1)\times(G_2,S,\phi_2)} &= |(G_1\times G_2)^{\mathrm{ab}}[|\mu(K)|]|^{-1}|G_1\times G_2|^{-|S\cup P_\infty|+1}\\ &= |G_1^{\mathrm{ab}}[|\mu(K)|]|^{-1}|G_1|^{-|S\cup P_\infty|+1}|G_2^{\mathrm{ab}}[|\mu(K)|]|^{-1}|G_2|^{-|S\cup P_\infty|+1}\\ &= M_{(G_1,S,\phi_1)}M_{(G_2,S,\phi_2)}.\end{aligned}$$

根据定义，这意味着

$$((G_1,S,\phi_1),(G_2,S,\phi_2))\in E(2,M).$$

因此，我们通过逆否命题证明了该结果。 □

6.3. 混合矩的界。我们将借助[Alb22 的定理 1.3 和 1.4]来证明定理 6.1。为应用这些结果，需要对 $\mathrm{inv}_X^{G\ S\ \Sigma}$ „的混合矩给出界。给定一个定义在C 上、具有有限矩 M_G的原对象范畴上的概率测度 μ ，混合矩 $M^{(j)}:\ C^j/\cong\to[0,\infty]$ 定义为

$$M^{(j)}_{(G_1,G_2,\ldots,G_j)}=\int\left(\prod_{i=1}^{j}\#\mathrm{Epi}(\mathscr{G},G_i)\right)\ d\mu(\mathscr{G}).$$

混合矩一般不一定有限，但我们将证明，在我们关注的情形下，它们是有限的。

引理 6.4。设 $M_{(G,\ S,\ \phi)} = |G^{\mathrm{ab}}[|\mu(K)|]| \cdot |G|^{-|S\cup P_\infty|+1}$ 为 μ_K^{MB}的有限矩。固定与定理 6.1 中相同的K、 G、 S、inv 和 Σ。那么

(a) 对每个正整数 k 以及每个 $j \in \{1、2、...、2k\}$,

$$\int_{\mathrm{Grp}(K)^{2k}} \mathrm{inv}_X^{G,S,\Sigma}\ dM^{(j)}(dM)^{2k-j} \ll X^{\frac{2k}{a_{\mathrm{inv}}(G)}+\epsilon}.$$

(b) 对每个整数 $j \in \{1,\ 2\}$,

$$\int_{\mathrm{Grp}(K)^2\setminus E(2,M)} \mathrm{inv}_X^{G,S,\Sigma}\ dM^{(j)}(dM)^{2-j} \ll X^{\frac{2}{a_{\mathrm{inv}}(G)}}(\log X)^{2b_{\mathrm{inv}}(K,G)-2\beta-1},$$

where

$$\beta = \min\left\{ \#\left\{ \begin{array}{c} K\text{-conjugacy classes } \kappa \subseteq G\setminus N \\ \text{with } w(\kappa) = a_{\mathrm{inv}}(G) \end{array} \right\} \middle| \begin{array}{c} N \trianglelefteq G \text{ a proper normal subgroup} \\ \text{with } N \text{ containing at least one} \\ \text{minimal weight element.} \end{array} \right\}.$$

此外，若 $G = \langle g \in G :\ w(g) = a_{\mathrm{inv}}(G)\rangle$ 由最小权元素生成，则$\beta \geqslant 1$。

关于 $2k^{\mathrm{th}}$ 混合矩也有类似于引理 6.4(b) 的结果，与 [Alb22 定理 1.5],一致，但证明定理 6.1 并不需要这些结果。

引理 6.4 是本文中技术性最强的结果，但归根结底是引理 6.3 的推论。主要方法是利用 [Alb22，引理 5.3]，将混合矩上界估计为一阶矩之和。[Alb22，引理 5.3] 的内容如下：设 C 是一个范畴，其中每个态射都能唯一地（在同构意义下）分解为一个满态射与一个单态射的复合。若 G_1、...、G_j是 C中的对象，且 $G_1 \times \cdots \times G_j$ 存在并且只有有限多个子对象，则

$$M^{(j)}_{(G_1,G_2,\ldots,G_j)} = \sum_{\substack{\iota: H\hookrightarrow G_1\times\cdots\times G_j \\ \rho_i\iota \text{ is an eipmorphism}}} M_H,$$

其中求和遍及所有满足以下条件的子对象 H：每个投影映射限制在 H上后都是一个满态射。特别地，这意味着 $M^{(j)}_{(G_1,\ G_2,\ \ldots,\ G_j)} < \infty$。

范畴 $\mathsf{Grp}(K)$中的许多对象都具有这些性质。

- 具有相同素位集上局部条件的元素之间的乘积为

$$(G, S, \phi) \times (H, S, \varphi) = (G \times H, S, \phi \times \varphi).$$

当素位集不同时，乘积未必存在，但这对我们的目的而言已经足够。

- 态射 $\pi\colon (G, S, \phi) \to (H, S', \varphi)$ 分解为

$$(G, S, \phi) \twoheadrightarrow (\mathrm{im}\ (\pi), S', \varphi) \hookrightarrow (H, S', \varphi),$$

这与群的态射分解方式相同。

利用这一结果，我们将用不同可容许不变量的积分来界定上文引理 6.4 中的量。随后，利用引理 5.4 和推论 5.5 得到渐近界。为了证明 (b) 部分中更强的界，我们将说明，避开 $E(2, M)$ 中的对象可以转化为避开某些分歧行为。

引理 6.4(a) 的证明。首先，我们注意到

$$\int_{\mathrm{Grp}(K)^{2k}} \mathrm{inv}_X^{G,S,\Sigma}\, dM^{(j)}(dM)^{2k-j} = \left(\int_{\mathrm{Grp}(K)^j} \mathrm{inv}_X^{G,S,\Sigma}\, dM^{(j)}\right)\left(\int_{\mathrm{Grp}(K)} \mathrm{inv}_X^{G,S,\Sigma}\, dM\right)^{2k-j}.$$

引理 5.4 和推论 5.5 的界

$$\int_{\mathrm{Grp}(K)} \mathrm{inv}_X^{G,S,\Sigma}\, dM \ll X^{\frac{1}{a_{\mathrm{inv}(C)}}+\epsilon},$$

因此，只需单独考虑 $M^{(j)}$ 因子。鉴于 $\mathbf{inv}_X^{G\,S\,\Sigma}$ ，，仅在形如 $(G、\ S(X)、\ \phi)$ 的对象上有支撑，其中 $S(X) = S \cup \{|p| \leqslant X\}$，我们可以将积分写为

$$\int_{\mathrm{Grp}(K)^j} \mathrm{inv}_X^{G,S,\Sigma}\, dM^{(j)} = \sum_{(G,S(X),\phi_i)\in \mathrm{Grp}(K)^j} \left(\prod_{i=1}^{j} \mathrm{inv}_X^{G,S,\Sigma}(G,S(X),\phi_i)\right) M^{(j)}_{((G,S(X),\phi_1),\ldots,(G,S(X),\phi_j))}.$$

设 $\varphi = \phi_1 \times \cdots \times \phi_j$，使得 $\rho_i\varphi = \phi_i$。然后我们使用 Alb22 的引理 5.3]，将混合矩 $M^{(j)}$ 界定为

$$\begin{aligned} M^{(j)}_{((G,S(X),\rho_1\varphi),\ldots,(G,S(X),\rho_j\varphi))} &= \sum_{\substack{(H,S(X),\psi)\leqslant(G^j,S(X),\varphi)\\ \forall i,\rho_i(H)=G}} M_{(H,S(X),\psi)} \\ &= \sum_{\substack{H\leqslant G^j\\ \mathrm{im}\ (\varphi)\leqslant H\\ \forall i,\rho_i(H)=G}} M_{(H,S(X),\varphi)} \end{aligned}$$

对于每个满足 $\rho_i(H) = G$ 的 $H \leqslant G^j$，以及所有 $i = 1$、2、.....、j，直积的泛性质给出了对象 $(G、\ S(X)、\ \phi_i) \in$ 与 $\mathbf{Grp}\,(K)^j$ 之间的双射；这些对象满足 $\mathrm{im}\ \left(\prod_{i=1}^{j}\phi_i\right) \leqslant H$，并且双射对应于对象集合 $(H、\ S(X)、\ \varphi) \in$ 与 $\mathbf{Grp}\,(K)$。因此，我们可以将对 $H \leqslant G^j$ 的求和移至外层，从而得到

$$\begin{aligned} &\sum_{\substack{H\leqslant G^j\\ \forall i,\rho_i(H)=G}} \sum_{(H,S(X),\varphi)\in\mathrm{Grp}(K)} \left(\prod_{i=1}^{j} \mathrm{inv}_X^{G,S,\Sigma}(G,S(X),\rho_i\varphi)\right) M_{(H,S(X),\varphi)} \\ &= \sum_{\substack{H\leqslant G^j\\ \forall i,\rho_i(H)=G}} \sum_{\substack{\varphi:F_{K,S(X)}\to H\\ \forall i,\ \rho_i\varphi\in\Sigma\\ \forall i,\ |\mathrm{inv}(\rho_i\varphi)|\leqslant X}} M_{(H,S(X),\varphi)}. \end{aligned}$$

鉴于对于每个有限处 p 都有 $|H|$ 个可能的非分歧映射 $\phi_p\colon\ G_{K_p} \to H$，我们可以针对更大的赋值集重新表述有限矩

$$\begin{aligned} M_{(H,S(X),\varphi)} &= |H^{\mathrm{ab}}[|\mu(K)|]|^{-1}|H|^{-|S(X)|+1} \\ &= |H|^{|S(X^j)|-|S(X)|}|H^{\mathrm{ab}}[|\mu(K)|]|^{-1}|H|^{-|S(X^j)|+1} \\ &= \sum_{\substack{\psi:F_{K,S(X^j)}\to H\\ \psi\ \text{unram at}\ p\notin S(X)\\ \psi|_{S(X)}=\varphi}} M_{(H,S(X^j),\psi)}. \end{aligned}$$

将其代入我们的积分中，我们可以得到界

$$\begin{aligned}
&\sum_{\substack{H\leqslant G^j\\ \forall i,\rho_i(H)=G}} \sum_{\substack{\varphi:F_{K,S(X)}\to H\\ \forall i,\ \rho_i\varphi\in\Sigma\\ \forall i,\ |\mathrm{inv}(\rho_i\varphi)|\leqslant X}} \sum_{\substack{\psi:F_{K,S(X^j)}\to H\\ \psi \text{ unram at } p\notin S(X)\\ \psi|_{S(X)}=\varphi}} M_{(H,S(X^j),\psi)}\\
&= \sum_{\substack{H\leqslant G^j\\ \forall i,\rho_i(H)=G}} \sum_{\substack{\psi:F_{K,S(X^j)}\to H\\ \forall i,\ \rho_i\psi\in\Sigma\\ \forall i,\ |\mathrm{inv}(\rho_i\psi)|\leqslant X}} M_{(H,S(X^j),\psi)}\\
&\leqslant \sum_{\substack{H\leqslant G^j\\ \forall i,\rho_i(H)=G}} \sum_{\substack{\psi:F_{K,S(X^j)}\to H\\ \forall i,\ \rho_i\psi\in\Sigma\\ \prod_{i=1}^j|\mathrm{inv}(\rho_i\psi)|\leqslant X^j}} M_{(H,S(X^j),\psi)}.
\end{aligned}$$

对于每个 $H\leqslant G^j$，定义不变量 $\mathrm{inv}_H\colon\prod_p \mathrm{Hom}(G_{K_p},H)\to I_K\,\mathbf{b}$

$$\mathrm{inv}_H(\pi)=\prod_{i=1}^{j}\mathrm{inv}(\rho_i(\pi)).$$

这是一个权函数为 $w_H(g_1,\ldots,g_j)=w(g_1)+\cdots+w(g_j)$ 的可容许不变量，并继承了 inv 的必要性质。此外，我们还为由 $\rho_i(\Sigma_p^j)=\Sigma_p$ 确定的局部条件族 $\Sigma_p^j\subseteq\mathrm{Hom}(G_{K_p},H)$ 定义 $\Sigma^j=(\Sigma_p^j)$，其中投影到每个坐标 $i=1,\ldots,j$。于是，该和可化简为

$$\begin{aligned}
&\sum_{\substack{H\leqslant G^j\\ \forall i,\rho_i(H)=G}} \sum_{(H,S(X^j),\psi)\in\mathrm{Grp}(K)} (\mathrm{inv}_H)_{X^j}^{H,S,\Sigma^j}(H,S(X^j),\psi)M_{(H,S(X^j),\psi)}\\
&= \sum_{\substack{H\leqslant G^j\\ \forall i,\rho_i(H)=G}} \int_{\mathrm{Grp}(K)} (\mathrm{inv}_H)_{X^j}^{H,S,\Sigma^j}\,dM.
\end{aligned}$$

由引理 5.4 和推论 5.5 可得结论，注意到最小权重必然满足

$$a_{\mathrm{inv}_H}(H)\geqslant a_{\mathrm{inv}}(G)$$

并且在推论 5.5 的情形下，$C=G$ 对于族 Σ^j。因此

$$\begin{aligned}
\int_{\mathrm{Grp}(K)^j}\mathrm{inv}_X^{G,S,\Sigma^j}\,dM^{(j)} &\leqslant \sum_{\substack{H\leqslant G^j\\ \forall i,\rho_i(H)=G}} \int_{\mathrm{Grp}(K)} (\mathrm{inv}_H)_{X^j}^{H,S,\Sigma^j}\,dM\\
&\ll \sum_{\substack{H\leqslant G^j\\ \forall i,\rho_i(H)=G}} (X^j)^{\frac{1}{a_{\mathrm{inv}}(G)}+\epsilon}\\
&\ll X^{\frac{j}{a_{\mathrm{inv}}(G)}+\epsilon}.
\end{aligned}$$

□

引理 6.4(b) 的要求更严格，因此我们不能像 (a) 部分那样采用宽松的界。相反，引理 6.3 将在控制局部数据中可能出现的最小指标元素数量方面发挥重要作用。

引理 6.4(b) 的证明。根据引理 6.3，我们知道 $((G_1,S,\phi_1),(G_2,S,\phi_2))\in \mathbf{Grp}(K)^2\backslash E(2,M)$ 意味着该群

$$D=\langle(\phi_1\times\phi_2)(G_{K_p}):p\in S\rangle$$

要么有一个 $\rho_i(D)\neq G_i$，要么对每个 i 都有 $\iota_i(G_i)\not\subseteq D$。我们将利用这一点改进 (a) 部分的证明，以界定积分。

首先假设 $j=2$。与 (a) 部分类似，我们计算

$$\begin{aligned}\int_{\mathrm{Grp}(K)^2\backslash E(2,M)}\mathrm{inv}_X^{G,S,\Sigma}\,dM^{(2)}&\leqslant\sum_{\substack{H\leqslant G^2\\ \forall i,\ \rho_i(H)=G}}\sum_{D\leqslant G^2}^{*}\sum_{\substack{(H,S(X),\varphi)\in\mathrm{Grp}(K)\\ \mathrm{im}\,(\varphi)\leqslant D}}\prod_{i=1}^{2}\mathrm{inv}_X^{G,S,\Sigma}(G,S(X),\rho_i\varphi)M_{(H,S(X),\varphi)}\\&=\sum_{\substack{H\leqslant G^2\\ \forall i,\ \rho_i(H)=G}}\sum_{D\leqslant G^2}^{*}\sum_{\substack{\varphi:F_{K,S(X)}\to H\\ \mathrm{im}\,(\varphi)\leqslant D\\ \varphi\in\Sigma\\ |\mathrm{inv}(\rho_i\varphi)|\leqslant X}}M_{(H,S(X),\rho_i\varphi)},\end{aligned}$$

中间求和中的 $*$ 表示求和范围是引理 6.3 所描述的那些 D。我们通过以下各项事实来界定它：

- 我们知道

$$M_{(H,S(X),\varphi)}M_{(G,S(X),\rho_2\varphi)}=\sum_{\substack{\psi:F_{K,S(X^2)}\to H\\ \psi\text{ unram at }p\notin S(X)\\ \psi|_{S(X)}=\varphi}}M_{(H,S(X^2),\psi)}$$

  与 (a) 部分中使用的等式类似。
- 令 $\Sigma_{H,\ D}=(\Sigma_{H,\ D,\ p})$ 为局部条件族 $\Sigma_{H,\ D,\ p}\subseteq\mathrm{Hom}(G_{K_p},H)$ 使得

$$\Sigma_{H,D,p}=\{f\in\Sigma_p^2\cap\mathrm{Hom}(G_{K_p},H):f(I_p)\leqslant D\}.$$

- 不变量 $\mathrm{inv}_H:\prod_p\mathrm{Hom}(G_{K_p},H)\to I_K$ 按照 (a) 部分中的定义为

$$\mathrm{inv}_H(\pi)=\mathrm{inv}(\rho_1\pi)\mathrm{inv}(\rho_2\pi)$$

  必然是可容许的，因为它继承了 inv 的这一性质，其权函数为$w_H(g_1,g_2)=w(g_1)+w(g_2)$。

按照 (a) 部分将这些结果结合起来，可得界

$$\begin{aligned}\int_{\mathrm{Grp}(K)^2\backslash E(2,M)}\mathrm{inv}_X^{G,S,\Sigma}\,(dM)^2&\leqslant\sum_{\substack{H\leqslant G^2\\ \forall i,\ \rho_i(H)=G}}\sum_{D\leqslant G^2}^{*}\sum_{\substack{\psi:F_{K,S(X^2)}\to H\\ \psi\in\Sigma_{H,D}\\ |\mathrm{inv}_H(\psi)|\leqslant X^2}}M_{(H,S(X^2),\psi)}\\&=\sum_{\substack{H\leqslant G^2\\ \forall i,\ \rho_i(H)=G}}\sum_{D\leqslant G^2}^{*}\sum_{(H,S(X^2),\psi)\in\mathrm{Grp}(K)}(\mathrm{inv}_H)_{X^2}^{H,S,\Sigma_{H,D}}(H,S(X^2),\psi)M_{(H,S(X^2),\psi)}\\&=\sum_{\substack{H\leqslant G^2\\ \forall i,\ \rho_i(H)=G}}\sum_{D\leqslant G^2}^{*}\int_{\mathrm{Grp}(K)}(\mathrm{inv}_H)_{X^2}^{H,S,\Sigma_{H,D}}\,dM.\end{aligned}$$

我们分别考虑各个加数。首先，假设 $H\not\subseteq D$。那么 $\Sigma_{H,\ D}$ 必然是不可容许的，因为 $\Sigma_{H,\ D,\ p}\subseteq\mathrm{Hom}(G_{K_p},D)$ 而 $\mathrm{Hom}_{\mathrm{ur}}(G_{K_p},H)\not\subseteq\mathrm{Hom}(G_{K_p},D)$ 对每个

赋值 p。因此，引理 5.4(b) 表明，每个这样的加数都由一个衰减函数所界

$$\int_{\mathrm{Grp}(K)} (\mathrm{inv}_H)_{X^2}^{H,S,\Sigma_{H,D}}\, dM = O\left(r^{-X/\log X}\right) = o(1).$$

现在假设 $H \subseteq D$。那么 $\Sigma_{H,\ D,\ p} = \mathrm{Hom}(G_{K_p},\ H)$ 除有限多个赋值 p 外，不施加任何局部条件。为表明这一点，我们记为 $\mathrm{inv}_{H,\ S,\ \Sigma_{H,\ X^2}\ \ \ D} = \mathrm{inv}_{X^2}^{H\ S}$。现在应用引理 5.4 和推论 5.5。与 (a) 部分一样，$a_{\mathrm{inv}_H}(H) \geqslant a_{\mathrm{inv}}(G)$ 由构造可知。若此不等式为严格不等式，则结论成立。

若 $a_{\mathrm{inv}_H}(H) = a_{\mathrm{inv}}(G)$，我们需要控制 $\log X$ 的幂。$H \leqslant G^2$ 中仅有的非恒等映射元素，其最小权重与 G 的最小权重相同，且形式为 $(g、\ 1)$ 或 $(1，$ 其中 $g)$ 对于 $w(g) = a_{\mathrm{inv}}(G)$ 成立，因为权函数由 $w_H(g_1、\ g_2) = w(g_1) + w(g_2)$ 给出。

令 $H_1 \leqslant G$ 为满足 $H_1 \times 1 = \ker \rho_2|_H = \iota_1(G) \cap H$ 的子群，对$H_2 \leqslant G$也作类似定义。这些群由核给出，意味着 $H_i \trianglelefteqslant G$。由引理 6.3 以及包含关系 $H \subseteq D$，可得 $H_i \subseteq \iota_i^{-1}(D) \neq G$，因此它们是真正规子群。接下来我们计算

$$\begin{aligned} b_{\mathrm{inv}_H}(K,H) &= \#\{K\text{-conjugacy classes in } H \text{ of minimal weight}\} \\ &= \sum_{i=1}^{2} \#\{K\text{-conjugacy classes in } H_i \text{ of minimal weight}\} \\ &\leqslant 2(b_{\mathrm{inv}}(K,G) - \beta) \\ &= 2b_{\mathrm{inv}}(K,G) - 2\beta. \end{aligned}$$

于是，$j = 2$ 的情形 (b) 随之成立。$j = 1$ 的情形采用相同的论证，其中界中只出现求和项 $H = G^2$。

若假设 $G = \langle g \in G : w(g) = a_{\mathrm{inv}}(G)\rangle$，则任意真正规子群 $N \trianglelefteqslant G$ 都不可能包含所有最小权重元素。因此，$G\backslash N$ 至少包含一个最小权重元素。此外，由 N 是正规子群这一事实可知，N 和 $G\backslash N$ 在共轭及可逆幂运算下均封闭，因此都是 K-共轭类的并集。于是，$G\backslash N$ 中至少存在一个最小权重的 K-共轭类。由于 N 是任意的，这意味着 $\beta \geqslant 1$。
□

6.4. 证明计数结果。有了这一结果，我们现在可以证明定理 6.1（定理 1.2 是其特例）。

定理 6.1 的证明。定理 6.1(i) 的证明由 [Alb22，推论 1.4] 和引理 6.4(a) 得出。[Alb22，推论 1.4] 指出

$$N(\mathscr{G}, \mathrm{inv}_X^{G,S,\Sigma}) = o\left(\max_{0\leqslant j\leqslant k} X^{\frac{1+\epsilon}{2k}} \left(\int_{\mathrm{Grp}(K)^{2k}} \mathrm{inv}_X^{G,S,\Sigma}\, dM^{(j)} (dM)^{2k-j}\right)^{1/2k}\right).$$

几乎处处。应用引理 6.4(a) 的界，这意味着

$$N(\mathscr{G}, \mathrm{inv}_X^{G,S,\Sigma}) = o\left(\max_{0\leqslant j\leqslant k} X^{\frac{1+\epsilon}{2k} + \frac{1}{a_{\mathrm{inv}}(G)} + \epsilon}\right)$$

几乎处处 y. 将 ϵ 替换为 $\epsilon/2$，并取充分大的 k，即可完成证明 .

我们分别结合 [Alb22, 定理 1.4]. [，利用 [Alb22, 定理 1.3(ii,iii)] 证明定理 6.1(ii,iii)。4] Alb22, 定理 1.4] 指出

$$\int_{\mathrm{proGrp}(K)}\left|N(\mathscr{G},\mathrm{inv}_X^{G,S,\Sigma})-\int_{\mathrm{Grp}(K)}\mathrm{inv}_X^{G,S,\Sigma}\,dM\right|^2 d\mu_K^{\mathrm{MB}}(\mathscr{G})\ll\max_{j\in\{1,2\}}\int_{\mathrm{Grp}(K)^2\backslash E(2,M)}\mathrm{inv}_X^{G,S,\Sigma}\,dM^{(j)}(dM)^{2-j},$$

根据引理 6.4，其上界为

$$X^{1/a_{\mathrm{inv}}(G)}(\log X)^{2b_{\mathrm{inv}}(K,G)-2\beta-1}.$$

如果 G 由最小权重元素生成，我们必然有 $\beta\geqslant 1$。

因此，根据推论 5.5

$$\int_{\mathrm{proGrp}(K)}\left|N(\mathscr{G},\mathrm{inv}_X^{G,S,\Sigma})-\int_{\mathrm{Grp}(K)}\mathrm{inv}_X^{G,S,\Sigma}\,dM\right|^2 d\mu_K^{\mathrm{MB}}(\mathscr{G})\ll\frac{1}{(\log X)^{2\beta-1}}\left(\int_{\mathrm{Grp}(K)}\mathrm{inv}_X^{G,S,\Sigma}\,dM\right)^2.$$

由 $\beta\geqslant 1$ 可得 $\frac{1}{(\log X)^{2\beta-1}}\leqslant\frac{1}{\log X}\to 0$。因此，[Alb22 定理 1.3(ii)] 直接证明了定理 6.1(ii)。

如果所有真正规子群 $N\trianglelefteqslant G$ 要么不含最小权重元素，要么与至少两个 K-共轭类的最小权重元素的交为平凡交，我们必然有 $\beta\geqslant 2$。因此

$$\int_{\mathrm{proGrp}(K)}\left|N(\mathscr{G},\mathrm{inv}_X^{G,S,\Sigma})-\int_{\mathrm{Grp}(K)}\mathrm{inv}_X^{G,S,\Sigma}\,dM\right|^2 d\mu_K^{\mathrm{MB}}(\mathscr{G})\ll\frac{1}{(\log X)^3}\left(\int_{\mathrm{Grp}(K)}\mathrm{inv}_X^{G,S,\Sigma}\,dM\right)^2$$
$$\ll\frac{\left(\int_{\mathrm{Grp}(K)}\mathrm{inv}_X^{G,S,\Sigma}\,dM\right)^2}{\left(\log\int_{\mathrm{Grp}(K)}\mathrm{inv}_X^{G,S,\Sigma}\,dM\right)^3}.$$

根据引理 5.4 和推论 5.5 可得 $\int_{\mathrm{Grp}(K)}\mathrm{inv}_X^{G,S,\Sigma}\,dM\ll X^{1/a_{\mathrm{inv}}(G)+\epsilon}\ll X^{2-}$，因此最后一个不等式成立。函数 $\psi(X)=(\log X)^3$ 是单调不减的，并满足 $\sum_n\frac{1}{(\log n)^3}<\infty$，因此 [Alb22, Theorem 1.3(iii)] 直接证明了定理 6.1(iii)。□

7. Making predictions for number field counting

我们的结果表明，只要我们预期绝对伽罗瓦群G_K 在带局部数据的群中是“典型的”，作者在 [Alb22, Heuristic 1.7] 中提出的广义计数启发式就适用于 Malle 猜想。当然，众所周知，按原表述的 Malle 猜想是错误的——Kl¨uners 在 $C_3\wr C_2\subseteq S_6$给出了第一个反例，其中 Malle 预测的 b-不变量过小 [Kl¨u05a]。Kl¨uners 的反例表明，对于按照 μ_K^{MB}分布的带局部数据的群，$G_{\mathbb{Q}}$ 存在某种非典型行为；具体而言，$\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$ 是 $G_{\mathbb{Q}}$的一个商。

引理 5.4 可以理解为将 μ_K^{MB}视为 Malle-Bhargava 启发式 [Bha07,Woo19] 的随机群版本。Malle-Bhargava 启发式指出，Malle 计数函数的增长率可以从 Malle-Bhargava 局部级数中读出

$$\frac{|G|}{|G^{\mathrm{ab}}[|\mu(K)|]|}\prod_p\left(\frac{1}{|G|}\sum_{f\in\mathrm{Hom}(G_{K_p},G)}p^{-(\nu_p\mathrm{disc}(f))s}\right),$$

前面可能还带有某个常数。$c(K,G)$ 的收敛欧拉乘积表示可以立即看出源自这个级数。Malle-Bhargava

原理与 Malle 猜想一样，当然在某些情况下是错误的。类比而言，这意味着我们预期带局部数据的随机群 μ_K^{MB}会遗漏某些行为，并在与 Malle-Bhargava 原理类似的情形下给出错误预测（例如 Kl¨uners 的反例）。

编纂一份绝对伽罗瓦群已知的“非典型”行为清单将很有用，也就是那些已知可能破坏 Malle-Bhargava 原理的行为。据作者所知，以下清单列出了目前所有已知的、与 Malle-Bhargava 原理有关的问题来源（包括首项常数的取值）：

（1）当 G 不是由最小指标元素生成时的情形。定理 1.2 甚至不涵盖这类情形，而且这是有充分理由的——这类排序往往会加剧非典型行为。在 $D_4 \subseteq S_4$ 的 [CYDO02] 和 Heis $_3 \subseteq S_9$ 的 [FK21] 中便可看到这一点：其首项常数由收敛的欧拉乘积构成的显式无穷和给出，而非仅由一个欧拉乘积给出。事实上，即使对于阿贝尔群，首项常数也可能是有限个收敛的欧拉乘积之和 [Wri89, Woo09]。

(2) 性质 E，正如 [LWZB19], 中所称：对于 G_K ，中心嵌入问题可解，当且仅当相应的局部嵌入问题可解。对于 μ_K^{MB}，这通常并不成立，尽管已知这种行为对于数域计数十分重要。在类群统计以及非分歧对象的相关统计中，该性质与 Schur 乘子中某些 $|\mu(K)|$- 挠元的大小有关，并可能导致前面的常数不同。一些作者通过考虑相应 Schur 乘子为平凡的群来规避这一问题 [LWZB19, BBH17], ；另一些作者则在不同形式下计算了 Schur 乘子预期产生的贡献 [RS14,Woo19,SW23] 。

(3) 获得额外的单位根。Kl¨uners 的反例表明， G-扩张 L/K 中， $\mu(L) \neq \mu(K)$ 的数量可以超出 Malle 预测的增长率而累积 [Kl¨u05a]。T¨urkelli[T¨ur15、Alb21], 对 Malle 的预测进行了修正，以反映这种行为，但这些修正并未明确处理首项常数。

(4) Grunwald 问题。并非所有局部条件都能在数域的全局扩张中实现。Wang 在修正 Grunwald-Wang 定理时首次注意到了这一点 [Wan50]：不存在在 $\mathbb{Q}$ 2 处完全惰性的 C_8-扩张。缺失的局部条件应当导致首项欧拉乘积中缺少相应项，这一点在阿贝尔群的情形中已有体现，见 [Woo09]。目前，确定 Grunwald 问题何时有正解仍是一个开放问题，参见 [Neu73,Har07,DLAN17,Mot18]。

(5) 公平与不公平计数函数。即使能够避免 Grunwald-Wang 反例，计数阿贝尔扩张时的首项常数也未必与定理 1.2 中的收敛的欧拉乘积一致。Wood 的一项结果表明，如果按照所谓的公平计数函数对扩张排序，这些首项常数便会一致 [Woo09] （ Wood 的主要结果远不止于此，但我们在此仅关注首项常数）。

Wood 为阿贝尔扩张一般性地定义了公平计数函数这一概念，但如何将这一定义推广到非阿贝尔群，还不明朗。作者个人认为，这是计数非阿贝尔扩张时最令人费解的障碍。阿贝尔群上的公平计数函数的典型例子是分歧素数乘积排序。人们预期这种排序

对非阿贝尔群也应当是公平的，但据作者所知，目前还没有人提出在此背景下对“公平”的一般性定义。

本文不试图解决这些问题。若能彻底解决其中任何一种情况，并将其纳入考量，都将是数域计数研究中的巨大进展，也将成为作者持续研究的课题。我们认为，克服这些障碍的一大难点在于它们彼此交织。在某种程度上，每种情况都会受到单位根存在与否的影响。有限群 G 往往会同时呈现其中几种情况，因此很难将它们逐一单独研究。

相反，我们简要讨论 μ_K^{MB}与这些情况之间的相互作用。这证实了数域领域长期以来的看法：对于分歧素数乘积排序，Malle-Bhargava 原理“在单位根之外基本正确”。

7.1. 常数项与已知情形一致。定理 6.1 与 Wood [Woo09] 证明的计数结果一致：对于按公平计数函数排序的阿贝尔扩张，只要伽罗瓦群的所有局部限制所对应的 Grunwald 问题都有正解，即适用该定理。这包括所有奇数阶阿贝尔群。否则，定理 6.1 与 Wood 的结果不一致，表明 Wood 的计数结果揭示了“Grunwald 问题”和“公平计数函数”这两类障碍。

此外，定理 1.2 与 S_n-扩张的渐近增长率相符，其中 $\mathbb{Q}$ 对应 $n=3$、4、5；对于 $n\geqslant 6$，其预测增长率也相符，精确到 Malle-Bhargava 局部级数 [Bha07] 前面的常数因子 $1/2$。这源于

$$\frac{1}{|S_n^{\mathrm{ab}}[|\mu(\mathbb{Q})|]|}=\frac{1}{|C_2[2]|}=\frac{1}{2}$$

出现在前置常数中的因子。

7.2. G 不是由最小指标元素生成的。这种障碍已知会影响数域计数。对 $D_4\subseteq S_4$ 扩张进行计数时，其首项常数是欧拉乘积的收敛和 [CYDO02]，，与定理 1.2 中的首项常数有显著差异。这类行为很常见，在 $C_2\wr H$-扩张 [Kl¨u12] 和 $\mathrm{Heis}_3\subseteq S_9$ [FK21] 中也会出现。造成这些问题的根本原因是：当 G 不是由最小指标元素生成时，存在某个子域，会出现在正比例的 G-扩张中。尽管子域以正比例出现在 G-扩张中会改变首项常数的行为，却也使确定渐近增长率变得更容易。这是作者与 Lemke Oliver、Wang 和 Wood 即将发表的合作成果所研究的主题：他们确定了若干个不是由最小指标元素生成的群对应的 Malle 计数函数的渐近增长率（包括与 Malle 猜想相符和不相符的情况）。

当 G 不是由最小指标元素生成时，根据引理 6.4(b)，有 $\beta=0$。因此，我们目前的方法无法以概率 1 产生渐近行为。

我们认为，仅凭带局部数据的随机群 μ_K^{MB} 的结构，就应当预期会出现这种情况。Alb22] 中的大数定律结果利用了随机变量 $\#\mathrm{Epi}(\mathscr{G},(G,S,\phi))$ 之间足够的独立性（或不相关性）得以证明。从某种意义上说，这种“独立性”是两个 G-扩张 L_1/K 和 L_2/K 之间 Frobenius 分布独立性的模型。根据切博塔廖夫密度，我们知道

当且仅当扩张互不相交，也就是说 $L_1 \cap L_2 = K$ 平凡时， L_1 和 L_2 中 Frobenius 的分布才相互独立。在这种情形下， [Alb22，定理 1.4] 可解释为：100% 的 G-扩张对都具有平凡交 $L_1 \cap L_2 = K$。

现在，假设 $N \trianglelefteq G$ 是 G 的一个真正规子群，且包含所有最小指标元素。对于一个固定的 G/N-扩张 $F/K,$，扭曲的 Malle 猜想 [Alb21] 利用 Malle-Bhargava 原理预测，正比例的 G-扩张 L/K 具有不变域 $L^N = F$。这与我们对 [Alb22，定理 1.4],所需的结论直接矛盾，表明在这些情形下，定理 1.2 不可能如原文所述那样成立。

这一论证表明，从某种意义上说， μ_K^{MB}已经看到了这一障碍。在此类情形中，我们需要不同的方法来研究计数函数，但人们不再期待得到类似定理 1.2 的结果。

7.3. 性质 E。性质 E 由 Liu–Wood–Zureick-Brown 在 [LWZB19]中如此命名，其中的“E”代表“扩张”。它等价于某种局部到整体性质：给定一个中心短正合列 $1 \to Z \to E \to G \to 1$，嵌入问题

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow \pi & & \\ 1 & \longrightarrow & Z & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

当且仅当相应的局部嵌入问题

$$\begin{array}{ccccccccc} & & & & & & G_{K_p} & & \\ & & & & & & \downarrow \pi|_{G_{K_p}} & & \\ 1 & \longrightarrow & Z & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

对 K 的每个赋值 p 都可解时，才可解。这迫使某些 E-扩张在某些 G-扩张存在的前提下存在，显然会对数域计数问题产生一些影响。文献中目前尚无这一性质具体影响 Malle 计数函数的实例，但作者了解到，Koymans–Pagano 即将发表的工作中有一个例子：他们利用性质 E 证明，对于某个二步幂零群，Malle 对分歧素数乘积排序所预测的 $\log X$ 次幂是错误的。

在上述图表中用带局部数据的群 $\mathscr{G} \in \mathbf{proGrp}(K)$ 替换绝对伽罗瓦群 G_K 后，我们可以讨论带局部数据的群的性质 E。要将 Malle-Bhargava 局部级数直接与中心嵌入问题联系起来，更难以表述；通过考察带局部数据的随机群 μ_K^{MB}，我们可以清楚地展现这种联系。

特别地，我们可以询问，相对于 μ_K^{MB}，性质 E 成立的概率是多少。可以证明，这一事件是可测的，但目前我们还无法计算其实际概率。鉴于已有关于非分歧对象统计的研究表明，其首项常数与 Malle-Bhargava 局部级数不一致，例如 [BBH17、LWZB19、Woo19、SW23],，我们预计相对于 μ_K^{MB}，性质 E 成立的概率严格小于 1。

不过，我们不会让本小节空手而归。值得一提的是，μ_K^{MB}“本质上”特化为 Liu–Wood–Zureick- Brown [LWZB19] 所定义的随机 Γ-群。我们考虑 $\mathscr{G}$ 形如 $H \rtimes \Gamma$ 的极大商，其中所有分歧都位于 H 之外，且 H 与 $|\mu(K)||\Gamma|$ 互素。给定任意 $\pi : F_{K,\, S} \to \Gamma$，若 π 可经由 $\mathscr{F}_{K,\, S}(r)$ 分解，则这种形式的 π 的最大非分歧扩张由

群

$$\begin{aligned}\mathscr{F}_{K,S}(r)/\langle\ker\pi|_{I_p}\rangle &= F_{K,S}/\langle r_i\in\ker\pi\ (i=1,...,|S|+u),\ker\pi|_{I_p}\rangle\\ &= \langle \mathrm{Fr}_p : p\in S\rangle_{|\mu(K)||\Gamma|}\rtimes\Gamma/\langle r_i\in\ker\pi\ (i=1,...,|S|+u)\rangle\\ &= \left(\langle \mathrm{Fr}_p : p\in S\rangle_{|\mu(K)||\Gamma|}/\langle r_i\gamma r_i^{-1}\gamma^{-1}\ (i=1,...,|S|+u \text{ and } \gamma\in\Gamma)\rangle\right)\rtimes\Gamma\end{aligned}$$

如果 π 对应于一个 Γ-扩张 $L/K,$，那么这个群就与 [LWZB19] 中提出的随机群完全相同（其中还包含一个由 Γ 构成的半直积）。这就是我们所说的这些随机群“本质上”相同。区别在于，π 经过$\mathscr{F}_{K,\ S}(r)$仅仅是对一个 Γ-扩张的建模，而并非严格等同于一个扩张。这是由于研究设定不同：我们的随机群旨在统计具有受限局部行为的扩张，因此这里对整个 $H\rtimes\Gamma$ 扩张进行了建模。与此同时，Liu–Wood–Zureick-Brown 构造随机群，只对非分歧的 H 部分进行建模，并遍历实际的 Γ-扩张（而非对 Γ-扩张的建模）。

值得注意的是，Liu–Wood–Zureick-Brown 形式为 $r\gamma r^{-1}\gamma^{-1}$ 的特殊关系，正是从我们纳入带局部数据的群定义中的惯性数据推导出来的。Liu–Wood– Zureick-Brown 通过对其随机群施加性质 E，构造出了这种关系表达式。这表明，在 μ_K^{MB}中纳入惯性数据至少涵盖了性质 E 的一部分。

7.4. 单位根行为。Kl¨uners 给出了 $C_3\wr C_2\subseteq S_6$ 的例子，其中 Malle 预测的增长率并不正确 [Kl¨u05a]。问题不只在于常数项；事实上，Malle 对该群预测的 $\log X$ 的幂也不正确。存在额外单位根时，计数函数的行为会发生变化。$\mathbb{Q}(\zeta_3)\subseteq L$ 的 $C_3\wr C_2$-扩张$L/\mathbb{Q}$渐近而言比其他 $C_3\wr C_2$-扩张更为丰富。根本原因在于，$\mathbb{Q}(\zeta_3)$ 的每个素理想要么整除 3，要么模 3 同余于 1；其他二次扩张并非如此，因此在此基础上，C_3-扩张有更多分歧方式。

在某种意义上，这使得由单位根生成的扩张具有“例外性”，体现了绝对伽罗瓦群的一些基本行为。带局部数据的随机群 μ_K^{MB} 并未纳入这种行为；事实上，我们可以证明，出现单位根行为的概率为 0。

定义 7.1. 设 L/K 为一个数域扩张。远离 L 的带局部数据的 $\mathsf{proGrp}_{\neg L}(K)$子范畴，定义为 $\mathsf{proGrp}(K)$ 中满足以下条件的子范畴，其对象满足

$$\mathrm{Hom}(\mathscr{G},(\mathrm{Gal}(E/K),\phi_{E/K}))=\varnothing$$

对每个满足 $K\neq E$的子扩张 $E\leqslant L$。

给定一个扩张 $M/K,$，相应的带局部数据的伽罗瓦群属于 $\mathsf{proGrp}_{\neg L}(K)$ 当且仅当 $M\cap L=K$。可能成为 Kl¨uners 风格反例来源的带局部数据的群，将是 $\mathsf{ProGrp}(K)\backslash\mathsf{proGrp}_{\neg K(\zeta^e)}(K)$ 中的对象，其中 e为某个整数。如下述定理所示，这些对象在该分布中出现的概率为 0：

定理 7.2. 设 L/K 是一个非平凡的数域有限扩张，μ_K^{MB} 是定理 1.1 给出的测度。那么

$$\mu_K^{\mathrm{MB}}\left(\mathrm{proGrp}(K)\backslash\mathrm{proGrp}_{\neg L}(K)\right)=0.$$

这意味着，以 $\mathbf{proGrp}_{\neg L}(K)$ 为条件计算概率，效果就像完全没有附加任何条件。因此，我们可以避开任意有限扩张 L/K，而不会丢失分布 μ_K^{MB} 中的任何信息。绝对伽罗瓦群则不具备这种性质；计算所有 G-扩张 L/K，与只计算满足 $L\cap K(\zeta^e)=K$ 的那些 G-扩张，可能会因影响 $\log X$ 的幂次而产生不同的渐近增长率。这一结果表明，带局部数据的随机群 μ_K^{MB} 可能更适合用于计算后一类扩张。

证明。任意元素 $(G,\phi)\in\mathbf{proGrp}(K)\backslash\mathbf{proGrp}_{\neg L}(K)$ 都存在一个到 $(\mathbf{Gal}(E/K),\phi_{E/K})$的态射，其中某个 $E\leqslant L$, $E\neq K$，并且由于 $\phi_{E/K}(G_{K_p})$ 的共轭元生成 $\mathbf{Gal}(E/K)$，该态射必为满态射。因此，它由某个满群同态 $\pi\colon G\to\mathbf{Gal}(E/K)$ 给出，其中 $\pi\phi_p=\phi_{E/K,p}$。

因此可得

$$\begin{aligned}\int_{\mathrm{proGrp}(K)\backslash\mathrm{proGrp}_{\neg L}(K)} d\mu_K^{\mathrm{MB}} &\leqslant \int_{\mathrm{proGrp}(K)\backslash\mathrm{proGrp}_{\neg L}(K)} \max_{\substack{E\leqslant L\\ E\neq K}} \#\mathrm{Epi}(\mathscr{G},(\mathrm{Gal}(E/K),\phi_{E/K}))d\mu_K^{\mathrm{MB}}\\ &\leqslant \max_{\substack{E\leqslant L\\ E\neq K}} \int_{\mathrm{proGrp}(K)\backslash\mathrm{proGrp}_{\neg L}(K)} \#\mathrm{Epi}(\mathscr{G},(\mathrm{Gal}(E/K),S,\phi_{E/K,S}))d\mu_K^{\mathrm{MB}}\\ &\leqslant \max_{\substack{E\leqslant L\\ E\neq K}} |\mathrm{Gal}(E/K)^{\mathrm{ab}}[|\mu(K)|]|^{-1}|\mathrm{Gal}(E/K)|^{-|S\cup P_\infty|+1}\end{aligned}$$

对于任意有限个素位 S。取 $S\to P_K$ 即可证明结论，注意到 $1<|\mathbf{Gal}(E/K)|<\infty$。□

T¨urkelli 对 Malle 猜想的预测提出了一项修正 [T¨ur15,Alb21]，，不过这项修正略显临时。基本思路是按 $\mu(L)$的同构类对 G-扩张 L/K 的计数进行分类，并对每种情况应用 Malle-Bhargava 原理。对于固定的有限群 G，在 G-扩张中，$\mu(L)$只能取有限多个同构类，因此渐近增长率由这些有限个个别情况中的最大增长率决定。

若能改进 μ_K^{MB} 的构造，以构造一种纳入单位根行为的新测度，并使 $\mathbf{proGrp}_{\neg K(\zeta^e)}(K)$ 必为零测集，那将很有意思；还可以考察这种改进后的测度是否与 T¨urkelli 的修正相符。

7.5. Grunwald 问题。若限制映射 (G,K,S) 有正解，则称 Grunwald 问题有正解：

$$\mathrm{Hom}(G_K,G)\to\prod_{p\in S}\mathrm{Hom}(G_{K_p},G)$$

该映射是满射。换言之，对于 S 中各赋值的每个局部限制，都能在某个全局扩张中实现。

Grunwald 问题可以立即推广到任意带局部数据的群，只需将 G_K 替换为所讨论的带局部数据的群 $\mathscr{G}$。接下来，我们可以询问相对于 μ_K^{MB}，Grunwald 问题有正解的概率。

定理 7.3. 对于每个 G 和 S， $\mathscr{G} \in \mathbf{proGrp}(K)$ 对 Grunwald 问题 $(G,\mathscr{G},S)$ 有正解这一事件相对于 μ_K^{MB} 的测度为 1。也就是说，

$$\mu_K^{\mathrm{MB}}\left(\left\{\mathscr{G}\in \mathrm{proGrp}(K)\middle| \begin{array}{c}\textit{for any finite group } G \textit{ and finite set of places } S,\\ \mathrm{Hom}(\mathscr{G},G)\to\prod_{p\in S}\mathrm{Hom}(G_{K_p},G) \textit{ is surjective}\end{array}\right\}\right)=1.$$

定理 7.3 并不令人意外，因为 μ_K^{MB} 是根据所有可能的局部数据构造的。然而，这与绝对伽罗瓦群 G_K 的行为截然不同。根据 Grunwald-Wang 定理，对于 $(C_8、\ \mathbb{Q}、\ \{2\})$, Grunwald 问题已知没有正解。这一失败的根源同样是单位根（具体来说，是 C_8 情形下的 8th 单位根），因此有理由认为，改进测度以纳入单位根行为，或许也能解决这一问题。

或者，我们知道，对于任意一组有限处 S，若 G 是奇数阶可解群，或 G 有泛扩张，则 Grunwald 问题有正解。这包括奇数阶阿贝尔群和对称群；对于这些群，我们看到 μ_K^{MB} 预测的增长率与数域计数结果一致（对于公平计数函数）。这表明，对于其他总能使 Grunwald 问题有正解的群，也可能存在类似结果；这有助于判断我们何时可以合理地期待定理 1.2 对数域计数作出准确预测。

定理 7.3 的证明。证明由定理 6.1 得出。对于每个 $\phi\in\prod_{p\in S}\mathrm{Hom}(G_{K_p},G)$，取由下式定义的 $\Sigma=(\Sigma_p)$

$$\Sigma_p=\begin{cases}\{\phi_p\} & p\in S\\ \mathrm{Hom}(G_{K_p},G) & p\notin S.\end{cases}$$

此外，将不变量 inv 取为以下方式给出的权函数：

- 若存在一个 $\mathbb{Q}$-共轭类（即在共轭和可逆幂运算下封闭的极小集合） $\kappa\subseteq G$，使得 $G\backslash\kappa$ 是 G的子群，则取权函数

$$w(g)=\begin{cases}0 & g=1\\ 1 & g\in\kappa\\ 2 & g\in G\backslash(\kappa\cup\{1\}).\end{cases}$$

- 否则，取权函数

$$w(g)=\begin{cases}0 & g=1\\ 1 & g\neq 1\end{cases}$$

给出分歧素数乘积排序。

我们声称，在这些排序下，定理 6.1(iii) 适用于每个群，从而以概率 1 证明$(G,\mathscr{G},S)$ Grunwald 问题有正解。对可列多个有限群 G 和有限位点集 S 应用可列可加性，即可完成证明。

如果不存在一个 $\mathbb{Q}$-共轭类（即在共轭和可逆幂下封闭的极小集合） $\kappa\subseteq G$，使得 $G\backslash\kappa$ 是 G 的子群，那么每个真正规子群 $N\trianglelefteq G$ 必然包含至少两个 K-共轭类。因此，定理 6.1(iii) 的条件自动满足。

或者，假设这样的 κ 存在。我们声称，G 的任何真正规子群都不可能包含最小权重元素。这样，定理 6.1(iii) 的条件便自动满足。注意，$G\backslash\kappa$ 是真子群必然意味着 $|G\backslash\kappa| \leqslant \frac{|G|}{2}$。任何包含最小指标元素的正规子群 $N \trianglelefteq G$ 都与 κ 有非平凡交，因此，由于它在共轭和可逆幂下封闭，也包含 κ。N 还必须包含 1，因此我们得到上界

$$\begin{aligned} |N| &\geqslant |\kappa| + 1 \\ &= |G| - |G\backslash\kappa| + 1 \\ &\geqslant |G| - \frac{|G|}{2} + 1 \\ &> \frac{|G|}{2}. \end{aligned}$$

Th我们，$[G : N] < 2$，这必然意味着 $N = G$ 不是一个真子群 p. □

7.6. 公平计数函数。Wood 证明，按公平计数函数对阿贝尔扩张进行排序，足以使首项常数表示为收敛的欧拉乘积 [Woo09]。对于数域K的阿贝尔 G-扩张，这个计数函数的首项常数与定理 6.1 一致，条件是 G 和 K 满足：每个 Grunwald 问题 $(G、K、S)$ 都有正解。因此，除 Grunwald 问题的障碍外，排序的公平性足以使定理 6.1 中阿贝尔群的增长率与 Malle 阿贝尔群计数函数的真实增长率一致。

自然会问，Wood 给出的公平性条件能否放宽。定理 6.1 在以下情形下，给出了与可容许不变量 inv 相对应的计数函数的渐近增长率，该函数用于计算到有限群 G 的满射：

(3) G 由关于 inv 的最小权重元素生成

自然会想知道，条件 (3) 是否足以使定理 6.1 中的渐近增长率与按 inv 排序、在数域 K 上计数 G 扩张的 Malle 计数函数的真实增长率一致。若果真如此，这将表明公平性障碍已被“G不由最小指标元素生成”这一障碍所涵盖。

然而，已知对 G-扩张进行计数时，这一结论并不成立。条件 (3) 不足以使定理 6.1 中的渐近增长率与 Malle 计数函数的真实增长率一致。Wood 在与作者的私人通信中分享了一个反例 [Woo22]：按照由权函数确定的可容许不变量 inv，对 $\mathbb{Q}(\sqrt{2})$的 $\mathbb{Z}/4\mathbb{Z}$-扩张进行排序

$$w(g) = \begin{cases} 0 & g = 0 \\ 1 & g = 1, 3 \\ 2 & g = 2. \end{cases}$$

显然，$\mathbb{Z}/4\mathbb{Z}$ 由最小权重元素生成，因此满足条件 (3)。然而，显式计算（Wood 沿着 Wright 对阿贝尔扩张 [Wri89,Woo22]的 Malle 猜想原始证明进行）表明

$$\#\{K/\mathbb{Q}(\sqrt{2}) : \mathrm{Gal}(K/\mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}/4\mathbb{Z}, |\mathrm{inv}(K/\mathbb{Q}(\sqrt{2}))| \leqslant X\} \sim cX$$

存在一个正常数 c，它由两个不同的收敛的欧拉乘积之和显式给出。这显然不同于定理 6.1 中给出的增长率，后者只涉及一个收敛的欧拉乘积。

Wood 的反例表明，除条件 (3) 外，排序还必须满足某种非平凡条件，才能使定理 6.1 与 Malle 计数函数的真实增长率相符。对于避开 Grunwald 问题障碍的阿贝尔群，公平性已足够；一个值得探讨的问题是，在此类情况下，公平性是否也是必要条件。

超越阿贝尔群的范畴后，[Woo09]中定义的公平计数函数概念无法直接推广到非阿贝尔群。据作者所知，尚无人提出将公平计数函数的概念推广到非阿贝尔扩张，唯一广为认可的是，按分歧素数乘积排序应被视为公平。出于类似原因，S_n次数为 n 的扩张的判别式排序或许也应被视为公平 [Bha07]。因此，很难确定对于哪些排序，我们应当预期定理 6.1 中的增长率会与 Malle 计数函数的真实增长率一致（即使假设可以避开所有其他障碍）。

粗略地说，阿贝尔扩张的“公平”计数函数这一定义的由来与 Grunwald 问题的由来相似。在 [Woo09]，中的生成狄利克雷级数计算中，会出现一个由最右极点具有最大阶数的欧拉乘积构成的有限和。当这个和相消为零时，可以证明整个生成狄利克雷级数也相消为零，从而对相应的 Grunwald 问题给出否定解答。当这个和不相消为零时，各个欧拉乘积可能产生不同的首项常数，必须将这些常数相加。公平计数函数则使这个和仅包含那些产生相同首项常数的欧拉乘积。鉴于这种联系，作者乐观地认为，将 Grunwald 问题纳入随机模型，将有助于阐明非阿贝尔扩张的公平计数函数应当是什么样的。特别地，沿着这一方向，一个值得采取的后续步骤是细化测度，将单位根行为纳入其中，并类比 Wood 在 [Woo09] 中的主要结果，探究哪些排序具有良好的局部概率。

References

[Alb20] Brandon Alberts. Malle 猜想的弱形式与可解群。《数论研究》，6(10)，2020 年 3 月。[Alb21] Brandon Alberts. 第一伽罗瓦上同调群的统计：Malle 猜想的一个精化。《代数与数论》，15(10):2513–2569，2021 年。[Alb22] Brandon Alberts. 范畴中随机对象的计数函数，2022 年 11 月。预印本见 https://arxiv/abs/2211.07129。[BBH17] Nigel Boston、Michael R. Bush 和 Farshid Hajir. 虚二次域的 p-类塔的启发式。《数学年刊》，368(1-2):633–669，2017 年 6 月。[Bha07] Manjul Bhargava. 局部域扩张的质量公式，以及关于数域判别式密度的猜想。《国际数学研究通报》，17，2007 年 7 月。[Bha14] Manjul Bhargava. 几何筛与不变量多项式无平方因子值的密度，2014 年 1 月。预印本见 https://arxiv.org/abs/1402.0031。[BSW15] Manjul Bhargava、Arul Shankar 和 Xiaoheng Wang. 全局域上的数的几何方法 I：预齐性向量空间，2015 年 12 月。预印本见 https://arxiv.org/abs/1512.03035。

[BW07] Manjul Bhargava 和 Melanie Matchett Wood. S_3-六次数域判别式的密度。美国数学会会刊，136(05):1581–1588，2007 年 12 月。[CL84] Henri Cohen 和 Hendrik. W. Lenstra. 数域类群的启发式。《数学讲义》之《数论：诺德韦克豪特，1983》，第 33–62 页，1984 年。[Cra94] Harald Cram´er. 关于素数的若干定理。《施普林格数学文集》，第 138–170 页，1994 年。[CYDO02] Henri Cohen、Francisco Diaz Y Diaz 和 Michel Olivier. $\mathbb{Q}$的四次二面体扩张的枚举。《数学汇刊》，133(1):65–93，2002 年 8 月。[DH71] Harold Davenport 和 Hans Heilbronn. 关于三次数域的密度。II。英国皇家学会会刊。伦敦。A辑：数学、物理与工程科学，322:405–420，1971 年。[DLAN17] Cyril Demarche、Giancarlo Lucchini Arteche 和 Danny Neftin. 齐性空间的 Grunwald 问题与逼近性质。格勒诺布尔傅里叶研究所年刊，67(3):1009–1033，2017 年。[DW88] Boris Datskovsky 和 David J. Wright. 三次扩张判别式的密度。《纯粹与应用数学杂志》，第 116–138 页，1988 年。[FK21] ´Etienne Fouvry 和 Peter Koymans. 九次 Heisenberg 扩张的 Malle 猜想，2021 年 2 月。[FW89] Eduardo Friedman 和 Lawrence C. Washington. 有限域上曲线除子类群的分布。《数论》，第 227–239 页，1989 年。[Gra95] Andrew Granville. Harald Cram´er 与素数分布。《斯堪的纳维亚精算杂志》，1995(1):12–28，1995 年。[Har07] David Harari. 关于有限代数群伽罗瓦上同调的一些逼近性质。《法国数学会通报》，135(4):549–564，2007 年。[Kl¨u05a] J¨urgen Kl¨uners. 关于 Malle 猜想中判别式渐近行为的一个反例。《数学报告》，(6):411–414，2005 年。.[Kl¨u05b] J¨urgen Kl¨uners. 关于具有给定伽罗瓦群的数域的渐近行为。《数学与应用》，Shaker，2005 年。[Kl¨u12] J¨urgen Kl¨uners. 以缠绕积为伽罗瓦群的数域的分布。《国际数论杂志》，08(3):845–858，2012 年。[LW20] Yuan Liu 和 Melanie Matchett Wood. 由 N 个生成元生成的自由群模去 $n+u$ 个 N 趋于无穷时的随机关系。《纯粹与应用数学杂志》（克雷尔杂志），2020(762):123–166，2020 年。[LWZB19] Yuan Liu、Melanie Matchett Wood 和 David Zureick-Brown. 最大非分歧扩张伽罗瓦群的预测分布，2019 年 7 月。预印本见 https://arxiv.org/abs/1907.05002。[M¨ak85] Sirpa M¨aki. 关于阿贝尔数域的密度。《芬兰科学院年刊》。A辑 I：数学。学位论文，0355-0087，54，1985 年。[Mal02] Gunter Malle. 关于伽罗瓦群的分布。《数论杂志》，92(2):315–329，2002 年。[Mal04] Gunter Malle. 关于伽罗瓦群的分布，II。《实验数学》，13(2):129–135，2004 年。[Mot18] Fran¸cois Motte. 关于 Malle 猜想与 Grunwald 问题，2018 年。https://arxiv.org/abs/1812.11376。[MTTW20] Riad Masri、Frank Thorne、Wei-Lun Tsai 和 Jiuya Wang. 关于 $g \times a$的 Malle 猜想，带有$g = s_3, s_4, s_5$，2020 年 5 月。.[Neu73] J¨urgen Neukirch.《代数数论中的嵌入问题》。《数学创见》，21(1-2):59–116，1973 年。[RS14] Simon Rubinstein-Salzedo. a4 数域的不变量与 Cohen–Lenstra 启发式。《国际数论杂志》，10(05):1259–1276，2014 年。[SW22] Will Sawin 和 Melanie Matchett Wood. 范畴中随机对象的矩问题，2022 年 10 月。[SW23] Will Sawin 和 Melanie Matchett Wood. 关于含有单位根的数域扩张类群分布的猜想，2023 年 1 月。

[T¨ur15] Seyfi T¨urkelli. Hurwitz 概形的连通分支与 Malle 猜想。《数论杂志》，155:163–201，2015 年。[Wan50] Shianghaw Wang. 关于 Grunwald 定理。《数学年刊》，51(2):471–484，1950 年。[Wan21] Jiuya Wang. 关于 $s_n \times a$ for $n = 3$,4,5 的 Malle 猜想。《数学汇刊》，157(1):83–121，2021 年。[Woo09] Melanie Matchett Wood. 阿贝尔域扩张中局部行为的概率。《数学汇刊》，146(01):102–128，2009 年 8 月。[Woo19] Melanie Matchett Wood. 非阿贝尔 Cohen–Lenstra 矩。《杜克数学杂志》，168(3):377–427，2019 年。[Woo22] Malanie Matchett Wood，2022 年。私人通信。[Wri89] David J. Wright. 阿贝尔扩张判别式的分布。《伦敦数学会会刊》，58(1):17–50，1989 年。