arXiv:2601.06283v1 [math.NT] 9 Jan 2026

p p进随机矩阵的特征值

JIAHE SHEN 和 ROGER VAN PESKI

Abstract. 我们建立了 p进随机矩阵特征值的基础理论，类比于复数域和 $\mathbb{C}$上的经典随机矩阵理论。Ellenberg-Jain-Venkatesh 提出用这类特征值统计作为 p进 L函数零点的模型，并计算了单位圆盘内特征值个数的极限分布。我们计算了一个具有哈尔分布的 $n \times n$ 矩阵的 n 特征值的完整联合分布，得到了与阿基米德情形类似的库仑气体型公式，其中范德蒙项导致了特征值排斥。

利用这些库仑气体密度函数，我们推导出特征值统计在$n \to \infty$时的渐近性。其中包括精确计算，例如给出一个闭式表达

$$\rho(x, y) = 1 - \theta_3(-\sqrt{p}; ||x - y||^2/p)$$

式，描述 $\mathbb{Z}_p$中特征值的极限二点相关，以及二次扩张中的类似结果。这些公式为 p进 L函数的零点提供了具体的数值预测。

对于 $\mathbb{Q}_p$ 的任意扩张中的特征值，我们还给出了关于其两两排斥以及每个扩张中预期特征值数量的精确估计。最后，我们计算了所有特征值均位于 $\mathbb{Z}_p$中的渐近概率。

我们的证明结合了多个不同领域的结果： p-adic 轨道积分、随机 p-adic 多项式的根、用于随机模的 Sawin-Wood 矩方法，以及与整数分拆上的测度相关的马尔可夫链。

Contents

1. 引言 2

1.1. 前言 2 1.2. 首要结果 4 1.3. 固定大小矩阵的扩张排序与联合特征值分布 6 1.4. $\mathbb{Q}_p$ 8的扩张中特征值的渐近结果 1.5. 实 Ginibre 情形中的相应结果 11 1.6. 关于具有独立系数的 $\mathbb{Z}_p$ 上随机多项式 11 1.7. 证明方法与本文结构 12

2. 预备知识 15 2.1. 一些一般记号 15´2.2. étale 代数 16¯2.3. 环 $\mathbb{Z}_p$、提升子空间与结式 17 3. 多个点处特征多项式取值的显式联合累积分布函数 20 3.1. 证明概要 20 3.2. 命题 3.3 的证明 21 3.3. 矩阵与 $\mathbb{Z}_p[\mathfrak{x}]$-模 25 3.4. 体积的分解与计算 29 4. 从特征多项式到特征值的联合分布 37 4.1. 定理 1.7 的证明 37

Date: 2026年1月13日。

4.2. 相关函数的平均及引理 1.13 的证明 41 5. 期望行列式、余核与矩方法 44 5.1. 代数准备 45 5.2. 定理 5.1 的证明 46 5.3. 定理 5.2 的证明 48 6. 极限相关函数及其性质 50 7. $\mathrm{GL}_n(\mathbb{Z}_p)$ 中 Haar 矩阵的特征值 54 8. 余核的马尔可夫链描述 56 9. 低次扩张中的极限相关函数 61 9.1. $\mathbb{Z}_p$ 61 中的特征值 9.2. 二次扩张 65 10. 特征值排斥的估计 71 11. 次数为 $r > 2$ 73 的扩张中的特征值平均数量 12. 所有特征值都在 $\mathbb{Z}_p$ 76 中的概率 参考文献 81

1. Introduction

1.1. 前言。 1972年4月的一天，在喝下午茶时，休·蒙哥马利向弗里曼·戴森提起了他当时尚未发表的猜想 [Mon73]，该猜想涉及黎曼ζ函数在 $\frac{1}{2} + i\mathbb{R}$上的非平凡零点分布。对虚部作适当归一化后，这些零点似乎如同实数轴上密度为 1 的随机点集，其相关性由以下公式给出

$$\mathbb{E}[\#\{\text{zeroes in } U\} \cdot \#\{\text{zeroes in } V\}] = \int_{U\times V} 1 - \left(\frac{\sin(\pi(x-y))}{\pi(x-y)}\right)^2 dxdy \tag{1.1}$$

对于任意互不相交的可测集 U， $V \subset \mathbb{R}$。

Dyson 立即认出，这个被积函数正是大型厄米矩阵或酉随机矩阵的特征值的极限二点相关函数。他和其他人一直在研究此类矩阵，将其作为重原子核能级的模型 [Tho13]。这一如今广为人知的轶事引发了一股研究热潮，人们致力于将这些观察推广到其他族的 L-函数，并研究 L-函数更精细的统计性质，例如对某一族 L-函数取平均后，靠近实数轴的零点的分布；参见 Katz-Sarnak 的综述[KS23] 或 Keating-Snaith 的综述 [ABDF11，第 24] 章。这些以及其他随机矩阵统计，如今已出现在纯数学、应用数学和物理学的众多领域中。

后来，Ellenberg-Jain-Venkatesh [EJV11] 提出了这一故事的 p进制版本，即关于 $\mathbb{Z}_p$ 上的随机矩阵的特征值也能模拟 p进 L函数 $\mathbb{Q}_p$中¯零点的渐近分布。这些零点是 $\mathbb{Q}_p$中的点。他们通过数值计算大量L函数族的零点，并将结果与随机矩阵方面的精确公式进行比较，发现以 1 为中心的 $\bar{\mathbb{Q}}_p$ 开单位球[1] 内零点个数与特征值个数的分布非常吻合。在 L函数方面，Delbourgo-Chao [DC15],Delbourgo-Knospe [DK23], Knospe [Kno24], Kundu-Washington[KW24b, KW24a],以及 Santato [San21]等多项研究计算了其他 L函数族的更多数据，发现这些结果与 [EJV11]提出的 λ不变猜想相当吻合。

除了落在单位球内的零点／特征值数量之外，几乎没有人研究其他关于零点／特征值的统计性质。考虑到经典的

[1]这个数 对于 K 中与数域相关、并在 [EJV11], 中研究的 L-函数，这个数被称为 he*Iwasawa* λ-*invariant*，并控制 K 上圆分塔中类数的增长。

L-函数／随机矩阵联系的成功，以及这一方向原始研究所发出的明确推动，这似乎令人惊讶：

> 更进一步，我们可以推测，p 进 L 函数更精细特征的分布也可以由随机矩阵模型预测；我们讨论一个有关零点间距的例子。这里的数值证据不那么有说服力，但也并非完全令人失望……-[EJV11, p3]

这个“例子”是开单位球中以 1 为中心的所有特征值／零点的差的平方的乘积（岩泽多项式的判别式）。这是一个高度非线性的统计量，因此未能完全吻合可能只是收敛较慢，也可能并非如此；但据我们所知，没有研究沿着 [EJV11] 之后的工作来探究是否属于这种情况。

从 Dyson 和 Montgomery 最初提出的相互作用及其后续发展的角度来看，很自然会想到研究随机矩阵一侧更精细的特征值统计。令人意外的是，自 [EJV11] 以来，即使是类似于 (1.1) 的二点相关函数这类基本统计量，其显式公式或估计的计算仍未解决。

本工作的目标是沿着经典研究复数域和实数域上的随机矩阵时所采用的思路，发展 p-进随机矩阵特征值的基础理论，尤其是给出这类显式的特征值统计。这些统计可以与来自 L-函数零点的数据进行比较，也可以与未来任何其他可能被认为存在 p-进随机矩阵统计的领域进行比较。如果经典随机矩阵理论的发展历程可以作为参考，那么这类统计可能并非只会出现在一个地方。

至于为何此前没有计算 p-进一侧的这类统计，一种可能的解释是，显然这比阿基米德情形更难做到。我们的证明结合了几条分别发展的研究脉络中的技巧——其中一些是在 [EJV11] 之后才发展起来的——据我们所知，这些技巧此前尚未被结合使用：

- p-进轨道积分，具体而言，是此前关于这一主题的研究中出现的某些模计数计算，例如 Yun [Yun13]。
- 具有独立系数的随机多项式的零点，其系数取自 $\mathbb{Z}_p$。我们使用 p-进 Kac-Rice 公式以及 Caruso [Car22]（沿用 Evans [Eva02] 的方法）提出的相关结果来研究这些问题，许多证明也受到 [Car22] 在这一情形下所用证明的启发。
- 离散随机矩阵的余核与随机模的矩方法。余核得到了充分研究，也适用于 Wood [Woo17]，的矩方法，但先验而言，它们是与特征值不同的统计量。不过，我们将对特征值的理解归结为对随机矩阵 A中多项式 $Z(A)$ 之余核的理解；在此基础上，我们可以使用 Sawin-Wood 广义矩方法 [SW22]，正如 Cheong-Yu [CY23] 将其应用于这一问题时所做的那样。
- 与整数分拆上的测度相关的马尔可夫链。具体来说，我们采用 Fulman [Ful01] 对一个马尔可夫链的对角化结果；该马尔可夫链由 Evans [Eva02] 独立发现，可用于抽样得到 p-进随机矩阵的余核。

我们希望，除了定理之外，本文还通过提供一个蓝图，展示如何将上述技巧结合起来证明未来的结果，从而具有一定价值。与关于 $\mathbb{R}$ 和 $\mathbb{C}$ 上随机矩阵的丰富文献相比，p-进情形仍有许多方面有待探索。例如，我们并未尝试研究哈尔分布之外的矩阵分布，也未涉及矩阵空间 $\mathrm{Mat}_n(\mathbb{Z}_p)$ 和 $\mathrm{GL}_n(\mathbb{Z}_p)$ 上的哈尔分布；不过，研究来自不同群或齐性空间的其他“对称类型”将是很自然的，我们相信同样的方法在这些情形下也会很有用。

非阿基米德情形之所以困难，一个原因是存在无穷多个 $\mathbb{Q}_p$ 的扩张，特征值可以取值于其中。这也是一个有趣之处，但为求简明，我们先介绍一些绕开这一问题的结果：要么¯只考虑 $\mathbb{Q}_p$ 中的特征值，要么考虑 $\mathbb{Q}_p$ 中的球而不区分扩张。这些结果以尽可能少的复杂性，展现了概率图景的诸多特征；

相关内容将在第 1.2 节中说明。第 1.3 节将回到不同扩张中的特征值这一问题，解释如何通过相关函数处理它们，并刻画一个 $n \times n$ 矩阵的特征值分布，这是我们所有渐近结果的出发点。第 1.4 节给出一些可由此推导出的、关于 $\mathbb{Q}_p$ 扩张中特征值的渐近性。第 1.5 节讨论阿基米德情形中的相关结果，以及我们受这些结果启发而在 p-adic 情形中证明的一个结果；第 1.6 节则更详细地讨论与随机多项式文献的联系。第 1.7 节概述证明思路及论文结构。

1.2. **首批结果**。 回顾一下， $\mathbb{Q}_p$ 配备了一个范数，我们记作 $||\cdot||$；该范数在 $\mathbb{Q}_p$ 上限制为通常的范数，其定义为：对 $u \in \mathbb{Z}_p^\times$，有 $||u \cdot p^k|| = p^{-k}$。矩阵 $A \in \mathrm{Mat}_n(\mathbb{Z}_p)$的所有特征值都位于 $\mathbb{Z}_p$中，即代数闭包 $\mathbb{Q}_p$ 内关于此范数的闭单位球，因为特征多项式的系数都属于闭单位球$\mathbb{Z}_p \subset \mathbb{Q}_p$。该空间不同的拓扑导致了与经典阿基米德随机矩阵理论截然不同的极限：

定理 1.1。 存在集合 $\mathcal{U}_1$、$\mathcal{U}_2$、……，使得

(1) $\bar{\mathbb{Z}}_p = \bigsqcup_{i \geq 1} \mathcal{U}_i$。*(2)* 每个集合 $\mathcal{U}_i$ 都是有限个半径为1 的开球的并集，其中球的个数为 d_i，这些球位于 $\mathbb{Z}_p$中，且彼此伽罗瓦共轭。*(3)* 令 $A \in$ 矩阵空间$_n(\mathbb{Z}_p)$ 为一个随机矩阵，其条目相互独立，且服从 $\mathbb{Z}_p$上的加性 *Haar* 概率测度。那么，对于任意有限组$\mathcal{U}_{i_1}$、……、$\mathcal{U}_{i_k}$，当 $n \to \infty$时，每个 $\mathcal{U}_{i_j}$ 中的特征值与其他 $\mathcal{U}_{i_{j'}}$ 中的特征值渐近独立，这种独立性体现为相关函数的因式分解（见定理 *6.3*）。此外， A 中落在 $\mathcal{U}_i$ 内的特征值个数，当 $n \to \infty$ 时，其分布收敛于一个取值于 $d_i\mathbb{Z}_{\geq 0}$的随机变量 N_i，其分布定义为

$$\mathbf{P}(N_i/d_i = j) = \left(\prod_{k \geq 1} (1 - p^{-d_i k}) \right) \cdot \frac{p^{-d_i j}}{\prod_{k=1}^{j} (1 - p^{-d_i k})} \tag{1.2}$$

对于 $j \geq 0$。

集合 $\mathcal{U}_i$ 具有如下明确描述。将 $\mathbb{F}_p[x]$ 中的非零首一不可约多项式按 F_1、F_2、……进行编号，其次数分别为 d_1、d_2、……。令 $\mathcal{U}_i \subset \mathbb{Z}_p$为所有满足以下条件的 $x \in \mathbb{Z}_p$的集合：x的最小多项式模 p约化后，是 F_i的幂。

这描绘出这样一幅特征值图景：特征值分布在一个由小岛组成的无限群岛 $\mathcal{U}_i$ 上，每个小岛上随机分布着少量特征值；这些特征值彼此相互作用，但不会与其他岛屿上的特征值发生作用。其中一个小岛是以 0 为中心的开单位球，对应于多项式 $F_1 = x$；而将 [EJV11] 与 L-函数的零点进行比较的主要随机矩阵结果，在此情形下是公式 (1.2) 的一个 GL_n 类比。事实上，定理 1.1 也可以通过修改 [EJV11], 的论证得到，不过我们将其作为用于其他结果的工具所产生的副产品来获得。

那么，接下来的问题便是：给定岛上的特征值之间的相互作用在渐近意义下呈现出怎样的形态 $\mathcal{U}_i$。为了理解这一点，有必要根据特征值所属的域扩张 $K/\mathbb{Q}_p$ 对它们加以区分。这种区分，以及研究特征值相关性而非落在某个球内的特征值数量，正是我们的方法与 [EJV11]的方法之间的核心差异。

对于那些位于 $\mathbb{Z}_p$ 中的特征值，较为简单的结果已能很好地反映一般情形，因此我们先陈述这些结果，再为一般扩张建立记号。

定理 1.2. 设 U、$V \subset \mathbb{Z}_p$ 是两个互不相交的可测集。对于每个 n，令 $A \in$ 矩阵空间$_n(\mathbb{Z}_p)$的条目相互独立，且服从 $\mathbb{Z}_p$ 上的加性 *Haar* 概率测度，并令

$Z_{U,\ n}$、$Z_{V,\ n}$ 分别表示 A 中位于 U 和 V 内的特征值个数。于是

$$\lim_{n\to\infty}\mathbb{E}[Z_{U,n}\cdot Z_{V,n}]=\int_{U\times V}\rho^{(\infty)}_{\mathbb{Q}_p,\mathbb{Q}_p}(x,y)dxdy, \tag{1.3}$$

其中，积分是相对于 *Haar* 概率测度进行的，极限二点相关函数为

$$\rho^{(\infty)}_{\mathbb{Q}_p,\mathbb{Q}_p}(x,y)=1-\theta_3(-\sqrt{p};||x-y||^2/p), \tag{1.4}$$

其中

$$\theta_3(z;t)=\prod_{i\geq 1}(1-t^i)(1+t^{i-1/2}z)(1+t^{i-1/2}/z)=\sum_{k\in\mathbb{Z}}t^{\frac{k^2}{2}}z^k$$

是一个雅可比 *theta* 函数。此外，

$$\lim_{n\to\infty}\mathrm{Cov}(Z_{U,n},Z_{V,n})=-\int_{U\times V}\theta_3(-\sqrt{p};||x-y||^2/p)dxdy\leq 0. \tag{1.5}$$

定理 1.2 可视为阿基米德情形下正弦核 (1.1) 的一个类比（不过，更贴近阿基米德情形的类比，是下文讨论的实 Ginibre 系综的实特征值的二点相关性）。在 (1.1) 或定理 1.2 中，取 U，V 为分别围绕两点 x和 y 的非常小的球，则被积函数可视为分别接近 x 和 y 的特征值对的密度。在经典情形下，被积函数在 $x-y\to 0$时趋于 0，这一事实印证了众所周知的特征值彼此排斥现象。从 theta 函数的求和形式很容易验证，定理 1.2 中的被积函数在 $x-y\to 0$ 时也趋于 0，这表明在 p-进情形下也存在二点排斥，(1.5) 中的负相关同样说明了这一点。尽管二点相关函数的这些性质所呈现的图景直观明了，我们却无法从概念上解释为何会特别出现雅可比 theta 函数这一神秘现象，因此亟待对此作出解释。

如果集合 U 和 V 彼此相距足够远，使得对所有 $x\in U,y\in V$ 都有 $||x-y||=1$，那么当 (1.5) 取等号时，U 和 V 中的特征值数量渐近不相关。这对应于定理 1.1 中 U,V 位于不同的集合 $\mathcal{U}_i$ 中。

定理 1.2 仅适用于 $\mathbb{Z}_p$ 中的特征值，而我们将在后文的定理 1.9 中证明，任意扩张中的特征值都存在成对排斥。

我们通过计算固定 n 处的联合特征值分布，并令 $n\to\infty$ 趋于极限，得到定理 1.2 以及定理 1.1 中的独立性结论等结果。对于一般扩张中的特征值，这需要一些铺垫；我们将在下一小节中对此作出说明。不过，其结果与所有特征值都在 $\mathbb{Z}_p$ 中这一特殊情形形式相似，我们现在就来陈述这一特殊情形。

推论 1.3（定理 1.7 的推论）。设 $A\in$ 矩阵空间$_n(\mathbb{Z}_p)$ 是一个随机矩阵，其条目相互独立，服从 $\mathbb{Z}_p$ 上的加性 *Haar* 概率测度，并以所有特征值都落在 $\mathbb{Q}_p$（因而也落在 $\mathbb{Z}_p$）这一正概率事件为条件。则其特征值 x_1、……、x_n 的联合密度正比于

$$\prod_{1\leq i<j\leq n}||x_i-x_j||. \tag{1.6}$$

这里，由于特征值没有规范的排序方式，该联合密度是相对于 *Haar* 概率测度在 $\mathbb{Z}_p^n$ 上向 $\mathbb{Z}_p^{\vee n}$ 的推前测度而言的。

推论 1.3与定理 1.2一样，与此前研究过的实与复随机矩阵系综有着引人注目的相似之处。推论 1.3 还显示出有限 n 下的一种排斥形式，因为当 x_i 接近 x_j 时，$||x_i-x_j||$ 很小。在 $\mathbb{R}$ 和 $\mathbb{C}$ 上的特征值密度中出现的相同范德蒙项，在文献中被称为库仑气体相互作用。据我们所知，这是它们首次出现在 p进随机矩阵理论中；起初，我们并未预料到它们会与阿基米德情形存在如此密切的类比。然而，这类 p进库仑气体（有时也称为对数库仑气体）已被数学领域的Webster[Web21、Web23] 和Sinclair [Sin22] 作为独立研究对象，而在物理学领域则由Z´u˜niga-Galindo与

Torba [ZGT20], Zambrano-Luna and Le´on-Cardenal [ZGZLLC22], and Veys [VZG25]。这些工作均未涉及随机矩阵，但Sinclair在 [Sin22] 中写道：“本文的备用标题包括‘p进塞尔伯格积分’或‘p进随机矩阵理论’，这是因为文中出现了塞尔伯格积分的一个非阿基米德版本.....与随机矩阵理论的联系（目前）仍较为初步，因为本文并未引入随机矩阵。”推论 1.3建立了这一联系。

1.3. 扩 张排序与固定大小矩阵的联合特征值分布 .

矩阵在 $\mathbb{Z}_p$ 上的特征值可以落在 $\mathbb{Q}_p$的无穷多个扩张中的任意一个中，并且渐近地以正概率如此，因此一般公式比推论 1.3 和定理 1.2 更复杂。

我们发现，非对称实随机矩阵的情形是一个很有帮助的思考模型。这里仅有两个扩张， $\mathbb{R}$ 和 $\mathbb{C}$，特征值可以落在其中，但也会出现相同的一般行为。 $n\times n$ 实*Ginibre*矩阵 是矩阵空间 $\mathrm{Mat}_n(\mathbb{R})$中的一种矩阵，其实数标准高斯矩阵元相互独立。对于实矩阵，特征值要么为实数，要么成共轭对出现；一般而言，有 ℓ 对共轭特征值和 $n-2\ell$ 个实特征值。直观上，人们可能会希望所有 n 个特征值的联合分布相对于 n 个 $\mathbb{C}$无序副本上的勒贝格测度绝对连续，并且可以用相对于该测度的单一密度函数来描述。事实并非如此，因为集合 $\mathbb{R}$ （在 $\mathbb{C}$中的勒贝格测度为 0）通常包含非零个特征值。

共轭对中的每一对都可以用开上半平面 $\mathbb{H}_+$ 中的一个代表元来描述，而开上半平面 $\mathbb{H}_+$正是 $\mathbb{C}\setminus\mathbb{R}$ 关于复共轭的商集。因此，可以将 n-元特征值组所处的空间认同为

$$\bigsqcup_{\ell=0}^{\lfloor\frac{n}{2}\rfloor}\mathbb{H}_+^{\vee\ell}\times\mathbb{R}^{\vee n-2\ell}, \tag{1.7}$$

这里取对称积，因为特征值没有规范的排序方式。当然， $\mathbb{R}$ 本身具有规范排序，并且复特征值可以按实部排序，因此特征值多重集可以认同为 $\mathbb{H}_+^\ell\times\mathbb{R}^{n-2\ell}$ 中某个适当有序子集上的点。对于每个 $0\le\ell\le\lfloor\frac{n}{2}\rfloor$，可以通过一组密度函数 $\rho_{n,\ell}$，相对于这些子集上的勒贝格测度，来指定空间 (1.7) 上的完整联合分布。

在 p-adic 情形下，整体而言情况相同，但与 (1.7) 类似的不交并中包含的分支要多得多，因为扩张也多得多。另一个问题是，一般而言，显式描述并排序与 ¯类似的商集并不简单。 $A\in\mathrm{Mat}_n(\mathbb{Q}_p)$ 的特征值位于代数闭包 $\mathbb{Q}_p$ 中，而 $\mathbb{Q}_p$在 $\mathbb{Q}_p$ 上是无限维的。如果 $x\in\mathbb{Q}_p$ 是某个矩阵 A 的特征值，那么 x 在 $\mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)$ 下的所有共轭元¯也都是特征值，并且 x 的最小多项式将作为 A 的特征多项式的一个不可约因子出现。将这样的特征值视为位于包含它的 $\mathbb{Q}_p$ 的最小扩张中是自然的。为此，我们将扩张 $K/\mathbb{Q}_p$ 中的new元素定义为

$$K^{\mathrm{new}}=K\setminus\bigcup_{\mathbb{Q}_p\subset L\subsetneq K}L \tag{1.8}$$

其中并集是对严格包含于 K 的扩张 L 取的，因此

$$\bar{\mathbb{Q}}_p=\bigsqcup_{K/\mathbb{Q}_p}K^{\mathrm{new}} \tag{1.9}$$

其中不交并是对所有有限扩张 K 取的。

¯ K中的单位球，等价地说，即 $\mathbb{Z}_p\cap K$，是整数环 $\mathcal{O}_K$；而矩阵 $A\in\mathrm{Mat}_n(\mathbb{Z}_p)$的特征值若位于 K中，则必定也位于 $\mathcal{O}_K$中。我们记作 $\mathcal{O}_K^{\mathrm{new}}=K^{\mathrm{new}}\cap\mathcal{O}_K$，并¯注意到，根据 (1.9)，特征值所在的集合 $\mathbb{Z}_p$ 是不交并 $\mathcal{O}_K^{\mathrm{new}}$。每个 $\mathcal{O}_K$ 都带有加性 Haar 概率测度 μ_K，其补集 $\mathcal{O}_K\setminus\mathcal{O}_K^{\mathrm{new}}$的测度为 0。

若要在我们的设定中，为类似于 (1.7) 的空间定义一个显式的概率测度，就需要描述每个 K^{new} 在伽罗瓦作用下的商集，并为它们排序。我们发现，采用等价的相关函数视角要容易得多；这种做法在经典随机矩阵理论中很常见。上文定理 1.2 中已经出现了$\mathbb{Z}_p$ 中特征值的二点相关函数。一般而言，我们按如下方式定义它们。

定义 1.4. 设 X 是 $\mathbb{Z}_p$ 的随机子集，满足对于任意 $\sigma \in \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)$， $\sigma(X) = X$ 的概率为 1；并且对于任意有限扩张 $K/\mathbb{Q}_p$， $X \cap \mathcal{O}_K$ 几乎必然有限。那么对于 $\mathbb{Q}_p$ 的扩张 $K_1, \dots, K_m$，我们称

$$\rho_{K_1,\dots,K_m} : \mathcal{O}_{K_1}^{\mathrm{new}} \times \cdots \times \mathcal{O}_{K_m}^{\mathrm{new}} \to \mathbb{R}_{\geq 0}$$

is X 的（$K_1, \dots, K_m$）-相关函数，如果对于任意有界可测函数 n

$$f : \mathcal{O}_{K_1}^{\mathrm{new}} \times \cdots \times \mathcal{O}_{K_m}^{\mathrm{new}} \to \mathbb{C},$$

我们有

$$\mathbb{E}\left[\sum_{\{x_1,\dots,x_m\}\subset X} f(x_1,\dots,x_m)\right] = \int_{\mathcal{O}_{K_1}^{\mathrm{new}}\times\cdots\times\mathcal{O}_{K_m}^{\mathrm{new}}} f(x_1,\dots,x_m)\rho_{K_1,\dots,K_m}(x_1,\dots,x_m)dx_1\cdots dx_m$$

其中求和遍历所有元组 $(x_1, \dots, x_m) \in \mathcal{O}_{K_1}^{\mathrm{new}} \times \cdots \times \mathcal{O}_{K_m}^{\mathrm{new}}$，使得其中任意两个 x_i 都不相等或互为伽罗瓦共轭，且 $\{x_1, \dots, x_m\} \in X$；积分则关于 $\prod_{i=1}^m \mathcal{O}_{K_i}$ 上的 Haar 概率测度进行。

若 X 是一个具有独立同分布加性 Haar 元素的随机矩阵 $A \in \mathrm{Mat}_n(\mathbb{Z}_p)$ 的特征值集合，我们将其（$K_1, \dots, K_m$）-相关函数记为 $\rho_{K_1,\dots,K_m}^{(n)}$。

相关函数使我们能够用有序乘积上的函数和积分，来表示随机点构型的子集上的期望；这些子集本身没有规范的排序。一般而言，在定义 1.4 中令 f 仅为可测集
$U \subset \mathcal{O}_{K_1}^{\mathrm{new}} \times \cdots \times \mathcal{O}_{K_m}^{\mathrm{new}}$ 的示性函数，则有

$$\mathbb{E}[Z_{U,n}] = \int_U \rho_{K_1,\dots,K_m}^{(n)}(x_1,\dots,x_m)dx_1\cdots dx_m \tag{1.10}$$

其中 $Z_{U,\,n}$ 是位于 U 中的不同且非共轭特征值的 m 元组 $(x_1, \dots\dots, x_m)$ 的数量。应将 $\rho_{K_1,\,\dots\dots,\,K_m}^{(n)}(x_1, \dots\dots, x_m)$ 理解为 m 个特征值在 $(x_1, \dots\dots, x_m)$ 附近的密度，具体来说，若 $U_1, \dots\dots, U_m$ 是围绕（彼此不同且非共轭的） $x_1, \dots\dots, x_m$ 的足够小的球，则

$$\mathbf{P}\text{（每个集合 } U_i \text{ 都包含一个特征值）} \approx \rho_{K_1,\,\dots\dots,\,K_m}(x_1, \dots, x_m)\mu_{K_1}(U_1)\cdots\mu_{K_m}(U_m)。 \tag{1.11}$$

我们只需通过用简单函数逼近 f，证明等式 (1.10) 即可；这些等式等价于一般情形下的定义 1.4。

特别地，相关函数 $\rho_{K_1,\dots,K_m}^{(n)}$ 确定了特征值落在 $K_1, \dots, K_m$中的事件下的特征值联合分布。因此，对所有满足$\sum_{i=1}^m [K_i\colon \mathbb{Q}_p] = n$的元组 $(K_1, \dots, K_m)$，这些相关函数构成的集合完整描述了随机 Haar 矩阵 $A \in$ 矩阵空间$_n(\mathbb{Z}_p)$的特征值联合分布。根据克拉斯纳定理 [Kra46a]，该相关函数集合也是有限的，因为每个次数下都只有有限多个 $\mathbb{Q}_p$ 的扩张。

下面的定理 1.7 给出了恰好这些相关函数的显式公式。为陈述该公式，我们先引入一些记号。

定义 1.5. 设 $x_1, \dots, x_m \in \mathbb{Q}_p$，并对每个 i，令 $\sigma_{i,l_i}(x_i)$ $1 \leq l_i \leq r_i$ 表示 x_i 的全体伽罗瓦共轭元。于是我们记作

$$\Delta_\sigma(x_1,\dots,x_m) = \Delta(\sigma_{1,1}(x_1),\dots,\sigma_{1,r_1}(x_1),\dots,\sigma_{m,1}(x_m),\dots,\sigma_{m,r_m}(x_m))$$

其中 $\Delta(z_1, \dots\dots, z_r) = \prod_{1\leq i<j\leq r}(z_i - z_j)$ 是通常的范德蒙德行列式。

注意，通常判别式的绝对值与 Δ_σ 的关系为

$$||\operatorname{Disc}(x_1,\dots,x_m)|| = ||\Delta_\sigma(x_1,\dots,x_m)||^2.$$

定义 1.6。设 $K/\mathbb{Q}_p$ 是次数为 r 的扩张，$\mathcal{O}_K$ 为其整数环，且 $x \in \mathcal{O}_K^{\mathrm{new}}$。于是我们定义

$$\mathrm{Mod}_{\mathbb{Z}_p[x]} = \{M \subset K \mid M \text{ is a } \mathbb{Z}_p[x]\text{-module, also a } \mathbb{Z}_p\text{-lattice of rank } r\}.$$

我们通过乘法定义了群 $K^\times$ 在 $\mathrm{Mod}^{\mathbb{Z}_p[x]}$ 上的典范作用；类似地，对于其子群 $\Lambda = \{\pi^n$，有：$n \in \mathbb{Z}\}$，其中 π 是 K 的一致化元。后一个作用只有有限多个轨道，我们将其数量记为 $\#(\Lambda\backslash \mathrm{Mod}^{\mathbb{Z}_p[x]})$。

最后，我们定义函数 $V\colon\ \mathcal{O}_K \to \mathbb{R}$（其隐式地依赖于 K），如下：

$$V(x) = \frac{1}{1-p^{-r/e}} \cdot ||\Delta_\sigma(x)|| \cdot \#(\Lambda\backslash \mathrm{Mod}_{\mathbb{Z}_p[x]})$$

其中，e 是 $K/\mathbb{Q}_p$ 的分歧指数。

定理 1.7。固定 $n \geq 1$，并令 K_1、…、K_m 为 $\mathbb{Q}_p$ 的扩张，且 $\sum_{i=1}^m [K_i\colon\ \mathbb{Q}_p] = n$。令 $U \subset \mathcal{O}_{K_1}^{\mathrm{new}} \times \cdots \times \mathcal{O}_{K_m}^{\mathrm{new}}$ 为任意可测集。令 $A \in \mathrm{Mat}_n(\mathbb{Z}_p)$ 为具有相互独立的 *Haar* 分布矩阵元的随机矩阵，并令 $Z_{U,n}$ 表示其位于 U 中的不同且互不共轭的特征值所组成的 m 元组 $(x_1$、…、$x_m)$ 的数量。那么

$$\mathbb{E}[Z_{U,n}] = \int_U \rho^{(n)}_{K_1,\dots,K_m}(x_1,\dots,x_m)dx_1\cdots dx_m,$$

其中

$$\rho^{(n)}_{K_1,\dots,K_m}(x_1,\dots,x_m) = (1-p^{-1})\cdots(1-p^{-n})||\Delta_\sigma(x_1,\dots,x_m)||\prod_{i=1}^m V(x_i) \tag{1.12}$$

并且，积分（以及 U 可测性的定义）均是相对于 $\mathcal{O}_{K_1}\times\cdots\times\mathcal{O}_{K_m}$ 上的 *Haar* 概率测度而言的。

关于二次扩张情形下 $\#(\Lambda\backslash\mathrm{Mod}^{\mathbb{Z}_p[x]})$ 的具体例子，参见命题 9.10。对于 $x \in \mathbb{Q}_p$，它就是 1，因此推论 1.3 立即由定理 1.7 得出。定理 1.7 表明，在推论 1.3 中 $\mathbb{Z}_p$ 上观察到的库仑气体行为，实际上是所有特征值都具有的一般现象，而不仅仅是 $\mathbb{Z}_p$ 中的特征值。范德蒙德项在定理 1.7 的一般情形下同样直接导致特征值排斥，我们将在定理 1.9 中对其进行量化。

从在其他现象（例如 L-函数的零点）中观察随机矩阵统计的角度来看，定理 1.7 的有限-n 分布并不是关键，关键在于 $n \to \infty$极限。在这些极限中，人们预期会看到普适分布；它们不受矩阵元素分布的影响，并且能够刻画随机矩阵理论之外的其他对象。

具体而言，我们希望计算极限$(K_1,\dots,K_m)$-相关函数

$$\rho^{(\infty)}_{K_1,\dots,K_m}(x_1,\dots,x_m) := \lim_{n\to\infty}\rho^{(n)}_{K_1,\dots,K_m}(x_1,\dots,x_m). \tag{1.13}$$

这些函数刻画了在 $x_1,\dots,x_m$ 附近同时出现特征值的渐近概率，因此共同决定了特征值的所有极限局部统计。

1.4. 扩张中特征值的渐近结果 $\mathbb{Q}_p$。**</style}我们已在定理 1.2 中给出了中特征值二点相关的精确公式，下面将给出二次扩张中特征值的类似结果。此结果涉及-相关函数 ()，通常简称为特征值的密度函数**。这不能与概率密度函数混淆；ρ_K 在 $\mathcal{O}_K^{\mathrm{new}}$上的积分通常不等于 1。

定理 1.8。设 $K/\mathbb{Q}_p$ 是一个非分歧二次扩张，$x \in K$ 是一个生成元，使得 $||x|| = 1$，因此 $\mathcal{O}_K = \mathbb{Z}_p[x]$，且 $\mathcal{O}_K$ 中的每个元素都可以唯一地写成 $a_0 + a_1 x$，其中 a_0、$a_1 \in \mathbb{Z}_p$。那么，极限密度函数仅依赖于 $||a_1||$，其表达式为

$$\rho_K^{(\infty)}(a_0 + a_1 x) = \frac{p^{-m}(1 + p^{-1} - 2p^{-m-1})}{1 - p^{-1}} \sum_{k \geq 0} p^{-\frac{(2m+1)k^2 + (4m+1)k}{2}} (1 - p^{-k-1}), \tag{1.14}$$

其中 m 由 $p^{-m} = ||a_1||$定义。

在 K 分歧的情形下，选择 $x \in K$ 为满足 $||x|| = p^{-1/2}$的生成元，则我们有

$$\rho_K^{(\infty)}(a_0 + a_1 x) = ||\operatorname{Disc}_{K/\mathbb{Q}_p}|| \frac{p^{-m}(1 - p^{-m-1})}{1 - p^{-1}} \sum_{k \geq 0} p^{-(m+1)k^2 - (2m+1)k} (1 - p^{-2k-2}) \tag{1.15}$$

对任意满足 $||a_1|| = p^{-m}$的 a_0、$a_1 \in \mathbb{Z}_p$。注意，当 p 为奇数时，项 $||$判别式$_{K/\mathbb{Q}_p}||$ 恰好就是p^{-1}。

由于二次扩张中的特征值 x 成共轭对出现，定理 1.7 中的范德蒙项表明，这一对中的两个特征值通过库仑相互作用彼此作用，因此不太可能彼此相邻。定理 1.8 表明情况确实如此：在非分歧情形下，相关函数展开为

$$\rho_K^{(\infty)}(a_0 + a_1 x) = p^{-m}(1 + O_m(p^{-1})) \tag{1.16}$$

关于 p^{-1}的级数，且 $p^{-m} = ||a_1|| = ||(a_0 + a_1 x) - \sigma(a_0 + a_1 x)||$，其中 σ 是 K的非平凡伽罗瓦自同构。因此，密度函数的主要贡献来自特征值与其共轭之间的库仑排斥。分歧情形也相同，差别仅在于与 m无关的乘法常数。

还要指出，定理 1.8 中的这些级数与定理 1.2 中 θ_3函数的级数公式类似。这三个级数都是常数与“部分 theta 函数” $\theta_P(z;\, t) = \sum_{k \geq 0} t^{k^2/2} z^k$的线性组合；文献中也有对这类函数的研究，参见例如 Warnaar[War03]。与定理 1.2 中的级数不同，定理 1.8 中的级数似乎无法写成乘积形式。

除 $\mathbb{Z}_p$ 和二次扩张的情形外，我们目前还没有精确的代数公式，但可以给出估计。下面的结果表明，在任意域扩张中，范德蒙项以一种直接明了的方式支配着特征值（的伽罗瓦轨道）之间的排斥。

定理 1.9 (正文中的定理 10.1)。设 $\mathcal{U}$ 是与次数为 d的不可约多项式 $F \in \mathbb{F}_p[x]$ 对应的提升子空间。设 x_1、$x_2 \in \mathcal{U}$ 是两个互不相同且不共轭的元素，并设 $\sigma_1(x_1) \ldots, \sigma_\ell(x_1)$ 和 $\sigma_1'(x_2) \ldots, \sigma_r'(x_2)$ 分别是 x_1 和 x_2的完整伽罗瓦轨道。那么，令 K_1、K_2 为 $\mathbb{Q}_p$ 的扩张（可以相同），使得 $x_1 \in K_1^{\text{new}}$、$x_2 \in K_2^{\text{new}}$，则有

$$\rho_{K_1,K_2}^{(\infty)}(x_1, x_2) = \rho_{K_1}^{(\infty)}(x_1) \cdot \rho_{K_2}^{(\infty)}(x_2) \cdot \left(\prod_{\substack{1 \leq i \leq \ell \\ 1 \leq j \leq r}} ||\sigma_i(x_1) - \sigma_j'(x_2)|| \right) \cdot I(x_1, x_2), \tag{1.17}$$

带有误差项

$$\prod_{k=1}^{\infty} (1 - p^{-kd}) < I(x_1, x_2) < \frac{1}{\prod_{k=1}^{\infty} (1 - p^{-kd})}. \tag{1.18}$$

(1.17) 的左侧表示找到两个特征值轨道的概率密度：一个靠近 x_1，另一个靠近 x_2；而右侧的 $\rho_{K_1}^{(\infty)}(x_1)$ 项表示找到一个靠近 x_1 的特征值轨道的概率密度，且与 x_2 附近的情况相互独立；$\rho_{K_2}^{(\infty)}(x_2)$ 也同理。乘积项等价于

x_1 和 x_2 的最小多项式的结式。由于提升子空间是半径为 1 的伽罗瓦共轭开球的并集，该乘积项始终严格小于 1，事实上至多为 p^{-1}。由于误差项 $I(x_1, x_2)$ 约等于 1，同时在 x_1 和 x_2 附近找到特征值轨道的可能性，比假设两处附近的特征值相互独立时更低；这是乘积项所体现的库仑型相互作用导致的。定理 1.1 和 1.9 共同表明，不同提升子空间中的特征值相互独立，而同一提升子空间中的特征值则按照库仑相互作用彼此排斥。

此外，自然也会想知道特征值如何分布到 $\mathbb{Q}_p$ 的扩张中，下面的定理给出了一些答案。

定理 1.10. 对于任意 $n \geq 1$，$A \in$矩阵空间$_n(\mathbb{Z}_p)$ 中具有相互独立的 *Haar* 元素的矩阵，其在 $\mathbb{Z}_p$ 中的特征值的期望数为 1。对于二次扩张 $K/\mathbb{Q}_p$,

$$\lim_{n\to\infty} \mathbb{E}[Z_{\mathcal{O}_K^{\mathrm{new}},n}] = \begin{cases} (1-p^{-1})\sum_{k\geq 0} \dfrac{(1-p^{-k-1})(1+p^{-k^2-2k-3})p^{-\frac{k^2+k}{2}}}{(1-p^{-k^2-2k-2})(1-p^{-k^2-2k-3})} & K \text{ unramified} \\ ||\operatorname{Disc}_{K/\mathbb{Q}_p}||(1-p^{-1})\sum_{k\geq 0} \dfrac{(1-p^{-2k-2})p^{-k^2-k}}{(1-p^{-k^2-2k-2})(1-p^{-k^2-2k-3})} & K \text{ ramified.} \end{cases}$$

此外，设 $K/\mathbb{Q}_p$ 为任意有限扩张，且 p^f 为其剩余域的阶数。那么 $\lim_{n\to\infty} \mathbb{E}[Z_{\mathcal{O}_K^{\mathrm{new}},n}]$ 存在、有限，并满足以下估计

$$\lim_{n\to\infty} \mathbb{E}[Z_{\mathcal{O}_K^{\mathrm{new}},n}] = ||\operatorname{Disc}_{K/\mathbb{Q}_p}|| \cdot \sum_{d|f} \mu\left(\frac{f}{d}\right) p^{d-f} + \mathcal{E}(K). \tag{1.20}$$

这里 μ 是莫比乌斯函数，而误差项 $\mathcal{E}(K)$ 满足以下界

$$-p^{-f}||\operatorname{Disc}_{K/\mathbb{Q}_p}|| < \mathcal{E}(K) < \frac{1+\tau(f)}{1-p^{-f}} p^{-f}||\operatorname{Disc}_{K/\mathbb{Q}_p}|| \tag{1.21}$$

其中 τ 是约数函数。

二次扩张中 $\mathbb{Z}_p$ 的特征值期望数量，是针对 L-函数零点进行数值检验的自然统计量。我们还在推论 9.6 中计算了 $\mathbb{Z}_p$ 中特征值数量的方差。如果人们对相关统计量感兴趣，例如研究二次扩张 K 中位于 0 周围开单位球内、而非闭单位球内的特征值数量，则可以采用与定理 1.10 中公式相同的方法推导出来，即在适当的集合上对定理 1.8 中的相关函数进行积分。我们希望很快能看到对此类 Ellenberg-Jain-Venkatesh 启发式的检验。

注1.11。 还可以考虑由 Haar 测度分布于（乘法）群 GL$_n(\mathbb{Z}_p)$ 上的矩阵，这正是 [EJV11] 最初作为 L-函数零点模型所研究的矩阵。事实上，除了由于可逆性而导致特征值不能位于 0 周围的开单位球内这一限制外，它们的特征值极限相关函数与 Mat$_n(\mathbb{Z}_p)$ 上加性 Haar 测度对应的极限相关函数完全相同；这在定理 7.5 中得到了证明。特别地， [EJV11] 中所考虑的 1 周围开单位球内的特征值，在平移 1 后，与 Mat$_n(\mathbb{Z}_p)$ 中 0 周围开单位球内的特征值具有相同的渐近分布。

第7节中给出的 GL$_n(\mathbb{Z}_p)$ 的有限-n 联合密度公式，也与矩阵空间$_n(\mathbb{Z}_p)$ 的公式几乎完全相同。我们没有写出 GL$_n(\mathbb{Z}_p)$ 的定理 1.10 的对应版本，但用同样的论证，将相同的密度函数在一个稍加限制的集合上积分即可轻松得到。

---

[2]细心的读者可能会注意到，定理 1.9 并未完全证明对排斥不等式

$$\rho^{(\infty)}_{\mathbb{Q}_p[x_1],\mathbb{Q}_p[x_2]}(x_1,x_2) < \rho^{(\infty)}_{\mathbb{Q}_p[x_1]}(x_1)\cdot\rho^{(\infty)}_{\mathbb{Q}_p[x_1]}(x_2) \tag{1.19}$$

当 $p=2$ 且结式为 p^{-1} 时，但我们在定理 10.2 中证明了一个额外的界，以展示此时的 (1.19)。

1.5. **实 Ginibre 情形中的相应结果**。实 Ginibre 系综的历史表明，将特征值分拣到不同扩张中所带来的困难有所增加。对于更简单的实对称矩阵情形，其中所有特征值都自动为实数，联合特征值分布的计算非常简短；Rosenzweig-Porter [RP60] 在这类矩阵作为物理模型被引入的大致同时完成了这一计算。相比之下，对于实 Ginibre 系综，Ginibre [Gin65] 计算了在所有特征值均为实数这一条件下的特征值联合分布（即推论 1.3 的对应结果）；但直到 20 多年后，Lehmann-Sommers [LS91] 才计算出任意数量实特征值对应的特征值联合分布（即定理 1.7 的对应结果）。

值得注意的是，[LS91] 中得到的联合密度与定理1.7的形式完全相同。它们的特点是包含特征值的范德蒙德因子，并乘以对所有特征值取积的某些势函数。当然，这些势函数的形式不同于我们的 $V(x)$，¯；或许更重要的是，$\mathbb{Z}_p$ 与 $\mathbb{C}$ 的几何结构不同，因此产生了截然不同的概率行为。

在 [LS91]中计算出实 Ginibre 系综的联合密度后，人们仍普遍认为，求得相关函数的 $n \to \infty$ 极限公式（例如定理 1.2 的类似结果）是无法解决的问题。然而，几年后，Borodin-Sinclair[BS 09] 和 Forrester-Nagao [FN07] 各自独立地利用 Sinclair[Sin07]的公式计算出了这些公式。这些研究利用了一种不显然的 Pfaff 点过程结构，而我们不知道它是否存在任何 p进类比。在 p进随机矩阵理论中，能否找到行列式点过程结构和 Pfaff 点过程结构的类似形式（如果存在的话），仍是一个令人振奋的开放问题；这些结构在经典随机矩阵理论中发挥了重要作用。

另一个自然的问题是，实 Ginibre 矩阵具有 k 个实特征值的概率。Edel man-Kostlan-Shub [EKS94] 和 Edelman [Ede97], 研究了这个问题；后者还独立地重新推导了 [LS91] 的联合密度。特别是，[Ede97] 证明，所有特征值均为实数的概率恰好为 $2^{-n(n-1)/4}$。在 p-进情形下，我们给出了这一结果的渐近版本，表明其具有相同的指数二次衰减。

定理 1.12. 设 $A \in$ 矩阵空间$_n(\mathbb{Z}_p)$ 服从加性 *Haar* 测度。 n

$$\mathbf{P}(all\ eigenvalues\ of\ A\ lie\ in\ \mathbb{Z}_p) = p^{-\frac{n^2}{2(p-1)} - \frac{1}{2}n\log_p n + O(n)}$$

当 $n \to \infty$ 时，其中隐含常数取决于 p。

定理 1.12 与下文定理 12.1 中 GL$_n(\mathbb{Z}_p)$ 的类似命题一并证明。在有限 n 下，为这些概率找到良好的精确表达式将很有意思；在 p-进情形下，这可类比于 [Ede97] 中实 Ginibre 情形的优美公式。

1.6.**与具有独立系数的** $\mathbb{Z}_p$ 上的随机多项式的关系。 </style}定理 1.10 中关于二次扩张内特征值极限期望数量的级数公式可由定理 1.8 轻松推导。同样，定理 1.2 给出了 $\mathbb{Z}_p$ 中特征值数量方差的公式（推论 9.6）。值得注意的是，在所有这些情形下，公式在代换 $p \leftrightarrow p^{-1}$ 后保持不变。据我们所知，此前尚未有人在 p-进随机矩阵理论中观察到这一现象。不过，Bhargava-Cremona-Fisher-Gajovi´c [BCFG22] 在类似公式中观察到了相同的 $p \leftrightarrow p^{-1}$ 不变性：这些公式给出了具有独立 Haar 分布系数的 $\mathbb{Z}_p$ 上的随机多项式在给定扩张中所含根的期望数量。对于这一情形下的不变性，[BCFG22, Conjecture 1.2], 曾提出一般性猜想，并在同一篇论文中证明了二次扩张、三次扩张以及 $\mathbb{Q}_p$自身的情形；此外，Shmueli [Shm22]还证明了一个更特殊的情形。最终，G-Wei-Yin [GWY23], 运用几何方法解决了一般情形，而该方法最终将问题归结为庞加莱对偶。正如 [GWY23] 所指出的，所用方法相当一般，我们希望它们也能应用于随机矩阵情形。

关于 p-adic 随机多项式的文献，还有几处值得进一步比较。这个课题早于 [BCFG22]: Evans [Eva06], 研究了具有相互独立随机系数的 p-adic 多项式的根，并计算了其期望数量

当多项式具有 Haar 系数时， $\mathbb{Q}_p$ 中的根的数量；Buhler-Goldstein-Moews-Rosenberg[BGMR06], 则计算了所有根都落在 $\mathbb{Q}_p$ 中的概率渐近性，这与定理 1.12 类似（该定理的证明用到了他们的结果）。此后，Kulkarni-Lerario [KL21], 、Ait El Manssour-Lerario [AEML 22], 、上述 [BCFG22],、Shmueli [Shm23],、Caruso [Car22] 等人延续了这一研究方向； [Car22] 的引言对这些进展作了很好的综述。

在这些工作中，与本文最相似的是 [Car22],，它启发了我们证明定理 1.7 的许多部分，我们也借鉴了下文详述的各种技巧。不同相关函数对应 $\mathbb{Q}_p$ 的不同扩张这一现象在该文中同样存在，尽管公式有所不同。具体而言， [Car22, Theorem C]明确计算了定理 1.8 中 $\rho_K^{(\infty)}(x)$的对应结果，得到了 p^{-1} 中的更简单有理函数，而不是级数。 [Car22, TheoremD] 计算了给定扩张中的根的期望数量；当剩余域较大时，得到的渐近结果与定理 1.10 基本相同。

总之，尽管我们得到的极限统计不同，但许多总体现象是相同的——库仑相互作用导致的排斥、每个扩张中的根数渐近有限、距离为 1 的根彼此独立，以及 $p \leftrightarrow p^{-1}$ 不变性——这些现象既出现在随机矩阵的特征值中，也出现在随机多项式的根中。

1.7. 证明方法与论文结构。 证明定理 1.7 是本文的主要技术环节之一，其余内容都是通过取 $n \to \infty$ 极限由此推出的。大多数结果还依赖于对期望行列式的计算，这些计算采用 Sawin-Wood 的矩方法 [SW22], ，但有了这些输入，大多数渐近结果的证明基本上彼此相互独立。一个例外是定理 1.2 和 1.8 中相关函数的精确计算：它们的证明相当相似，并依赖于另一项技术输入，即与分拆上的测度以及随机矩阵的余核相关的马尔可夫链。

在第 2 节给出一些必要的预备知识后，第 3 节和第 4 节几乎全部用于证明定理 1.7。定理 1.7 证明中的关键步骤在第 3 节完成，即计算一个公式（定理 3.1），用于给出集合的 Haar 测度

$$\{A \in \mathrm{Mat}_n(\mathbb{Z}_p) \mid ||P_A(x_i)|| \le p^{-s_i}, \quad \forall 1 \le i \le m\} \tag{1.22}$$

特征多项式 P_A 在点 $x_1, \dots, x_m$ （及其伽罗瓦共轭）处取值较小的矩阵。这些点应被视为特征值的替代，因此，这给出了一个便于处理的集合，可用来刻画特征值接近 $x_1, \dots, x_m$ 及其共轭元的矩阵。这个想法受到 Caruso 关于具有独立同分布系数的多项式之根的工作 [Car22]中对类似集合的讨论启发。

我们发现，(1.22) 中的矩阵可以唯一表示为多项式 $f(A)$，其中 A的特征值恰好为 $x_1, \dots, x_m$ 及其共轭元，并且 f满足某些性质。这引出了对映射

$$\begin{aligned} \mathrm{GL}_n(\mathbb{Q}_p) &\to \mathrm{Mat}_n(\mathbb{Q}_p) \\ U &\mapsto UC(Z)U^{-1} \end{aligned} \tag{1.23}$$

其中 $C(Z)$ 是次数为 n 的首一多项式 Z 的伴随矩阵，该多项式的根为 $x_1, \dots, x_m$。我们关注此映射的像与集合 $\mathrm{Mat}_n(\mathbb{Z}_p) \subset \mathrm{Mat}_n(\mathbb{Q}_p)$ 的交集；我们的 Haar 测度支撑在该集合上。这个交集的测度是一个轨道积分，许多研究都讨论过这类轨道积分。我们使用了若干与轨道积分相关的结果，这些结果见 Yun [Yun13] 的一篇札记。

利用上述全部内容，我们将集合 (1.22) 表示为小块的不交并，通过若干步骤逐次对其进行分解，并记录每一步中这些小块的（有限）数量。最后，我们可以通过线性化并进行李代数计算，求出最小块的测度。这一部分类似于阿基米德随机矩阵文献中通过雅可比计算来求特征值联合密度的方法，不过要复杂得多。

计算出集合 (1.22) 的测度公式后，我们必须让 s_i 变大并取极限，以提取定理 1.7 中的相关函数。这里的策略沿用了 Caruso [Car22] 对随机多项式所采用的方法，而所需工具是其中引入的 p-adic Kac-Rice 公式。这一工作在第 4 节中完成，并由此证明定理 1.7。

我们指出，在所有这些计算中，将特征值元组（x_1，.....，x_m）所在的空间赋予 $E = K_1 \times \cdots \times K_m$上的代数结构非常有用，因为这样一来，该元组本身就是特征多项式的一个根。这种关于 ´étale 代数的观点也曾被用于，例如 [Car22]，以及关于轨道积分的工作中，例如 [Yun13]。

本文余下部分将致力于从定理 1.7 推导出上述渐近结果。除定理 1.12 外，这些结果都依赖于相关函数。它们都源自以下结论；该结论本质上是定理 1.7 的一个推论，但其重要性足以在此完整陈述。

引理 1.13。设 K_1 是 $\mathbb{Q}_p$ 的扩张，K_m 是 $r := \sum_{i=1}^m [K_i : \mathbb{Q}_p]$。对于任意 $n \geq r$，一个具有独立同分布的加性 ***Haar*** 元素的 $n \times n$ 矩阵 A 的特征值（$(K_1$，.....，$K_m)$）相关函数为

$$\rho^{(n)}_{K_1,\ldots,K_m}(x_1,\ldots,x_m) = \prod_{i=0}^{r-1}(1-p^{-n+i}) \cdot ||\Delta_\sigma(x_1,\ldots,x_m)|| \cdot \left(\prod_{i=1}^m V(x_i)\right) \cdot \mathbb{E}||\det(Z(\tilde{A}))||, \quad (1.24)$$

其中 $Z(x) = \prod_{i=1}^m Z_i(x)$ 是 $Z_i \in \mathbb{Z}_p[x]$ 的最小多项式，而 $A \in$ 矩阵空间$_{n-r}(\mathbb{Z}_p)$ 服从加性 ***Haar*** 测度。

它是通过对第 4 节中的定理 1.7 积分消去其余未被 $x_1, \ldots, x_m$ 及其伽罗瓦共轭元计入的 $n-r$ 特征值，并利用定理 1.7 中相关函数的乘积结构推导而来。这一积分产生了$\mathbb{E}||\det(Z(A))||$ 项，它是对这些其他特征值取平均所得。

乍看之下，引理 1.13 似乎并未让计算 A 特征值极限相关函数的问题变得更容易，因为其中出现了另一个随机矩阵 A 的行列式，而该矩阵具有相同的元素分布！然而，行列式的期望比联合特征值分布更容易处理（尽管对于一般的 Z仍然不容易）。

项 $V(x_i)$ 与 n 相互独立，对于较小的扩张，其显式计算相对容易。因此，计算极限特征值统计的难点在于理解 $n \to \infty$ 的 $\mathbb{E}||\det(Z(A))||$ 极限。当 Z 是一次多项式时，计算很常规；但即便是二次多项式（定理 1.2 和 1.8 所需），要进行精确计算也出乎意料地困难，我们付出了巨大努力才得以完成。在定理 1.7 的证明之后，本文剩余的大部分技术工作都致力于理解这类极限。

第一个关键观察是，对于任意非奇异的 $A \in$矩阵空间$_n(\mathbb{Z}_p)$，

$$||\det(A)|| = \frac{1}{\#\operatorname{Cok}(A)}, \quad (1.25)$$

其中 $\operatorname{Cok}(A) = \mathbb{Z}_p^n / A\mathbb{Z}_p^n$ 是余核。余核是一个阿贝尔群（而且，对于 $\operatorname{Cok}(Z(A))$，还具有额外的 $\mathbb{Z}_p[T]/(Z(T))$-模结构），所以先验地它比行列式更复杂。然而，这种额外结构实际上让研究变得更容易。

转向余核会引入一项重要工具：Wood及其合作者已发展出一套通用方法，通过所谓的矩方法处理随机群和模的极限。Wood早期工作的动机 [Woo19、Woo17]是研究余核本身的分布；余核出现在关于随机图的类群和雅可比矩阵的科恩-伦斯特拉启发式中。随后出现了许多关于余核的论文，其中包括大量研究随机矩阵中多项式 $Z(A)$ 的余核的文献，例如 Cheong-Huang [CH21、CH25], Cheong-Kaplan [CK22],Cheong-Liang-Strand [CLS23], 以及 Lee [Lee23]。Sawin-Wood [SW22] 的通用结果为随机模提供了一种矩方法，Cheong-Yu [CH25]将其应用于 $\operatorname{Cok}(Z(A))$。这给出了 $\operatorname{Cok}(Z(A))$ 极限分布的完整答案，不过结果是用某些 Ext 群来表述的，而这些群在实践中可能很难计算

。我们在第5节中使用 [SW22] 和 [CH25] 的这些结果，证明了若干关于期望行列式的结论。关于矩阵多项式余核的文献相对较新，据我们所知，它的出现仅仅是因为这自然推广了具有独立条目的单个矩阵的余核；本工作似乎是它首次应用于另一个问题。

第6节利用这些结果证明极限相关函数 $\rho_{K_1,\dots,K_m}^{(\infty)}$ 的存在性及其基本性质。特别是，定理 1.1 中陈述的独立性（并在定理 6.3 中˜详细给出）可由此从矩方法得出的 $\mathbb{E}||\det(Z(A))||$ 的因式分解性质推导出来。值得明确指出，我们将定理 1.1 列为第一个定理，是因为它是一个富有启发性且足够简单的概率论结论，能帮助阐明后续内容；但从技术层面来看，它并不像本文中的其他一些结果那样新颖或困难。我们几乎是在试图理解一般相关函数的过程中，顺带得出了这一结论；不过，也可以通过稍微扩展 [EJV11]中的论证，直接采用另一种方法证明它。我们的其他结果则并非如此，其所用方法与 [EJV11]的方法相当不同。

第7节具体阐明了注1.11中的主张：$\mathrm{GL}_n(\mathbb{Z}_p)$ 中 Haar 分布元素具有相同的渐近局部统计，唯一的例外是 0 周围的开单位球内没有特征值。我们在该节证明的 $\mathrm{GL}_n(\mathbb{Z}_p)$ 的有限-n 联合分布公式，也与定理 1.7 中的公式非常相似。

为了更深入地理解 $\mathrm{Cok}(Z(A))$，从而精确计算定理 1.2 和 1.8（两者合起来涵盖了 Z 次数为二的情形），我们必须借助另一领域的研究成果。首先要说明的是，Haar 分布的 $A\in \mathrm{Mat}_n(\mathbb{Z}_p)$ 可以通过以下方式生成：先从 $\mathrm{Mat}_n(\mathbb{Z}/p\mathbb{Z})$ 中抽取一个均匀随机矩阵，再将该矩阵均匀随机提升至 $\mathrm{Mat}_n(\mathbb{Z}/p^2\mathbb{Z})$，然后将所得矩阵均匀随机提升至 $\mathrm{Mat}_n(\mathbb{Z}/p^3\mathbb{Z})$，依此类推。群 $\mathrm{Cok}(A)/p^d\mathrm{Cok}(A)$ 仅取决于 $\mathrm{Mat}_n(\mathbb{Z}/p^d\mathbb{Z})$ 中的约化 $A \pmod{p^d}\in$，因此，若按上述方式抽样 A，我们也会逐步抽样得到 $\mathrm{Cok}(A)/p\,\mathrm{Cok}(A)$，$\mathrm{Cok}(A)/p^2\,\mathrm{Cok}(A)$.....。每一步中，我们都可以用一组 d整数 $\lambda_1\geq\ldots\geq\lambda_d\geq 0$ 来参数化 $\mathrm{Cok}(A)/p^d\,\mathrm{Cok}(A)$，其定义如下：

$$\lambda_i=\mathrm{rank}_{\mathbb{F}_p}(p^{i-1}\,\mathrm{Cok}(A)/p^i\,\mathrm{Cok}(A)) \tag{1.26}$$

（由于 $p^{i-1}\mathrm{Cok}(A)/p^i\,\mathrm{Cok}(A)$ 是 p-挠的，因此它是一个 $\mathbb{F}_p$-向量空间）。完整集合 $\lambda_1\geq\lambda_2\geq\ldots$ 是一个整数分拆；对于随机的 A，它是一个随机分拆。我们提到，这些分拆上的测度属于 Borodin-Corwin 开发的所谓 *Macdonald* 过程 这一更广泛框架 [BC14], 例如参见 [VP21],；它们也曾出现在 Fulman 关于有限域上随机矩阵的共轭类的研究中 [Ful02]，不过我们在这里并未用到这两种联系。

一个我们确实用到的、并不显然的事实是，给定 λ_{i+1} 的概率在条件为$\lambda_1,\ldots,\lambda_i$时仅取决于 λ_i，也就是说，这一过程构成一个离散时间马尔可夫链。此外，这个转移概率仅取决于 λ_i，而与 i无关；换言之，$\lambda_1,\lambda_2,\ldots$由非负整数上的齐次递降马尔可夫链生成。这一结果由 Evans 证明[Eva02]。根据该马尔可夫链转移概率的显式描述，计算 $\mathbb{E}[||\det(A)||]$ 非常直接。

然而，对于非线性多项式 $Z(A)$，我们没有这样简单的模 p，p^2，...提升马尔可夫结构。克服这一困难的关键，是定理 5.1˜中利用矩方法证明的一个“线性化”结果。该结果表明，$\lim_{n\to\infty}\mathbb{E}[1/\#\,\mathrm{Cok}(Z(A))]$ 等于若干矩阵余核大小的混合矩：B_1，...，B_m。每个矩阵 B_i的边缘分布均服从 $\mathbb{Q}_p$某个适当扩张上的 Haar 测度，因此其余核具有上述马尔可夫链描述。然而，一般而言，不同 i之间存在相关性，因而会有多个相关联的马尔可夫链副本，它们同步演化若干步后再彼此分离。在 Z 次数为二次的情形下，这些结果可化为单个马尔可夫链副本第 m^{th} 步某些函数的期望；这些期望是对整数 λ_1，λ_2，...，λ_m的 m重求和。

Fulman [Ful01] 早于 [Eva02], 便研究过这一马尔可夫链，研究动机是有限域上的随机矩阵理论。文献 [Ful01]给出了该马尔可夫链的显式对角化，并利用它给出了 Andrews-Gordon 恒等式和 Rogers-Ramanujan 恒等式的概率论证明；前者是 m重、形式相似的求和。利用这种对角化，我们能够将 m重求和化为单重求和，其中 m 作为参数出现，见定理 1.2 和 1.8。

在第 8 节中，我们将介绍本研究背景下的马尔可夫链以及所需的计算引理。在第 9 节中，我们将利用这些内容证明定理 1.2 和 1.8，并利用它们求出 $\mathbb{Z}_p$ 中特征值数量方差的级数表达式（推论 9.6），以及证明定理 1.10 的次数为 2 的部分。

我们计算出的期望，从某种意义上说，是安德鲁斯-戈登恒等式的变形版本；我们不知道，那些看似能够使计算大幅简化的代数奇迹（见注 8.9）是否暗示着某种更深层的理论。对于 Z 次数为 3 以及˜更高的情形，我们可以通过这种方法计算出 $\lim_{n\to\infty}\mathbb{E}[1/\#\mathrm{Cok}(Z(A))]$ 的级数展开中的许多项，但要一般性地理解这些级数的结构似乎十分困难，因此我们将其留待未来研究。

第 10 节涉及定理 1.9 中所给成对排斥估计的证明，以及另一个估计（定理10.2）；当 $p=2$时，需要该估计来确认排斥现象仍然成立。

第 11 节专门证明高次数扩张情形下定理 1.10 的估计。该方法沿用了 [Car22] 处理随机多项式的根的方法，以 [Yun13] 的某些界以及第5节中关于期望行列式的结果作为输入。基本思想是，对于很大一部分特征值元组（即生成相关域扩张的整数环的那些元组），密度函数实际上具有简单的精确形式，而我们可以估计其余特征值元组所产生的相对较小的贡献。

第 12 节涉及定理 1.12 的证明，以及 $\mathrm{GL}_n(\mathbb{Z}_p)$ 的类似结果。这些结果关注的是特征值的一个整体性质，而非局部性质，即它们是否全部位于 $\mathbb{Z}_p$中，因此无法通过任意给定相关函数的渐近性来处理。相反，我们依赖于与独立系数随机多项式之间一种<style id='4'>先验上令人惊讶的联系。由定理 1.7 可立即得到，相关函数

$$\rho^{(n)}_{\mathbb{Q}_p^n}(x_1,\dots,x_n)=\frac{(1-p^{-1})\cdots(1-p^{-n})}{(1-p^{-1})^n}\prod_{1\le i<j\le n}||x_i-x_j|| \tag{1.27}$$

特征值的联合分布具有简单的范德蒙德形式（推论 1.3 即由此得证）。对于一个次数为 n 、系数相互独立且取自 $\mathbb{Z}_p$ 上加性 Haar 测度的首一多项式，其根在 $\mathbb{Q}_p^n$ 上的密度函数具有相同的范德蒙德形式，只是前面没有常数因子（去掉首一条件的情形已在 [Car22] 中证明，我们的证明与之类似）。这种对应使我们能够将随机多项式领域中的渐近性结果移植过来；相关结果早在很久以前就已由 Buhler-Goldstein-Moews-Rosenberg [BGMR06]证明。

致谢。我们感谢 Alexei Borodin、Jordan Ellenberg、Nathan Hayford、Chao Li、Will Sawin、Akshay Venkatesh、Joe Webster 和 Zhiwei Yun 的有益交流与评论。J.S. 获得了美国国家科学基金会资助（DMS-2246576）和西蒙斯研究者资助（929852，首席研究员：Ivan Corwin）。

2. Preliminaries

2.1. 一些一般记号。 以下记号将频繁使用。我们始终固定一个素数 p；除少数另有说明之处外，p 不必是奇数。我们¯将 $||\cdot||$ 记为 $\mathbb{Q}_p$ 上的标准范数，或其在 $\mathbb{Q}_p$任意子域上的限制，并将 $\mathrm{val}(x)=-\log_p(||x||)\in\mathbb{Q}$ 记为 p-进赋值。 K 或 K_i 始终表示 $\mathbb{Q}_p$的有限扩张。

_ $\mathbb{Z}_p$ 表示 $\mathbb{Q}_p$中的闭单位球。我们用 $\mathbf{P}(\cdots)$ 表示概率；除非另有说明，该概率是关于 $\mathrm{Mat}_n(\mathbb{Z}_p)$ 上的加性 Haar 概率测度而言的。 $P_A(x)$ 表示

矩阵 A的特征多项式。 q-Pochhammer 符号为

$$(a;q)_n := \prod_{i=0}^{n-1}(1-aq^i)$$

对于 $n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$。我们常用 RHS(x.yz) 表示方程 (x.yz) 的右端，类似地，用 LHS(x.yz) 表示左端。

许多章节都在该节开头详细说明的特定设定下展开，因此，如果读者跳读正文中的某个结果，却遇到未作解释的记号，我们建议先查看该节的开头。

´2.2. **étale 代数**。 在引言中的讨论里，我们经常遇到扩张元组 $K_1, \ldots, K_m$，它们都在 $\mathbb{Q}_p$ 上。正如我们将看到的，后续章节也会涉及此类元组的代数结构，因此有必要引入 ´étale 代数这一概念。读者还可参阅 [Bou98, Chapter 5.6]或 [Coh12, Chapter 2.1.2] 了解更多信息。

定义 2.1. [Coh12，定义 2.1.2] 有限 ´étale 代数是指在 $\mathbb{Q}_p$ 上有限次的代数 E，其中不含非零幂零元。

在本文余下部分，我们只讨论在 $\mathbb{Q}_p$ 上有限次的 ´étale 代数，而“´étale 代数”一词将始终默认包含这一条件。

命题 2.2. [Coh12，推论 2.1。6] 每个 *´étale* 代数 $E/\mathbb{Q}_p$ 都同构于如下形式之一:

$$E \cong K_1 \times K_2 \times \cdots \times K_m$$

其中 K_1、……、 K_m 是 $\mathbb{Q}_p$ 上的有限域扩张。

此外，给定 $E = K_1 \times \cdots \times K_m$，记

$$E^{\text{new}} := \{\mathfrak{x} = (x_1, \ldots, x_m) \in E \mid \mathbb{Q}_p[\mathfrak{x}] = E\}$$

为 E 中的新 元素，并且 $\mathcal{O}_E^{\text{new}} := \mathcal{O}_E \cap E^{\text{new}}$。给定 $\mathfrak{x} \in E$，当且仅当它的最小多项式（即满足 $f(\mathfrak{x}) = 0$ 的最低次数首一多项式 $f \in \mathbb{Q}_p[x]$ ）的次数等于 $E/\mathbb{Q}_p$的次数时，它才是新的。

值得一提的是，我们也可以将集合 E^{new} 写成

$$E^{\text{new}} = \{\mathfrak{x} = (x_1, \ldots, x_m) \in K_1^{\text{new}} \times \cdots \times K_m^{\text{new}} \mid x_1, \ldots, x_m \text{ lie in distinct Galois orbits}\}.$$

特别地， E^{new} （分别为 $\mathcal{O}_E^{\text{new}}$）将是真子集 $K_1^{\text{new}} \times \cdots \times K_m^{\text{new}}$（分别为 $\mathcal{O}_{K_1}^{\text{new}} \times \cdots \times \mathcal{O}_{新K_m}$），当且仅当至少有一对域 K_i同构。$\mathcal{O}_{K_1} \times \cdots \times \mathcal{O}_{K_m}$带有乘积 Haar 概率测度，关于该测度， $\mathcal{O}_{新E}$ 具有满测度。

我们赋予$E \cong K_1 \times K_2 \times \cdots \times K_m$绝对值 $||\cdot||$，其定义为

$$||(x_1, \ldots, x_m)|| = \max\{||x_1||, \ldots, ||x_m||\} \quad (x_i \in K_i).$$

在这种情况下，我们令 $\mathcal{O}_E = \mathcal{O}_{K_1} \times \mathcal{O}_{K_2} \times \cdots \times \mathcal{O}_{K_m}$为 E的子环，由范数不超过 1 的元素组成。我们定义范数映射 $\text{Nm}^{E/\mathbb{Q}_p}$： $E \to \mathbb{Q}_p$，其定义为

$$\text{Nm}_{E/\mathbb{Q}_p}(x_1, \ldots, x_m) = \text{Nm}_{K_1/\mathbb{Q}_p}(x_1) \cdots \text{Nm}_{K_m/\mathbb{Q}_p}(x_m).$$

$\text{Nm}^{E/\mathbb{Q}_p}(x_1, \ldots, x_m)$ 也等于标量乘法（x_1，……， x_m）的行列式，将其视为 $\mathbb{Q}_p$-向量空间 E上的线性映射。

我们还定义有限 ´étale $\mathbb{Q}_p$-代数 $E = K_1 \times \cdots \times K_m$ 的判别式为 $\text{Disc}^{E/\mathbb{Q}_p} = \text{Disc}^{K_1/\mathbb{Q}_p} \cdots \text{Disc}^{K_m/\mathbb{Q}_p}$。对于所有 $\mathfrak{x} = (x_1, \ldots, x_m) \in E$，定义 $\text{Disc}(\mathfrak{x}) := 0$ 当 $\mathfrak{x}$不属于 E^{new}时，且

$$\text{Disc}(\mathfrak{x}) := \prod_{(i,l_i) \neq (j,l_j)} (\sigma_{i,l_i}(x_i) - \sigma_{j,l_j}(x_j)) = \prod_{i=1}^{m} \text{Nm}_{K_i/\mathbb{Q}_p} Z'(x_i) \in \mathbb{Q}_p$$

当 $\mathfrak{x} \in E^{\text{new}}$ 时。这里，对所有 $1 \leq i \leq m$, $\sigma_{i,1}(x_i) = x_i, \ldots, \sigma_{i,r_i}(x_i)$ 都是 x_i 的伽罗瓦共轭，而 $Z \in \mathbb{Q}_p[x]$ 是 $(x_1, \ldots, x_m)$ 的最小多项式。

对于 $\mathbb{Q}_p$ 上的有限 ´étale 代数 $E = K_1 \times \cdots \times K_m$，我们用 $\mathrm{Aut}_{\mathbb{Q}_p}(E)$ 表示 E 的 $\mathbb{Q}_p$-代数自同构群，并以 $m_E := m$ 表示 E 的域分量数。

命题 2.3. 设 E 是 $\mathbb{Q}_p$ 上的有限 ´*étale* 代数，且 $\mathfrak{x} \in E^{\mathrm{new}}$，使得 $E = \mathbb{Q}_p[\mathfrak{x}]$。那么，每个元素 $\tau \in \mathrm{Aut}_{\mathbb{Q}_p}(E)$ 都可写成如下形式

$$\begin{aligned} \tau : E &\to E \\ f(\mathfrak{x}) &\mapsto f(\mathfrak{y}), \quad f \in \mathbb{Q}_p[x]. \end{aligned} \tag{2.1}$$

其中 $\mathfrak{y} \in E^{\mathrm{new}}$ 与 $\mathfrak{x}$ 具有相同的最小多项式。因此，我们有

$$\#\mathrm{Aut}_{\mathbb{Q}_p}(E) = \#\{\mathfrak{y} \in E^{\mathrm{new}} : \ \mathfrak{x} \text{ 和 } \mathfrak{y} \text{ 在 } \mathbb{Q}_p\text{. 中具有相同的最小多项式}\}$$

证明。一方面，对于所有 $\tau \in \mathrm{Aut}_{\mathbb{Q}_p}(E)$，$\tau(\mathfrak{x})$ 必须与 $\mathfrak{x}$ 具有相同的最小多项式。另一方面，(2.1) 中给出的每个映射 τ 确实都是一个同构。□

当下标可由上下文明确时，我们通常直接写作 $\mathrm{Aut}(E)$。.....的定义

$$||\cdot||, \mathrm{Nm}_{E/\mathbb{Q}_p}, \mathrm{Disc}_{E/\mathbb{Q}_p}, \#\,\mathrm{Aut}(E)$$

不依赖于所选的同一化 $E \cong K_1 \times \cdots \times K_m$。

从现在起，当 $E = K_1 \times \cdots \times K_m$ 时，我们也将用记号 $\rho_E^{(n)}(x_1, \ldots, x_m)$ 或 $\rho_{K_1 \times \cdots \times K_m}^{(n)}(x_1, \ldots, x_m)$ 表示 $\rho_{K_1, \ldots K_m}^{(n)}(x_1, \ldots, x_m)$，并用 $\rho_E^{(\infty)}(x_1, \ldots, x_m)$ 或 $\rho_{K_1 \times \cdots \times K_m}^{(\infty)}(x_1, \ldots, x_m)$ 表示 $\rho_{K_1, \ldots K_m}^{(\infty)}(x_1, \ldots, x_m)$。

2.3. 环 $\mathbb{Z}_p$、提升子空间与结式。

令 $\mathbb{Z}_p = \{y \in \mathbb{Q}_p \mid ||y|| \le 1\}$ 为 $\mathbb{Q}_p$ 上的代数整数环，这是 $A \in \mathrm{Mat}_n(\mathbb{Z}_p)$ 的特征值所在的空间。用 $\{F_1 = x, F_2, \ldots\}$ 表示 $\mathbb{F}_p$ 上首一不可约多项式的集合，并记 $d_i := \deg F_i$。于是 $\mathbb{Z}_p$ 是不交并

$$\bar{\mathbb{Z}}_p = \bigsqcup_{i=1}^{\infty} \mathcal{U}_i, \tag{2.2}$$

其中对于所有的 $i \ge 1$、$\mathcal{U}_i$，F_i上的提升子空间定义为

$$\mathcal{U}_i := \{y \in \bar{\mathbb{Z}}_p \mid \text{the residue of the minimal polynomial of } y \text{ is a power of } F_i\}. \tag{2.3}$$

例如，不可约多项式 $F_1 = x \in \mathbb{F}_p[x]$ 对应于开单位圆盘 $\mathcal{U}_1 = \{y \in \mathbb{Q}_p \mid ||y|| < 1\}$。显然，$\mathcal{U}_1$ 是 $\mathbb{Z}_p$中的唯一极大理想。

引理 2.4。（亨泽尔引理，强形式）设 $Z(x) \in \mathbb{Z}_p[x]$ 为首一多项式，且 $Z(x) \in \mathbb{F}_p[\overline{x}]$ 为 $Z(x)$的剩余。假设存在一个分解

$$\overline{Z}(x) = \overline{Z}_1(x)\overline{Z}_2(x),$$

其中 $\overline{Z}_1(x)$ $\overline{Z}_2(x) \in \mathbb{F}_p[x]$ 互素。那么 $Z(x)$ 可作如下分解

$$Z(x) = Z_1(x)Z_2(x),$$

使得 $Z_1(\overline{x})$ 是 $Z_1(x)$的剩余，而 $Z_2(x)$ 是 $Z_2(\overline{x})$的剩余。

证明。参见 [Neu13，定理 II.4.6]。□

现在，假设

$$Z_1(x) = a_{r_1}x^{r_1} + a_{r_1-1}x^{r_1-1} + \cdots + a_0, \quad Z_2(x) = b_{r_2}x^{r_2} + b_{r_2-1}x^{r_2-1} + \cdots + b_0 \in \mathbb{Z}_p[x]$$

分别为次数 r_1, r_2 非零的多项式。记 $x_{i,1}, \ldots, x_{i,r_i}$ 为 Z_i 的根，其中 $i = 1,2$（注意，根可能不属于 $\mathbb{Z}_p$）。那么这两个多项式 $Z_1(x)$ $Z_2(x)$ 的结式，记作 $\mathrm{Res}(Z_1, Z_2)$，定义为

$$\mathrm{Res}(Z_1, Z_2) = a_{r_1}^{r_2} b_{r_2}^{r_1} \prod_{l_1=1}^{r_1} \prod_{l_2=1}^{r_2} (x_{1,l_1} - x_{2,l_2}) \in \mathbb{Z}_p.$$

我们进一步定义 $\mathrm{Res}(Z_1,0) = \mathrm{Res}(0,Z_2) = 0$。结式描述了两个多项式的根之间的距离。它满足一些基本性质，我们不加证明地列出如下。

命题 2.5. 设 $Z_1, Z_2, Z_3 \in \mathbb{Z}_p[x]$。则结果式具有以下性质：

(1) $\mathrm{Res}(Z_1,Z_2) = \mathrm{Res}(Z_2,Z_1)$。*(2)* $\mathrm{Res}(Z_1,Z_2) = 0$ 当且仅当它们有一个公共根。*(3)* $\mathrm{Res}(Z_1Z_2,Z_3) = \mathrm{Res}(Z_1,Z_3)\,\mathrm{Res}(Z_2,Z_3)$。

(4) 若 是首一的，则 $\mathrm{Res}(Z_1,Z_3) = \mathrm{Res}(Z_1 - Z_2Z_3, Z_3)$。

命题 2.6. 设 $Z_1 \in \mathbb{Z}_p[x]$ 为首一多项式，且 $Z_2 \in \mathbb{Z}_p[x]$具有非零剩余。此外，假设 Z_1 的剩余是 F_i 的幂，且其次数为 d_i。那么我们有

$$||\operatorname{Res}(Z_1,Z_2)|| = p^{-kd_i},$$

其中 $k \geq 0$ 是一个整数。特别地，当且仅当 $F_i \nmid Z_2$ (模 p) 时，$k = 0$。

证明。我们先说明 Z_2 的剩余不能被 F_i 整除的情形。在这种情况下，在剩余域上应用欧几里得算法，可得存在 $f_1(x)$ $f_2(x) \in \mathbb{Z}_p[x]$，使得

$$f_1(x)Z_1(x) + f_2Z_2(x) \in 1 + p\mathbb{Z}_p[x].$$

因此，对于 Z_1 的任意根 x_1，我们有 $||f_2(x_1)Z_2(x_1)|| = 1$。由于 $||f_2(x_1)||$，$||Z_2(x_1)|| \leq 1$，我们必有 $||f_2(x_1)|| = ||Z_2(x_1)|| = 1$。因此，我们有

$$||\operatorname{Res}(Z_1,Z_2)|| = \prod_{x_1} ||Z_2(x_1)|| = 1,$$

其中乘积遍历 Z_1 的所有根 x_1。

接下来，假设 Z_2 的剩余可被 F_i 整除。我们只需验证结式 $||\mathrm{Res}(Z_1,Z_2)||$ 的绝对值是 p^{-d_i} 的正整数幂。证明方法是对 $\deg Z_1$ 使用归纳法。若 $\deg Z_1 = d_i$，则可写成 $Z_2 = Z_3Z_1 + p^kZ_4$，其中$Z_3 \in \mathbb{Z}_p[x]$、$k \geq 1$，且 $Z_4 \in \mathbb{Z}_p[x]$ 的次数为 $\leq d_i - 1$，其剩余非零。在这种情况下，应用命题 2.5 得

$$\begin{aligned} ||\operatorname{Res}(Z_1,Z_2)|| &= ||\operatorname{Res}(Z_1,Z_3Z_1 + p^kZ_4)|| \\ &= ||\operatorname{Res}(Z_1,p^kZ_4)|| \\ &= p^{-kd_i}||\operatorname{Res}(Z_1,Z_4)|| \\ &= p^{-kd_i}. \end{aligned} \tag{2.4}$$

这里，最后一行成立是因为 Z_4 的剩余不可被 F_i 整除。

现在我们假设当 $\deg Z_1 \leq (n-1)d_i$ 时该断言已得到证明，并证明当 $\deg Z_1 = nd_i$ 时该断言成立。根据引理 2.4，我们有分解 $Z_2 = Z_3Z_4$，其中 $Z_3 \in \mathbb{Z}_p[x]$ 是首一的，其剩余是 F_i 的幂，且 $Z_4 \in \mathbb{Z}_p[x]$ 的剩余不可被 F_i 整除。于是有

$$||\operatorname{Res}(Z_1,Z_2)|| = ||\operatorname{Res}(Z_1,Z_3)|| \cdot ||\operatorname{Res}(Z_1,Z_4)|| = ||\operatorname{Res}(Z_1,Z_3)||.$$

如果 $\deg Z_3 < \deg Z_1 = nd_i$，那么将 Z_1 与 Z_3 互换，根据归纳假设即可得证。如果 $\deg Z_3 \geq \deg Z_1$，那么我们可以写成 $Z_3 = Z_4Z_1 + p^kZ_5$，其中 $Z_4 \in \mathbb{Z}_p[x]$、$k \geq 1$，以及次数为 $\leq nd_i - 1$ 且剩余非零的 $Z_5 \in \mathbb{Z}_p[x]$。应用命题 2.5，得到

$$\begin{aligned} ||\operatorname{Res}(Z_1,Z_3)|| &= ||\operatorname{Res}(Z_1,Z_4Z_1 + p^kZ_5)|| \\ &= ||\operatorname{Res}(Z_1,p^kZ_5)|| \\ &= p^{-nkd_i}||\operatorname{Res}(Z_1,Z_5)||. \end{aligned} \tag{2.5}$$

再次由引理 2.4，得 $Z_5 = Z_6Z_7$，其中 $Z_6 \in \mathbb{Z}_p[x]$ 是首一的，且其剩余是 F_i 的幂，而 $Z_7 \in \mathbb{Z}_p[x]$ 的剩余不能被 F_i 整除。因此，

$$||\operatorname{Res}(Z_1,Z_3)|| = p^{-nkd_i}||\operatorname{Res}(Z_1,Z_5)|| = p^{-nkd_i}||\operatorname{Res}(Z_1,Z_6)||,$$

根据关于 $\deg Z_6$ 的归纳假设，它必定是 p^{-d_i} 的正幂。 □

下面的命题直观地指出， $\mathbb{Z}_p$ 中的两个元素当且仅当它们落在同一个提升子空间中时彼此接近。这是命题 2.6 的直接推论，因此此处略去证明。

命题 2.7。 设 $x_1 \in \mathcal{U}_i$、 $x_2 \in \mathcal{U}_j$ 和 $Z_1(x)$ $Z_2(x)$ 分别表示 x_1、 x_2 的最小多项式。则有：

(1) 若 $i \neq j$，则 $||\mathrm{Res}(Z_1, Z_2)|| = 1$。*(2)* 若 $i = j$，则 $||\mathrm{Res}(Z_1, Z_2)|| = p^{-kd_i}$，其中 $k \geq 1$ 是一个整数。

命题 2.8。 设我们有一个首一 $Z(x) \in \mathbb{Z}_p[x]$ ，其剩余 $F(x) \in \mathbb{F}_p[x]$ 不可约，因此 $Z(x)$ 也不可约。设 $d =$ 次数 F，并设

$$\sigma_1(x), \ldots, \sigma_d(x)$$

是 Z的根。这里， x 是 Z的根，且 $\sigma_1 = \mathrm{id}. . . , \sigma_d \in \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)$。那么，对所有 $1 \leq j < k \leq d$，我们有 $||\sigma_j(x) - \sigma_k(x)|| = 1$。

证明。 我们只需证明 $Z(x)$的判别式属于 $\mathbb{Z}_p^\times$。这等价于说明 $F(x)$的判别式非零。由于 $F(x)$没有重根，故得证。□

命题 2.9。 设 $F_i \in \mathbb{F}_p[x]$ 是首一且不可约的， $\mathcal{U}_i$ 是与 F_i对应的提升子空间。设 $Z_i \in \mathbb{Z}_p[x]$ 是首一的，其剩余为 F_i。设 $d_i = \deg F_i$，并令

$$\sigma_{i,1}(x_i), \ldots, \sigma_{i,d_i}(x_i)$$

是 Z_i的根。那么， $\mathcal{U}_i$ 可以写成如下不交并

$$\mathcal{U}_i = \bigsqcup_{j=1}^{d_i} (\sigma_{i,j}(x_i) + \mathcal{U}_1). \tag{2.6}$$

证明。 回顾强三角不等式并应用命题 2.8，我们知道 (2.6) 中的并确实是不交的。

($\subset$)：设 $x_i' \in \mathcal{U}_i$。记 $Z_{i'}$ 为 x_i'的最小多项式。应用命题 2.7，得到 $||\mathrm{Res}(Z_i, Z_{i'})|| < 1$，且 $\mathrm{Res}(Z_i, Z_{i'})$ 是 $Z_i(x_i')$ 的伽罗瓦共轭元之积，因此可推出 $||Z_i(x_i')|| = \prod_{j=1}^{d_i} ||\sigma_{i,j}(x_i) - x_i'|| < 1$。因此，存在 $1 \leq j \leq d_i$ 使得$||\sigma_{i,j}(x_i) - x_i'|| < 1$，且 $x_i' \in \sigma_{i,j}(x_i) + \mathcal{U}_1$。

($\supset$)：取 $y \in \mathcal{U}_1$，使得 $||y|| < 1$。记

$$\sigma_1(y), \ldots, \sigma_r(y)$$

为 y 的所有伽罗瓦共轭元。那么该多项式的剩余

$$\prod_{1 \leq j \leq d_i} \prod_{1 \leq l \leq r} (x - \sigma_{i,j}(x_i) - \sigma_l(y)) = \prod_{1 \leq l \leq r} Z_i(x - \sigma_l(y))$$

等于 于 $Z_i(x)^r = F_i^r$。因此，对于所有 $1 \leq j \leq d_i$ 和 $y \in \mathcal{U}_1$，都有 $\sigma_{i,j}(x_i) + y \in \mathcal{U}_i$. □

注 2.10. 选取多项式 Z_i 及其根 x_i 的方法并不唯一，但总会得到与上文相同的不交并分解。因此，从现在起，我们将用 $\mathcal{U}_{i,j}$ 表示 (2.6) 中的集合 $\sigma_{i,j}(x_i)+\mathcal{U}_1$ ，其中 x_i 将隐式选取。由于伽罗瓦群在这些部分上具有传递作用，我们可以推知，落在每个 $\mathcal{U}_{i,j}, 1 \leq j \leq d_i$ 内的特征值数量必须相等。事实上，任何其他（伽罗瓦不变的）特征值统计量在所有圆盘 $\mathcal{U}_{i,j}$上都相同，因为任一圆盘 $\mathcal{U}_{i,j}$ 中的特征值都与 $\mathcal{U}_{i,1}$中的特征值共轭。

3. Explicit joint CDF of characteristic polynomial values at multiple points

本节中，我们将采用以下设定。令

(1) $E = K_1 \times K_2 \times \cdots \times K_m$ 是 $\mathbb{Q}_p$上的有限 ´étale 代数，其作为$\mathbb{Q}_p$-向量空间的维数为 r。这里，对于所有 $1 \le i \le m$， $K_i/\mathbb{Q}_p$ 都是次数为 r_i的有限域扩张，其中 $r_1 + \cdots + r_m = r$。(2) $\mathfrak{x} = (x_1, \ldots, x_m) \in \mathcal{O}_E^{\mathrm{new}}$，使得对于所有 $1 \le i \le m$，$x_i \in \mathcal{O}_{K_i}^{\mathrm{new}}$，且 $E = \mathbb{Q}_p[\mathfrak{x}]$。(3) π_i 是 $\mathcal{O}_{K_i}$的一个一致化元，使得 $\pi_i\mathcal{O}_{K_i}$ 是 $\mathcal{O}_{K_i}$的唯一极大理想。(4) $\Lambda_E = \prod_{i=1}^m \pi_i^{\mathbb{Z}} \subset E^\times$ 是与 $\mathcal{O}_E^\times = \mathcal{O}_{K_1}^\times \times \cdots \times \mathcal{O}_{K_m}^\times$互补的自由 $\mathbb{Z}$-模。(5) $\Lambda_{K_i} = \pi_i^{\mathbb{Z}} \subset K_i^\times$是与 $\mathcal{O}_{K_i}^\times$互补的自由 $\mathbb{Z}$-模，使得 $\Lambda_E = \prod_{i=1}^m \Lambda_{K_i}$。(6) L_i 是 $K_i/\mathbb{Q}_p$的正规闭包。(7) $\sigma_{i,1}(x_i) = x_i, \ldots, \sigma_{i,r_i}(x_i)$ 是 L_i中 x_i 的共轭元，其中$\sigma_{i,1} = \mathrm{id} \ldots, \sigma_{i,r_i} \in \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)$

(8) $Z_i(x)$ 是 x_i 的最小多项式，其次数为 r_i。由于元素 x_1、……， x_m在伽罗瓦自同构作用下属于不同的轨道，因此多项式 Z_1、……， Z_m 互不相同。(9) $Z(x) = \prod_{i=1}^m Z_i(x)$，它是次数为 $r = r_1 + \cdots + r_m$ 的首一多项式。(10) e_i 是扩张 $K_i/\mathbb{Q}_p$ 的分歧指数，因此 $\#(\mathcal{O}_{K_i} : \pi_i\mathcal{O}_{K_i}) = p^{r_i/e_i}$。(11) $\mathbf{P}(\cdots)$ 是矩阵空间 $\mathrm{Mat}_r(\mathbb{Z}_p)$ 上的（可加）Haar 概率测度。

本节旨在证明以下结果。粗略地说，它计算了一个 $r \times r$ 矩阵的特征多项式在给定的一组 r 点处取极小值的概率。事实证明，这一结果涵盖了证明定理 1.7 所需的大部分工作，因为特征值必须非常接近这些 r 点。

定理 3.1。 假设 $A \in$ 矩阵空间$_r(\mathbb{Z}_p)$ 服从 *Haar* 分布。那么对于所有满足 $s_i > r \operatorname{val}\mathrm{Disc}(\mathfrak{x})$ 的元组 $s = (s_1, \ldots, s_m) \in (\frac{1}{e_1}\mathbb{N}, \ldots, \frac{1}{e_m}\mathbb{N})$，只要对所有 $1 \le i \le m$，我们都有

$$\prod_{i=1}^m p^{s_i r_i} \cdot \mathbf{P}(\operatorname{val} P_A(x_i) \ge s_i, \forall 1 \le i \le m) = \frac{(1-p^{-1})\cdots(1-p^{-r})}{||\Delta_\sigma(x_1, \ldots, x_m)||} \prod_{i=1}^m V(x_i), \tag{3.1}$$

其中 Δ_σ 和 V 的定义见定义 *1.5* 和 *1.6*。

3.1. 证明概要。 在定理 3.1 中，我们希望计算集合的测度

$$\{A \in \mathrm{Mat}_r(\mathbb{Z}_p) \mid \operatorname{val}(P_A(x_i)) \ge s_i, \quad \forall 1 \le i \le m\}. \tag{3.2}$$

回顾第 1.7 节中的概述；现在我们来更具体地说明。令

$$\mathcal{X} = \{A \in \mathrm{Mat}_r(\mathbb{Z}_p) \mid P_A = Z\}, \tag{3.3}$$

可以将 (3.2) 视为与 $\mathcal{X}$“接近”的矩阵集合，其中“接近”完全根据特征多项式来定义。首先，我们在命题 3.3 中证明，(3.2) 中的矩阵可以唯一地表示为 $A = f(A_0)$，其中 $A_0 \in \mathcal{X}$，且 $f \in \mathbb{Z}_p[x]$ 是一个“只让矩阵稍微移动一点”的多项式。更准确地说， f 属于以下集合。

定义 3.2。 令 $s = (s_1, \ldots, s_m) \in (\frac{1}{e_1}\mathbb{N}, \ldots, \frac{1}{e_m}\mathbb{N})$，使得对于所有$1 \le i \le m$都有 $s_i > r \operatorname{val}\mathrm{Disc}(\mathfrak{x})$。记

$$F_{Z,s} := \{f \in \mathbb{Z}_p[x] \mid \deg f \le r-1, \operatorname{val}(f(x_i) - x_i) + \operatorname{val} Z'(x_i) \ge s_i \text{ for all } 1 \le i \le m\}. \tag{3.4}$$

当 $s_1, \ldots, s_m$可由上下文明确推出时，我们将 $F_{Z,\,s}$简写为 F_Z。

命题 3.3。 令 $s = (s_1, \ldots, s_m) \in (\frac{1}{e_1}\mathbb{N}, \ldots, \frac{1}{e_m}\mathbb{N})$，使得对于所有$1 \le i \le m$都有 $s_i > r \operatorname{val}\mathrm{Disc}(\mathfrak{x})$，并令 $F_Z = F_{Z,\,s}$ 如定义 *3.2* 中所述。则映射

$$\begin{aligned} \{(f, A_0) \mid A_0 \in \mathcal{X}, f \in F_Z\} &\to \{A \in \mathrm{Mat}_r(\mathbb{Z}_p) \mid \operatorname{val}(P_A(x_i)) \ge s_i, \quad \forall 1 \le i \le m\} \\ (f, A_0) &\mapsto f(A_0) \end{aligned} \tag{3.5}$$

是一个双射。

由于 f 是多项式，因此

$$f(TA_0T^{-1}) = Tf(A_0)T^{-1}, \tag{3.6}$$

命题 3.3 表明，研究 $\mathcal{X}$ 中在共轭作用下的轨道是很自然的。若允许由所有 $\mathrm{GL}_r(\mathbb{Q}_p)$ 中的元素进行共轭，根据有理标准形，只有一个轨道，其代表元是 Z 的伴随矩阵 $C(Z)$（见定义 3.8）。然而，该轨道 $\{TC(Z)T^{-1}:\ T\in \mathrm{GL}_r(\mathbb{Q}_p)\}$ 并不包含于 $\mathrm{Mat}_r(\mathbb{Z}_p)$ 中，因此它比我们的集合 $\mathcal{X}$ 更大。

因此，考虑由更小的群 $\mathrm{GL}_r(\mathbb{Z}_p)$ 进行共轭所得到的轨道更为自然；这些轨道自然会包含于 $\mathrm{Mat}_r(\mathbb{Z}_p)$ 中。这些轨道的结构更为复杂。然而，事实证明（推论 3.21），对这些轨道进行参数化的自然方式是使用模的集合

$$\mathrm{Mod}_{\mathbb{Z}_p[\mathfrak{x}]} = \{M \subset E \mid M \text{ is a } \mathbb{Z}_p[\mathfrak{x}]\text{-module, also a } \mathbb{Z}_p\text{-lattice of rank } r\}, \tag{3.7}$$

或者更确切地说，使用在标量乘法下的商集 $E^\times\backslash \mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$，这与类群类似。这种参数化在轨道积分的相关文献中已经得到了理解

$$\int_{\mathrm{GL}_r(\mathbb{Q}_p)} \mathbb{1}_{gC(Z)g^{-1}\in \mathrm{Mat}_r(\mathbb{Z}_p)} dg$$

例如 [Yun13], ，但我们会自成一体地阐述所需内容（不过，在证明参数化之后，我们会不加证明地使用 [Yun13] 中关于上述类群类似物的某些结论）。

这使得集合 (3.2) 成为以下集合的不交并

$$\{Tf(A_{\mathcal{C}})T^{-1} \mid T \in \mathrm{GL}_r(\mathbb{Z}_p), f \in F_Z\} \tag{3.8}$$

其中 $A_{\mathcal{C}}$ 是某些代表矩阵，因此问题归结为计算这些集合的测度。

(3.8) 中的集合还可以进一步分解为有限个集合的平移（通过共轭）

$$\{(I_r+\Delta T)f(A_{\mathcal{C}})(I_r+\Delta T)^{-1} \mid \Delta T \in p^{\mathcal{M}}\,\mathrm{Mat}_r(\mathbb{Z}_p), f \in F_Z\}, \tag{3.9}$$

这些集合的测度都相同。这将在引理 3.22 和命题 3.23 中完成。

(3.9) 中的矩阵 ΔT 很小，而 (3.9) 中的集合可以利用李括号的像，以线性方式明确描述，见引理 3.26 和引理 3.28。根据这一描述，我们在命题 3.27 中计算其测度。

3.2. **命题 3.3 的证明**。 我们先证明命题 3.3 所需的结果。下面的引理将克拉斯纳引理 [Kra46b] 推广到 ´étale 代数的情形，其基本含义是，任何一个由接近于 $(x_1,\dots,x_m)$ 的元素组成的序列 $(\tilde{x}_1,\dots,\tilde{x}_m)$，都具有与 $(x_1,\dots,x_m)$ 类似的度量和代数性质。

引理 3.4。 设我们有一个元素序列

$$\tilde{\mathfrak{x}} = (\tilde{x}_1,\dots,\tilde{x}_m), \quad \tilde{x}_1,\dots,\tilde{x}_m \in \bar{\mathbb{Q}}_p,$$

使得对所有 $1\le i\le m$，均有 $||x_i-\tilde{x}_i|| < ||\mathrm{Disc}(\mathfrak{x})||$。那么

(1) 对所有满足 $(i,l_i)\neq(j,l_j)$ 的不同自同构对 $\sigma_{i,l_i},\sigma_{j,l_j}$，均有 e

$$||\sigma_{i,l_i}(\tilde{x}_i)-\sigma_{j,l_j}(\tilde{x}_j)|| = ||\sigma_{i,l_i}(x_i)-\sigma_{j,l_j}(\tilde{x}_j)|| = ||\sigma_{i,l_i}(x_i)-\sigma_{j,l_j}(x_j)||.$$

(2) 这些元素

$$\sigma_{1,1}(\tilde{x}_1),\dots,\sigma_{1,r_1}(\tilde{x}_1),\dots,\sigma_{m,1}(\tilde{x}_m),\dots,\sigma_{m,r_m}(\tilde{x}_m)$$

两两不同。

(3) 对所有的 $1\le i\le m$，我们有 $\mathbb{Q}_p[\tilde{x}_i]\supset\mathbb{Q}_p[x_i]$。此外，我们有 $\mathbb{Q}_p[\tilde{\mathfrak{x}}]\supset E=\mathbb{Q}_p[\mathfrak{x}]$.

证明。 首先，注意对于每一对 $(i,l_i)\neq(j,l_j)$，

$$||x_j-\tilde{x}_j||<||\operatorname{Disc}(\mathfrak{x})||\leq||\sigma_{i,l_i}(x_i)-\sigma_{j,l_j}(x_j)||, \tag{3.10}$$

其中，第一个不等式由假设得出，第二个不等式是因为 $||\operatorname{Disc}(\mathfrak{x})||$ 是若干因子 ≤ 1 的乘积，其中一个因子是 $||\sigma_{i,\,l_i}(x_i)-\sigma_{j,\,l_j}(x_j)||$。换言之，$x_j$ 比 $\tilde{x}_j$ 更近，而不是更接近它的任何一个伽罗瓦共轭元或其他 $x_i,\ i\neq j$ 的伽罗瓦共轭元。由于伽罗瓦自同构 $\sigma_{j,\,l_j}$ 不会影响 (3.10) 左边的距离，我们有

$$||\sigma_{j,l_j}(x_j)-\sigma_{j,l_j}(\tilde{x}_j)||<||\sigma_{i,l_i}(x_i)-\sigma_{j,l_j}(x_j)||. \tag{3.11}$$

由于 $||a+b||=||a||$ 当 $||a||>||b||$ 时，这意味着

$$\begin{aligned}||\sigma_{i,l_i}(x_i)-\sigma_{j,l_j}(\tilde{x}_j)||&=||\sigma_{i,l_i}(x_i)-\sigma_{j,l_j}(x_j)+\sigma_{j,l_j}(x_j)-\sigma_{j,l_j}(\tilde{x}_j)||\\&=||\sigma_{i,l_i}(x_i)-\sigma_{j,l_j}(x_j)||,\end{aligned} \tag{3.12}$$

这严格大于 $||x_i-\tilde{x}_i||=||\sigma_{i,\,l_i}(x_i)-\sigma_{i,\,l_i}(\tilde{x}_i)||$，由 (3.10) 可知。因此我们也有

$$\begin{aligned}||\sigma_{i,l_i}(\tilde{x}_i)-\sigma_{j,l_j}(\tilde{x}_j)||&=||\sigma_{i,l_i}(\tilde{x}_i)-\sigma_{i,l_i}(x_i)+\sigma_{i,l_i}(x_i)-\sigma_{j,l_j}(\tilde{x}_j)||\\&=||\sigma_{i,l_i}(x_i)-\sigma_{j,l_j}(\tilde{x}_j)||.\end{aligned} \tag{3.13}$$

结合 (3.12) 和 (3.13) 即可证明 (1)。

接下来，对于所有 $(i,\ l_i)\neq(j,\ l_j)$，我们有 $||\sigma_{i,\,l_i}(\tilde{x}_i)-\sigma_{j,\,l_j}(\tilde{x}_j)||=||\sigma_{i,\,l_i}(x_i)-\sigma_{j,\,l_j}(x_j)||>0$。这就证明了 (2)。

最后，根据 (2)，对于所有满足 $\sigma(x_i)\neq x_i$ 的 $\sigma\in\operatorname{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)$，我们有 $\sigma(\tilde{x}_i)\neq\tilde{x}_i$。取逆否命题，对于每个 $\sigma\in\operatorname{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)$，$\sigma(\tilde{x}_i)=\tilde{x}_i$ 蕴含 $\sigma(x_i)=x_i$。因此 $\operatorname{Gal}(\mathbb{Q}_p/\mathbb{Q}_p[\tilde{x}_i])\subseteq\operatorname{Gal}(\mathbb{Q}_p/\mathbb{Q}_p[x_i])$，这意味着 $\mathbb{Q}_p[\tilde{x}_i]\supset\mathbb{Q}_p[x_i]$。

此外，对于每个 $\sigma\in\operatorname{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)$ 和 $1\leq i\leq m$，我们都有 $\sigma(x_i)=\sigma_{i,l_i}(x_i)$，其中某个 $1\leq l_i\leq r_i$。因此，对于所有 $j\neq i$，

$$\begin{aligned}||\sigma(\tilde{x}_i)-\sigma_{i,l_i}(x_i)||&=||\sigma(\tilde{x}_i)-\sigma(x_i)||\\&=||\tilde{x}_i-x_i||.\end{aligned} \tag{3.14}$$

由 (3.10)，令 i,j 反向，且令 σ_{j,l_j} 为 id，可得

$$\begin{aligned}\text{RHS}(3.14)&<||x_j-\sigma_{i,l_i}(x_i)||\\&=||x_j-\sigma_{i,l_i}(x_i)+\tilde{x}_j-x_j||\\&=||\tilde{x}_j-\sigma_{i,l_i}(x_i)||,\end{aligned} \tag{3.15}$$

最后一行用到了强三角不等式，以及事实 $||\tilde{x}_j-x_j||\lhd||x_j-\sigma_{i,l_i}(x_i)||$；后者同样由 (3.10) 得出。

因此，$\sigma(\tilde{x}_i)$ 和 $\tilde{x}_j$ 到 $\sigma_{i,l_i}(x_i)$ 的距离不同，所以特别地 $\sigma(\tilde{x}_i)\neq\tilde{x}_j$。由于这一断言对所有 $i\neq j$ 和 $\sigma\in\operatorname{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)$ 都成立，$\tilde{x}_1,\dots,\tilde{x}_m$ 的最小多项式彼此不同，并且

$$\mathbb{Q}_p[\tilde{\mathfrak{x}}]=\mathbb{Q}_p[\tilde{x}_1]\times\cdots\times\mathbb{Q}_p[\tilde{x}_m]\supset\mathbb{Q}_p[x_1]\times\cdots\times\mathbb{Q}_p[x_m]=E=\mathbb{Q}_p[\mathfrak{x}],$$

证明（3）。 □

下面引理的目的是说明：如果次数小于 $r-1$ 的多项式 f 在每个 $x_i,1\leq i\leq m$ 上的取值都很小，那么 f 的所有系数都很小。

推论 3.5。 设 $f(x)\in\mathbb{Q}_p[x]$ 的次数为 $\leq r-1$，$u\in\mathbb{R}$，且对所有 $1\leq i\leq m$，赋值 $f(x_i)$ – 赋值 $Z'(x_i)\geq u$。则 $f(x)$ 的系数的赋值都为 $\geq u$。

证明。 由于 u 同时出现在假设和结论中，如果我们证明对某个 k，p^kf 成立，那么对 f 也成立。因此，不失一般性，我们可以假设 $u>r\operatorname{val}\operatorname{Disc}(\mathfrak{x})$。考虑 $Z(x)=Z(x)+f(x)$ 的根，它是一个次数为 r 的首一多项式。对于任意固定的 $1\leq i\leq m$，Z 的 r 个根到 x_i 的 r 距离。这些距离的乘积恰好为

$$||\tilde{Z}(x_i)||=||f(x_i)||\leq||Z'(x_i)||p^{-u}\leq p^{-u}<||\operatorname{Disc}(\mathfrak{x})||^r.$$

˜因此，我们可以找到 Z的一个根 $\tilde{x}_i$，使得 $||\tilde{x}_i - x_i|| < ||\operatorname{Disc}(\mathfrak{x})||$。由于对所有 $1 \le i \le m$都存在这样的 $\tilde{x}_i$，我们可以应用引理 3.4 的 (2)，推出这些根

$$\sigma_{1,1}(\tilde{x}_1), \dots, \sigma_{1,r_1}(\tilde{x}_1), \dots, \sigma_{m,1}(\tilde{x}_m), \dots, \sigma_{m,r_m}(\tilde{x}_m)$$

都是不同的 ˜异的，因此必定是多项式 Z 的所有根。此外，对于所有 $1 \le i \le m$，我们有

$$\begin{aligned} \operatorname{val}(x_i - \tilde{x}_i) &= \operatorname{val} \tilde{Z}(x_i) - \sum_{(j,l_j)\neq(i,1)} \operatorname{val}(x_i - \sigma_{j,l_j}(\tilde{x}_j)) \\ &= \operatorname{val} \tilde{Z}(x_i) - \sum_{(j,l_j)\neq(i,1)} \operatorname{val}(x_i - \sigma_{j,l_j}(x_j)) \\ &= \operatorname{val} f(x_i) - \operatorname{val} Z'(x_i) \\ &\ge u. \end{aligned} \tag{3.16}$$

˜这里第二个等式来自引理 3.4 的 (1)，第三个等式则是因为 $Z(x_i) = f(x_i)$，因为 x_i 是 Z 的一个根。因此，对于所有 $1 \le l_i \le r_i$，$\operatorname{val}(\sigma_{i,\,l_i}(x_i - \tilde{x}_i)) \ge u$，所以当我们展开表达式时

$$f(x) = \tilde{Z}(x) - Z(x) = \prod_{i=1}^{m}\prod_{l_i=1}^{r_i}(x - \sigma_{i,l_i}(x_i) + \sigma_{i,l_i}(x_i - \tilde{x}_i)) - \prod_{i=1}^{m}\prod_{l_i=1}^{r_i}(x - \sigma_{i,l_i}(x_i)),$$

这个多项式的所有系数的赋值都必须为 $\ge u$。 □

下面的结果直观地表明，如果 Z_0 是一个在 Z 的根上取值较小的多项式，那么 Z 和 Z_0 的根自然可以配成彼此接近的若干对，并且这些对中的元素可以通过多项式相互交换。

命题 3.6. 设 $s = (s_1, \dots, s_m) \in (\frac{1}{e_1}\mathbb{N}, \dots, \frac{1}{e_m}\mathbb{N})$ 使得对所有$1 \le i \le m$都有 $s_i > r \operatorname{val} \operatorname{Disc}(\mathfrak{x})$。设 $Z_0 \in \mathbb{Z}_p[x]$ 是任意一个次数为 r 的首一多项式，且对所有$1 \le i \le m$都有 $\operatorname{val} Z_0(x_i) = s_i$。那么，存在唯一一组 Z_0 的根 $x'_1, \dots, x'_m$，满足

$$||x'_i - x_i|| < ||\operatorname{Disc}(\mathfrak{x})|| \qquad \textit{for all } 1 \le i \le m. \tag{3.17}$$

此外，存在唯一的次数为 $\le r-1$ 的多项式 $f, g \in \mathbb{Z}_p[x]$，使得 at

$$x'_i = f(x_i) \qquad \textit{and} \qquad x_i = g(x'_i) \qquad \textit{for all } 1 \le i \le m, \tag{3.18}$$

其中 f 满足

$$\operatorname{val}(f(x_i) - x_i) = s_i - \operatorname{val} Z'(x_i), \quad \textit{for all } 1 \le i \le m,$$

特别地，$f \in F_Z$ （回忆定义 *3.2*）。

证明。对任意固定的 $1 \le i \le m$，Z_0 的 r 个根给出到 x_i的 r 个距离。这些距离的乘积恰好为

$$||Z_0(x_i)|| = p^{-s_i} < ||\operatorname{Disc}(\mathfrak{x})||^r.$$

因此，我们可以找到 Z_0 的一个根 x'_i，使得

$$||x'_i - x_i|| < ||\operatorname{Disc}(\mathfrak{x})||. \tag{3.19}$$

由于对所有 $1 \le i \le m$ 都存在这样的 x'_i，我们可以应用引理 3.4 的 (2) 得出这些根

$$\sigma_{1,1}(x'_1), \dots, \sigma_{1,r_1}(x'_1), \dots, \sigma_{m,1}(x'_m), \dots, \sigma_{m,r_m}(x'_m)$$

彼此互不相同，因此必定是多项式 Z_0 的全部根。记 $\mathfrak{x}' = (x'_1、\dots\dots、x'_m)$。一方面，根据引理 3.4 的(3)，有 $\mathbb{Q}_p[\mathfrak{x}'] \supset E = \mathbb{Q}_p[\mathfrak{x}]$。另一方面，$x'_1、\dots\dots、x'_m$ 是次数为 r 的多项式 Z_0 的根，因此，从 $\mathbb{Q}_p$-向量空间的角度看，$\mathbb{Q}_p[\mathfrak{x}']$ 的维数为 $\le r$。这两个观察共同推出 $\mathbb{Q}_p[\mathfrak{x}'] = E = \mathbb{Q}_p[\mathfrak{x}]$。于是有

$$x'_i = f(x_i), x_i = g(x'_i), \quad \forall 1 \le i \le m \tag{3.20}$$

对于某些多项式 f、$g \in \mathbb{Q}_p[x]$，通过在必要时分别减去 x_i 和 x_i' 的最小多项式的倍数，可以设它们的次数为 $\leq r-1$。此外，对于所有$1 \leq i \leq m$，有

$$\begin{aligned}\operatorname{val}(f(x_i)-x_i) &= \operatorname{val}(x_i'-x_i)\\ &= \operatorname{val} Z_0(x_i) - \sum_{(j,l_j)\neq(i,1)} \operatorname{val}(x_i-\sigma_{j,l_j}(x_j'))\\ &= s_i - \sum_{(j,l_j)\neq(i,1)} \operatorname{val}(x_i-\sigma_{j,l_j}(x_j))\\ &= s_i - \operatorname{val} Z'(x_i).\end{aligned} \tag{3.21}$$

此处第三个等式由引理 3.4 的 (1) 得出。应用推论 3.5，$c_0,\dots,c_{r-1}$的系数满足 $f(x)-x$

$$\begin{aligned}\operatorname{val}(c_i) &\geq \min_i(s_i - 2\operatorname{val} Z'(x_i))\\ &> \min_i(r\operatorname{val}\operatorname{Disc}(\mathfrak{x}) - 2\operatorname{val} Z'(x_i))\\ &\geq 0,\end{aligned} \tag{3.22}$$

其中最后一行照常利用了以下事实：判别式是范数为 ≤ 1 的项的乘积，而 $Z'(x_i)$ 是这些项的一个子集的乘积。因此，我们有 $f \in \mathbb{Z}_p[x]$。由于

$$\operatorname{val}(g(x_i')-x_i') = \operatorname{val}(x_i'-x_i) = s_i - \operatorname{val} Z'(x_i) \tag{3.23}$$

根据 (3.21)，证明的其余部分对 g 也适用，并得出 $g \in \mathbb{Z}_p[x]$。

I最后，我们证明这些构造的唯一性。由引理 3.4 的 (1)，我们有

$$||\sigma_{j,l_j}(x_j')-x_i|| = ||\sigma_{j,l_j}(x_j)-x_i|| \geq ||\operatorname{Disc}(\mathfrak{x})||, \quad \forall (j,l_j)\neq(i,1),$$

因此，选取满足 (3.17) 的 Z_0 的根 $x_1',\dots,x_m'$ 的方式是唯一的。此外，给定任意一个次数为 $\leq r-1$ 的多项式 $f_1 \in \mathbb{Q}_p[x]$，使得

$$f_1(x_i) = x_i', \quad \forall 1 \leq i \leq m,$$

我们有 $f_1 - f$ 是一个次数为 $\leq r-1$ 的多项式，使得 $(f_1-f)(x_i) = 0$ 对所有 $1 \leq i \leq m$ 都成立。因此 $(f_1-f)(\mathfrak{x}) = 0$，又由于 $\mathfrak{x}$ 的最小多项式为 Z，次数为 r，我们必有 $f_1 - f = 0$。同样的论证表明 g 的唯一性。□

命题 *3.3* 的证明。我们首先验证映射 (3.5) 定义良好。由于 A_0 的根为 $x_1,\dots,x_m$ 及其伽罗瓦共轭，矩阵 $A = f(A_0)$ 的根为 $f(x_1)\dots,f(x_m)$ 及其共轭元。我们要证明矩阵 A 属于 (3.5) 中所要求的集合。为了将引理 3.4 应用于序列 $f(x_1)\dots,f(x_m)$，我们必须验证 $||f(x_i)-x_i|| < ||\operatorname{Disc}(\mathfrak{x})||$。为此，注意到

$$\begin{aligned}\operatorname{val}(f(x_i)-x_i) &\geq s_i - \operatorname{val} Z'(x_i)\\ &> r\operatorname{val}\operatorname{Disc}(\mathfrak{x}) - \operatorname{val} Z'(x_i)\\ &\geq \operatorname{val}\operatorname{Disc}(\mathfrak{x}),\end{aligned} \tag{3.24}$$

其中，最后一个不等式成立是因为当 $r=1$ 时，我们有 $\operatorname{val}(Z'(x_i)) = 0$；而当 $r \geq 2$ 时，我们有 $\operatorname{val}\operatorname{Disc}(\mathfrak{x}) \geq \operatorname{val} Z'(x_i)$。现在，在第二个等式中应用引理 3.4 的 (1)，可知对所有 $1 \leq i \leq m$，

$$\begin{aligned}\operatorname{val}(P_A(x_i)) &= \sum_{j=1}^{m}\sum_{l_j=1}^{r_j} \operatorname{val}(f(\sigma_{j,l_j}(x_j))-x_i)\\ &= \operatorname{val}(f(x_i)-x_i) + \sum_{(j,l_j)\neq(i,1)} \operatorname{val}(\sigma_{j,l_j}(x_j)-x_i)\\ &= \operatorname{val}(f(x_i)-x_i) + \operatorname{val}(Z'(x_i))\\ &\geq s_i.\end{aligned} \tag{3.25}$$

因此，映射 (3.5) 是定义良好的。

现在我们定义逆映射。为此，先取任意满足 $\mathrm{val}(P_A(x_i)) \geq s_i, \forall 1 \leq i \leq m$ 的 $A \in \mathrm{Mat}_r(\mathbb{Z}_p)$。应用命题 3.6，可得到两个多项式 $f_A, g_A \in \mathbb{Z}_p[x]$，它们交换了 P_A 和 Z 的根，因此映射

$$\begin{aligned} \{A \in \mathrm{Mat}_r(\mathbb{Z}_p) \mid \mathrm{val}(P_A(x_i)) \geq s_i, \quad \forall 1 \leq i \leq m\} &\to \{(f, A_0) \mid A_0 \in \mathcal{X}, f \in F_Z\} \\ A &\mapsto (f_A, g_A(A)) \end{aligned} \tag{3.26}$$

是良定义的。

最后，我们证明所构造的映射互为逆映射。设 f_B, g_B 是由命题 3.6 与矩阵 B 的特征值相对应的多项式。那么我们必须证明

(1) 设 $A \in \mathrm{Mat}_r(\mathbb{Z}_p)$ 满足对所有 $1 \leq i \leq m$ 均有 $\mathrm{val}(P_A(x_i)) \geq s_i$。那么 $f_A(g_A(A)) = A$，其中 f_A 和 g_A 如上所述。(2) 对任意 $f \in F_Z, A_0 \in \mathcal{X}$，有 $f_{f(A_0)} = f$ 且 $g_{f(A_0)}(f(A_0)) = A_0$。

我们首先证明 (1)。对所有 $1 \leq i \leq m$，记 $x_i' = f_A(x_i)$。事实上，我们有 $f_A(g_A(x_i')) = f_A(x_i) = x_i'$, $\forall 1 \leq i \leq m$。这意味着 $P_A(x) \mid f_A(g_A(x)) - x$，因此根据凯莱–哈密顿定理，$f_A(g_A(A)) = A$。

接下来证明 (2)。多项式 f 具有如下性质：对于每个 i，$f(x_i)$ 是 $f(A_0)$ 的特征值，因此命题 3.6 的唯一性部分意味着 $f_{f(A_0)} = f$。此外，由于多项式 f 和 $g_{f(A_0)}$ 交换了 A_0 和 $f(A_0)$ 的相应特征值，我们对所有 $1 \leq i \leq m$ 都有 $g_{f(A_0)}(f(x_i)) = x_i$。这意味着 $Z(x) \mid g_{f(A_0)}(f(x)) - x$，因此根据凯莱–哈密顿定理，$g_{f(A_0)}(f(A_0)) = A_0$。证明完毕。□

推论 3.7。设 $s = (s_1, \ldots, s_m) \in (\frac{1}{e_1}\mathbb{N}, \ldots, \frac{1}{e_m}\mathbb{N})$ 使得对所有$1 \leq i \leq m$均有 $s_i > r \operatorname{val} \mathrm{Disc}(\mathfrak{x})$。假设 $A \in$矩阵空间$_r(\mathbb{Z}_p)$ 满足对所有 $1 \leq i \leq m$均有 $\mathrm{val}(P_A(x_i)) \geq s_i$。令 f 与命题 *3.3* 中的双射相同，使得

$$f(\sigma_{1,1}(x_1)), \ldots, f(\sigma_{1,r_1}(x_1)), \ldots, f(\sigma_{m,1}(x_m)), \ldots, f(\sigma_{m,r_m}(x_m))$$

给出了 A 的所有特征值。对所有 $1 \leq i \leq m$，记 $x_i' = f(x_i)$。于是我们有

$$||P_A'(x_i)|| = ||P_A'(x_i')|| = ||Z'(x_i)||.$$

证明。首先，我们有

$$\begin{aligned} ||P_A'(x_i')|| &= \prod_{(j,l_j) \neq (i,1)} ||\sigma_{j,l_j}(x_j') - x_i'|| \\ &= \prod_{(j,l_j) \neq (i,1)} ||\sigma_{j,l_j}(x_j) - x_i|| \\ &= ||Z'(x_i)||, \end{aligned} \tag{3.27}$$

其中第二行由引理 3.4 得出。接下来，注意到 $P_A' \in \mathbb{Z}_p[x]$，我们有

$$||P_A'(x_i') - P_A'(x_i)|| \leq ||x_i' - x_i|| < ||\mathrm{Disc}(\mathfrak{x})|| \leq ||Z'(x_i)||,$$

这意味着

$$||P_A(x_i)|| = ||P_A'(x_i) - P_A'(x_i') + P_A'(x_i')|| = ||P_A'(x_i')|| = ||Z'(x_i)||.$$

□

3.3. **矩阵与** $\mathbb{Z}_p[\![\mathfrak{x}]\!]$-模。 </style}回顾一下，在 (3.7) 中定义的 $\mathrm{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]}$，它由 E 中秩满的 $\mathbb{Z}_p$-子格组成，且这些子格是 $\mathbb{Z}_p[\![\mathfrak{x}]\!]$-模。我们有一个通过标量乘法作用的典范群作用 $E^\times \ \mathrm{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]}$。如 [Yun13], 第 4 页所述，其子群 $\Lambda_E \subset E^\times$ 对 $\mathrm{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]}$ 的作用只有有限多个轨道，记为 $\#(\Lambda_E \backslash \mathrm{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]})$。我们将 $\mathrm{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]}$ 中在常数乘法下的等价类集合记为 $E^\times \backslash \mathrm{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]}$；对每个 $M \in \mathrm{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]}$，记包含 M 的等价类为 $[M] = \{xM \mid x \in E^\times\}$。

将 $\mathrm{GL}_r(\mathbb{Z}_p)\backslash\mathcal{X}$ 记为 $\mathcal{X}$ 中元素在 $\mathrm{GL}_r(\mathbb{Z}_p)$ 的共轭作用下形成的轨道。对于 $\mathbb{Q}_p$-共轭，只有一个轨道：回顾有理标准形定理，它指出每个满足 $P_A = Z$ 的 $A \in \mathrm{Mat}_r(\mathbb{Q}_p)$ 都可写成 $A = TC(Z)T^{-1}$，其中 $T \in \mathrm{GL}_r(\mathbb{Q}_p)$；并回顾 $C(Z)$ 的定义：

定义 3.8. 对于每个次数为 r 的首一 $Z(x) = x^r + c_{n-1}x^{r-1} + \cdots + c_0 \in \mathbb{Z}_p[x]$，记

$$C(Z) = \begin{pmatrix} 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & \dots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -c_{n-1} \end{pmatrix} \in \mathrm{Mat}_r(\mathbb{Z}_p)$$

Z 的伴随矩阵。

下文将这些 $\mathrm{GL}_r(\mathbb{Z}_p)\backslash\mathcal{X}$ 中的轨道与格等价类对应起来 s.

命题 3.9. 给定任意格 $M \in$ 模$_{\mathbb{Z}_p[\mathfrak{x}]}$，固定 M 的一个 $\mathbb{Z}_p$-基，并令 A_M 为 $\mathfrak{x}$ 在此基下作用的矩阵。那么映射

$$\begin{aligned} \mathrm{Mod}_{\mathbb{Z}_p[\mathfrak{x}]} &\to \mathrm{GL}_r(\mathbb{Z}_p)\backslash\mathcal{X} \\ M &\mapsto [A_M] \end{aligned} \tag{3.28}$$

是满射　此外，它可经由商集 $E^\times\backslash$模$_{\mathbb{Z}_p[\mathfrak{x}]}$ 分解，而由此得到的矩 p

$$\begin{aligned} E^\times\backslash \mathrm{Mod}_{\mathbb{Z}_p[\mathfrak{x}]} &\to \mathrm{GL}_r(\mathbb{Z}_p)\backslash\mathcal{X} \\ [M] &\mapsto [A_M] \end{aligned} \tag{3.29}$$

是双射。

证明。映射 (3.28) 显然定义良好，因为改变 $\mathbb{Z}_p$-基的选取，仅相当于用 $\mathrm{GL}_r(\mathbb{Z}_p)$ 中的一个矩阵对 A_M 施加共轭作用。

对于满射性，任取 $A \in \mathcal{X}$。根据有理标准形，存在某个 $T \in \mathrm{GL}_r(\mathbb{Q}_p)$，使得 $A = TC(Z)T^{-1}$。令 $M \subset E$ 为元素 $T^{-1}(1), \dots, T^{-1}(\mathfrak{x}^{r-1})$ 的 $\mathbb{Z}_p$-张成空间，其中我们将 T 视为 E 上的线性变换，方法是将 $\mathbb{Q}_p^r$ 的标准基向量依次对应于 $1, \mathfrak{x}, \dots, \mathfrak{x}^{r-1} \in E$。显然，此 M 的秩为满秩。此外，由于 $\mathfrak{x}$ 对基 $1, \mathfrak{x}, \dots, \mathfrak{x}^{r-1}$ 的作用由矩阵 $C(Z)$ 表示，它对基 $T^{-1}(1), \dots, T^{-1}(\mathfrak{x}^{r-1})$ 的作用则由 $TC(Z)T^{-1} = A$ 表示。特别地，由于 $A \in \mathrm{Mat}_{r\times r}(\mathbb{Z}_p)$，它将此基的 $\mathbb{Z}_p$-张成空间映到其自身，即 $AM \subset M$。因此，由于 A 表示了 $\mathfrak{x}$ 在此基下对 M 的作用，M 不仅是一个 $\mathbb{Z}_p$-格，也是一个 $\mathbb{Z}_p[\mathfrak{x}]$-模，$M \in \mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$。由于 $\mathfrak{x}$ 对 M 的作用由矩阵 $TC(Z)T^{-1} = A$ 表示，$M \mapsto [A]$ 在映射 (3.28) 下成立，从而证明了满射性。

现在我们证明该映射可经由商集 $E^\times\backslash\mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$ 分解。设 $\mathcal{C} \in E^\times\backslash\mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$ 是任意一个等价类。若

$$M_1, M_2 \in \mathcal{C},$$

则 $M_2 = uM_1$，其中 $u \in E^\times$。特别地，$u \in E$，因此对于某个多项式 $f \in \mathbb{Q}_p[x]$，有 $u = f(\mathfrak{x})$。于是 u 与 $\mathfrak{x}$ 的作用可交换，因此固定一组基 $\mathbf{v}_1, \dots, \mathbf{v}_r$，其属于 M_1，则 $\mathfrak{x}$ 在 $\mathbf{v}_1, \dots, \mathbf{v}_r$ 上的作用，以及在基 $u\mathbf{v}_1, \dots, u\mathbf{v}_r$ 上的作用（该基属于 M_2），由同一个矩阵描述。因此$[A_{M_1}] = [A_{M_2}]$。

最后，我们证明映射 (3.29) 是单射。设对于某些 $M_1, M_2 \in \mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$，有$[A_{M_1}] = [A_{M_2}]$。那么存在一个 $\mathbb{Z}_p$-基 $\mathbf{v}1, \dots, \mathbf{v}_r$，属于 M_1；以及一个 $\mathbb{Z}_p$-基 $\mathbf{w}1, \dots, \mathbf{w}_r$，属于$M_2$，使得 $\mathfrak{x}$ 在这两组基下都由同一个矩阵 A 表示。令 $U \in \mathrm{End}^{\mathbb{Q}_p}(E)$ 为满足对每个 i 都有 $U\mathbf{v}_i = \mathbf{w}_i$ 的线性映射，则 $UM_1 = M_2$ 和 U 与 A 交换。由于 U 与 A交换，它们可以同时对角化。由于 A 在 $\mathbb{Q}_p$ 上与 $C(Z)$ 共轭，其特征值由 Z的根给出，即 $\mathfrak{x}$ 的坐标及其伽罗瓦共轭。由于 $\mathfrak{x} \in E^{\mathrm{new}}$，$\mathfrak{x}$ 中的多项式生成 E。因此，对于某个多项式 f，有 $U = f(A)$，也就是说，U由多项式 $f(\mathfrak{x})$ 表示。由于 U 可逆，$f(\mathfrak{x}) \in E^\times$。

因此，对于某个 $u = f(\mathfrak{x})$，有 $M_2 = uM_1 \in E^\times$，故 M_1 和 M_2 属于同一个等价类 $\mathcal{C} \in E^\times\backslash\mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$。这证明了单射性。□

本小节余下部分将基于命题 3.9 中给出的字典，进一步建立其性质。

定义 3.10. 给定 $M \in \mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$，我们将 $\mathrm{End}(M) \subset \mathrm{End}^{\mathbb{Q}_p}(E)$ 记为满足 $TM \subset M$ 且与 $\mathfrak{x}$ 通过乘法作用相交换的 $\mathbb{Q}_p$-线性映射 T 在 E 上的集合。类似地，我们将 $\mathrm{Aut}(M) \subset \mathrm{End}(M)$ 记为满足 $TM = M$ 的映射。

引理 3.11. 给定一个格类 $\mathcal{C} \in E^\times\backslash$矩阵空间$^{\mathbb{Z}_p[\mathfrak{x}]}$ 以及 $M_1, M_2 \in \mathcal{C}$,

$$\mathrm{End}(M_1) = \mathrm{End}(M_2) \tag{3.30}$$

and

$$\mathrm{Aut}(M_1) = \mathrm{Aut}(M_2). \tag{3.31}$$

证明. $M_2 = uM_1$ 对某个 $u \in E^\times$ 成立，并给定任意 $T \in \mathrm{End}(M_1)$，显然 $uTu^{-1} \in \mathrm{End}(M_2)$。但是，$u$ 是 $\mathfrak{x}$ 中的多项式，并且 T 与 $\mathfrak{x}$ 的作用相交换，因此 $uTu^{-1} = T$。于是 $T \in \mathrm{End}(M_1) \Rightarrow T \in \mathrm{End}(M_2)$，结论得证。□

定义 3.12。对于任意类 $\mathcal{C} \in E^\times\backslash\,\mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$，令 $\mathrm{End}(\mathcal{C}) = \mathrm{End}(M)$，其中 $M \in \mathcal{C}$ 是任意选取的代表元；由引理 3.11 可知，这与 M的选取无关。类似地定义 $\mathrm{Aut}(\mathcal{C})$。

注 3.13。重申命题 3.9 证明中的一个有用观点：给定任意格$M \in \mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$及其一组固定基 $\mathbf{v}_1, \ldots, \mathbf{v}_r$，对于 $u \in E^\times$，任意其他格 uM都有相应的基 $u\mathbf{v}_1, \ldots, u\mathbf{v}_r$。$\mathfrak{x}$在 M这组基下的作用矩阵，与 $\mathfrak{x}$在 uM的基 $u\mathbf{v}_1, \ldots, u\mathbf{v}_r$下的作用矩阵相同，因为 u是 $\mathfrak{x}$的多项式，因而与 $\mathfrak{x}$可交换。因此，虽然 M 的基和矩阵 A_M 的选取不是规范的，但只需为整个类 $[M]$选取一次，而不必为该类中的每个模分别选取。

记号 3.14。从现在起，每当我们讨论格 $M \in \mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$时，都会默认（非典范地）固定一个 $\mathbb{Z}_p$-基 $\mathbf{v}_1$，.....，$\mathbf{v}_r$ of M。类似地，如果我们讨论等价类 $\mathcal{C} \in E^\times\backslash\mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$，就会固定其中一个格 $M \in \mathcal{C}$ 的一个 $\mathbb{Z}_p$-基，并据此根据注 3.13 固定 $\mathcal{C}$ 中所有其他格的另一个基。我们用 $A_{\mathcal{C}}$ 表示 $\mathfrak{x}$ 在此基下作用所对应的矩阵。

利用这个基，我们将自由地把 E 与 $\mathbb{Q}_p^r$ 视为同一对象，并把线性映射集合 $\mathrm{End}^{\mathbb{Q}_p}(E)$（以及由此得到的各种子集，例如 $\mathrm{End}(\mathcal{C})$，$\mathrm{Aut}(\mathcal{C})$）与 $\mathrm{Mat}_r(\mathbb{Q}_p)$ 视为同一对象，这与命题 3.9 类似。我们也常常将 E 及其子集（例如 $\mathcal{O}_E$ ）视为 $\mathrm{End}^{\mathbb{Q}_p}(E)$ 中的线性映射，方法是考察它们通过乘法的作用，并由此写出诸如 $\mathrm{End}(\mathcal{C}) \subset \mathcal{O}_E$ 这样的包含关系（见命题 3.19）。总之[3]:

在 E 和 $M \subset E$上的线性映射	矩阵
$\mathfrak{x}$	$A_{\mathcal{C}} \in$矩阵空间$_r(\mathbb{Z}_p)$
E	$\mathbb{Q}_p[A_{\mathcal{C}}] \subset$矩阵空间$_r(\mathbb{Q}_p)$
$\mathbb{Z}_p[\mathfrak{x}]$	$\mathbb{Z}_p[A_{\mathcal{C}}]$
$\mathrm{End}(\mathcal{C})$	$\mathbb{Q}_p[A_{\mathcal{C}}] \cap$ 矩阵空间$_{r\times r}(\mathbb{Z}_p)$
$\mathrm{Aut}(\mathcal{C})$	$\mathbb{Q}_p[A_{\mathcal{C}}] \cap \mathrm{GL}_r(\mathbb{Z}_p)$
$E^\times = \{f(\mathfrak{x}) \mid f \in \mathbb{Q}_p[x], f(x_i) \neq 0, \forall 1 \leq i \leq m\}$	$\mathbb{Q}_p[A_{\mathcal{C}}] \cap \mathrm{GL}_r(\mathbb{Q}_p) = \{f(A_{\mathcal{C}}) \mid f \in \mathbb{Q}_p[x], \quad f(x_i) \neq 0, \quad \forall 1 \leq i \leq m\}$
$\mathcal{O}_E$	$\{B \in \mathbb{Q}_p[A_{\mathcal{C}}] : P_B \in \mathbb{Z}_p[x]\}$

注意，我们有时将 E 视为向量空间 $\mathbb{Q}_p^r$，有时则将其视为该向量空间上由乘法给出的线性映射。

[3]表中 $\mathrm{End}(\mathcal{C})$ 与 $\mathrm{Aut}(\mathcal{C})$ 的同一化并非完全显然，见引理 3.15。

引理 3.15。 在采用记号 *3.14* 中所述的基时，我们有

$$\mathrm{End}(\mathcal{C}) = \mathbb{Q}_p[A_{\mathcal{C}}] \cap \mathrm{Mat}_{r\times r}(\mathbb{Z}_p) \tag{3.32}$$

and

$$\mathrm{Aut}(\mathcal{C}) = \mathbb{Q}_p[A_{\mathcal{C}}] \cap \mathrm{GL}_r(\mathbb{Z}_p). \tag{3.33}$$

证明。 取 $M \in \mathcal{C}$。在我们选定的 M 基下，集合 $\mathrm{Mat}_{r\times r}(\mathbb{Z}_p)$ 恰好是将 M 映到自身的矩阵集合。$\mathrm{End}(\mathcal{C}) = \mathrm{End}(M)$ 中的元素（通过定义 3.12 进行同一化）还与 $\mathfrak{x}$的作用可交换。由此可知，它们是$\mathfrak{x}$ 作用所对应的矩阵 $A_{\mathcal{C}}$ 的多项式，正如命题 3.9 的证明中所示。同一化 (3.33) 由 (3.32) 立即得出。□

鉴于命题 3.9，为 $\mathcal{X}$ 的各个分量命名并为每个分量选取一个代表元是很自然的。

定义 3.16。 对于每个类 $\mathcal{C} \in E^\times\backslash\mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$，用 $\mathcal{X}_{\mathcal{C}}$ 表示 $\mathrm{GL}_r(\mathbb{Z}_p)\backslash\mathcal{X}$ 中与之对应的轨道；根据命题 3.9，该轨道对应于 $\mathcal{C}$ 。

对于刚才定义的所有 $\mathbb{Z}_p$-格，以下基本术语很有用。

定义 3.17. 设 $L_0 \subset \mathbb{Z}_p^k$ 是一个秩为 k_0 的 $\mathbb{Z}_p$-子模。那么存在唯一一个秩相同的极大子模 $L_0 \subset L \subset \mathbb{Z}_p^k$，其明确表达式为

$$L = (L_0 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \cap \mathbb{Z}_p^k.$$

We 称 L 为 L_0的极大扩张。如果 $L_0 = L$，则称 L_0 在 $\mathbb{Z}_p^k$中是极大的。

命题 3.18. 设 $L_0 \subset \mathbb{Z}_p^k$是秩为 k_0 的子模，且 $e_1, \ldots, e_{k_0} \in \mathbb{Z}_p^k$是 L_0的一组 $\mathbb{Z}_p$-基。则以下条件等价:

(1) L_0 是极大的。*(2)* 存在 $e_{k_0+1}, \ldots, e_k \in \mathbb{Z}_p^k$，使得序列 $e_1, \ldots, e_k$ 构成 $\mathbb{Z}_p^k$的一组 $\mathbb{Z}_p$-基。*(3)* $\mathbb{Z}_p^k/L_0$ 是秩为 $k - k_0$ 的自由 $\mathbb{Z}_p$-模。

证明。 我们将以循环方式证明上述断言等价。

(1) → (3)：我们用反证法证明。假设 $\mathbb{Z}_p^k/L_0$ 含有非平凡挠元。根据模的第二同构定理，存在一个秩为 k_0 的模 $L \subset \mathbb{Z}_p^k$，使得 L_0 是 L 的真子模。这与我们的假设矛盾，因为 L_0 是极大的。

(3) → (2)：假设 $\mathbb{Z}_p^k/L_0$ 是秩为 $k - k_0$ 的自由 $\mathbb{Z}_p$-模。取它的一组 $\mathbb{Z}_p$-基 $e_{k_0+1} + L_0$, ……， $e_k + L_0$，其中 e_{k_0+1}，……， $e_k \in \mathbb{Z}_p^k$。那么序列 e_1，……， e_k 构成 $\mathbb{Z}_p^k$ 的一组 $\mathbb{Z}_p$-基。

(2) → (1)：假设存在 e_{k_0+1}，……， $e_k \in \mathbb{Z}_p^k$，使得序列 e_1，……， e_k 构成 $\mathbb{Z}_p^k$ 的一组$\mathbb{Z}_p$-基。令 $L \supset L_0$ 为 L_0 的极大扩张，并设 $L_1 = \bigoplus_{i=k_0+1}^k \mathbb{Z}_p e_i$。于是我们有 $L_0 + L_1 = \mathbb{Z}_p^k \supset L$。注意到 $L_1 \cap L = 0$，我们有 $L_0 = L$，因此 L_0 是极大的。□

命题 3.19。 我们有如下包含关系

$$\mathbb{Z}_p[A_{\mathcal{C}}] \subset \mathrm{End}(\mathcal{C}) \subset \mathcal{O}_E, \tag{3.34}$$

它们都是秩为 r 的自由 $\mathbb{Z}_p$-模。此外， $\mathbb{Z}_p[A_{\mathcal{C}}]$ 在矩阵空间$r(\mathbb{Z}_p)$ 中的极大扩张是$\mathrm{End}(\mathcal{C})$。

证明。 由引理 3.15，

$$\mathrm{End}(\mathcal{C}) = \mathbb{Q}_p[A_{\mathcal{C}}] \cap \mathrm{Mat}_r(\mathbb{Z}_p).$$

由于 $A_{\mathcal{C}} \in\mathrm{Mat}_r(\mathbb{Z}_p)$ 本身，(3.34) 中的第一个包含关系显然成立。

对于第二个包含关系，由于 $\mathrm{End}(\mathcal{C}) \subset$ 矩阵空间$_r(\mathbb{Z}_p)$，$\mathrm{End}(\mathcal{C})$ 中的任意元素 $A \in$ 都必须具有系数属于 $\mathbb{Z}_p$ 的特征多项式。因此，根据 Cayley-Hamilton 定理， A 满足一个 $\mathbb{Z}_p[x]$ 中的首一多项式。此外，$\mathrm{End}(\mathcal{C}) \subset \mathbb{Q}_p[A_{\mathcal{C}}] = E$ （根据我们将$\mathcal{C}$与由乘法给出的线性映射进行同一化的约定

），因此 A 被同一化为 E 中满足系数属于 $\mathbb{Z}_p$ 的首一多项式的一个元素，即 $\mathcal{O}_E$ 中的一个元素。这就证明了第二个包含关系。

最后，由于 $\mathrm{End}(\mathcal{C})$ 是一个 $\mathbb{Q}_p$-向量空间与 $\mathrm{Mat}_r(\mathbb{Z}_p)$ 的交集，因此它在 $\mathrm{Mat}_r(\mathbb{Z}_p)$ 中是极大的。结合 (3.34) 中的第一个包含关系可知，$\mathbb{Z}_p[A_{\mathcal{C}}]$ 在 $\mathrm{Mat}_r(\mathbb{Z}_p)$ 中的极大扩张是 $\mathrm{End}(\mathcal{C})$。□

例3.20。注意，命题 *3.19* 中的两个包含关系都可能是严格的，也可能不是严格的。当 $\mathcal{C} = [\mathbb{Z}_p[\mathfrak{x}]]$ 时，我们有 $\mathrm{End}(\mathcal{C}) = \mathbb{Z}_p[\mathfrak{x}]$，这一般可能是 $\mathcal{O}_E$ 的真子集。当 $\mathcal{C} = [\mathcal{O}_E]$ 时，我们有 $\mathrm{End}(\mathcal{C}) = \mathcal{O}_E$，因此第二个包含关系不是严格的。不过，在下面的例子中，$\mathbb{Z}_p[\mathfrak{x}]$ 严格包含于 $\mathcal{O}_E$。设 $E = \mathbb{Q}_p[\sqrt{p}]$ 是一个域且 $\mathfrak{x} = p\sqrt{p}$。那么 $\mathbb{Z}_p[\mathfrak{x}] = \mathbb{Z}_p[p\sqrt{p}]$ 就成为 $\mathcal{O}_E = \mathbb{Z}_p[\sqrt{p}]$ 的真子集。

3.4. **分解并计算体积**。现在我们可以将定理 3.1 中的矩阵集合分解为由这些模类索引的子集：

推论 3.21。设 $(s_1, \dots, s_m) \in (\frac{1}{e_1}\mathbb{N}, \dots, \frac{1}{e_m}\mathbb{N})$ 满足 $s_i > r \operatorname{val}\mathrm{Disc}(\mathfrak{x})$ 对所有 $1 \le i \le m$ 均成立。那么

$$\{A \in \mathrm{Mat}_{r\times r}(\mathbb{Z}_p) \mid \operatorname{val}(P_A(x_i)) \ge s_i, \quad \forall 1 \le i \le m\} = \bigsqcup_{\mathcal{C}\in E^\times\backslash \mathrm{Mod}_{\mathbb{Z}_p[\mathfrak{x}]}} \{T f(A_{\mathcal{C}}) T^{-1} \mid f \in F_Z, T \in \mathrm{GL}_r(\mathbb{Z}_p)\}, \quad (3.35)$$

其中回顾一下，F_Z 来自定义 *3.2*，$A_{\mathcal{C}}$ 来自记号 *3.14*。

证明。由命题 3.9，我们有

$$\begin{aligned} \mathrm{LHS}(3.35) &= \{f(A_0) \mid f \in F_Z, A_0 \in \mathcal{X}\} \\ &= \bigcup_{\mathcal{C}\in E^\times\backslash \mathrm{Mod}_{\mathbb{Z}_p[\mathfrak{x}]}} \{f(A_0) \mid f \in F_Z, A_0 \in \mathcal{X}_{\mathcal{C}}\} \\ &= \bigcup_{\mathcal{C}\in E^\times\backslash \mathrm{Mod}_{\mathbb{Z}_p[\mathfrak{x}]}} \{T f(A_{\mathcal{C}}) T^{-1} \mid f \in F_Z, T \in \mathrm{GL}_r(\mathbb{Z}_p)\}. \end{aligned} \quad (3.36)$$

现在只需证明上述表达式确实是不交并。假设存在 $\mathcal{C}_1, \mathcal{C}_2 \in \mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$，$T_1, T_2 \in \mathrm{GL}_r(\mathbb{Z}_p)$ 和 $f_1, f_2 \in F_Z$，使得

$$T_1 f_1(A_{\mathcal{C}_1}) T_1^{-1} = f_1(T_1 A_{\mathcal{C}_1} T_1^{-1}) = f_2(T_2 A_{\mathcal{C}_2} T_2^{-1}) = T_2 f_2(A_{\mathcal{C}_2}) T_2^{-1}.$$

那么命题 3.3 蕴含 $f_1 = f_2$，且 $T_1 A_{\mathcal{C}_1} T_1^{-1} = T_2 A_{\mathcal{C}_2} T_2^{-1}$。因此我们有 $\mathcal{X}_{\mathcal{C}_1} = \mathcal{X}_{\mathcal{C}_2}$，以及 $\mathcal{C}_1 = \mathcal{C}_2$，证明至此完成。□

现在我们希望计算这些集合的测度

$$\{T f(A_{\mathcal{C}}) T^{-1} \mid f \in F_Z, T \in \mathrm{GL}_r(\mathbb{Z}_p)\} \quad (3.37)$$

它们出现在 (3.35) 中。我们将按照下面的引理进一步把它们分解为更小的集合，然后计算这类集合的数量及其测度。如何自然地将它们分解？由于 $f(A_{\mathcal{C}})$ 在矩阵空间 $_r(\mathbb{Z}_p)$ 中的中心化子是 $\mathrm{End}(\mathcal{C})$，且其与 $\mathrm{GL}_r(\mathbb{Z}_p)$ 的交为 $\mathrm{Aut}(\mathcal{C})$，因此在推论 3.21 中，自然的做法是对这个群取商集。由于这个商集仍然是无限的（$\mathrm{Aut}(\mathcal{C})$ 的秩为 r，而 $\mathrm{GL}_r(\mathbb{Z}_p)$ 的秩为 r^2），为了处理有限个集合，自然的做法也是将所有矩阵对 p 的一个大幂取模。

引理 3.22。设 $\mathcal{C} \in E^\times\backslash \mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$，且 $\mathcal{M} \in \mathbb{N}$ 充分大。设 T_1、…、$T_k \in \mathrm{GL}_r(\mathbb{Z}/p^{\mathcal{M}}\mathbb{Z})$ 是 $\mathrm{Aut}(\mathcal{C}) \pmod{p^{\mathcal{M}}}$ 在 $\mathrm{GL}_r(\mathbb{Z}_p/p^{\mathcal{M}}\mathbb{Z}_p)$ 中的左陪集代表元，使得

$$\mathrm{GL}_r(\mathbb{Z}_p/p^{\mathcal{M}}\mathbb{Z}_p) = \bigsqcup_{i=1}^{k} \tilde{T}_i \,\mathrm{Aut}(\mathcal{C}) \pmod{p^{\mathcal{M}}}.$$

~ ~设 T_1、…、T_k是 T_1、…、T_k在$\mathrm{GL}_r(\mathbb{Z}_p)$中的任意提升，使得

$$\mathrm{GL}_r(\mathbb{Z}_p) = \bigsqcup_{i=1}^{k} \{(T_i + \Delta T)\,\mathrm{Aut}(\mathcal{C}) \mid \Delta T \in p^{\mathcal{M}}\,\mathrm{Mat}_r(\mathbb{Z}_p)\}.$$

Then

$$\{Tf(A_{\mathcal{C}})T^{-1} \mid f \in F_Z, T \in \mathrm{GL}_r(\mathbb{Z}_p)\}$$
$$= \bigsqcup_{i=1}^{k} \{(T_i + \Delta T) f(A_{\mathcal{C}}) (T_i + \Delta T)^{-1} \mid \Delta T \in p^{\mathcal{M}}\,\mathrm{Mat}_r(\mathbb{Z}_p), f \in F_Z\}. \quad (3.38)$$

此外，(3.38) 右侧的每个集合都与集合$\{(I_r + p^{\mathcal{M}}\Delta T) f(A_{\mathcal{C}}) (I_r + p^{\mathcal{M}}\Delta T)^{-1} \mid \Delta T \in p^{\mathcal{M}}$矩阵空间$_r(\mathbb{Z}_p)$ $f \in F_Z\}$具有相同的 ***Haar*** 测度。

证明。 我们先证明 RHS(3.38) 中的各个分量互不相交。假设有 $\Delta T_i, \Delta T_j \in p^{\mathcal{M}}$ 矩阵空间$_r$($\mathbb{Z}_p$) 和 $f_i, f_j \in F_Z$，满足

$$(T_i + \Delta T_i) f_i(A_{\mathcal{C}}) (T_i + \Delta T_i)^{-1} = (T_j + \Delta T_j) f_j(A_{\mathcal{C}}) (T_j + \Delta T_j)^{-1},$$

将其改写为

$$f_i((T_i + \Delta T_i) A_{\mathcal{C}} (T_i + \Delta T_i)^{-1}) = f_j((T_j + \Delta T_j) A_{\mathcal{C}} (T_j + \Delta T_j)^{-1}).$$

于是命题 3.3 推出 $f_i = f_j$，并且

$$(T_i + \Delta T_i) A_{\mathcal{C}} (T_i + \Delta T_i)^{-1} = (T_j + \Delta T_j) A_{\mathcal{C}} (T_j + \Delta T_j)^{-1}. \quad (3.39)$$

由 (3.39) 可得 $(T_j + \Delta T_j)^{-1}(T_i + \Delta T_i) \in \mathrm{Aut}(\mathcal{C})$，因此 $i = j$，从而证明了互不相交性。

现在证明 (3.38)。考虑 (3.38) 左侧的任意元素。每个 $T \in \mathrm{GL}_r(\mathbb{Z}_p)$ 中的元素都可以表示为 $(T_i + \Delta T)B$ 的形式，其中 $1 \le i \le k$，$\Delta T \in p^{\mathcal{M}}$ 矩阵空间$_r(\mathbb{Z}_p)$，且 $B \in \mathrm{Aut}(\mathcal{C})$。由于 B 与 $A_{\mathcal{C}}$的作用可交换，$Bf(A_{\mathcal{C}}) = f(A_{\mathcal{C}})B$，因此

$$(T_i + \Delta T) B f(A_{\mathcal{C}}) B^{-1} (T_i + \Delta T)^{-1} = (T_i + \Delta T) f(A_{\mathcal{C}}) (T_i + \Delta T)^{-1}.$$

这说明 LHS(3.38)⊂RHS(3.38)，反向包含显然成立 .

最后，所有此类集合的测度都与 $T_i = I_r$ 的测度相同，这一点可由共轭作用 T_i 以及 Haar 测度的定义性质得出。□

现在还需要计算这些集合的数量以及每个集合的测度。第一项任务比较简单。

命题 3.23。设 $\mathcal{C} \in E^{\times}\backslash$模$\mathbb{Z}_p[\mathfrak{x}]$。那么

$$\#(\mathrm{GL}_r(\mathbb{Z}_p/p^{\mathcal{M}}\mathbb{Z}_p)/\,\mathrm{Aut}(\mathcal{C}) \pmod{p^{\mathcal{M}}}) = p^{\mathcal{M}(r^2-r)} \frac{(1-p^{-1})\cdots(1-p^{-r})\#(\mathcal{O}_E^{\times}/\,\mathrm{Aut}(\mathcal{C}))}{\prod_{i=1}^{m}(1-p^{-r_i/e_i})\#(\mathcal{O}_E/\,\mathrm{End}(\mathcal{C}))}$$

对所有正整数 $\mathcal{M}$。对于右侧的商集，请注意，$\mathcal{O}_E^{\times}/\,\mathrm{Aut}(\mathcal{C})$ 是群的商，而 $\mathcal{O}_E/\mathrm{End}(\mathcal{C})$ 是环的商。为了使这些表达式有意义，我们按照记号 ***3.14*** 将 E 和 $\mathrm{End}(\mathcal{C})$ 视为矩阵环。

证明。 一方面，我们有

$$\#\,\mathrm{GL}_r(\mathbb{Z}_p/p^{\mathcal{M}}\mathbb{Z}_p) = (1-p^{-1})\cdots(1-p^{-r})p^{\mathcal{M}r^2}. \quad (3.40)$$

另一方面，$\mathrm{End}(\mathcal{C})$ ⊂矩阵空间$_r(\mathbb{Z}_p)$ 是一个秩为 r 的极大格，因此

$$\#\,\mathrm{End}(\mathcal{C}) \pmod{p^{\mathcal{M}}} = \#(\mathbb{Z}/p^{\mathcal{M}}\mathbb{Z})^r = p^{\mathcal{M}r}. \quad (3.41)$$

回想一下，$\mathrm{End}(\mathcal{C}) \subset \mathcal{O}_E$ 是一个满秩子模。此外，对于所有 $T \in \mathrm{Aut}(M)$，我们有$T + p^{\mathcal{M}}\,\mathrm{End}(\mathcal{C}) \subset \mathrm{Aut}(M)$。因此，$\mathrm{Aut}(\mathcal{C})$ 是 $\mathrm{End}(\mathcal{C})$ 中形如 $T + p^{\mathcal{M}}\mathrm{End}(\mathcal{C})$ 的子集的不交并，其中 $T \in \mathrm{Aut}(\mathcal{C})$。于是

$$\begin{aligned}\frac{\#\,\mathrm{Aut}(\mathcal{C}) \pmod{p^{\mathcal{M}}}}{\#\,\mathrm{End}(\mathcal{C}) \pmod{p^{\mathcal{M}}}} &= \frac{\#\,\mathrm{Aut}(\mathcal{C}) \pmod{p^{\mathcal{M}}}}{\#\mathcal{O}_E^{\times} \pmod{p^{\mathcal{M}}}} \frac{\#\mathcal{O}_E^{\times} \pmod{p^{\mathcal{M}}}}{\#\mathcal{O}_E \pmod{p^{\mathcal{M}}}} \frac{\#\mathcal{O}_E \pmod{p^{\mathcal{M}}}}{\#\,\mathrm{End}(\mathcal{C}) \pmod{p^{\mathcal{M}}}} \\ &= \frac{\#\mathcal{O}_E^{\times} \pmod{p^{\mathcal{M}}}}{\#\mathcal{O}_E \pmod{p^{\mathcal{M}}}} \cdot \frac{\#(\mathcal{O}_E/\,\mathrm{End}(\mathcal{C}))}{\#(\mathcal{O}_E^{\times}/\,\mathrm{Aut}(\mathcal{C}))} \\ &= \prod_{i=1}^{m}(1-p^{-r_i/e_i}) \cdot \frac{\#(\mathcal{O}_E/\,\mathrm{End}(\mathcal{C}))}{\#(\mathcal{O}_E^{\times}/\,\mathrm{Aut}(\mathcal{C}))},\end{aligned} \tag{3.42}$$

最后一步用到了这样一个事实：一个 $\mathcal{O}_E$ 中的元素属于$\mathcal{O}_E^{\times}$，当且仅当每个 K_i 坐标投影到剩余域 $\mathcal{O}_{K_i}/\pi_i\mathcal{O}_{K_i}$中的非零元素，而该剩余域的大小为$p^{r_i/e_i}$。(3.41)和(3.42)中的结果结合起来得到

$$\#(\mathrm{Aut}(\mathcal{C}) \pmod{p^{\mathcal{M}}}) = \frac{\#(\mathcal{O}_E/\,\mathrm{End}(\mathcal{C}))}{\#(\mathcal{O}_E^{\times}/\,\mathrm{Aut}(\mathcal{C}))} \prod_{i=1}^{m}(1-p^{-r_i/e_i})p^{\mathcal{M}r}. \tag{3.43}$$

(3.40)和(3.43)中的阶数之比就是我们所求商集的阶数。

□

最后，计算集合(3.37)的测度可归结为计算单个集合的 Haar 测度：

$$\{(I_r + p^{\mathcal{M}}\Delta T)f(A_{\mathcal{C}})(I_r + p^{\mathcal{M}}\Delta T)^{-1} \mid \Delta T \in \mathrm{Mat}_r(\mathbb{Z}_p), f \in F_Z\}.$$

我们用非常接近单位矩阵的矩阵对矩阵 $f(A_{\mathcal{C}})$施加共轭作用，因此自然会想到转到李代数，并将问题线性化。

回想一下，$\mathrm{Mat}_r(\mathbb{Z}_p)$是一个秩为 r^2的 $\mathbb{Z}_p$-模；对于 $A \in \mathcal{X}$，$\mathbb{Z}_p[\mathfrak{x}] \cong \mathbb{Z}_p[A] \subset \mathrm{Mat}_r(\mathbb{Z}_p)$是一个秩为 r的 $\mathbb{Z}_p$-子模。此外，根据命题 3.19，$\mathbb{Z}_p[A_{\mathcal{C}}]$ 的极大扩张是 $\mathrm{End}(\mathcal{C})$。

定义 3.24. 对于 $\mathcal{C} \in E^{\times}\backslash$模$_{\mathbb{Z}_p[\mathfrak{x}]}$，我们定义

$$\mathrm{End}(\mathcal{C})^{\perp} = \mathrm{Im}([\cdot, A_{\mathcal{C}}]\,|_{\mathrm{Mat}_r(\mathbb{Z}_p)}) = \{TA_{\mathcal{C}} - A_{\mathcal{C}}T \mid T \in \mathrm{Mat}_r(\mathbb{Z}_p)\},$$

李括号 $[\cdot, A_{\mathcal{C}}]$ 在 $\mathrm{Mat}_{r\times r}(\mathbb{Z}_p)$ 上的像。

下面的引理说明记号 $\mathrm{End}(\mathcal{C})^{\perp}$ 是合理的。

引理 3.25. 设 $\mathcal{C} \in E^{\times}\backslash$模$_{\mathbb{Z}_p[\mathfrak{x}]}$。则

$$\mathrm{End}(\mathcal{C}) \cap \mathrm{End}(\mathcal{C})^{\perp} = 0$$

以及 $\mathrm{End}(\mathcal{C}) + \mathrm{End}(\mathcal{C})^{\perp} \subset$矩阵空间$_r(\mathbb{Z}_p)$ 是一个满秩为 r^2 的 $\mathbb{Z}_p$-子模。此外，它的指数为

$$\#(\mathrm{Mat}_r(\mathbb{Z}_p)/\,\mathrm{End}(\mathcal{C}) + \mathrm{End}(\mathcal{C})^{\perp}) = p^{\mathrm{val}\,\mathrm{Disc}(\mathfrak{x})} = ||\,\mathrm{Disc}(\mathfrak{x})||^{-1}.$$

证明。将 $\mathrm{Mat}_{r\times r}(\mathbb{Z}_p) \cong \mathbb{Z}_p^r \otimes \mathbb{Z}_p^r$ 认作……，线性算子 $[\cdot, A] : \mathrm{Mat}_r(\mathbb{Z}_p) \to \mathrm{Mat}_r(\mathbb{Z}_p)$ 在基 $e_1 \otimes e_1$、……、$e_r \otimes e_1$、……、$e_1 \otimes e_r$、……、$e_r \otimes e_r$ 下由矩阵给出

$$A \otimes I_r - I_r \otimes A = \begin{pmatrix} a_{1,1}I_r - A & a_{1,2}I_r & \cdots & a_{1,r}I_r \\ a_{2,1}I_r & a_{2,2}I_r - A & \cdots & a_{2,r}I_r \\ \vdots & \vdots & \ddots & \vdots \\ a_{r,1}I_r & a_{r,2}I_r & \cdots & a_{r,r}I_r - A \end{pmatrix},$$

其中 $\otimes$是克罗内克积。我们断言该矩阵的特征多项式为$x^{r^2} + \cdots + \mathrm{Disc}(\mathfrak{x})x^r$。

¯为此，注意到上述矩阵经 $\mathrm{GL}_{r^2\times r^2}(\mathbb{Q}_p)$ 中的一个 r-块矩阵共轭后，得到分块对角矩阵

$$\begin{aligned}\mathrm{diag}_{r^2\times r^2}(\sigma_{1,1}(x_1)I_r-A,\dots,\sigma_{1,r_1}(x_1)I_r-A,\sigma_{2,1}(x_2)I_r-A,\dots,\sigma_{2,r_2}(x_2)I_r-A,\dots,\\ \sigma_{m,1}(x_m)I_r-A,\dots,\sigma_{m,r_m}(x_m)I_r-A),\end{aligned}\tag{3.44}$$

通过对 $A\otimes I_r$ 部分进行对角化，并回想 $\sigma_{i,\ j}(x_i)$ 是任意 $A\in\mathcal{X}$的特征值。(3.44) 中的分块形式具有如下特征多项式：

$$\begin{aligned}\prod_{i=1}^{m}\prod_{l_i=1}^{r_i}\det((x-\sigma_{i,l_i}(x_i))I_r+A)&=\prod_{(i,l_i)}\prod_{(j,l_j)}(x-\sigma_{i,l_i}(x_i)+\sigma_{j,l_j}(x_j))\\&=x^{r^2}+\cdots+\mathrm{Disc}(\mathfrak{x})x^r.\end{aligned}\tag{3.45}$$

现在回到矩阵的讨论。记 e_1，……， e_r 为 $\mathrm{End}(\mathcal{C})$ 的一个 $\mathbb{Z}_p$-基。由于 $\mathrm{End}(\mathcal{C})\subset\mathrm{Mat}_r(\mathbb{Z}_p)$ 是极大的，根据命题 3.18，我们可以将该序列扩充为 e_1，……， e_{r^2}，从而得到 $\mathrm{Mat}_r(\mathbb{Z}_p)$ 的一个 $\mathbb{Z}_p$-基。因为 A 与 $\mathrm{End}(\mathcal{C})$ 的元素可交换，所以李括号 $[\cdot,A]$ 在基 e_1，……， e_{r^2} 下的矩阵具有如下形式：

$$\begin{pmatrix}0&H\\0&D\end{pmatrix}\in\mathrm{Mat}_{r^2\times r^2}(\mathbb{Z}_p).$$

根据上文对特征多项式的讨论， $D\in\mathrm{Mat}_{(r^2-r)\times(r^2-r)}(\mathbb{Z}_p)$ 的行列式为 $\mathrm{Disc}(\mathfrak{x})$。在此情形下，$\mathrm{End}(\mathcal{C})^\perp$ 是由 $\begin{pmatrix}0&H\\0&D\end{pmatrix}$ 的列向量生成的自由 $\mathbb{Z}_p$-模。因此，$\mathrm{End}(\mathcal{C})\cap\mathrm{End}(\mathcal{C})^\perp=0$；又因为 $\mathrm{End}(\mathcal{C})$ 是 $[\cdot,A]$ 的核，所以 $\mathrm{End}(\mathcal{C})+\mathrm{End}(\mathcal{C})^\perp\subset\mathrm{Mat}_r(\mathbb{Z}_p)$ 是一个满秩为 r^2 的 $\mathbb{Z}_p$-子模。最后，由于 $\det(D)=\mathrm{Disc}(\mathfrak{x})$，我们有

$$\#(\mathrm{Mat}_r(\mathbb{Z}_p)/(\mathrm{End}(\mathcal{C})+\mathrm{End}(\mathcal{C})^\perp))=\left|\left|\det\begin{pmatrix}I_r&H\\0&D\end{pmatrix}\right|\right|^{-1}=||\,\mathrm{Disc}(\mathfrak{x})||^{-1}.$$

□

引理 3.26. 设 $\mathcal{C}\in E^\times\backslash\mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$ 和 $f\in F_Z$。则

$$\{Tf(A_\mathcal{C})-f(A_\mathcal{C})T\mid T\in\mathrm{Mat}_r(\mathbb{Z}_p)\}=\{TA_\mathcal{C}-A_\mathcal{C}T\mid T\in\mathrm{Mat}_r(\mathbb{Z}_p)\},$$

这里回顾一下，右边正是 $\mathrm{End}(\mathcal{C})^\perp$。

证明。 设 $A=A_\mathcal{C}$。包含关系

$$\{f(A)T-Tf(A)\mid T\in\mathrm{Mat}_r(\mathbb{Z}_p)\}\subset\{AT-TA\mid T\in\mathrm{Mat}_r(\mathbb{Z}_p)\}$$

实际上对任意多项式 $f\in\mathbb{Z}_p[x]$都成立；要证明这一点，只需证明对于所有 $k\geq1$， $f(x)=x^k$。这必然成立，因为

$$A^kT-TA^k=A(A^{k-1}T+A^{k-2}TA+\cdots+TA^{k-1})-(A^{k-1}T+A^{k-2}TA+\cdots+TA^{k-1})A,$$

它属于 $\mathrm{End}(\mathcal{C})^\perp$。

为证明反向包含，记 $A'=f(A)$。设对所有 $1\leq i\leq m$， $x_i'=f(x_i)$。根据命题 3.6，存在一个次数为 $\leq r-1$ 的 $g\in\mathbb{Z}_p[x]$，使得 $x_i=g(x_i')$。此时，对于所有 $1\leq i\leq m$，我们有 $g(f(x_i))=g(x_i')=x_i$，因此 $Z(x)\mid g(f(x))-x$。由 Cayley-Hamilton 定理，$A=g(f(A))=g(A')$ 可以表示为 A'的多项式。对 f 使用相同的论证可得

$$\{g(A')T-Tg(A')\mid T\in\mathrm{Mat}_r(\mathbb{Z}_p)\}\subset\{A'T-TA'\mid T\in\mathrm{Mat}_r(\mathbb{Z}_p)\},$$

并回想起 $g(A')=A$， $A'=f(A)$，这正是我们想要证明的。 □

下面的命题直观地测量一个微分元素的体积。

命题 3.27. 固定 $s=(s_1,\dots,s_m)\in(\frac{1}{e_1}\mathbb{N},\dots,\frac{1}{e_m}\mathbb{N})$，使得对所有 $1\le i\le m$ 都有 $s_i>r\operatorname{val}\operatorname{Disc}(\mathfrak{x})$。令 $\mathcal{C}\in E^\times\backslash\mathrm{Mod}^{\mathbb{Z}_p[\mathfrak{x}]}$。那么对于所有充分大的 $\mathcal{M}\in\mathbb{Z}$，我们有

$$\mathbf{P}(\{(I_r+\Delta T)f(A_{\mathcal{C}})(I_r+\Delta T)^{-1}\mid \Delta T\in p^{\mathcal{M}}\operatorname{Mat}_r(\mathbb{Z}_p), f\in F_Z\})=\frac{\#(\mathcal{O}_E/\operatorname{End}(\mathcal{C}))}{p^{\sum_i s_ir_i+\mathcal{M}(r^2-r)}},$$

其中，商集 $\mathcal{O}_E$ 和 $\operatorname{End}(\mathcal{C})$ 按照命题 *3.23* 视为矩阵环。

我们首先陈述一个关键引理，在此基础上证明命题 3.27，然后再回到该引理的证明。

引理 3.28。在与命题 *3.27* 相同的设定下，对于所有充分大的 $\mathcal{M}\in\mathbb{Z}$，我们有

$$\{(I_r+\Delta T)f(A_{\mathcal{C}})(I_r+\Delta T)^{-1}\mid \Delta T\in p^{\mathcal{M}}\operatorname{Mat}_r(\mathbb{Z}_p), f\in F_Z\}=A_{\mathcal{C}}+\prod_{i=1}^m\frac{\pi_i^{e_is_i}}{||Z'(x_i)||}\mathcal{O}_{K_i}+p^{\mathcal{M}}\operatorname{End}(\mathcal{C})^\perp,\quad(3.46)$$

其中，我们按照通常的记号 *3.14*，将 $\mathcal{O}_{K_i}\subset E$ 与 矩阵空间$r\times r(\mathbb{Q}_p)$ 的一个子集等同起来。

基于引理 *3.28* 的命题 *3.27* 的证明。对引理 3.28 中的集合进行平移不会改变其 Haar 测度，因此我们必须证明

$$\mathbf{P}\left(\prod_{i=1}^m\frac{\pi_i^{e_is_i}}{||Z'(x_i)||}\mathcal{O}_{K_i}+p^{\mathcal{M}}\operatorname{End}(\mathcal{C})^\perp\right)=\frac{\#(\mathcal{O}_E/\operatorname{End}(\mathcal{C}))}{p^{\sum_i s_ir_i+\mathcal{M}(r^2-r)}}.$$

由于

$$\prod_{i=1}^m\frac{\pi_i^{e_is_i}}{||Z'(x_i)||}\mathcal{O}_{K_i}+p^{\mathcal{M}}\operatorname{End}(\mathcal{C})^\perp$$

is 它是 $\mathrm{Mat}_r(\mathbb{Z}_p)$ 的一个 $\mathbb{Z}_p$-子模，而后者的测度为 1，因此只需证明

$$\#\left(\operatorname{Mat}_r(\mathbb{Z}_p)/\left(\prod_{i=1}^m\frac{\pi_i^{e_is_i}}{||Z'(x_i)||}\mathcal{O}_{K_i}+p^{\mathcal{M}}\operatorname{End}(\mathcal{C})^\perp\right)\right)=\frac{p^{\sum_i s_ir_i+\mathcal{M}(r^2-r)}}{\#(\mathcal{O}_E/\operatorname{End}(\mathcal{C}))}.\quad(3.47)$$

事实上，根据引理 3.25，我们有

$$\begin{aligned}\mathrm{LHS}(3.47)&=\#\left(\left(\operatorname{End}(\mathcal{C})+\operatorname{End}(\mathcal{C})^\perp\right)/\left(\prod_{i=1}^m\frac{\pi_i^{e_is_i}}{||Z'(x_i)||}\mathcal{O}_{K_i}+p^{\mathcal{M}}\operatorname{End}(\mathcal{C})^\perp\right)\right)\\&\quad\times\#(\operatorname{Mat}_r(\mathbb{Z}_p)/(\operatorname{End}(\mathcal{C})+\operatorname{End}(\mathcal{C})^\perp))\\&=\#\left((\operatorname{End}(\mathcal{C})+\operatorname{End}(\mathcal{C})^\perp)/\left(\prod_{i=1}^m\frac{\pi_i^{e_is_i}}{||Z'(x_i)||}\mathcal{O}_{K_i}+p^{\mathcal{M}}\operatorname{End}(\mathcal{C})^\perp\right)\right)||\cdot\operatorname{Disc}(\mathfrak{x})||^{-1}\\&=\frac{p^{\mathcal{M}(r^2-r)}}{||\operatorname{Disc}(\mathfrak{x})||}\#\left(\operatorname{End}(\mathcal{C})/\prod_{i=1}^m\frac{\pi_i^{e_is_i}}{||Z'(x_i)||}\mathcal{O}_{K_i}\right),\end{aligned}\quad(3.48)$$

其中在最后一步，我们利用了 $\operatorname{End}(\mathcal{C})\cap\operatorname{End}(\mathcal{C})^\perp=0$ 和 $\operatorname{End}(\mathcal{C})^\perp$ 的秩为 r^2-r。此外，回想一下 $\mathcal{O}_E=\prod_{i=1}^m\mathcal{O}_{K_i}$。由此可得

$$\begin{aligned}\#\left(\operatorname{End}(\mathcal{C})/\prod_{i=1}^m\frac{\pi_i^{e_is_i}}{||Z'(x_i)||}\mathcal{O}_{K_i}\right)&=\frac{\#(\mathcal{O}_E/\prod_{i=1}^m\frac{\pi_i^{e_is_i}}{||Z'(x_i)||}\mathcal{O}_{K_i})}{\#(\mathcal{O}_E/\operatorname{End}(\mathcal{C}))}\\&=\frac{\prod_{i=1}^m\#(\mathcal{O}_{K_i}/\frac{\pi_i^{e_is_i}}{||Z'(x_i)||}\mathcal{O}_{K_i})}{\#(\mathcal{O}_E/\operatorname{End}(\mathcal{C}))}\\&=\frac{\prod_{i=1}^m p^{s_ir_i}||Z'(x_i)||^{r_i}}{\#(\mathcal{O}_E/\operatorname{End}(\mathcal{C}))}.\end{aligned}\quad(3.49)$$

因此我们有

$$\mathrm{LHS}(3.47) = \frac{p^{\mathcal{M}(r^2-r)}}{||\operatorname{Disc}(\mathfrak{x})||}\frac{p^{\sum_i s_i r_i}\prod_{i=1}^m ||Z'(x_i)||^{r_i}}{\#(\mathcal{O}_E/\operatorname{End}(\mathcal{C}))} = \mathrm{RHS}(3.47),$$

其中，最后一个等式成立是因为 $\prod_{i=1}^m ||Z'(x_i)||^{r_i} = ||\mathbf{Disc}(\mathfrak{x})||$。证明到此结束。 □

现在我们回到引理 3.28 的证明。

引理 *3.28* 的证明。令 $A = A_{\mathcal{C}}$。我们证明 (3.46) 的 (⊂) 和 (⊃)。

(⊂) 对于所有这样的 f 和 ΔT,

$$(I_r + \Delta T)f(A)(I_r + \Delta T)^{-1} - A = (I_r + \Delta T)f(A)(I_r - \Delta T + (\Delta T)^2 - \cdots) - A$$

属于集合

$$f(A) - A + \Delta T f(A) - f(A)\Delta T + p^{2\mathcal{M}}\operatorname{Mat}_r(\mathbb{Z}_p).$$

因此，我们只需证明当 $\mathcal{M}$充分大时，

$$f(A) - A + \Delta T f(A) - f(A)\Delta T + p^{2\mathcal{M}}\operatorname{Mat}_r(\mathbb{Z}_p) \subset \prod_{i=1}^m \frac{\pi_i^{e_i s_i}}{||Z'(x_i)||}\mathcal{O}_{K_i} + p^{\mathcal{M}}\operatorname{End}(\mathcal{C})^\perp.$$

我们已经知道 $f(A) - A \subset \prod_{i=1}^m \frac{\pi_i^{e_i s_i}}{||Z'(x_i)||}\mathcal{O}_{K_i}$。由引理 3.26 可得 $\Delta T f(A) - f(A)\Delta T \in p^{\mathcal{M}}\operatorname{End}(\mathcal{C})^\perp$。因此，我们还需证明 $p^{2\mathcal{M}}$ 矩阵空间$_r(\mathbb{Z}_p) \subset \prod_{i=1}^m \frac{\pi_i^{e_i s_i}}{||Z'(x_i)||}\mathcal{O}_{K_i} + p^{\mathcal{M}}\operatorname{End}(\mathcal{C})^\perp$。当 $\mathcal{M}$ 充分大时，有 $p^{\mathcal{M}}$矩阵空间$_r(\mathbb{Z}_p) \subset \operatorname{End}(\mathcal{C}) + \operatorname{End}(\mathcal{C})^\perp$，因为后者是一个满秩子格；同理，$p^{\mathcal{M}}\operatorname{End}(\mathcal{C}) \subset \prod_{i=1}^m \frac{\pi_i^{e_i s_i}}{||Z'(x_i)||}\mathcal{O}_{K_i}$。在这种情况下，

$$p^{2\mathcal{M}}\operatorname{Mat}_r(\mathbb{Z}_p) \subset p^{\mathcal{M}}\operatorname{End}(\mathcal{C}) + p^{\mathcal{M}}\operatorname{End}(\mathcal{C})^\perp \subset \prod_{i=1}^m \frac{\pi_i^{e_i s_i}}{||Z'(x_i)||}\mathcal{O}_{K_i} + p^{\mathcal{M}}\operatorname{End}(\mathcal{C})^\perp,$$

因此，(⊂) 得证。

(⊃) 我们首先断言，(3.46) 的右侧可以改写为

$$A + \prod_{i=1}^m \frac{\pi_i^{e_i s_i}}{||Z'(x_i)||}\mathcal{O}_{K_i} + p^{\mathcal{M}}\operatorname{End}(\mathcal{C})^\perp$$
$$= \{\tilde{f}(A) + \Delta\tilde{T}A - A\Delta\tilde{T} \mid \tilde{f} \in F_Z, \Delta\tilde{T} \in p^{\mathcal{M}}\operatorname{Mat}_{r\times r}(\mathbb{Z}_p)\}. \quad (3.50)$$

这是通过在定义 3.24 中重新命名 $\Delta\tilde{T} = p^{\mathcal{M}}\Delta T$，并注意到将定义 3.2 略作改写可得

$$\prod_{i=1}^m \frac{\pi_i^{e_i s_i}}{||Z'(x_i)||}\mathcal{O}_{K_i} = \{\tilde{f}(\mathfrak{x}) - \mathfrak{x} \mid \tilde{f} \in F_Z\} \quad (3.51)$$

~ ~，右侧对应于矩阵集合 $\{f(A) - A \mid f \in F_Z\}$。

因此，我们只需证明：对于任意这样的 $\tilde{f} \in F_Z$ 和 $\Delta\tilde{T} \in p^{\mathcal{M}}$ 矩阵空间$_r(\mathbb{Z}_p)$，存在 $\Delta T \in p^{\mathcal{M}}$矩阵空间$_r(\mathbb{Z}_p)$ 以及 $f \in F_Z$，使得

$$(I_r + \Delta T)^{-1}(\tilde{f}(A) + \Delta\tilde{T}A - A\Delta\tilde{T})(I_r + \Delta T) = f(A). \quad (3.52)$$

其思路是模仿亨泽尔引理的证明，通过~ ~ ~共轭作用 $f(A) + \Delta T A - A\Delta T$，依次使用一系列矩阵 $I_r + \Delta T_j$，逐步构造 ΔT 和 f，使其达到所需形式。

我们断言，存在一个由 F_Z 中的多项式构成的序列 $(f_j)_{j\geq 1}$，以及矩阵序列

~ ~ ~ ~$(\Delta T_j)_{j\geq 1}$, $(\Delta\tilde{T}_j)_{j\geq 1}$，其初始项为 $f_1 = f$, $\Delta T_1 = \Delta T$，使得

$$(I_r + \Delta T_j)^{-1}(f_j(A) + \Delta\tilde{T}_j A - A\Delta\tilde{T}_j)(I_r + \Delta T_j) = f_{j+1}(A) + \Delta\tilde{T}_{j+1}A - A\Delta\tilde{T}_{j+1}, \quad (3.53)$$

$$\Delta T_j, \Delta\tilde{T}_j \in p^{\lfloor (j+1)\mathcal{M}/2\rfloor}\operatorname{Mat}_r(\mathbb{Z}_p), \quad (3.54)$$

（即两个矩阵在每一步的范数都更小），并且

$$f_{j+1}(A) - f_j(A) \in p^{\lfloor (j+1)\mathcal{M}/2 \rfloor} \operatorname{Mat}_r(\mathbb{Z}_p). \tag{3.55}$$

只需证明 (3.53)、(3.54) 和 (3.55)，因为这样多项式 f_j 就会收敛到极限 f_∞。这是因为非阿基米德范数满足强三角不等式；又由于~(3.54)，当 $j \to \infty$ 时，$\Delta T_j A - A\Delta T_j$ 项收敛到 0，因此我们有

$$\prod_{j=1}^{\infty}(I_r + \Delta T_j)^{-1}(\tilde{f}(A) + \Delta\tilde{T}A - A\Delta\tilde{T}) \prod_{j=1}^{\infty}(I_r + \Delta T_j)^{-1} = f_\infty(A). \tag{3.56}$$

取 $f = f_\infty$ 和 $\Delta T = \prod_{j=1}^{\infty}(I_r + \Delta T_j) - I_r$，即可得到 (3.52)。现在我们来给出构造。

令 $j \geq 1$。在第 j^{th} 步，我们将以 f_j 和 $\Delta\tilde{T}_j$ 作为输入（注意，当 $j = 1$ 时，我们已经有了这些，因为我们令 $f_1 = f$ 和 $\Delta T_1 = \Delta T$），并找出满足 (3.53)、(3.54) 和 (3.55) 的多项式 f_{j+1} 以及~矩阵 ΔT_j，ΔT_{j+1}。共分两步。

(1) 我们找到 $\Delta T_j \in p^{\lfloor (j+1)\mathcal{M}/2 \rfloor} \operatorname{Mat}_r(\mathbb{Z}_p)$，使得 $\Delta T_j f_j(A) - f_j(A)\Delta T_j = \Delta\tilde{T}_j A - A\Delta\tilde{T}_j$。根据引理 3.26，这总是可以实现的。~(2) 考虑 $(I_r + \Delta T_j)$ 对 $f_j(A) + \Delta T_j A - A\Delta T_j$ 的共轭作用：

$$\begin{aligned}(I_r + \Delta T_j)^{-1}(f_j(A) + \Delta\tilde{T}_j A - A\Delta\tilde{T}_j)(I_r + \Delta T_j) = (I_r - \Delta T_j + \Delta T_j^2 - \cdots)\cdot \\ (f_j(A) + \Delta\tilde{T}_j A - A\Delta\tilde{T}_j)(I_r + \Delta T_j) \subset f_j(A) + p^{(j+1)\mathcal{M}-1} \operatorname{Mat}_r(\mathbb{Z}_p).\end{aligned}$$

当 $\mathcal{M}$ 足够大时（且这一条件是一致的，不依赖于 $j \geq 1$ 的具体取值），必有

$$p^{(j+1)\mathcal{M}-1} \operatorname{Mat}_r(\mathbb{Z}_p) \subset \prod_{i=1}^{m} \frac{\pi_i^{e_i s_i}}{||Z'(x_i)||}\mathcal{O}_{K_i} + p^{\lfloor (j+2)\mathcal{M}/2 \rfloor} \operatorname{End}(\mathcal{C})^\perp.$$

由 (3.51)，

$$f_j(A) + \prod_{i=1}^{m} \frac{\pi_i^{e_i s_i}}{||Z'(x_i)||}\mathcal{O}_{K_i} = \{g(A) : g \in F_Z\}, \tag{3.57}$$

因此，存在 $f_{j+1} \in F_Z$ 和 $\Delta\tilde{T}_{j+1} \in p^{\lfloor (j+2)\mathcal{M}/2 \rfloor} \operatorname{Mat}_r(\mathbb{Z}_p)$，使得 (3.53) 成立。

~这就构造出了满足 (3.53)、(3.54) 和 (3.55) 的序列 $(f_j)_{j\geq 1}$，$(\Delta T_j)_{j\geq 1}$，$(\Delta T_j)_{j\geq 1}$，故证毕。□

推论 3.29。取定 $s = (s_1, \ldots, s_m) \in (\frac{1}{e_1}\mathbb{N}, \ldots, \frac{1}{e_m}\mathbb{N})$，使得对所有 $1 \leq i \leq m$，都有 $s_i > r$ $\operatorname{val}\operatorname{Disc}(\mathfrak{x})$。设 $\mathcal{C} \in E^\times \backslash$模$\mathbb{Z}_p[\mathfrak{x}]$。则有

$$\mathbf{P}(\{Tf(A_\mathcal{C})T^{-1} \mid T \in \mathrm{GL}_r(\mathbb{Z}_p), f \in F_Z\}) = \frac{(1-p^{-1})\cdots(1-p^{-r})}{\prod_{i=1}^{m}(1-p^{-r_i/e_i})p^{s_i r_i}} \#(\mathcal{O}_E^\times / \operatorname{Aut}(\mathcal{C})). \tag{3.58}$$

证明。回顾引理 3.22 中公式 (3.38) 的不交并中的每个集合都具有相同的测度。根据命题 3.23，共有

$$\#(\mathrm{GL}_r(\mathbb{Z}_p/p^\mathcal{M}\mathbb{Z}_p)/\operatorname{Aut}(\mathcal{C}) \pmod{p^\mathcal{M}}) = p^{\mathcal{M}(r^2-r)} \frac{(1-p^{-1})\cdots(1-p^{-r})\#(\mathcal{O}_E^\times/\operatorname{Aut}(\mathcal{C}))}{\prod_{i=1}^{m}(1-p^{-r_i/e_i})\#(\mathcal{O}_E/\operatorname{End}(\mathcal{C}))}$$

这些元素。因此，我们有

$$\begin{aligned}\mathrm{LHS}(3.58) &= p^{\mathcal{M}(r^2-r)}\frac{(1-p^{-1})\cdots(1-p^{-r})\#(\mathcal{O}_E^\times/\operatorname{Aut}(\mathcal{C}))}{\prod_{i=1}^m(1-p^{-r_i/e_i})\#(\mathcal{O}_E/\operatorname{End}(\mathcal{C}))}\\ &\quad\times\mathbf{P}(\{(I_r+\Delta T)f(A_{\mathcal{C}})(I_r+\Delta T)^{-1}\mid \Delta T\in p^{\mathcal{M}}\operatorname{Mat}_r(\mathbb{Z}_p), f\in F_Z\})\\ &= \frac{(1-p^{-1})\cdots(1-p^{-r})}{\prod_{i=1}^m(1-p^{-r_i/e_i})p^{s_ir_i}}\frac{\#(\mathcal{O}_E^\times/\operatorname{Aut}(\mathcal{C}))}{\#(\mathcal{O}_E/\operatorname{End}(\mathcal{C}))}\#(\mathcal{O}_E/\operatorname{End}(\mathcal{C}))\\ &= \frac{(1-p^{-1})\cdots(1-p^{-r})}{\prod_{i=1}^m(1-p^{-r_i/e_i})p^{s_ir_i}}\#(\mathcal{O}_E^\times/\operatorname{Aut}(\mathcal{C})),\end{aligned}\tag{3.59}$$

其中第二个等式由命题 3.27 得出。由此即得证明。 □

以下 Yun13] 的结果使我们能够简化公式中对 $\mathcal{C}\in E^\times\backslash\mathbf{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]}$ 的求和。

命题 3.30。 对于商集 $\#(\Lambda_E\backslash\mathrm{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]})$，以下等式成立：

$$\sum_{\mathcal{C}\in E^\times\backslash\operatorname{Mod}_{\mathbb{Z}_p[\![\mathfrak{x}]\!]}}\#(\mathcal{O}_E^\times/\operatorname{Aut}(\mathcal{C}))=\#(\Lambda_E\backslash\operatorname{Mod}_{\mathbb{Z}_p[\![\mathfrak{x}]\!]}),\tag{3.60}$$

and

$$\#(\Lambda_E\backslash\operatorname{Mod}_{\mathbb{Z}_p[\![\mathfrak{x}]\!]})||\Delta_\sigma(x_1,\dots,x_m)||=\prod_{i=1}^m\#(\Lambda_{K_i}\backslash\operatorname{Mod}_{\mathbb{Z}_p[x_i]})||\Delta_\sigma(x_i)||.\tag{3.61}$$

证明。 (3.60) 出自 [Yun13，第 2 节14], ，具体来说，是 _[Yun13, (2.17)] 之后的句子“Now weclaim...”；其中的 Cl(*R*) 和 X_R 分别对应于我们记号中的 $E^\times\backslash\mathbf{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]}$ 和 $\mathbf{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]}$。对于 (3.61)，注意到

$$\begin{aligned}\frac{\prod_{i=1}^m||\Delta_\sigma(x_i)||}{||\Delta_\sigma(x_1,\dots,x_m)||} &= \frac{\prod_{i=1}^m||\Delta(\sigma_{i,1}x_i,\dots,\sigma_{i,r_i}x_i)||}{||\Delta(\sigma_{1,1}x_1,\dots,\sigma_{1,r_1}x_1,\dots,\sigma_{m,1}x_m,\dots,\sigma_{m,r_m}x_m)||}\\ &= \prod_{1\le i<j\le m}\prod_{l_i=1}^{r_i}\prod_{l_j=1}^{r_j}||\sigma_{i,l_i}(x_i)-\sigma_{j,l_j}(x_j)||^{-1}\\ &= \prod_{1\le i<j\le m}||\operatorname{Res}(Z_i,Z_j)||^{-1}\\ &= p^{\sum_{1\le i<j\le m}\operatorname{val}(\operatorname{Res}(Z_i,Z_j))}.\end{aligned}\tag{3.62}$$

这里，对于所有 $1\le i<j\le m$，Res(Z_i, Z_j) 表示第 2.3 节中的多项式 Z_i, Z_j 的结式。因此，为了证明 (3.61)，我们只需证明

$$\#(\Lambda_E\backslash\operatorname{Mod}_{\mathbb{Z}_p[\![\mathfrak{x}]\!]})=p^{\sum_{1\le i<j\le m}\operatorname{val}(\operatorname{Res}(Z_i,Z_j))}\cdot\prod_{i=1}^m\#(\Lambda_{K_i}\backslash\operatorname{Mod}_{\mathbb{Z}_p[x_i]}),$$

这与 [Yun13，推论 4.10][4]完全相同。 □

注 3.31。 注意，我们研究的是 $E^\times$ 和 Λ 在同一个模集 $\mathbf{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]}$上的群作用。群 Λ 是 $E^\times$的一个子群，因此生成更多轨道。事实上，(3.60) 中商集 $\#(\mathcal{O}_E^\times/\operatorname{Aut}(\mathcal{C}))$ 的阶就是类 $\mathcal{C}$在 Λ的群作用下的轨道数。

现在，我们可以开始证明定理 3.1 了。

[4]按照 [Yun13，推论 4.10], 中的记号，对于所有 $1\le i\le m$，我们取 $q=p$、 $O_\gamma=\#(\Lambda_E\backslash\mathbf{Mod}^{\mathbb{Z}_p[\![\mathfrak{x}]\!]})$、 $B(\gamma)=\{1,2,\dots,m\}$ 以及 $O_{\gamma_i}^{L_i}=\#(\Lambda_{K_i}\backslash\mathbf{Mod}^{\mathbb{Z}_p[x_i]})$。根据 [Yun13，第 4.1], 小节中的定义，记号 $\rho(\gamma)$ 等于 $\sum_{1\le i<j\le m}\operatorname{val}(\operatorname{Res}(Z_i,Z_j))$，这正是我们在此所需的表达式。

定理 *3.1* 的证明。 当 $s=(s_1,\dots,s_m)\in(\frac{1}{e_1}\mathbb{N},\dots,\frac{1}{e_m}\mathbb{N})$ 满足 $s_i>r$ val Disc(𝔯) 对所有 $1\le i\le m$ 均成立时，我们有（回忆定义 3.16 中的记号）：

$$\begin{aligned}\mathrm{LHS}(3.1)&=\prod_{i=1}^{m}p^{s_ir_i}\cdot\sum_{\mathcal{C}\in E^\times\backslash\mathrm{Mod}_{\mathbb{Z}_p[\mathfrak{x}]}}\mathbf{P}(\{Tf(A_{\mathcal{C}})T^{-1}\mid T\in\mathrm{GL}_r(\mathbb{Z}_p),f\in F_Z\})\\&=\sum_{\mathcal{C}\in E^\times\backslash\mathrm{Mod}_{\mathbb{Z}_p[\mathfrak{x}]}}\frac{(1-p^{-1})\cdots(1-p^{-r})}{\prod_{i=1}^{m}(1-p^{-r_i/e_i})}\#(\mathcal{O}_E^\times/\mathrm{Aut}(\mathcal{C}))\\&=\frac{(1-p^{-1})\cdots(1-p^{-r})}{\prod_{i=1}^{m}(1-p^{-r_i/e_i})}\#(\Lambda_E\backslash\mathrm{Mod}_{\mathbb{Z}_p[\mathfrak{x}]})\\&=\frac{(1-p^{-1})\cdots(1-p^{-r})}{||\Delta_\sigma(x_1,\dots,x_m)||}\prod_{i=1}^{m}\frac{\#(\Lambda_{K_i}\backslash\mathrm{Mod}_{\mathbb{Z}_p[x_i]})||\Delta_\sigma(x_i)||}{(1-p^{-r_i/e_i})}\\&=\mathrm{RHS}(3.1).\end{aligned}\tag{3.63}$$

其中，第一个等式由推论 3.21 得出，第二个等式来自推论 3.29，第三个等式来自 (3.60)，第四个等式来自 (3.61)。因此，证明完毕。□

注 3.32。 我们注意到，Boreico 未发表的学位论文中也出现了类似的公式和技巧 [Bor16，第 3] 节（在我们找到这里的证明后，感谢 Akshay Venkatesh 提醒我们注意到这一点）。该工作研究了随机矩阵的特征多项式系数的联合分布这一相关问题。在 [Bor16，第 3.3.26(b) 定理中给出了这些系数关于 Haar 测度的联合密度 $\rho(f)$]。其中的公式类似于 (3.63) 的第二行，包含一个无穷和。看来，对 (3.63) 进行进一步简化——在对每个格类 $\mathcal{C}$ 所对应的概率测度求和时，项 #($\Lambda_E\backslash$Mod$^{\mathbb{Z}_p[\mathfrak{x}]}$) 出现——也可能导出一个类似于 (3.1) 右端的更简单的 $\rho(f)$ 表达式，但 [Bor16] 中并未这样做。

4. From characteristic polynomial to joint distribution of eigenvalues

除非另有说明，本节沿用上一节开头给出的相同记号。

4.1. 定理 1.7 的证明。

下面的命题使我们可以专注于 ´étale 代数中的新元素。

命题 4.1。 令 $A\in$矩阵空间$_n(\mathbb{Z}_p)$ 服从 *Haar* 分布。则有

$$\mathbf{P}(A\ \textit{has repeated eigenvalues})=0.$$

命题 4.1 是下述引理的直接推论，该引理是 p-进情形下的[CT05]类比。

引理 4.2。 令 $n\ge1$ 为一个整数，且令 $f\in\mathbb{Z}_p[\mathbf{x}_1,\dots,\mathbf{x}_n]:\ \mathbb{Z}_p^n\to\mathbb{Z}_p$ 为系数属于 $\mathbb{Z}_p$ 的非零多项式。令 $(a_1,\dots,a_n)\in\mathbb{Z}_p^n$ 关于 *Haar* 概率测度服从随机分布。则有

$$\mathbf{P}(f(a_1,\dots,a_n)=0)=0.$$

基于引理 *4.2* 的命题 *4.1* 证明。 考虑特征多项式P_A。其判别式可视为关于 A的 n^2 元多项式，表示为

$$\begin{aligned}f:\mathrm{Mat}_n(\mathbb{Z}_p)&\to\mathbb{Z}_p\\A&\mapsto\mathrm{Disc}(P_A).\end{aligned}\tag{4.1}$$

f 的零点集恰好是具有重根的矩阵 $A \in \mathrm{Mat}_n(\mathbb{Z}_p)$。显然， f 并非恒为零，因为存在一个没有重根的矩阵 $\mathrm{Mat}_n(\mathbb{Z}_p)$。由此，应用引理 4.2 即可完成证明。□

引理 *4.2* 的证明。 我们对 n 使用归纳法给出证明。当$n = 1$时，该命题显然成立。现在，假设该断言对 $n-1$ 成立。给定 $f \in \mathbb{Z}_p[\mathbf{x}_1, \dots, \mathbf{x}_n]$，我们写成

$$f = \sum_{j \in \mathbb{N}} f_j(\mathbf{x}_1, \dots, \mathbf{x}_{n-1}) \mathbf{x}_n^j,$$

其中多项式 f_j 的系数属于 $\mathbb{Z}_p$。由于 f 非零，存在某个 $j \in \mathbb{N}$使得 f_j非零。当 $f(a_1, \dots, a_n) = 0$ 时，序列 $(a_1, \dots, a_{n-1})$ 必须满足以下情形之一：

(1) $f_j(a_1, \dots, a_{n-1}) = 0$。根据归纳假设，此情形的概率为零。(2) $f_j(a_1, \dots, a_{n-1}) \neq 0$。在此情形下，满足 $f(a_1, \dots, a_n) =0$ 的 a_n只有有限多个，其概率同样为零。

因此，证明完毕。 □

为准备定理 1.7 的证明，我们陈述如下 p-进 Kac-Rice 公式，这是 [Car22, 定理 2.1] 的推广版本：

引理 4.3。 对于固定的 $A \in$矩阵空间$_r(\mathbb{Z}_p)$ 以及一个紧开子集 $U \subset \mathcal{O}_E^{\mathrm{new}}$，对所有整数 $s \geq 0$，有

$$\#\{\mathfrak{x} \in U \mid P_A(\mathfrak{x}) = 0\} = \lim_{s \to \infty} \int_U I_s(\mathfrak{x}, A) d\mathfrak{x},$$

其中极限沿非负整数 $s \in \mathbb{N}$ 取得，并且对于 $\mathfrak{x} = (x_1, \dots, x_m)$，

$$I_s(\mathfrak{x}, A) = p^{sr} \prod_{i=1}^m ||P_A'(x_i)||^{r_i} \cdot \mathbb{1}_{\mathrm{val}\, P_A(x_i) \geq s, \forall 1 \leq i \leq m}.$$

证明。 假设我们有 $\mathfrak{y} = (y_1, \dots, y_m) \in U$，且 $P_A(\mathfrak{y}) = 0$。对每个 $1 \leq i \leq m$ 应用 [CRV14, 引理 3.4][5]，存在一个正整数 S_{y_i}，使得下式成立：

(1) $||P_A'(x_i)|| = ||P_A'(y_i)||$，以及 $x_i \in y_i + \frac{\pi_i^{e_i S_{y_i}}}{||P_A'(y_i)||}\mathcal{O}_{K_i}$。 (2)

对任意整数 $s > S_{y_i}$，多项式 P_A 给出一个双射

$$y_i + \frac{\pi_i^{e_i s}}{||P_A'(y_i)||}\mathcal{O}_{K_i} \leftrightarrow \pi_i^{e_i s}\mathcal{O}_{K_i}. \tag{4.2}$$

取 $S_{\mathfrak{y}} = \max_i S_{y_i}$，由 (4.2) 立即可得，对于任意整数 $s > S_{\mathfrak{y}}$， P_A构成一个双射

$$\mathfrak{y} + \prod_{i=1}^m \frac{\pi_i^{e_i s}}{||P_A'(y_i)||}\mathcal{O}_{K_i} \leftrightarrow \prod_{i=1}^m \pi_i^{e_i s}\mathcal{O}_{K_i}. \tag{4.3}$$

在这种情况下，对于所有 $s > S_{\mathfrak{y}}$，我们都有

$$\begin{aligned}
\int_{\mathfrak{y} + \prod_{i=1}^m \frac{\pi_i^{e_i S_{\mathfrak{y}}}}{||P_A'(y_i)||}\mathcal{O}_{K_i}} I_s(\mathfrak{x}, A) d\mathfrak{x} &= \int_{\mathfrak{y} + \prod_{i=1}^m \frac{\pi_i^{e_i S_{\mathfrak{y}}}}{||P_A'(y_i)||}\mathcal{O}_{K_i}} p^{sr} \prod_{i=1}^m ||P_A'(y_i)||^{r_i} \mathbb{1}_{P_A(\mathfrak{x}) \in \prod_{i=1}^m \pi_i^{e_i s}\mathcal{O}_{K_i}} d\mathfrak{x} \\
&= p^{sr} \prod_{i=1}^m ||P_A'(y_i)||^{r_i} \int_{\mathfrak{y} + \prod_{i=1}^m \frac{\pi_i^{e_i s}}{||P_A'(y_i)||}\mathcal{O}_{K_i}} d\mathfrak{x} \\
&= 1.
\end{aligned} \tag{4.4}$$

[5]CRV14 引理 3.4] 的表述在记号上稍显繁复，但我们在此使用的特例与 Car22 定理 2.1] 证明中随后使用的特例完全相同。这两个结果都是针对严格可微函数表述的；这类函数特别包括所有多项式。

此外，由于 P_A 是 (4.3) 中各集合之间的双射，且后一个集合包含 0，$\mathfrak{y}$ 是 P_A 在集合 $\mathfrak{y}+\prod_{i=1}^{m}\pi_i^{e_iS_{\mathfrak{y}}}/||P_A'(y_i)||\mathcal{O}_{K_i}$ 中的唯一零点。因此，P_A 的零点构成 U 的离散子集。由于 U 是紧的，所以 U 中只有有限多个零点，记为

$$\mathfrak{y}_1=(y_{1,1},\dots,y_{1,m}),\dots,\mathfrak{y}_n=(y_{n,1},\dots,y_{n,m}).$$

取一个整数 S，使得 $S>\max\{S_{\mathfrak{y}_1},\dots,S_{\mathfrak{y}_n}\}$，且集合

$$U_k=\mathfrak{y}_k+\prod_{i=1}^{m}\frac{\pi_i^{e_iS}}{||P_A'(y_{k,i})||}\mathcal{O}_{K_i},\quad 1\le k\le n$$

两两不交。记 V为 U中 $U_1\cup\cdots\cup U_n$的补集。由于 V是紧的，且 P_A在其上不为零，我们推得当 s 足够大时，对所有 $\mathfrak{x}\in V$都有 $||P_A(\mathfrak{x})||\ge p^{-s}$。因此，当 $\mathfrak{x}\in V$时，$I_s(\mathfrak{x},A)$ 中的示性函数恒为 0。于是

$$\int_U I_s(\mathfrak{x},A)d\mathfrak{x}=\int_V I_s(\mathfrak{x},A)d\mathfrak{x}+\sum_{i=1}^{n}\int_{U_i}I_s(\mathfrak{x},A)d\mathfrak{x}=0+\sum_{i=1}^{n}1=n,$$

证明至此结束。 □

注 4.4。虽然在引理 4.3 中我们尚未假设 A具有互异特征值，但在$\mathcal{O}_E^{\mathrm{new}}$上不会出现含有重复项的特征值组，因此限制在$\mathcal{O}_E^{\mathrm{new}}$上时，$P_A$ 的所有根均互不相同。

下面的引理对于定理 1.7 的证明至关重要，定理 1.7 是[Eva06，命题 2.3]的一个应用。

引理 4.5. 对于固定的 $A\in$矩阵空间$_r(\mathbb{Z}_p)$，以及一个开子集 $U\subset\mathcal{O}_E^{\mathrm{new}}$，对所有整数$s\ge 0$，我们有：

$$\int_U I_s(\mathfrak{x},A)d\mathfrak{x}=p^{sr}\int_{\prod_{i=1}^{m}\pi_i^{e_is}\mathcal{O}_{K_i}}\#\{\mathfrak{x}\in U\mid P_A(\mathfrak{x})=\mathfrak{y}\}d\mathfrak{y}. \tag{4.5}$$

证明. 我们将 $E=K_1\times\cdots\times K_m$视为 $\mathbb{Q}_p$-向量空间 $\mathbb{Q}_p^r$。类似地，每个分量K_i 都视为 $\mathbb{Q}_p^{r_i}$。我们回顾一下 $\mathbb{Q}_p$-向量空间之间映射的雅可比矩阵定义，例如参见 [Eva06，第282]页。对于任意多项式 $f\in\mathbb{Q}_p[x]$和任意元素 $\mathfrak{x}=(x_1,\dots,x_m)\in E$，注意到 $f(\mathfrak{x})=(f(x_1)\dots,f(x_m))$，因此雅可比矩阵 Jf是一个分块对角矩阵，每个域分量 K_i对应一个$r_i\times r_i$块。我们将此块记为 $J_{K_i}f$，它正是映射 $f:K_i\to K_i$ 的雅可比矩阵，其中我们再次将 K_i 视为 $\mathbb{Q}_p^{r_i}$。

根据 [Eva06，命题 2.3][6]，，我们有

$$\mathrm{RHS}(4.5)=p^{sr}\int_U||\det(JP_A(\mathfrak{x}))||\mathbb{1}_{\mathrm{val}\,P_A(x_i)\ge s,\forall 1\le i\le m}d\mathfrak{x}. \tag{4.6}$$

这里，$JP_A(\mathfrak{x})$ 是在 E 上的标量乘法 $P_A'(\mathfrak{x})$，而 $\det(JP_A(\mathfrak{x}))$ 是将 $JP_A(\mathfrak{x})$ 视为线性映射时的行列式。同样，对于每个 $1\le i\le m$，我们用 $J_{K_i}P_A(x_i)$ 表示在 K_i 上的 $P_A'(x_i)$ 的标量乘法，并用 $\det(J_{K_i}P_A(x_i))$ 表示其行列式。若我们为每个 $1\le i\le m$ 选取 K_i 的一组基，那么这些向量共同构成 E 的一组自然基。这意味着

$$\begin{aligned}||\det(JP_A(\mathfrak{x}))||&=\prod_{i=1}^{m}||\det(J_{K_i}P_A(x_i))||\\&=\prod_{i=1}^{m}||\mathrm{Nm}_{K_i/\mathbb{Q}_p}P_A'(x_i)||\\&=\prod_{i=1}^{m}||P_A'(x_i)||^{r_i}.\end{aligned} \tag{4.7}$$

[6]采用 [Eva06], 中的记号，我们取 $f=P_A$、$g=\mathbb{1}_{\prod_{i=1}^{m}\pi_i^{e_is}\mathcal{O}_{K_i}}$ 和 $X=U$。

结合（4.6）和（4.7），可得

$$\mathrm{RHS}(4.5) = \int_U p^{sr} \prod_{i=1}^{m} ||P_A'(x_i)||^{r_i} \cdot \mathbb{1}_{\mathrm{val}\, P_A(x_i) \geq s, \forall 1 \leq i \leq m} dx_1 \cdots dx_m = \mathrm{LHS}(4.5),$$

由此得证。 □

备注 4.6. 读者可能会注意到，引理 4.3 和引理 4.5 的陈述密切相关。事实上，在证明

$$\#\{\mathfrak{x} \in U \mid P_A(\mathfrak{x}) = \mathfrak{y}\} = \#\{\mathfrak{x} \in U \mid P_A(\mathfrak{x}) = 0\} \tag{4.8}$$

对于所有 $\mathfrak{y} \in \prod_{i=1}^m \pi_i^{e_i s}\mathcal{O}_{K_i}$，当 s 足够大时成立后，可以由引理 4.5 推出引理 4.3。具体而言，对于这样的 s,

$$\begin{aligned} \int_U I_s(\mathfrak{x}, A) d\mathfrak{x} &= p^{sr} \int_{\prod_{i=1}^m \pi_i^{e_i s}\mathcal{O}_{K_i}} \#\{\mathfrak{x} \in U \mid P_A(\mathfrak{x}) = \mathfrak{y}\} d\mathfrak{y} \\ &= p^{sr} \int_{\prod_{i=1}^m \pi_i^{e_i s}\mathcal{O}_{K_i}} \#\{\mathfrak{x} \in U \mid P_A(\mathfrak{x}) = 0\} d\mathfrak{y} \\ &= \#\{\mathfrak{x} \in U \mid P_A(\mathfrak{x}) = 0\}, \end{aligned} \tag{4.9}$$

即可得出引理 4.3。然而，证明 (4.8) 已经涵盖了引理 4.3 证明中的大部分工作。

现在回到定理 1.7 的证明。我们的论证沿用了 [Car22，定理 2.6] 的证明。

定理 *1.7* 的证明。为使记号与前面的引理保持一致，我们继续用 r 表示矩阵的大小，并记 $\sum_{i=1}^m [K_i : \mathbb{Q}_p] = r$，尽管定理本身使用 n 代替 r。由命题 4.1，只需证明 U 是 $\mathcal{O}_E^{\mathrm{new}}$ 中的可测集这一情形。

首先，我们假设 $U \subset \mathcal{O}_E^{\mathrm{new}}$ 是紧开集。在这种情况下，由引理 4.3 可得

$$\mathbb{E}[Z_{U,r}] = \int_{\mathrm{Mat}_r(\mathbb{Z}_p)} \lim_{s\to\infty} \int_U I_s(\mathfrak{x}, A) d\mathfrak{x} dA.$$

显然，$I_s(\mathfrak{x}, A)$ 处处非负，并且

$$\begin{aligned} \int_U I_s(\mathfrak{x}, A) d\mathfrak{x} &= p^{sr} \int_{\prod_{i=1}^m \pi_i^{e_i s}\mathcal{O}_{K_i}} \#\{\mathfrak{x} \in U \mid P_A(\mathfrak{x}) = \mathfrak{y}\} d\mathfrak{y} \\ &\leq p^{sr} \int_{\prod_{i=1}^m \pi_i^{e_i s}\mathcal{O}_{K_i}} r^r d\mathfrak{y} \\ &= r^r, \end{aligned} \tag{4.10}$$

其中第一行由引理 4.5 得出，第二行则是一个直接的估计，因为 P_A 在 $\mathbb{Q}_p$ 中有 $\leq r$ 个根，因此有 r^r r 元根组。由于这个估计与 s 无关，勒贝格控制收敛定理给出

$$\mathbb{E}[Z_{U,r}] = \lim_{s\to\infty} \int_{\mathrm{Mat}_r(\mathbb{Z}_p)} \int_U I_s(\mathfrak{x}, A) d\mathfrak{x} dA = \lim_{s\to\infty} \int_U \int_{\mathrm{Mat}_r(\mathbb{Z}_p)} I_s(\mathfrak{x}, A) dA d\mathfrak{x}, \tag{4.11}$$

其中第二个等号由托内利定理得出。

现在我们希望应用定理 3.1，在 s 足够大时计算上述积分。由于 val Disc(·) 是紧集 U 上的连续函数，存在 $\mathfrak{y} \in U$ 使得

val Disc(𝔶) 取得最大值。在这种情况下，当 $s > r$ val Disc(𝔶) 时，我们有

$$\begin{aligned}\int_{\mathrm{Mat}_r(\mathbb{Z}_p)} I_s(\mathfrak{x}, A)dA &= \int_{\mathrm{Mat}_r(\mathbb{Z}_p)} p^{sr}\prod_{i=1}^{m}||P'_A(x_i)||^{r_i}\cdot \mathbb{1}_{\mathrm{val}\, P_A(x_i)\geq s,\forall 1\leq i\leq m}dA \\ &= p^{sr}\prod_{i=1}^{m}||Z'(x_i)||^{r_i}\int_{\mathrm{Mat}_r(\mathbb{Z}_p)}\mathbb{1}_{\mathrm{val}\, P_A(x_i)\geq s,\forall 1\leq i\leq m}dA \\ &= p^{sr}||\operatorname{Disc}(\mathfrak{x})||\mathbf{P}(\mathrm{val}\, P_A(x_i)\geq s,\forall 1\leq i\leq m) \\ &= \rho_E^{(r)}(\mathfrak{x}).\end{aligned} \tag{4.12}$$

这里第二个等式由推论 3.7 得出，最后一个等式由定理 3.1 得出。因此，当 $s > r$ val Disc(𝔶) 时，我们有

$$\int_U\int_{\mathrm{Mat}_r(\mathbb{Z}_p)} I_s(\mathfrak{x}, A)dAd\mathfrak{x} = \int_U \rho_E^{(r)}(\mathfrak{x})d\mathfrak{x}. \tag{4.13}$$

结合（4.11）和（4.13），即可证明在 U 为紧集且包含于 $\mathcal{O}_E^{\mathrm{new}}$ 中的情况下的定理 1.7。

现在我们将结果推广到 $\mathcal{O}_E^{\mathrm{new}}$ 的任意开子集。具体而言，如果 U 在 $\mathcal{O}_E^{\mathrm{new}}$ 中是开集，则我们可以构造 $\mathcal{O}_E^{\mathrm{new}}$ 的紧开子集递增序列（U_m）$_{m\geq 1}$，使得 $\bigcup_{m\geq 1} U_m = U$。根据我们刚刚证明的情形，有

$$\mathbb{E}[Z_{U_m,r}] = \int_{U_m}\rho_E^{(r)}(\mathfrak{x})d\mathfrak{x}. \tag{4.14}$$

此外，$A \in$ Mat$_r(\mathbb{Z}_p)$ 上的函数序列（$Z_{U_m,\ r}$）$_{m\geq 1}$ 非负、单调递增，并逐点收敛于 $Z_{U,\ r}$。因此我们有

$$\begin{aligned}\mathbb{E}[Z_{U,r}] &= \lim_{m\to\infty}\mathbb{E}[Z_{U_m,r}] \\ &= \lim_{m\to\infty}\int_{U_m}\rho_E^{(r)}(\mathfrak{x})d\mathfrak{x}. \\ &= \int_U \rho_E^{(r)}(\mathfrak{x})d\mathfrak{x},\end{aligned} \tag{4.15}$$

其中第一行和最后一行由单调收敛定理推出。

沿用上述类似的方法，考虑一个递减的开集序列，我们可以推得该结果对任意 G_δ-集（即开集的可数交）都成立。还要回顾一下，任意可测集 U 的测度为 $\mu_E(U) = \inf_V \mu_E(V)$，其中下确界取遍所有开集 $V \supset U$。因此，对于任意零测集 U_0，我们都有一个开集递减序列 $U_1 \supset U_2 \supset \ldots \supset U_0$，满足 $U_0' := \bigcap_{m\geq 1} U_m$ 的测度为 0。由于 $U_0' \supset U_0$ 是一个 G_δ 集，这就给出 $\mathbb{E}[Z_{U_0,r}] \leq \mathbb{E}[Z_{U_0',r}] = 0$，从而有 $\mathbb{E}[Z_{U_0,r}] = 0$。

现在，令 $U \subset \mathcal{O}_E^{\mathrm{new}}$ 为任意可测集。和之前一样，存在一个由 U_m 表示的开子集递减序列（$_{m\geq 1}$），使得每个开集都包含 U，并且当 m 趋于无穷大时，$U_m \backslash U$ 的测度趋于零。在这种情况下，$\bigcap_{m\geq 1} U_m$ 是一个包含 U 的 G_δ-集，而（$\bigcap_{m\geq 1} U_m$）$\backslash U$ 的测度为零。因此，

$$\mathbb{E}[Z_{U,r}] = \mathbb{E}[Z_{\bigcap_{m\geq 1} U_m,r}] = \int_U \rho_E^{(r)}(\mathfrak{x})d\mathfrak{x} + \int_{(\bigcap_{m\geq 1} U_m)\backslash U}\rho_E^{(r)}(\mathfrak{x})d\mathfrak{x} = \int_U \rho_E^{(r)}(\mathfrak{x})d\mathfrak{x}.$$

证明到此结束。 □

4.2. **相关函数的平均与引理 1.13 的证明**。 根据联合分布 $\rho_E^{(n)}$ 的形式，对于仅依赖于特征值的函数，我们可以写出其在 Mat$_n(\mathbb{Z}_p)$ 上的期望，这正是下面推论的目的。回顾第 3 节开头，$n_E(K)$ 是直积分解 $E \cong K_1 \times \cdots \times K_{m_E}$ 中与 K 同构的因子数量。

命题 4.7。 设 $A \in$ 矩阵空间$_n(\mathbb{Z}_p) \to \mathbb{R}$ 服从 ***Haar*** 分布。那么，对于任意仅依赖于特征值的有界可测函数 h：矩阵空间$_n(\mathbb{Z}_p)$，有

$$\mathbb{E}[h(A)] = \sum_E \int_{\mathcal{O}_E} \frac{1}{\#\operatorname{Aut}(E)} h(x_1, \dots, x_{m_E}) \rho_E^{(n)}(x_1, \dots, x_{m_E}) dx_1 \cdots dx_{m_E}.$$

这里，求和 $\sum_E$遍历 $\mathbb{Q}_p$上所有次数为 r 的 ***´étale*** 代数 $E = K_1 \times \cdots \times K_{m_E}$ 的同构类。符号 h（x_1，……，x_{m_E}）表示 h 在任意一个矩阵 $A \in$ 矩阵空间 $_n$（$\mathbb{Z}_p$）上的取值，该矩阵的特征值为 x_1、……、x_{m_E} 及其伽罗瓦共轭元。

下面的引理将用于命题 4.7 的证明。

引理 4.8。 设 $E := K_1 \times \cdots \times K_m$，其中 K_1、……、K_m 与引理 ***1.13*** 中的相同。设 $E' = K_{m+1} \times \cdots \times K_{m+m_{E'}}$ 是一个次数为 $n-r$的 ***´étale*** 代数。此外，设 $U \subset \mathcal{O}_{K_1}^{\mathrm{new}} \times \cdots \times \mathcal{O}_{\text{新的}K_m}$ 为一个可测集，并记 $Z_{U,n}(x_1, \dots, x_{m+m_{E'}})$ 为 $Z_{U,n}$（在引理 ***1.13*** 中定义）在任意一个以 $x_1, \dots, x_{m+m_{E'}}$ 及其伽罗瓦共轭为特征值的矩阵 $A \in$ 矩阵空间$_n(\mathbb{Z}_p)$ 上的取值。

那么，对所有 $(x_1, \dots, x_{m+m_{E'}}) \in \mathcal{O}_{E \times E'}^{\mathrm{new}}$，都有

$$Z_{U,n}(x_1, \dots, x_{m+m_{E'}}) = \frac{1}{\#\operatorname{Aut}(E')} \sum_{\tau \in \operatorname{Aut}(E \times E')} \mathbb{1}_{\tau(x_1, \dots, x_{m+m_{E'}}) \in U \times \mathcal{O}_{E'}}.$$

特别地，当 $n = r$ 时，有

$$Z_{U,n}(x_1, \dots, x_m) = \sum_{\tau \in \operatorname{Aut}(E)} \mathbb{1}_{\tau(x_1, \dots, x_m) \in U}.$$

证明。 设 $A \in \mathrm{Mat}_n(\mathbb{Z}_p)$ 为一个以 $x_1, \dots, x_{m+m_{E'}}$ 及其伽罗瓦共轭为特征值的矩阵。考虑集合

$$\mathcal{S} := \{\tau(x_1, \dots, x_{m+m_{E'}}) : \tau \in \operatorname{Aut}(E \times E')\},$$

这恰好是 $E \times E'$ 中最小多项式等于 P_A（即 A 的特征多项式）的元素集合。

对于所有满足 $y_1, \dots, y_m$ 是 A 的互不相同且不共轭的特征值的 $\mathfrak{y} := (y_1, \dots, y_m) \in U$，记 $P_{\mathfrak{y}} \in \mathbb{Z}_p[x]$ 为 $\mathfrak{y}$ 的最小多项式。那么，有

$$\begin{aligned} \#\{\mathfrak{y}' \in \mathcal{O}_{E'} : (\mathfrak{y}, \mathfrak{y}') \in \mathcal{S}\} &= \{\mathfrak{y}' \in \mathcal{O}_{E'} : P_{\mathfrak{y}} \cdot P_{\mathfrak{y}'} = P_A\} \\ &= \{\mathfrak{y}' \in \mathcal{O}_{E'} : P_{\mathfrak{y}'} = P_A / P_{\mathfrak{y}}\} \\ &= \#\operatorname{Aut}(E'). \end{aligned} \tag{4.16}$$

这里，$P_{\mathfrak{y}'} \in \mathbb{Z}_p[x]$ 是 $\mathfrak{y}'$的最小多项式，最后一行由命题 2.3 得出。因此，我们有

$$\#(\mathcal{S} \cap (U \times \mathcal{O}_{E'})) = \#\operatorname{Aut}(E') \cdot Z_{U,n}.$$

$n = r$ 的情形可立即作为一个特例得出。 □

命题 *4.7* 的证明。 由于等式两边关于 h 都是线性的，只需证明 h（视为特征值的函数）的支集包含于某个给定同构类 $E = K_1 \times \cdots \times K_m$ 的情形。首先，假设 $h = Z_{U,n}$，其中 $U \subset \mathcal{O}_{K_1}^{\mathrm{new}} \times \cdots \times \mathcal{O}_{K_m}^{\mathrm{new}}$ 是可测的

集合。应用定理 1.7，我们得到

$$\begin{aligned}\mathbb{E}[Z_{U,n}] &= \int_U \rho_E^{(n)}(x_1,\dots,x_{m_E})dx_1\cdots dx_{m_E}\\ &= \int_{\mathcal{O}_E} \mathbb{1}_{(x_1,\dots,x_{m_E})\in U}\rho_E^{(n)}(x_1,\dots,x_{m_E})dx_1\cdots dx_{m_E}\\ &= \int_{\mathcal{O}_E} \frac{1}{\#\operatorname{Aut}(E)}\sum_{\tau\in\operatorname{Aut}(E)} \mathbb{1}_{\tau(x_1,\dots,x_{m_E})\in U}\rho_E^{(n)}(x_1,\dots,x_{m_E})dx_1\cdots dx_{m_E}\\ &= \int_{\mathcal{O}_E} \frac{1}{\#\operatorname{Aut}(E)} Z_{U,n}(x_1,\dots,x_{m_E})\rho_E^{(n)}(x_1,\dots,x_{m_E})dx_1\cdots dx_{m_E}.\end{aligned} \tag{4.17}$$

这里，第三行成立是因为对应于任意一个 $\tau\in\mathrm{Aut}(E)$ 的被加项的积分都相同，而最后一行则由引理 4.8 得出。

验证上述情形 $h = Z_{U,\ n}$ 后，我们便知道当 h 是简单函数时等式成立，也就是说，它是可测集的示性函数的有限线性组合。最后，由于有界可测函数可以被一列简单函数一致逼近，因此结论得证。□

注 4.9。在命题 6.4 中，我们将看到，相关函数 $\rho^{(n)}_{E}(x_1,\ \dots\dots,\ x_{m_E})$ 在 $\mathcal{O}_E$ 中有界。因此，当 h 可积时，我们可以将命题 4.7 推广到这种情形。

基于 相关函数在定理 1.7 中的表达式，接下来我们转向引理 1.13 .

引理 *1.13* 的证明。沿用定理 1.7 的记号，对于任意可测集 $U\subset\mathcal{O}_{K_1}^{\mathrm{new}}\times\cdots\times\mathcal{O}_{K_m}^{\mathrm{new}}$，我们仍用 $Z_{U,n}$ 表示 A 中落在 U 内的互不相同且互不共轭的特征值组成的 m 元组 $(x_1,\dots,x_m)$ 的个数。由于有界可测函数可由一列简单函数一致逼近，因此只需对与任意可测集 $U\subset\mathcal{O}_{K_1}^{\mathrm{new}}\times\cdots\times\mathcal{O}_{K_m}^{\mathrm{new}}$ 相关联的 $Z_{U,n}$ 验证该引理。

记 $E:=K_1\times\cdots\times K_m$。那么，包含 E 的 $\mathbb{Q}_p$ 上次数为 n 的 ´étale 代数同构于一个 ´étale 代数 $E\times E'$，其中 $E'=K_{m+1}\times\cdots\times K_{m+m_{E'}}$ 的次数为 $n-r$。$Z_{U,n}$ 是矩阵空间 $\mathrm{Mat}_{n\times n}(\mathbb{Z}_p)$ 上仅依赖于特征值的有界可测函数，因此由命题 4.7 可得

$$\mathbb{E}[Z_{U,n}] = \sum_{E'}\int_{\mathcal{O}_E\times\mathcal{O}_{E'}} \frac{Z_{U,n}(x_1,\dots,x_{m+m_E})}{\#\operatorname{Aut}(E\times E')}\rho^{(n)}_{E\times E'}(x_1,\dots,x_{m+m_E})dx_1\cdots dx_{m+m_E} \tag{4.18}$$

其中，我们将 $Z_{U,n}(x_1,\dots,x_{m+m_{E'}})$ 记作 $Z_{U,n}$ 在以 $x_1,\dots,x_{m+m_{E'}}$ 及其伽罗瓦共轭为特征值的任意矩阵上的取值；$\sum_{E'}$ 遍历次数为 $n-r$ 的 ´étale 代数 $E'=K_{m+1}\times\cdots\times K_{m+m_{E'}}$ 的所有同构类。根据命题 4.1，以概率 1，A 没有重特征值，因此我们可以将积分域限制在满足 $(x_1,\dots,x_{m+m_E})\in\mathcal{O}^{\mathrm{new}}_{E\times E'}$ 的子集上，而不改变积分值。于是，我们可以使用引理 4.8 中 $Z_{U,n}$ 的表达式，得到

$$\begin{aligned}\mathrm{RHS}(4.18) &= \sum_{E'}\frac{1}{\#\operatorname{Aut}(E')}\int_{\mathcal{O}_E\times\mathcal{O}_{E'}}\sum_{\tau\in\operatorname{Aut}(E\times E')}\frac{\mathbb{1}_{\tau(x_1,\dots,x_{m+m_{E'}})\in U\times\mathcal{O}_{E'}}}{\#\operatorname{Aut}(E\times E')}\\ &\quad\times\rho^{(n)}_{E\times E'}(x_1,\dots,x_{m+m_{E'}})dx_1\cdots dx_{m+m_{E'}}\\ &= \sum_{E'}\int_{\mathcal{O}_E\times\mathcal{O}_{E'}}\sum_{\tau\in\operatorname{Aut}(E\times E')}\frac{\mathbb{1}_{\tau(x_1,\dots,x_{m+m_{E'}})\in U\times\mathcal{O}_{E'}}}{\#\operatorname{Aut}(E')\#\operatorname{Aut}(E\times E')}(1-p^{-1})\cdots(1-p^{-n})\\ &\quad\times\prod_{i=1}^{m+m_{E'}}V(x_i)\cdot||\Delta_\sigma(x_1,\dots,x_{m+m_{E'}})||dx_1\cdots dx_m dx_{m+1}\cdots dx_{m+m_{E'}}.\end{aligned} \tag{4.19}$$

注意，对于上述求和中的所有 E'，每个 ´étale 代数同构 $\tau\in\mathrm{Aut}(E\times E')$ 对整个求和的贡献都相同。因此，我们只需处理 $\tau=\mathrm{id}$ 为

恒等映射的情形，由此可得

$$\begin{aligned}\mathbb{E}[Z_{U,n}] = \sum_{E'} \int_{\mathcal{O}_E \times \mathcal{O}_{E'}} & \frac{\mathbb{1}_{(x_1,\dots,x_m)\in U}}{\#\operatorname{Aut}(E')}(1-p^{-1})\cdots(1-p^{-n}) \\ & \times \prod_{i=1}^{m+m_{E'}} V(x_i)\cdot ||\Delta_\sigma(x_1,\dots,x_{m+m_{E'}})||dx_1\cdots dx_m dx_{m+1}\cdots dx_{m+m_{E'}}\end{aligned} \tag{4.20}$$

对于上述求和中的所有 E'，对 $\mathcal{O}_E \times \mathcal{O}_{E'}$ 的积分是有限的，因为 $\mathbb{E}[Z_{U,n}]$ 是有限的，且被积函数非负，因此它必定可积。因此，根据富比尼定理，我们可以将 (4.20) 中的积分改写为累次积分，即先对 x_{m+1}、……、$x_{m+m_{E'}}$ 积分，再对 x_1、……、x_m 积分。根据克拉斯纳定理 [Kra46a]，每个次数的 $\mathbb{Q}_p$ 扩张只有有限多个，因此次数为 $n-r$ 的 ´étale 代数 E' 只有有限多个同构类。因此，我们可以将求和 $\sum_{E'}$ 移到对 $\mathcal{O}_E$ 的积分之外，于是 (4.20) 得到

$$\begin{aligned}\mathbb{E}[Z_{U,n}] = \int_U (1-p^{r-n-1})\cdots(1-p^{-n})||\Delta_\sigma(x_1,\dots,x_m)|| \left(\prod_{i=1}^m V(x_i)\right)(1-p^{-1})\cdots(1-p^{r-n}) \\ \times \left(\sum_{E'}\int_{\mathcal{O}_{E'}} \frac{1}{\#\operatorname{Aut}(E')}\frac{||\Delta_\sigma(x_1,\dots,x_{m+m_{E'}})||}{||\Delta_\sigma(x_1,\dots,x_m)||}\prod_{i=m+1}^{m_{E'}} V(x_i)dx_{m+1}\cdots dx_{m+m_{E'}}\right) dx_1\cdots dx_m.\end{aligned} \tag{4.21}$$

现在我们将用期望行列式来表示内层求和。注意，当 $E' \simeq K_{m+1}\times\cdots\times K_{m+m_{E'}}$，且固定矩阵 $A \in$ 矩阵空间$_{n-r}(\mathbb{Z}_p)$ 的特征值为 $x_{m+1}\in\mathcal{O}_{K_{m+1}}^{\mathrm{new}}$、……、$x_{m+m_{E'}}\in\mathcal{O}_{K_{m+m_{E'}}}^{\mathrm{new}}$ 及其伽罗瓦共轭时，我们有

$$||\det(Z(\tilde{A}))|| = \prod_{i=m+1}^{m+m_E} ||\operatorname{Nm}_{K_i/\mathbb{Q}_p} Z(x_i)|| = \frac{||\Delta_\sigma(x_1,\dots,x_{m+m_{E'}})||}{||\Delta_\sigma(x_1,\dots,x_m)||\cdot||\Delta_\sigma(x_{m+1},\dots,x_{m+m_{E'}})||}.$$

因此，应用命题 4.7，并考虑 $h(A) = ||\det(Z(A))||$，其中 $A\in \mathrm{Mat}_{n-r}(\mathbb{Z}_p)$ 服从 Haar 分布，我们得到

$$\begin{aligned}\mathbb{E}||\det(Z(\tilde{A}))|| &= \sum_{E'}\int_{\mathcal{O}_{E'}} \frac{1}{\#\operatorname{Aut}(E')}\cdot\frac{||\Delta_\sigma(x_1,\dots,x_{m+m_{E'}})||}{||\Delta_\sigma(x_1,\dots,x_m)||\cdot||\Delta_\sigma(x_{m+1},\dots,x_{m+m_{E'}})||} \\ &\quad\times \rho_{E'}^{(n-r)}(x_{m+1},\dots,x_{m+m_{E'}})dx_{m+1}\cdots dx_{m+m_{E'}} \\ &= \sum_{E'}\int_{\mathcal{O}_{E'}} \frac{(1-p^{-1})\cdots(1-p^{r-n})}{\#\operatorname{Aut}(E')}\prod_{i=m+1}^{m+m'_E} V(x_i) \\ &\quad\times \frac{||\Delta_\sigma(x_1,\dots,x_{m+m_{E'}})||}{||\Delta_\sigma(x_1,\dots,x_m)||}dx_{m+1}\cdots dx_{m+m_{E'}}.\end{aligned} \tag{4.22}$$

结合 (4.21) 和 (4.22)，证明得证。 □

5. Expected determinants, cokernels, and the moment method

本节的主要结果——定理 5.1 和 5.2——讨论期望行列式的极限 $\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||$。定理 5.2 指出，在某些受限假设下，这些期望可以因式分解；定理 1.1 中不同提升子空间内特征值的独立性正是由此得出的。定理 5.1 的适用范围更广，但它只是将所求期望化为相关随机变量乘积的期望。这种“线性化”非常有用，不过即使经过线性化，这些期望仍然很难计算。这两个结果的证明都依赖于 Sawin-Wood [SW22], 提出、并由 Cheong-Yu [CY23]应用于随机模的矩方法工具。

定理 5.1。 设 $n \geq 1$ 和 A 按 矩阵空间$_n(\mathbb{Z}_p)$ 上的加性 *Haar* 测度分布。假设 $Z = \prod_{i=1}^m Z_i(x) \in \mathbb{Z}_p[x]$ 的次数为 r，其中多项式 $Z_i(x) \in \mathbb{Z}_p[x]$、 $1 \leq i \leq m$ 均为首一、互异且不可约。设 r_i 为 $Z_i(x)$的次数，因此 $r = r_1 + \cdots + r_m$，并设x_i 为 $Z_i(x)$的一个根。那么，对任意 $k \geq 0$，极限 $\lim_{n\to\infty} \mathbb{E}||\det(Z(A))||^k$ 均存在，且等于

$$\lim_{n\to\infty} \mathbb{E}[||\det(Z(A))||^k] = \lim_{n\to\infty} \mathbb{E}\left[\prod_{i=1}^m ||\det(A_0 + x_i A_1 + \cdots + x_i^{r-1} A_{r-1})||^{r_i k}\right], \tag{5.1}$$

其中， A_0、 ...、 A_{r-1} 在 矩阵空间$_n(\mathbb{Z}_p)$ 上服从独立同分布的 *Haar* 分布。

定理 5.2。 设 $n \geq 1$ 和 A 服从 矩阵空间$_n(\mathbb{Z}_p)$ 上的加性 *Haar* 测度。令$Z = \prod_{i=1}^m Z_i(x) \in \mathbb{Z}_p[x]$，其中多项式 $Z_i(x) \in \mathbb{Z}_p[x]$、 $1 \leq i \leq m$ 均为首一多项式，且没有重根。此外，假设剩余类 $Z_i(x) \in \mathbb{F}_p[x]$、 $1 \leq i \leq m$ 是 $\mathbb{F}_p[x]$ 中不同不可约多项式的幂。那么，当 n 趋于无穷大时，联合随机变量

$$(||\det(Z_1(A))||, \ldots, ||\det(Z_m(A))||)$$

依分布收敛到由 m 个相互独立的随机变量组成的元组，因此

$$\lim_{n\to\infty} \mathbb{E}[||\det(Z(A))||^k] = \prod_{i=1}^m \lim_{n\to\infty} \mathbb{E}[||\det(Z_i(A))||^k] \tag{5.2}$$

对所有 $k \geq 0$ 均成立。

我们指出，取极限是必要的；对于固定的 n，上述定理中的等式并不成立。

5.1. **代数准备**。 在本小节中，我们继续采用第 3 节和第 4 节中的记号，并将 $R := \mathbb{Z}_p[x]/(Z(x)) \cong \mathbb{Z}_p[\mathfrak{x}]$ 记作简称。回顾一下，对于一个环 L，矩阵 $A \in$Mat$_n(L)$ 的余核 为

$$\mathrm{Cok}_L(A) := L^n/AL^n. \tag{5.3}$$

有时我们希望让 A 作用于 M^n，其中 M 是一个 L-模，并记作 Cok$_M(A) := M^n/AM^n$。当下标可由上下文明确时，我们通常直接写作 Cok。

对于 $A \in$Mat$_n(\mathbb{Z}_p)$，阿贝尔 p-群

$$\mathrm{Cok}_{\mathbb{Z}_p}(Z(A)) = \mathbb{Z}_p^n/Z(A)\mathbb{Z}_p^n \tag{5.4}$$

also 具有上述定义的 R-模结构，其中 $x \in R$ 的作用为 A .

此外，正如 Lee [Lee23], 所指出的，我们有

$$\mathrm{Cok}_{\mathbb{Z}_p}(Z(A)) \cong \mathrm{Cok}_{\mathbb{Z}_p[\mathfrak{x}]}(A - \mathfrak{x}I_n), \tag{5.5}$$

其中该同构是 R-模之间的同构。我们将交替使用表达式 (5.5) 中的两种形式；前者自然地联系到所需的行列式，而后者以线性形式表示，更易于处理。

引理 5.3. 设 K 是 $\mathbb{Q}_p$ 的一个扩张，次数为 r， $\mathcal{O}_K$ 是其整数环，且 $A \in$矩阵空间$_n(\mathcal{O}_K)$ 是非奇异的。于是有 # 余核$(A) = ||\det(A)||^{-r}$。

证明。 设 π 是 $\mathcal{O}_K$的一个一致化元， e 是 $K/\mathbb{Q}_p$的分歧指数，因此 val$(\pi) = \frac{1}{e}$，且 #$(\mathcal{O}_K\colon \pi\mathcal{O}_K) = p^{r/e}$。根据史密斯标准形（即在左右两侧分别乘以 GL$_n(\mathcal{O}_K)$ 中的元素），不失一般性，可假设

$$A = \mathrm{diag}(\pi^{\lambda_1}, \ldots, \pi^{\lambda_n}), \quad \lambda_1 \geq \ldots \geq \lambda_n \geq 0.$$

在这种情况下，我们有

$$\#\,\mathrm{Cok}(A) = \#(\mathcal{O}_K^n : A\mathcal{O}_K^n) = \prod_{i=1}^n \#(\mathcal{O}_K : \pi^{\lambda_i}\mathcal{O}_K) = \prod_{i=1}^n p^{r\lambda_i/e} = p^{r(\lambda_1+\cdots+\lambda_n)/e}.$$

此外，我们有 $\det(A) = \pi^{\lambda_1+\cdots+\lambda_n}$，因此 $||\det(A)||^{-r} = p^{r(\lambda_1+\cdots+\lambda_n)/e}$。证明至此完成。□

下面的引理是一个有用的中间步骤。

引理 5.4。 设 $A_\mathfrak{x} = A_0 + A_1\mathfrak{x} + \cdots + A_{r-1}\mathfrak{x}^{r-1} \in$ 矩阵空间$_n(\mathbb{Z}_p[\mathfrak{x}])$ 为非奇异，其中 $\mathfrak{x} = (x_1, \ldots, x_m) \in \mathcal{O}_{K_1}^{\mathrm{new}} \times \cdots \times \mathcal{O}_{K_m}^{\mathrm{new}}$，且 $A_0, \ldots, A_{r-1} \in$ 矩阵空间 $_n(\mathbb{Z}_p)$。那么我们有

$$\#\operatorname{Cok}(A_\mathfrak{x}) = \prod_{i=1}^{m} ||\det(A_0 + A_1x_i + \cdots + A_{r-1}x_i^{r-1})||^{-r_i}.$$

证明。我们首先转而考虑 $\mathcal{O}_E$ 上的余核，它们比 $\mathbb{Z}_p[\mathfrak{x}]$ 上的余核具有更好的因式分解性质。我们知道 $\#(\mathcal{O}_E : \mathbb{Z}_p[\mathfrak{x}]) < \infty$ 是有限的。若记

$$a_1 + \mathbb{Z}_p[\mathfrak{x}]^n, \ldots, a_m + \mathbb{Z}_p[\mathfrak{x}]^n$$

为 $\mathbb{Z}_p[\mathfrak{x}]^n$ 在 $\mathcal{O}_E^n$ 中的陪集，则

$$A_\mathfrak{x}(a_1 + \mathbb{Z}_p[\mathfrak{x}]^n), \ldots, A_\mathfrak{x}(a_m + \mathbb{Z}_p[\mathfrak{x}]^n)$$

给出了 $A_\mathfrak{x}\mathcal{O}_E^n$ 中的所有 $A_\mathfrak{x}\mathbb{Z}_p[\mathfrak{x}]^n$ 陪集。因此，我们有 $\#(A_\mathfrak{x}\mathcal{O}_E^n : A_\mathfrak{x}\mathbb{Z}_p[\mathfrak{x}]^n) = \#(\mathcal{O}_E^n : \mathbb{Z}_p[\mathfrak{x}]^n)$，并且

$$\begin{aligned}
\#\operatorname{Cok}(A_\mathfrak{x}) &= \#(\mathbb{Z}_p[\mathfrak{x}]^n : A_\mathfrak{x}\mathbb{Z}_p[\mathfrak{x}]^n) \\
&= \#(\mathcal{O}_E^n : A_\mathfrak{x}\mathcal{O}_E^n)\frac{\#(A_\mathfrak{x}\mathcal{O}_E^n : A_\mathfrak{x}\mathbb{Z}_p[\mathfrak{x}]^n)}{\#(\mathcal{O}_E^n : \mathbb{Z}_p[\mathfrak{x}]^n)} \\
&= \#(\mathcal{O}_E^n : A_\mathfrak{x}\mathcal{O}_E^n) \\
&= \prod_{i=1}^{m} \#(\mathcal{O}_{K_i}^n : (A_0 + A_1x_i + \cdots + A_{r-1}x_i^{r-1})\mathcal{O}_{K_i}^n).
\end{aligned} \tag{5.6}$$

这里，最后一行成立是因为 $\mathcal{O}_E \cong \prod_{i=1}^m \mathcal{O}_{K_i}$ 和 $A_\mathfrak{x}$ 通过 $A_0 + A_1x_i +$作用在 i^{th} 因子上 $\cdots + A_{r-1}x_i^{r-1}$。此外，由引理 5.3，我们有

$$\begin{aligned}
\#(\mathcal{O}_{K_i}^n/(A_0 + A_1x_i + \cdots + A_{r-1}x_i^{r-1})\mathcal{O}_{K_i}^n) &= \#\operatorname{Cok}_{\mathcal{O}_{K_i}}(A_0 + A_1x_i + \cdots + A_{r-1}x_i^{r-1}) \\
&= ||\det(A_0 + A_1x_i + \cdots + A_{r-1}x_i^{r-1})||^{-r_i}.
\end{aligned} \tag{5.7}$$

(5.6) 和 (5.7) 合起来即得证明。 □

5.2. **定理 5.1 的证明**。 本小节的目标是证明定理 5.1。我们采用前面的准备小节中给出的相同记号。下面的引理使我们可以用一个元素独立同分布且服从 Haar 分布的矩阵来替换 $A - \mathfrak{x}I_n$。

引理 5.5。 对于所有有限的 $\mathbb{Z}_p[\mathfrak{x}]$-模 M，我们有

$$\lim_{n\to\infty} \mathbf{P}(\operatorname{Cok}(A - \mathfrak{x}I_n) \cong M) = \lim_{n\to\infty} \mathbf{P}(\operatorname{Cok}(A_\mathfrak{x}) \cong M),$$

其中，A 在 矩阵空间$_n(\mathbb{Z}_p)$中服从 *Haar* 分布，而 $A_\mathfrak{x}$ 在 矩阵空间$_n(\mathbb{Z}_p[\mathfrak{x}])$中服从 *Haar* 分布。换言之，随机余核 余核$(A - \mathfrak{x}I)$、余核$(A_\mathfrak{x})$ 依分布收敛到相同的极限。

证明。 我们的证明基于随机 $\mathbb{Z}_p[\mathfrak{x}]$-模上的矩方法。对于任意有限$\mathbb{Z}_p[\mathfrak{x}]$-模 M，根据 [CY23，定理 1.12][7]

$$\lim_{n\to\infty} \mathbb{E}[\#\operatorname{Sur}_{\mathbb{Z}_p[\mathfrak{x}]}(\operatorname{Cok}(A - \mathfrak{x}I_n), M)] = 1.$$

这里，$\#\operatorname{Sur}^{\mathbb{Z}_p[\mathfrak{x}]}(\cdot, \cdot)$ 表示 $\mathbb{Z}_p[\mathfrak{x}]$-模满射的数量。根据 [SW22，引理 6.3]，矩 1 性质良好（即同一篇论文中定义的增长条件），因此根据 [SW22，定理 1.8]，矩收敛到 1 意味着依分布收敛

[7]该定理讨论的是 $(\mathbb{Z}/p^k\mathbb{Z})[\mathfrak{x}]$-模，但取足够大的 k，使得 $p^kM = 0$，即可得到我们所用的形式。

随机模收敛到由这些矩刻画的极限分布。因此，只需证明

$$\lim_{n\to\infty}\mathbb{E}[\#\operatorname{Sur}_{\mathbb{Z}_p[\mathfrak{x}]}(\operatorname{Cok}(A_{\mathfrak{x}}),M)]=1$$

对所有有限的 $\mathbb{Z}_p[\mathfrak{x}]$-模 M 均成立。

为证明这一点，注意到

$$\begin{aligned}\mathbb{E}[\#\operatorname{Sur}_{\mathbb{Z}_p[\mathfrak{x}]}(\operatorname{Cok}(A_{\mathfrak{x}}),M)]&=\int_{\operatorname{Mat}_n(\mathbb{Z}_p[\mathfrak{x}])}\#\operatorname{Sur}_{\mathbb{Z}_p[\mathfrak{x}]}(\operatorname{Cok}(A_{\mathfrak{x}}),M)dA_{\mathfrak{x}}\\&=\int_{\operatorname{Mat}_n(\mathbb{Z}_p[\mathfrak{x}])}\sum_{F\in\operatorname{Sur}_{\mathbb{Z}_p[\mathfrak{x}]}(\operatorname{Cok}(A_{\mathfrak{x}}),M)}1dA_{\mathfrak{x}}\\&=\sum_{F\in\operatorname{Sur}_{\mathbb{Z}_p[\mathfrak{x}]}(\mathbb{Z}_p[\mathfrak{x}]^n,M)}\mathbf{P}(F(A_{\mathfrak{x}}\mathbb{Z}_p[\mathfrak{x}]^n)=0).\end{aligned}\tag{5.8}$$

由于 $A_{\mathfrak{x}}$ 的各列相互独立，我们有

$$\begin{aligned}\mathbf{P}(F(A_{\mathfrak{x}}\mathbb{Z}_p[\mathfrak{x}]^n)=0)&=\mathbf{P}(F(\omega)=0)^n\\&=\mathbf{P}(\omega\in\operatorname{Ker}F)^n\\&=\frac{1}{\#(\mathbb{Z}_p[\mathfrak{x}]^n/\operatorname{Ker}F)^n}\\&=\frac{1}{(\#M)^n},\end{aligned}\tag{5.9}$$

其中 $\omega\in\mathbb{Z}_p[\mathfrak{x}]^n$ 服从 Haar 分布。由于 $\#\operatorname{Hom}_{\mathbb{Z}_p[\mathfrak{x}]}(\mathbb{Z}_p[\mathfrak{x}]^n,M)=(\#M)^n$，我们有

$$\begin{aligned}\mathrm{RHS}(5.8)&=\sum_{F\in\operatorname{Sur}_{\mathbb{Z}_p[\mathfrak{x}]}(\mathbb{Z}_p[\mathfrak{x}]^n,M)}\frac{1}{(\#M)^n}\\&=1-\sum_{F\in\operatorname{Hom}_{\mathbb{Z}_p[\mathfrak{x}]}(\mathbb{Z}_p[\mathfrak{x}]^n,M)\setminus\operatorname{Sur}_{\mathbb{Z}_p[\mathfrak{x}]}(\mathbb{Z}_p[\mathfrak{x}]^n,M)}\frac{1}{(\#M)^n}.\end{aligned}\tag{5.10}$$

上述表达式小于 1。另一方面，由于任何非满同态的像都是某个 $N\subsetneq M$，我们有

$$\begin{aligned}\sum_{F\in\operatorname{Hom}_{\mathbb{Z}_p[\mathfrak{x}]}(\mathbb{Z}_p[\mathfrak{x}]^n,M)\setminus\operatorname{Sur}_{\mathbb{Z}_p[\mathfrak{x}]}(\mathbb{Z}_p[\mathfrak{x}]^n,M)}\frac{1}{(\#M)^n}&\le\sum_{N\subsetneq M}\sum_{F\in\operatorname{Hom}_{\mathbb{Z}_p[\mathfrak{x}]}(\mathbb{Z}_p[\mathfrak{x}]^n,N)}\frac{1}{(\#M)^n}.\\&=\sum_{N\subsetneq M}\frac{(\#N)^n}{(\#M)^n}\\&\le\#\{N\subsetneq M\mid N\text{ is a }\mathbb{Z}_p[\mathfrak{x}]\text{-module}\}\frac{1}{2^n}.\end{aligned}\tag{5.11}$$

该量的极限为 0，因此 $\lim_{n\to\infty}\mathbb{E}[\#\operatorname{Sur}_{\mathbb{Z}_p[\mathfrak{x}]}(\text{余核}(A_{\mathfrak{x}}),M)]=1$。证明至此完成。□

定理 *5.1* 的证明。由引理 5.3，我们有

$$||\det(Z(A))||^k=\#\operatorname{Cok}(Z(A))^{-k}=\#\operatorname{Cok}(A-\mathfrak{x}I_n)^{-k}.$$

当 n 趋于无穷大时，根据引理 5.5，随机变量

$$\#\operatorname{Cok}(A-\mathfrak{x}I_n)^{-k},\#\operatorname{Cok}(A_0+A_1\mathfrak{x}+\cdots+A_{r-1}\mathfrak{x}^{r-1})^{-k}$$

弱收敛到相同的分布。由于这些随机变量始终小于或等于 1，因此我们有

$$\begin{aligned}\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||^k &= \lim_{n\to\infty}\mathbb{E}\left[\#\operatorname{Cok}(A-\mathfrak{x}I_n)^{-k}\right]\\ &= \lim_{n\to\infty}\mathbb{E}\left[\#\operatorname{Cok}(A_0+A_1\mathfrak{x}+\cdots+A_{r-1}\mathfrak{x}^{r-1})^{-k}\right]\\ &= \lim_{n\to\infty}\mathbb{E}\prod_{i=1}^{m}||\det(A_0+x_iA_1+\cdots+x_i^{r-1}A_{r-1})||^{r_ik},\end{aligned} \tag{5.12}$$

最后一行由引理 5.4 得出。证明至此完成。 □

5.3. **定理 5.2 的证明**。本小节中，我们证明定理 5.2。我们将采用以下设定，它与前几小节中的设定略有不同：

(1) $Y_1(x)\ldots,Y_m(x)\in\mathbb{Z}_p[x]$ 为首一多项式，且剩余类 $\overline{Y}_i(x)\in\mathbb{F}_p[x],1\le i\le m$ 互不相同且不可约。(2) $d_i\ge 1$ 为 Y_i的次数。(3) $Z_1(x)\ldots,Z_m(x)\in\mathbb{Z}_p[x]$ 为首一多项式，使得对所有 $1\le i\le m$，剩余类 $Z_i(x)\in\mathbb{F}_p[x]$是Y_i的幂。这里要求多项式 $Z_i(x)$ $1\le i\le m$ 没有重根，但不要求它们不可约。(4) r_i 为 Z_i的次数，且可被 d_i整除。(5) $Z(x)=\prod_{i=1}^m Z_i(x)$，它是次数为 $r:=r_1+\cdots+r_m$的首一多项式。(6) $R=\mathbb{Z}_p[x]/(Z(x))$为商环。(7) $R_i:=\mathbb{Z}_p[x]/(Z_i(x))$，因此我们可以将 R写成乘积 $R=R_1\times\cdots\cdots R_m$。(8) $\mathfrak{m}_i=(p,Y_i(x))/(Z_i(x))$为环 R_i的唯一极大理想。(9) $\mathbb{F}_{p^{d_i}}\cong\mathbb{Z}_p[x]/(p,Y_i(x))=R_i/\mathfrak{m}_i$ 为相应的商域。

下述命题的内容实质上已包含在 [CY23, 定理 1.3]，中；此外，它还是 [SW22, 引理 6.3] 的一个具体例子。该命题描述了 $\operatorname{Cok}(A-\mathfrak{x}I_n)$ 的极限分布。

命题 5.6. 对于有限的 R-模 M，我们有

$$\lim_{n\to\infty}\mathbf{P}(\operatorname{Cok}(Z(A))\cong M)=\frac{1}{\#\operatorname{Aut}_R(M)}\prod_{j=1}^{m}\prod_{i=1}^{\infty}(1-p^{-id_j})$$

若存在一个非负整数 $s\ge 0$ 和一个短正合列

$$0\to R^s\to R^s\to M\to 0$$

（换言之，M 是两个秩相同的自由 R-模的商集）；否则，我们有$\lim_{n\to\infty}\mathbf{P}(\operatorname{Cok}(Z(A))\cong M)=0$。

下述引理是证明命题 5.6 所必需的准备。

Lemma 5.7. 假设存在一个非负整数 $s\ge 0$ 和一个短正合列

$$0\to R^s\to R^s\to M\to 0.$$

于是我们有 $\#\operatorname{Ext}^1_R(M,\mathbb{F}_{p^{d_j}})=\#\operatorname{Hom}_R(M,\mathbb{F}_{p^{d_j}})$。

证明。由于 R^s 是自由的，我们总有

$$\operatorname{Ext}^1_R(R^s,\mathbb{F}_{p^{d_j}})=0.$$

将 Ext函子应用于短正合列 $0\to R^s\to R^s\to M\to 0$，我们得到以下 R-模的正合列：

$$0\to\operatorname{Hom}_R(M,\mathbb{F}_{p^{d_j}})\to\operatorname{Hom}_R(R^s,\mathbb{F}_{p^{d_j}})\to\operatorname{Hom}_R(R^s,\mathbb{F}_{p^{d_j}})\to\operatorname{Ext}^1_R(M,\mathbb{F}_{p^{d_j}})\to 0.$$

因此，

$$\#\operatorname{Ext}^1_R(M,\mathbb{F}_{p^{d_j}})=\frac{\#\operatorname{Hom}_R(R^s,\mathbb{F}_{p^{d_j}})}{\#\operatorname{Hom}_R(R^s,\mathbb{F}_{p^{d_j}})}\#\operatorname{Hom}_R(M,\mathbb{F}_{p^{d_j}})=\#\operatorname{Hom}_R(M,\mathbb{F}_{p^{d_j}}),$$

至此证明完毕。 □

命题 *5.6* 的证明。 一方面，根据定义，对于每个固定的 $n\geq 1$ 和 $A\in$矩阵空间$_n(\mathbb{Z}_p)$，余核 $(Z(A))$ 是两个秩为 n 的自由 R-模的商集，因此，对于那些无法表示为两个自由 R-模之商集的 M，必有 $\lim_{n\to\infty}\mathbf{P}($ 余核 $(A-\mathfrak{x}I_n)\cong M)=0$。另一方面，假设 M 来自一个短正合列

$$0\to R^s\to R^s\to M\to 0$$

其中 $s\geq 0$。根据 [CY23，定理 1.3], ，我们有

$$\lim_{n\to\infty}\mathbf{P}(\operatorname{Cok}(Z(A))\cong M)=\frac{1}{\#\operatorname{Aut}_R(M)}\prod_{j=1}^{m}\prod_{i=1}^{\infty}\left(1-\frac{\#\operatorname{Ext}^1_R(M,\mathbb{F}_{p^{d_j}})}{\#\operatorname{Hom}_R(M,\mathbb{F}_{p^{d_j}})}p^{-id_j}\right).\tag{5.13}$$

应用引理 5.7，证明即告完成。 □

推论 5.8。 对于所有整数 $k\geq 0$，我们有

$$\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||^k=\prod_{j=1}^{m}\prod_{i=1}^{\infty}(1-p^{-id_j})\cdot\sum_{M}\frac{1}{\#\operatorname{Aut}_R(M)(\#M)^k},$$

其中，求和遍历所有有限 R-模 M 的同构类，这些模可以表示为两个秩相同的自由 R-模的商集。

证明。 由引理 5.3，我们总有 $||\det(Z(A))||^k=\ ^1\!/_{\#\operatorname{Cok}(Z(A))^k}$。然后，证明可由命题 5.6 得出。 □

定理 *5.2* 的证明。 注意，模自同构的数量满足关系

$$\#\operatorname{Aut}_{R_1\times\cdots\times R_m}(M_1\times\cdots\times M_m)=\prod_{i=1}^{m}\#\operatorname{Aut}_{R_i}(M_i).\tag{5.14}$$

这里，对所有 $1\leq i\leq m$， M_i 都是有限 R_i-模。因此，应用两次命题 5.6，可得

$$\begin{aligned}\lim_{n\to\infty}\mathbf{P}(\operatorname{Cok}(Z_i(A))\cong M_i,\forall 1\leq i\leq m)&=\lim_{n\to\infty}\mathbf{P}(\operatorname{Cok}(Z(A))\cong M_1\times\cdots\times M_m)\\&=\frac{1}{\#\operatorname{Aut}_{R_1\times\cdots\times R_m}(M_1\times\cdots\times M_m)}\prod_{j=1}^{m}\prod_{i=1}^{\infty}(1-p^{-id_j})\\&=\prod_{j=1}^{m}\frac{1}{\#\operatorname{Aut}_{R_j}(M_j)}\prod_{i=1}^{\infty}(1-p^{-id_j})\\&=\prod_{i=1}^{m}\lim_{n\to\infty}\mathbf{P}(\operatorname{Cok}(Z_i(A))\cong M_i).\end{aligned}\tag{5.15}$$

由引理 5.3，我们对所有 $1\leq i\leq m$ 都有 $||\det(Z_i(A))||=\ ^1\!/_{\#\operatorname{Cok}(Z_i(A))}$。因此，证明得证。 □

注 5.9. 定理 5.2 中的独立性结论也适用于_ _$Z_1,\ldots,Z_m\in\mathbb{F}_p[x]$ 不再是不同不可约多项式的幂、但仍两两互素的情形。事实上，在引理 2.4 中应用亨泽尔引理，我们可以进一步将 $Z_1,\ldots,Z_m$ 分解为

$$Z_i=\prod_{l_i=1}^{j_i}Z_{i,l_i},\forall 1\leq i\leq m,$$

其中，剩余类 $Z_{1,1},\dots,Z_{1,j_1},\dots,Z_{m,1},\dots,Z_{m,j_m}\in\mathbb{F}_p[x]$ 是不同不可约多项式的幂。在这种情况下， $Z_1,\dots,Z_m$ 情形的独立性断言可直接由 $Z_{1,1},\dots,Z_{1,j_1},\dots,Z_{m,1},\dots,Z_{m,j_m}$上的断言推出。

特别地，考虑这样的情形：每个 $Z_i(x)$都是某个$x_i\in\mathbb{Z}_p$的最小多项式，且满足 $\mathbb{Z}_p[x_i]=\mathcal{O}_{K_i}$，其中 $K_i:=\mathbb{Q}_p[x_i]$。在这种情况下，元素 $x_1,\dots,x_m$位于不同的提升子空间中，而多项式 $Z_1,\dots,Z_m$不可约。在这些假设下，期望行列式的极限具有简单的形式：

命题 5.10. 假设对于所有 $1\le i\le m$, $Z_i(x)$ 都是某个$x_i\in\mathbb{Z}_p$ 的最小多项式，且满足 $\mathbb{Z}_p[x_i]=\mathcal{O}_{K_i}$，其中 $K_i:=\mathbb{Q}_p[x_i]$。那么对于所有整数 $k\ge 0$，有

$$\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||^k=\prod_{i=1}^{m}\prod_{j=1}^{k}(1-p^{-jd_i}).$$

证明. 令 $E:=K_1\times\cdots\times K_m$。在这种情况下，对于所有 $1\le i\le m$，都有 $R_i\cong\mathcal{O}_{K_i}$，且 $R=R_1\times\cdots\times R_m\cong\mathcal{O}_E$。注意，每个有限的 $\mathcal{O}_E$-模 M都同构于以下形式之一

$$M\cong M_1\times\cdots\times M_m$$

其中，对所有 $1\le i\le m$， $M_i\cong\prod_{j=1}^{\infty}(\mathcal{O}_{K_i}/\pi_i^{\lambda_j^i}\mathcal{O}_{K_i})$ 是由某个$\lambda_1^i\ge\lambda_2^i\ge\ldots\ge 0$确定的有限 $\mathcal{O}_{K_i}$-模（其中只有有限多个非零）。这意味着每个有限 $\mathcal{O}_E$-模都是两个秩相同的自由 $\mathcal{O}_E$-模的商集。应用 [SW22, 引理 6.3] ，取$u=k$ 并回顾引理 5.7，我们推得

$$\nu(M)=\frac{\prod_{j=1}^{m}\prod_{i=1}^{\infty}(1-p^{-(i+k)d_j})}{\#\operatorname{Aut}_{\mathcal{O}_E}(M)(\#M)^k}$$

给出了定义在所有有限 $\mathcal{O}_E$-模上的概率测度。因此，我们有

$$\sum_M\frac{1}{\#\operatorname{Aut}_{\mathcal{O}_E}(M)(\#M)^k}=\prod_{j=1}^{m}\prod_{i=1}^{\infty}(1-p^{-(i+k)d_j})^{-1}.$$

将上述等式与推论 5.8 合并即可得到证明。 □

6. Limiting correlation functions and their properties

本节主要利用上一节的结果，证明以下关于极限相关函数 $\rho_E^{(\infty)}$ 的基本结果。在证明这些结果时，我们还将建立一些相关函数的界，这些界在后文中会用到。回顾一下，对于一个 ´étale 代数$E=K_1\times\cdots\times K_m$，记号 $\rho_E^{(\infty)}$ 与引言中使用的记号 $\rho_{K_1,\dots,K_m}^{(\infty)}$ 可以互换。

定理 6.1。 设 $K_1,\dots,K_m$ 是 $\mathbb{Q}_p$ 的有限扩张，且 $E:=K_1\times\cdots\times K_m$。此外，设 $(x_1,\dots,x_m)\in\mathcal{O}_{K_1}^{\mathrm{new}}\times\cdots\times\mathcal{O}_{K_m}^{\mathrm{new}}$。那么极限

$$\rho_E^{(\infty)}(x_1,\dots,x_m):=\lim_{n\to\infty}\rho_E^{(n)}(x_1,\dots,x_m)\tag{6.1}$$

存在，其中 $\rho_E^{(n)}(x_1,\dots,x_m)=\rho_{K_1,\dots,K_m}^{(n)}(x_1,\dots,x_m)$ 如引理 *1.13* 中所定义，并且可显式表示为

$$\rho_E^{(\infty)}(x_1,\dots,x_m)=||\Delta_\sigma(x_1,\dots,x_m)||\cdot\left(\prod_{i=1}^{m}V(x_i)\right)\cdot\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||.\tag{6.2}$$

此处， $A\in$ 矩阵空间$_n(\mathbb{Z}_p)$ 服从 *Haar* 分布，而 $Z(x)=\prod_{i=1}^{m}Z_i(x)$，其中 $Z_i(x)\in\mathbb{Z}_p[x]$ 是 x_i的最小多项式。

定理 6.2。 设 $E:=K_1\times\cdots\times K_m$，其中 $K_1,\ldots,K_m$ 是 $\mathbb{Q}_p$的有限扩张。那么，对于所有可测的 $U\subset\mathcal{O}_{K_1}^{\mathrm{new}}\times\cdots\times\mathcal{O}_{K_m}^{\mathrm{new}}$，

$$\lim_{n\to\infty}\mathbb{E}[Z_{U,n}]=\int_U\rho_E^{(\infty)}(x_1,\ldots,x_m)dx_1\cdots dx_m.$$

定理 6.3。 令 $k_1<k_2<\ldots<k_m$ 为正整数。对每个 i，令 $x_{i,\,1}$、……、$x_{i,\,j_i}$ 为 $\mathcal{U}_{k_i}$ 中元素组成的序列，该序列给出相应的 *étale* 代数 $E_i=\mathbb{Q}_p[\,(x_{i,\,1}$、……、$x_{i,\,j_i})\,]$。令 $E=E_1\times\cdots\times E_m$。则定理 *6.1* 的极限相关函数满足

$$\rho_E^{(\infty)}(x_{1,1},\ldots,x_{1,j_1},\ldots,x_{m,1},\ldots,x_{m,j_m})=\prod_{i=1}^m\rho_{E_i}^{(\infty)}(x_{i,1},\ldots,x_{i,j_i}).\tag{6.3}$$

定理 6.3 表明，不同提升子空间中的特征值的局部统计在渐近意义下相互独立。

定理 *6.1* 的证明。 我们只需证明元素 x_1、……、$x_m\in\mathbb{Z}_p$ 属于不同伽罗瓦轨道的情形，因为否则极限必为零。由定理 5.1 可知，极限 $\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||$ 存在。因此，根据引理 1.13 中有限规模相关函数 $\rho_E^{(n)}(x_1$、……、$x_m)$ 的表达式，可以直接推出本定理。□

乍看之下，定理 6.2 似乎可由定理 6.1 显然得出，但我们需要验证确实可以交换积分与取极限的顺序，这正是下述命题的目的。

命题 6.4。 设 $E:=K_1\times\cdots\times K_m$，其中 K_1、…、K_m 是 $\mathbb{Q}_p$的有限扩张。此外，设 $(x_1$、…、$x_m)\in\mathcal{O}_{K_1}^{\mathrm{new}}\times\cdots\times\mathcal{O}_{K_m}^{\mathrm{new}}$。对于所有 $1\le i\le m$，设 $r_i:=[K_i:\ \mathbb{Q}_p]$，$e_i$ 为 $K_i/\mathbb{Q}_p$ 的分歧指数，且 $Z_i\in\mathbb{Z}_p[x]$ 为 x_i的最小多项式。那么，我们有

$$\rho_E^{(n)}(x_1,\ldots,x_m)\le||\operatorname{Disc}_{E/\mathbb{Q}_p}||\cdot\prod_{1\le i\le m}\frac{1}{1-p^{-r_i/e_i}}\cdot\prod_{1\le i<j\le m}||\operatorname{Res}(Z_i,Z_j)||.\tag{6.4}$$

定理 *6.2* 的证明（假设命题 *6.4* 成立）。 对于所有 $1\le i\le m$，设 $r_i:=[K_i:\ \mathbb{Q}_p]$，且 e_i为 $K_i/\mathbb{Q}_p$的分歧指数。根据命题 6.4，对于所有 $(x_1,\ldots,x_m)\in\mathcal{O}_{K_1}^{\mathrm{new}}\times\cdots\times\mathcal{O}_{K_m}^{\mathrm{new}}$，我们有

$$\rho_{K_1,\ldots,K_m}^{(n)}(x_1,\ldots,x_m)\le\prod_{i=1}^m\frac{1}{1-p^{-r_i/e_i}}.$$

结论现在可由有界收敛定理立即得到。 □

现在回到命题 6.4。下述引理中的轨道积分估计是 [Yun13, Theorem1.5] 的一个较弱版本。

引理 6.5。 设 $K/\mathbb{Q}_p$ 是一个有限扩张。假设 $x\in\mathcal{O}_K^{\mathrm{new}}$满足 $\mathbb{F}_p[x\ (\text{模 }p)]=\mathbb{F}_{p^d}$，其中 $x\ (\text{模 }p)$ 是 x 在 K 的剩余域中的像。当 $\mathbb{Z}_p[x]$ 是 $\mathcal{O}_K$ 的真子集时，有

$$\frac{\#(\Lambda\setminus\operatorname{Mod}_{\mathbb{Z}_p[x]})}{\#(\mathcal{O}_K/\mathbb{Z}_p[x])^2}\le p^{-d}+2p^{-2d}.$$

证明。 设 δ 是 $\mathbb{Z}_p[x]$ 的 Serre 不变量（见 [Yun13, Subsection 4.1]），于是 $\#(\mathcal{O}_K/\mathbb{Z}_p[x])=p^{d\delta}$。由于 $\mathbb{Z}_p[x]$ 是 $\mathcal{O}_K$的真子集，因此有 $\delta>0$。

我们先进行一些组合计算作为准备。我们用 $\mathbb{Y}$ 表示分拆$\lambda=(\lambda_1,\ \lambda_2,\ \ldots\ldots)$ $\lambda_1\ge\lambda_2\ge\cdots$的集合，这些分拆是最终为零的非负整数（有限或无限）序列。对于仅在末尾零的个数不同的两个这样的序列，我们不作区分，

即末尾附有一串零。令 $|\lambda| := \sum_{i\geq 1}\lambda_i$，且 $l(\lambda) := \#\{i \mid \lambda_i > 0\}$。注意，对所有$n,\ k \geq 1$,

$$\begin{aligned}\#\{\lambda \in \mathbb{Y} \mid |\lambda| = n, l(\lambda) = k\} &= \#\{\lambda_1 \geq \ldots \geq \lambda_k \geq 1 \mid \lambda_1 + \cdots + \lambda_k = n\} \\ &\leq \#\{\lambda_1, \ldots, \lambda_k \geq 1 \mid \lambda_1 + \cdots + \lambda_k = n\} \\ &= \binom{n-1}{k-1}.\end{aligned} \tag{6.5}$$

因此,

$$\begin{aligned}\#\{\lambda \in \mathbb{Y} \mid |\lambda| \leq \delta, l(\lambda) = k\} &= \sum_{n\leq\delta} \#\{\lambda \in \mathbb{Y} \mid |\lambda| = n, l(\lambda) = k\} \\ &\leq \sum_{n\leq\delta} \binom{n-1}{k-1} \\ &= \binom{\delta}{k},\end{aligned} \tag{6.6}$$

其中最后一步是通过反复应用帕斯卡恒等式得到的。根据 [Yun13, Theorem 1.5][8]中的上界，我们有

$$\begin{aligned}\#(\Lambda \backslash \mathrm{Mod}_{\mathbb{Z}_p[x]}) &\leq \sum_{|\lambda|\leq\delta} p^{d(\delta - l(\lambda))} + \sum_{|\lambda|<\delta} p^{d(|\lambda| - l(\lambda))} \\ &\leq \sum_{|\lambda|\leq\delta} p^{d(\delta - l(\lambda))} + \sum_{|\lambda|\leq\delta-1} p^{d(\delta-1 - l(\lambda))} \\ &\leq \sum_{k=0}^{\delta} p^{d(\delta-k)} \binom{\delta}{k} + \sum_{k=0}^{\delta-1} p^{d(\delta-1-k)} \binom{\delta-1}{k} \\ &= (1+p^d)^\delta + (1+p^d)^{\delta-1}.\end{aligned} \tag{6.7}$$

这里第三行由 (6.6) 得出，最后一行则是二项式定理。因此，我们得到不等式

$$\frac{\#(\Lambda \backslash \mathrm{Mod}_{\mathbb{Z}_p[x]})}{\#(\mathcal{O}_K/\mathbb{Z}_p[x])^2} \leq \frac{(1+p^d)^\delta + (1+p^d)^{\delta-1}}{p^{2d\delta}} \leq p^{-d} + 2p^{-2d}$$

代入 $\delta = 1$ 即可得到，因为中间的表达式关于 δ递减。 □

命题 *6.4* 的证明。 对于所有 $1 \leq i \leq m$，若 $\mathbb{Z}_p[x_i] = \mathcal{O}_{K_i}$，则有 $\#(\Lambda_i \backslash \mathrm{Mod}^{\mathbb{Z}_p[x_i]}) = 1$。否则，根据引理 6.5，我们有

$$\frac{\#(\Lambda_i \backslash \mathrm{Mod}_{\mathbb{Z}_p[x_i]})}{\#(\mathcal{O}_{K_i}/\mathbb{Z}_p[x_i])^2} \leq p^{-d_i} + 2p^{-2d_i} \leq 1,$$

其中 $d_i := [\mathbb{F}_p[x_i \text{ (模 } p)] \colon \mathbb{F}_p] \geq 1$。因此，无论上述哪种情况成立，我们始终有

$$\frac{\#(\Lambda_i \backslash \mathrm{Mod}_{\mathbb{Z}_p[x_i]})}{\#(\mathcal{O}_{K_i}/\mathbb{Z}_p[x_i])^2} \leq 1.$$

[8]用 [Yun13 的记号，定理 1.5] 对应于我们的 p，而 O_γ 是我们的 $\#(\Lambda \backslash \mathrm{Mod}^{\mathbb{Z}_p[x]})$。乘积 $\prod_{i\in B(\gamma)}$ 在我们的情形下只有一项，且 $d_i = d,\ \delta_i = \delta$，因此 $\rho(\gamma) = 0$。

根据引理 1.13 给出的表达式，我们有

$$\begin{aligned}\rho_E^{(n)}(x_1,\dots,x_m) &\le ||\Delta_\sigma(x_1,\dots,x_m)|| \cdot \prod_{i=1}^m V(x_i)\\ &= \prod_{1\le i<j\le m} ||\operatorname{Res}(Z_i,Z_j)|| \cdot \prod_{i=1}^m \frac{\#(\Lambda_i\setminus \operatorname{Mod}_{\mathbb{Z}_p[x_i]})||\Delta_\sigma(x_i)||^2}{1-p^{-r_i/e_i}}\\ &= \prod_{1\le i<j\le m} ||\operatorname{Res}(Z_i,Z_j)|| \cdot \prod_{i=1}^m \frac{\#(\Lambda_i\setminus \operatorname{Mod}_{\mathbb{Z}_p[x_i]})||\operatorname{Disc}_{K_i/\mathbb{Q}_p}||}{(1-p^{-r_i/e_i})\#(\mathcal{O}_{K_i}/\mathbb{Z}_p[x_i])^2} \qquad (6.8)\\ &\le \prod_{1\le i<j\le m} ||\operatorname{Res}(Z_i,Z_j)|| \cdot \prod_{i=1}^m \frac{||\operatorname{Disc}_{K_i/\mathbb{Q}_p}||}{1-p^{-r_i/e_i}}\\ &= ||\operatorname{Disc}_{E/\mathbb{Q}_p}|| \cdot \prod_{1\le i\le m} \frac{1}{1-p^{-r_i/e_i}} \cdot \prod_{1\le i<j\le m} ||\operatorname{Res}(Z_i,Z_j)||.\end{aligned}$$

这里，第三行是由 [Car22]第 10 页的结果得到的。 □

定理 *6.3* 的证明。我们只需证明这些元素

$$x_{1,1},\dots,x_{1,j_1},\dots,x_{m,1},\dots,x_{m,j_m}\in\bar{\mathbb{Z}}_p$$

属于不同的伽罗瓦轨道的情形，因为否则两边都必为零。对于 $1\le i\le m$，令 Z_i表示 $\{x_{i,l}$ 的最小多项式： $1\le l\le j_i\}$。于是，多项式 Z_1，…， Z_m 满足定理 5.2 中的条件，因此

$$\lim_{n\to\infty}\mathbb{E}||\det(Z(A))|| = \prod_{i=1}^m \lim_{n\to\infty}\mathbb{E}||\det(Z_i(A))||.$$

这里， $Z(x):=\prod_{i=1}^m Z_i(x)$，且 $A\in$ 矩阵空间$_n(\mathbb{Z}_p)$ 服从 Haar 分布。此外，如命题 2.7 所示，不同提升子空间中的特征值之间的距离始终为 1，这意味着

$$||\Delta_\sigma(x_{1,1},\dots,x_{1,j_1},\dots,x_{m,1},\dots,x_{m,j_m})|| = \prod_{i=1}^m ||\Delta_\sigma(x_{i,1},\dots,x_{i,j_i})||.$$

因此，由定理 6.1 可得

$$\begin{aligned}\mathrm{LHS}(6.3) &= \left(\prod_{i=1}^m\prod_{l_i=1}^{j_i} V(x_{i,l_i})\right)\cdot||\Delta_\sigma(x_{1,1},\dots,x_{1,j_1},\dots,x_{m,1},\dots,x_{m,j_m})||\cdot\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||\\ &= \left(\prod_{i=1}^m\prod_{l_i=1}^{j_i} V(x_{i,l_i})\cdot||\Delta_\sigma(x_{i,1},\dots,x_{i,j_i})||\right)\cdot\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||\\ &= \prod_{i=1}^m\left(\prod_{l_i=1}^{j_i} V(x_{i,l_i})\cdot||\Delta_\sigma(x_{i,1},\dots,x_{i,j_i})||\cdot\lim_{n\to\infty}\mathbb{E}||\det(Z_i(A))||\right)\\ &= \mathrm{RHS}(6.3).\end{aligned} \qquad (6.9)$$

证明到此结束。 □

定理 *1.1* 的证明。 定理 1.1 中出现的集合 $\mathcal{U}_1,\mathcal{U}_2,\dots$ 恰好是第 2.3 节中引入的提升子空间。不交并 (1) 显然成立，而 (2) 已在命题 2.9 中证明。位于不同提升子空间中的特征值的渐近独立性已在定理 6.3 中证明，因此剩下的只是求出每个提升子空间中特征值数量的极限。

最后，将 $A \in \mathrm{Mat}_n(\mathbb{Z}_p)$ 转换为系数属于 $\mathbb{F}_p$ 的剩余域版本后，我们可以应用 [She25, 推论 1.2][9] ，从而得出 A中位于 $\mathcal{U}_i$ 的特征值数量依分布收敛，而极限随机变量 N_i 的分布律见该处。 □

我们注意到，上文使用的 She 的结果是在一般矩阵元素分布的情形下证明的。对于 $\mathbb{F}_p$ 中的均匀随机元素（这正是我们此处所需的情形），第二作者在其未发表的本科毕业论文 [VP18], 的推论 3.1.13 中也使用 Fulman 的著作 [Ful97] 中针对 $\mathrm{GL}_n(\mathbb{F}_q)$ 情形所采用的相同论证证明了这些结果。我们目前还不知道如何证明我们所研究的、更精细的特征值统计的普适性（提升子空间中特征值的数量除外），但这是一个非常有趣的问题。

下面给出一个简单的精确计算，求出在 $\mathcal{O}_E = \mathbb{Z}_p[\mathfrak{x}]$ 这一（定义并不十分明确的）特殊情形下的极限相关函数。这将有助于第 11 节中的后续估计。

定理 6.6。 设 $E = K_1 \times \cdots \times K_m$ 是 $\mathbb{Q}_p$ 上的有限 *étale* 代数，且 $\mathfrak{x} = (x_1, \ldots, x_m) \in \mathcal{O}_E$ 满足 $\mathcal{O}_E = \mathbb{Z}_p[\mathfrak{x}]$。那么我们有 $\rho_E^{(\infty)}(\mathfrak{x}) = ||\mathrm{Disc}_{E/\mathbb{Q}_p}||$。

证明。 在这种情况下，对所有 $1 \le i \le m$，我们都有 $\mathbb{Z}_p[x_i] = \mathcal{O}_{K_i}$，因此

$$\#(\Lambda_i \backslash \mathrm{Mod}_{\mathbb{Z}_p[x_i]}) = \#(\Lambda_i \backslash \mathrm{Mod}_{\mathcal{O}_{K_i}}) = 1.$$

[Car22] 第 10 页的结果表明，当 $\mathbb{Z}_p[x_i] = \mathcal{O}_{K_i}$ 时， $||\Delta_\sigma(x_i)||^2 = |\mathrm{Disc}_{K_i/\mathbb{Q}_p}||$。因此， $||\Delta_\sigma(x_1, \ldots..., x_m)|| = ||\mathrm{Disc}_{E/\mathbb{Q}_p}||^{1/2}$。此外，令 p^{f_i} 表示 $\mathcal{O}_{K_i}$ 的剩余域的阶，于是 $V(x_i) = \frac{||\mathrm{Disc}_{K_i/\mathbb{Q}_p}||^{1/2}}{1-p^{-f_i}}$，其中 V 如定义 1.6 所述。

由定理 6.1，我们有

$$\begin{aligned}\rho_E^{(\infty)}(\mathfrak{x}) &= \prod_{i=1}^m V(x_i) \cdot ||\Delta_\sigma(x_1, \ldots, x_m)|| \cdot \lim_{n\to\infty} \mathbb{E}||\det(Z(A))|| \\ &= \prod_{i=1}^m \frac{||\mathrm{Disc}_{K_i/\mathbb{Q}_p}||^{1/2}}{1-p^{-f_i}} \cdot ||\mathrm{Disc}_{E/\mathbb{Q}_p}||^{1/2} \cdot \prod_{i=1}^m (1-p^{-f_i}) \\ &= ||\mathrm{Disc}_{E/\mathbb{Q}_p}||.\end{aligned} \tag{6.10}$$

这里，第二行由命题 5.10 得出。证明至此完成。 □

7. Eigenvalues of Haar matrices in $\mathrm{GL}_n(\mathbb{Z}_p)$

本节的主要结果定理 7.5 表明，在考虑显然的限制后，$\mathrm{GL}_n(\mathbb{Z}_p)$ 的极限相关函数与矩阵空间$_n(\mathbb{Z}_p)$ 的相同。我们还将证明关于极限前相关函数的结果。我们沿用第 3 节中的记号，但本节还要求对所有 $1 \le i \le m$，都有$||x_i|| = 1$；等价地， $Z_i(x)$ 的常数项属于 $\mathbb{Z}_p^\times$。

定理 7.1。 假设 A 是随机的，并服从 $\mathrm{GL}_r(\mathbb{Z}_p)$ 上的 *Haar* 概率测度。那么对于所有满足以下条件的元组 $s = (s_1, \ldots, s_m) \in (\frac{1}{e_1}\mathbb{N}, \ldots, \frac{1}{e_m}\mathbb{N})$： 对所有 $1 \le i \le m$, 均有 $s_i > r \operatorname{val} \mathrm{Disc}(\mathfrak{x})$，我们有

$$\prod_{i=1}^m p^{s_i r_i} \cdot \mathbf{P}(\operatorname{val} P_A(x_i) \ge s_i, \forall 1 \le i \le m) = \frac{1}{||\Delta_\sigma(x_1, \ldots, x_m)||} \prod_{i=1}^m V(x_i). \tag{7.1}$$

引理 7.2. 假设 $A \in$矩阵空间$_r(\mathbb{Z}_p)$ 满足 $\mathrm{val} P_A(x_i) > r \operatorname{val} \mathrm{Disc}(\mathfrak{x})$ 对所有 $1 \le i \le m$ 都成立。那么 $A \in \mathrm{GL}_r(\mathbb{Z}_p)$。

[9]按照 [She25，推论 1.2]，中的记号，我们令 f_i 为 $F_i \in \mathbb{F}_p[x]$，它是与 (2.3) 中的 $\mathcal{U}_i$ 相对应的不可约多项式。因此，该多项式的次数为 d_i。此外，我们令 ν_{f_i} 为 N_i/d_i的分布律。

定理 *7.1* 的证明（假设引理 *7.2* 成立）。引理 7.2 表明，我们要计算其在 (7.1) 中概率的集合与 (3.1) 中的集合完全相同。区别在于，在 (7.1) 中，它被视为 $\mathrm{GL}_r(\mathbb{Z}_p)$ 的子集，而在 (3.1) 中，它被视为 $\mathrm{Mat}_r(\mathbb{Z}_p)$ 的子集。因此，我们有

$$\begin{aligned}\mathrm{LHS}(7.1) &= \frac{\mathrm{RHS}(3.1)}{\mathbf{P}(A \in \mathrm{GL}_r(\mathbb{Z}_p) \mid A \text{ Haar-distributed in } \mathrm{Mat}_r(\mathbb{Z}_p))} \\ &= \frac{\frac{(1-p^{-1})\cdots(1-p^{-r})}{||\Delta_\sigma(x_1,\ldots,x_m)||}\prod_{i=1}^m V(x_i)}{(1-p^{-1})\cdots(1-p^{-r})} \\ &= \mathrm{RHS}(7.1),\end{aligned} \tag{7.2}$$

由此证明得证。 □

现在我们回到引理 7.2 的证明。

引理 *7.2* 的证明。应用命题 3.3，P_A 的根可写为

$$f(\sigma_{i,l_i}(x_i)), \quad 1 \le i \le m, 1 \le l_i \le r_i,$$

其中 $f \in F_Z$（回顾定义 3.2）。根据强三角不等式，$||\sigma_{i,\ l_i}(x_i)|| = 1$ 和 $f \in F_Z$ 蕴含

$$||f(\sigma_{i,l_i}(x_i))|| = ||f(\sigma_{i,l_i}(x_i)) - \sigma_{i,l_i}(x_i) + \sigma_{i,l_i}(x_i)|| = ||\sigma_{i,l_i}(x_i)|| = 1.$$

因此，P_A 的常数项属于 $\mathbb{Z}_p^\times$，且 $A \in \mathrm{GL}_r(\mathbb{Z}_p)$。 □

接下来的两个结果给出了相关函数的表达式。

定理 7.3. 固定 $n \ge 1$，并令 $K_1, \ldots, K_m$ 为 $\mathbb{Q}_p$ 的扩张，其中 $\sum_{i=1}^m [K_i : \mathbb{Q}_p] = n$。令 $U \subset \mathcal{O}_{K_1}^{\mathrm{new}} \times \cdots \times \mathcal{O}_{K_m}^{\mathrm{new}}$ 为任意可测集。设 $A \in \mathrm{GL}_n(\mathbb{Z}_p)$ 服从乘法 ***Haar*** 分布，且 $Z_{U,n}$ 表示其特征值中落在 U 内的 m 元组 $(x_1, \ldots, x_m)$ 的数量。那么

$$\mathbb{E}[Z_{U,n}] = \int_U \rho^{(n),\mathrm{GL}}_{K_1,\ldots,K_m}(x_1,\ldots,x_m)dx_1\cdots dx_m,$$

其中相关函数的显式表达式为

$$\rho^{(n),\mathrm{GL}}_{K_1,\ldots,K_m}(x_1,\ldots,x_m) = ||\Delta_\sigma(x_1,\ldots,x_m)|| \cdot \left(\prod_{i=1}^m V(x_i)\right) \cdot \mathbb{1}_{x_i \in \mathcal{O}_{K_i}^\times, \forall 1 \le i \le m}, \tag{7.3}$$

积分（以及 U 可测性的定义）是相对于 $\mathcal{O}_{K_1} \times \cdots \times \mathcal{O}_{K_m}$ 上的 ***Haar*** 概率测度进行的。

定理 7.4. 令 $K_1, \ldots, K_m$ 为 $\mathbb{Q}_p$ 的扩张，且 $r := \sum_{i=1}^m [K_i : \mathbb{Q}_p]$。设 $A \in \mathrm{GL}_n(\mathbb{Z}_p)$服从大小为 $n \ge r$ 的乘法 ***Haar*** 分布。那么，A 的特征值的 $(K_1, \ldots, K_m)$ 相关函数$\rho^{(n),K_1 \ldots ,,K_m}_{\mathrm{GL}}(x_1, \ldots, x_m)$ 具有如下形式

$$\rho^{(n),\mathrm{GL}}_{K_1,\ldots,K_m}(x_1,\ldots,x_m) = ||\Delta_\sigma(x_1,\ldots,x_m)|| \cdot \left(\prod_{i=1}^m V(x_i)\right) \cdot \mathbb{E}||\det(Z(\tilde{A}))||. \tag{7.4}$$

这里 $Z(x) = \prod_{i=1}^m Z_i(x)$ 的次数为 r，$Z_i \in \mathbb{Z}_p[x]$ 是 x_i 的最小多项式，其次数为 r_i，˜，并且 $A \in \mathrm{GL}_{n-r}(\mathbb{Z}_p)$ 服从乘法 ***Haar*** 测度分布。

定理 *7.3* 和定理 *7.4* 的证明。它们可以由定理 7.1 推得，证明方法与第 4 节中由定理 3.1 推得定理 1.7 和引理 1.13 的证明完全相同。□

定理 7.5。设 K_1、…、K_m 是 $\mathbb{Q}_p$ 的有限扩张，且 $E := K_1 \times \cdots \times K_m$。对于所有 $1 \le i \le m$，取 $x_i \in \mathcal{O}_{K_i}^{\mathrm{new}}$，使得 x_1、…、x_m 属于彼此不同的伽罗瓦轨道。那么，相关函数的极限

$$\rho^{(\infty),\mathrm{GL}}_E(x_1,\ldots,x_m) := \lim_{n\to\infty} \rho^{(n),\mathrm{GL}}_E(x_1,\ldots,x_m)$$

存在，且由下式给出

$$\rho_E^{(\infty),\mathrm{GL}}(x_1,\dots,x_m)=\rho_E^{(\infty)}(x_1,\dots,x_m)\cdot \mathbb{1}_{x_i\in\mathcal{O}_{K_i}^\times,\forall 1\le i\le m}.$$

以下引理将有助于证明定理 7.5。

引理 7.6. 设 $A\in \mathrm{GL}_n(\mathbb{Z}_p)$ 服从乘法 *Haar* 分布，且 $A\in$ 矩阵空间$_n(\mathbb{Z}_p)$ 服从加法 *Haar* 分布。此外，设 $Z\in\mathbb{Z}_p[x]$ 与定理 *7.4* 中的相同，因此其常数项属于 $\mathbb{Z}_p^\times$。那么，我们有

$$\lim_{n\to\infty}\mathbb{E}||\det(Z(\tilde{A}))||=\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||.$$

证明. 注意到， A 的分布与在$||\det(A)||=1$条件下 A 的分布相同。因此，我们有

$$\mathbb{E}||\det(Z(\tilde{A}))||=\mathbb{E}\left[||\det(Z(A))|| \middle| ||\det(A)||=1\right].$$

此外，剩余$Z\in\mathbb{F}_p[x]$ 与 $\overline{x}\in\mathbb{F}_p[x]$互素。因此，由注 5.9 可知，当 n趋于无穷大时，联合随机变量 $(||\det(Z(A))||,||\det(A)||)$ 弱收敛到一对相互独立的变量。因此

$$\lim_{n\to\infty}\mathbb{E}||\det(Z(\tilde{A}))||=\lim_{n\to\infty}\mathbb{E}\left[||\det(Z(A))|| \middle| ||\det(A)||=1\right]=\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||,$$

完成证明。 □

定理 *7.5* 的证明。 我们只需证明元素 $x_1,\dots,x_m\in\mathbb{Z}_p$属于不同伽罗瓦轨道的情形，因为否则极限必为零。如果某个 x_i 不属于 $\mathcal{O}_{K_i}^\times$，那么显然有 $\rho^{(\infty)}{}_{,E}{}^{\mathrm{GL}}(x_1,\dots,x_m)=\lim_{n\to\infty}\rho^{(n)}{}_{,E}{}^{\mathrm{GL}}(x_1,\dots,x_m)=0$。否则，根据定理 7.4 和引理 7.6，我们有

$$\rho_E^{(\infty),\mathrm{GL}}(x_1,\dots,x_m)=||\Delta_\sigma(x_1,\dots,x_m)||\cdot\left(\prod_{i=1}^m V(x_i)\right)\cdot\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||.$$

这里，矩阵 $A\in$矩阵空间$_n(\mathbb{Z}_p)$ 服从 Haar 分布。上述等式右侧恰好是定理 6.1 中 $\rho_E^{(\infty)}(x_1,\dots,x_m)$ 的表达式。□

注 7.7。 关于 $\mathrm{GL}_n(\mathbb{Z}_p)$ 中结果的另一种观点如下。显然，对于 $\mathrm{GL}_n(\mathbb{Z}_p)$ 情形，特征值不可能位于 0 周围的开单位圆盘内。因此，我们也可以将相关函数视为定义在 $\mathcal{O}^\times{}_{,K_1}{}^{\mathrm{new}}\times\cdots\times\mathcal{O}^\times{}_{,K_m}{}^{\mathrm{new}}$ 上的函数，其中 $\mathcal{O}^\times{}_{,K_i}{}^{\mathrm{new}}:=\mathcal{O}_{K_i}^\times\cap\mathcal{O}_{K_i}^{\mathrm{new}}$。此外，我们还可以在 $\mathcal{O}_{K_i}^\times$ 上赋予乘法哈尔概率测度。在这种情况下，关于这些乘法 Haar 测度之积的相关函数表达式与定理 7.5 中的相同，只需去掉示性函数，并将 $V:\mathcal{O}_{K_i}^{\mathrm{new}}\to\mathbb{R}$ 替换为

$$\begin{aligned}V^{\mathrm{GL}}:\mathcal{O}_{K_i}^{\times,\mathrm{new}}&\to\mathbb{R}\\ x_i&\mapsto||\Delta_\sigma(x_i)||\cdot\#(\Lambda\backslash\mathrm{Mod}_{\mathbb{Z}_p[x_i]}).\end{aligned}\tag{7.5}$$

可以看出， V^{GL}在 $\mathcal{O}^\times{}_{,K_i}{}^{\mathrm{new}}$中的值与 V仅相差一个常数因子 $1-p^{-r_i/e_i}$，而该因子恰好是 $\mathcal{O}_{K_i}^\times$ 在 $\mathcal{O}_{K_i}$中的加性 Haar 测度。

8. Markov chain description of the cokernel

在定理 5.1 中，我们证明了，为了求出极限相关函数而需要计算的各项 $\lim_{n\to\infty}\mathbb{E}[||\det(Z(A))||]$，可表示为相关矩阵的行列式的$p$-进赋值的某些混合矩，其中 $A_0+x_iA_1+\ldots+x_i^{r-1}A_{r-1}$ 遍历 Z的根。为了证明定理 5.1，我们的策略是考虑余核而非行列式；我们也将采用同样的视角来更明确地计算这些混合矩。基本思想是，对于 $\mathbb{Z}_p$ 上的单个 Haar 矩阵 A ，或某个更一般的 $\mathcal{O}_K$，人们可以

依次抽样 Cok$(A)/(\pi)$，Cok$(A)/(\pi^2)$.....，并且（并不显然地）可以用一个齐次马尔可夫链来表述这一过程。矩阵 $A_0+x_iA_1+\ldots+x_i^{r-1}A_{r-1}$的每个余核都可以用这种方式单独抽样，但对于不同的 i，底层马尔可夫链的副本通常会彼此相关。本节从 Fulman 和 Evans 关于这一马尔可夫链的已知结果开始，并利用这些结果证明一个适用于我们将遇到的各类期望的通式。

回顾 q-Pochhammer 记号

$$(a;t)_n := \prod_{i=0}^{n-1}(1-at^i) \tag{8.1}$$

对于 $n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$。

定义 8.1 ([Ful01，定理 2])。对于固定参数 $t \in (0,\ 1)$ 和 $u \in (0,\ t^{-1})$，在 $\mathbb{Z}_{\geq 0}$ 上定义马尔可夫核 $\mathcal{K}(\cdot,\ \cdot)$，如下所示：

$$\mathcal{K}(a,b) = \mathcal{K}_{t,u}(a,b) = \begin{cases} \frac{t^{b^2}u^b(t;t)_a(ut;t)_a}{(t;t)_{a-b}(t;t)_b(ut;t)_b} & 0 \leq b \leq a \\ 0 & \text{else} \end{cases}. \tag{8.2}$$

我们有时也允许初始状态为 ∞，并定义转移概率

$$\mathcal{K}(\infty,b) = \lim_{a\to\infty}\mathcal{K}(a,b) = (ut;t)_\infty \frac{t^{b^2}u^b}{(t;t)_b(ut;t)_b} \tag{8.3}$$

至有限状态。

显然，$\mathcal{K}$ 定义一个马尔可夫核并非易事，但这一点已在 [Ful01 的定理 2]中得到证明。Evans [Eva02] 在研究 p-进随机矩阵的初等因子（有时也称为奇异数，并且等价于余核）时，独立地发现了同一个马尔可夫链。

定义 8.2。设 K 是一个带有一致化元 π 且剩余域同构于 $\mathbb{F}_q$的非阿基米德局部域，并设 M 是一个 $\mathcal{O}_K$-模。那么对于任意 $i \in \mathbb{Z}_{\geq 1}$，我们定义

$$M_i' := \mathrm{rank}_{\mathbb{F}_q}(\pi^{i-1}M/\pi^iM), \tag{8.4}$$

注意到 $\pi^{i-1}M/\pi^iM$ 具有$\mathcal{O}_K/\pi\mathcal{O}_K \cong \mathbb{F}_q$-向量空间的结构。

或者，根据主理想整环上模的结构定理，任何如上所述的模 M 都同构于 $\bigoplus_{i\geq 0}\mathcal{O}_K/\pi^{\lambda_i}\mathcal{O}_K$，其中 $\lambda_1 \geq \lambda_2 \geq \ldots \geq 0$为整数，且其中只有有限多个非零。等价地，也可以定义

$$M_i' = \#\{j : \lambda_j \geq i\}. \tag{8.5}$$

命题 8.3 ([Eva02, 定理 3。5])。设 K 是一个剩余域大小为 q的非阿基米德局部域，且 A 是一个在 $\mathcal{O}_K$上具有独立同分布的 ***Haar*** 分布元素的 $n \times n$ 矩阵。那么，随机序列 余核$(A)_1'$、余核$(A)_2'$、.....服从定义 ***8.1*** 中以状态 n为起始状态的马尔可夫链 $\mathcal{K}_{q^{-1},\ 1}$。换言之，

$$\Pr(\mathrm{Cok}(A)_1' = b) = \mathcal{K}_{q^{-1},1}(n,b), \tag{8.6}$$

and

$$\Pr(\mathrm{Cok}(A)_{i+1}' = b|\ \mathrm{Cok}(A)_i' = a) = \mathcal{K}_{q^{-1},1}(a,b) \tag{8.7}$$

对所有 $i \geq 1$均成立。

这一简单事实——对于每个 u，它都是一个马尔可夫核；此事实已由 [Ful01, 定理 2], 证实——已足以计算任意 Haar 矩阵 A的 $\mathbb{E}[|\det(A)|]$：

命题 8.4。设 $\lambda_1, \lambda_2, \ldots$ 的分布与定义 ***8.1*** 中马尔可夫链 $\mathcal{K}_{t,u}$ 的各步相同，其初始状态固定为 $\lambda_0 = n \in \mathbb{N} \cup \{\infty\}$。那么对于 $k \in \mathbb{Z}_{\geq 0}$,

$$\mathbb{E}[t^{k(\lambda_1+\lambda_2+\ldots)}] = \frac{(ut;t)_k}{(ut^{n+1};t)_k}, \tag{8.8}$$

其中，当 $n=\infty$ 时，我们将分母视为1。

证明。 显式公式中，~~因子 $(t;t)_a(ut;t)_a$~~ $(t;t)_b(ut;t)_b$ 会在任意无穷乘积中相消，

$$\mathcal{K}(n,\lambda_1)\mathcal{K}(\lambda_1,\lambda_2)\cdots$$

除了第一个 $(t;\ t)_n(ut;t)_n$ 之外。因此得到

$$\begin{aligned}\mathbb{E}[t^{k(\lambda_1+\lambda_2+\ldots)}] &= \sum_{\substack{\lambda_1\geq\lambda_2\geq\ldots\geq 0\\ \lambda_1\leq n}}\left((t;t)_n(ut;t)_n\prod_{i\geq 0}\frac{t^{\lambda_{i+1}^2}u^{\lambda_{i+1}}}{(t;t)_{\lambda_i-\lambda_{i+1}}}\right)\cdot t^{k(\lambda_1+\ldots)}\\ &= \frac{(ut;t)_n}{(ut^{k+1};t)_n}\sum_{\substack{\lambda_1\geq\lambda_2\geq\ldots\geq 0\\ \lambda_1\leq n}}(t;t)_n(ut^{k+1};t)_n\prod_{i\geq 0}\frac{t^{\lambda_{i+1}^2}(ut^k)^{\lambda_{i+1}}}{(t;t)_{\lambda_i-\lambda_{i+1}}} \qquad (8.9)\\ &= \frac{(ut;t)_n}{(ut^{k+1};t)_n}\sum_{\substack{\lambda_1\geq\lambda_2\geq\ldots\geq 0\\ \lambda_1\leq n}}\prod_{i\geq 0}\mathcal{K}_{t,ut^k}(\lambda_i,\lambda_{i+1}).\end{aligned}$$

最后一行中的和恰好为 1，而 q-Pochhammer 符号的商在约去因子后等于所需的表达式。□

推论 8.5。 设 $K/\mathbb{Q}_p$ 是一个次数为 r 、剩余域大小为 q的扩张。设 $A\in$矩阵空间$_n(\mathcal{O}_K)$ 服从 *Haar* 分布。那么，对于任意 $k\geq 0$,

$$\mathbb{E}[|\det(A)|^{rk}] = \frac{(q^{-1};q^{-1})_k}{(q^{-n-1};q^{-1})_k}. \qquad (8.10)$$

证明。 根据引理 5.3，我们有

$$\mathbb{E}[|\det(A)|^{rk}] = \mathbb{E}[\#\operatorname{Cok}(A)^{-k}]. \qquad (8.11)$$

根据命题 8.3，这等于 $\mathbb{E}[(q^{-1})_{k(\lambda_1+\lambda_2+\ldots)}]$，其中 $\lambda_0=n$和 $\lambda_1,\ \lambda_2,\ \ldots$是马尔可夫链 $\mathcal{K}_{q^{-1},1}$的连续步骤。由 $u=1,\ t=q^{-1}$，结论即由命题 8.4 得出。□

对于定理 5.1 中这类更一般的期望，我们需要了解马尔可夫核 $\mathcal{K}$ 的更精细性质。作为一个 $\mathbb{Z}_{\geq 0}\times\mathbb{Z}_{\geq 0}$ 矩阵，它具有显式的对角化；这一性质曾用于为罗杰斯-拉马努金恒等式给出一种新的证明，见 [Ful01]。为了陈述这一结果，使用共轭矩阵 M 更为方便，其定义如下

$$M(a,b)=M_{t,u}(a,b)=\begin{cases}\frac{t^{b^2}u^b}{(t;t)_{a-b}} & b\leq a\\ 0 & \text{else}\end{cases}, \qquad (8.12)$$

它不再是马尔可夫核，但在代数上更简单，并且其实已基本出现在命题 8.4 的证明中。

命题 8.6 ([Ful01，定理 3])。 定义矩阵 $U=(U(i,j))_{i,\ j\in\mathbb{Z}_{\geq 0}}$如下

$$U(i,j)=U_{t,u}(i,j)=\begin{cases}\frac{1}{(t;t)_{i-j}(ut;t)_{i+j}} & i\geq j\\ 0 & i<j\end{cases}. \qquad (8.13)$$

那么， U的列$(U(i,j))^{i\in\mathbb{Z}_{\geq 0}}$是 M的特征向量，并且 $M=UEU^{-1}$其中$E=E_{t,u}$是 $\mathbb{Z}_{\geq 0}\times\mathbb{Z}_{\geq 0}$对角矩阵，其$(i,i)$项为 $i=0$对应的 $u^it^{i^2}$，$1,\ldots$

此外，对角化中的逆矩阵各项都有显式表达式

$$U^{-1}(i,j)=\begin{cases}\frac{(-1)^{i-j}t^{\binom{i-j}{2}}(1-ut^{2i})(ut;t)_{i+j-1}}{(t;t)_{i-j}} & i\geq j\\ 0 & i<j\end{cases}. \qquad (8.14)$$

在此处的情形 $i=j=0$，我们必须按照负指标 q-*Pochhammer* 符号的标准约定来解释$(ut;t)_{-1}=1/(1-u)$。

请注意，我们的 U 在 [Ful01]，中称为 A，但我们已经用 A 表示 Haar 矩阵。

推论 8.7。设 $m \geq 1$，并设 $\xi \in \mathbb{C}$。设 $\lambda_1, \ldots, \lambda_m$ 是马尔可夫链 $\mathcal{K} = \mathcal{K}_{t,\ u}$ 从 $\lambda_0 = n$ 开始时依次经过的状态，其中 $n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$。那么

$$\mathbb{E}[\xi^{\lambda_1+\cdots+\lambda_m} f(\lambda_m)] = (t;t)_n (ut;t)_n \sum_{\substack{d \geq \ell \geq 0 \\ d \leq n}} U_{t,u\xi}(n,d) E_{t,u\xi}(d,d)^m U^{-1}_{t,u\xi}(d,\ell) \frac{f(\ell)}{(t;t)_\ell (ut;t)_\ell}, \quad (8.15)$$

对任意函数 $f:\ \mathbb{Z}_{\geq 0} \to \mathbb{R}$。这里，若 $n = \infty$，我们假设 f 衰减得足够快，从而左侧有定义，并令

$$U_{t,u\xi}(\infty, d) = \lim_{n\to\infty} U_{t,u\xi}(n,d) = \frac{1}{(t;t)_\infty (u\xi t;t)_\infty}. \quad (8.16)$$

证明。所需的期望为

$$\begin{aligned}
&\sum_{\lambda_1 \geq \ldots \geq \lambda_m \geq 0} \prod_{i=0}^{m-1} \mathcal{K}(\lambda_i, \lambda_{i+1}) \xi^{\lambda_1+\cdots+\lambda_m} f(\lambda_m) \\
&= \sum_{\lambda_1 \geq \ldots \geq \lambda_m \geq 0} (t;t)_n (ut;t)_n \prod_{i=0}^{m-1} \frac{t^{\lambda_{i+1}^2} u^{\lambda_{i+1}}}{(t;t)_{\lambda_i - \lambda_{i+1}}} \cdot \frac{1}{(t;t)_{\lambda_m} (ut;t)_{\lambda_m}} \xi^{\lambda_1+\cdots+\lambda_m} f(\lambda_m) \qquad (8.17) \\
&= (t;t)_n (ut;t)_n \sum_{\lambda_1 \geq \lambda_1 \geq \ldots \geq \lambda_m \geq 0} \prod_{i=0}^{m-1} M_{t,u\xi}(\lambda_i, \lambda_{i+1}) \cdot \frac{f(\lambda_m)}{(t;t)_{\lambda_m} (ut;t)_{\lambda_m}}.
\end{aligned}$$

利用命题 8.6 对矩阵$M_{t,\ u\xi}$ 对角化，可得

$$\mathrm{RHS}(8.17) = (t;t)_n (ut;t)_n \sum_{\lambda_m \geq 0} (U_{t,u\xi} E^m_{t,u\xi} U^{-1}_{t,u\xi})(n, \lambda_m) \frac{f(\lambda_m)}{(t;t)_{\lambda_m} (ut;t)_{\lambda_m}}, \quad (8.18)$$

将矩阵乘积展开并以 ℓ替换 λ_m后，即得到所需的表达式。□

为了进一步简化这类期望，推论 8.7 提供了一条自然的思路：将函数 f 写成$M_{t的u\xi}$ 特征向量（即$U_{t的u\xi}$列）的函数。下一个结果针对下一节相关函数中出现的函数给出了这种表示；这些函数属于推论 8.7 的 $u = 1 \xi = t^2$ 情形。

引理 8.8。设

$$F_j(i) = \begin{cases} \frac{1}{(t;t)_{i-j} (t^3;t)_{i+j}} & i \geq j \\ 0 & i < j \end{cases}, \quad (8.19)$$

由 U_{t,t^2} 的 j^{th} 列给出的 $\mathbb{Z}_{\geq 0}$ 上的函数。令 g_1、g_2、g_3 为 $\mathbb{Z}_{\geq 0}$ 上由

$$g_1(\ell) = \frac{1}{(t;t)_\ell (t;t)_\ell} \left(\frac{1-t}{1-t^{\ell+1}} \right)^2 \quad (8.20)$$

$$g_2(\ell) = \frac{1}{(t;t)_\ell (t;t)_\ell} \frac{1-t}{1-t^{\ell+1}} \quad (8.21)$$

$$g_3(\ell) = \frac{1}{(t;t)_\ell (t;t)_\ell} \frac{1-t^2}{1-t^{2\ell+2}}. \quad (8.22)$$

那么这些函数具有特征基展开

$$g_1 = \sum_{j\geq 0} \frac{(-1)^j t^{\binom{j+1}{2}}(1+t^{j+1})}{1+t} F_j \tag{8.23}$$

$$g_2 = \sum_{j\geq 0} \frac{t^{j^2+j}(1-t^{2j+2})}{1-t^2} F_j \tag{8.24}$$

$$g_3 = \sum_{j\geq 0} \frac{t^{\binom{j+1}{2}}(1-t^{j+1})}{1-t} F_j. \tag{8.25}$$

证明。(8.23)、(8.24) 和 (8.25) 中的每一个都是类似的计算，我们给出第一个，并概述其余两个。在每种情况下，我们只需在函数每隔 $\ell \in \mathbb{Z}_{\geq 0}$ 取值时验证该恒等式。将 $F_j(i)$ 稍作改写为下式会很有用

$$F_j(i) = \begin{cases} \frac{(t;t)_2}{(t;t)_{i-j}(t;t)_{i+j+2}} & i \geq j \\ 0 & i < j \end{cases}. \tag{8.26}$$

现在证明在固定 ℓ 处取值的 (8.23)。令

$$E_j^{(1)} = \frac{(-1)^j t^{\binom{j+1}{2}}(1-t)^2}{(1-t^{\ell+1})(t;t)_{\ell-j}(t;t)_{\ell+j+1}}, \tag{8.27}$$

通过初等验证可得

$$E_j^{(1)} - E_{j+1}^{(1)} = (1-t)^2 \frac{(-1)^j t^{\binom{j+1}{2}}(1+t^{j+1})}{(t;t)_{\ell-j}(t;t)_{\ell+j+2}} = \frac{(-1)^j t^{\binom{j+1}{2}}(1+t^{j+1})}{1+t} F_j(\ell) \tag{8.28}$$

对于 $j = 0$、.....、$\ell - 1$。因此，(8.23) 在 ℓ 处取值时的右端恰为

$$\sum_{j=0}^{\ell} \frac{(-1)^j t^{\binom{j+1}{2}}(1+t^{j+1})}{1+t} F_j(\ell) = E_0^{(1)} - E_\ell^{(1)} + \frac{(-1)^\ell t^{\binom{\ell+1}{2}}(1+t^{\ell+1})}{1+t} F_\ell(\ell). \tag{8.29}$$

利用恒等式 $(1-t^{\ell+1})(t;\ t)_{2\ell+1} = (t;t)_{2\ell+2}/(1+t^{\ell+1})$，我们得到 (8.29) 的最后两项相等，因此 (8.29) 就是 $E_0^{(1)} = g_1(\ell)$。这就证明了 (8.23)。

要证明 (8.24)，可使用相同的望远镜求和论证，但采用不同的公式

$$E_j^{(2)} = \frac{(1-t)t^{j^2+j}}{(t;t)_{\ell-j}(t;t)_{\ell+j+1}} \tag{8.30}$$

来代替 $E_j^{(1)}$。证明 (8.25) 时，则使用

$$E_j^{(3)} = \frac{(1-t^2)t^{\binom{j+1}{2}}}{(1+t^{\ell+1})(t;t)_{\ell-j}(t;t)_{\ell+j+1}}. \tag{8.31}$$

在每种情况下，$E_0^{(k)} = g_k(\ell)$ 和 $E_j^{(k)} - E_{j+1}^{(k)}$ 给出了 (8.24) 或 (8.25) 右侧求和中的各项在 ℓ处的取值；这些项经望远镜求和后，只留下 $E_0^{(k)}$ 项。□

注 8.9. 我们指出，引理 8.8 中 g_1, g_2, g_3 的特征基展开形式格外简单，而任意有理函数 g 的特征基展开通常远没有这么显式。这一代数奇迹使推论 8.10 中的级数公式如此简洁，进而也使定理 1.2 和定理 1.8 中的公式如此简洁，而我们尚不了解这一奇迹的来源。推论 8.10 中的三个公式，若将左端写成关于 $\lambda_1 \geq \ldots \geq \lambda_m \geq 0$ 的显式求和，则可视为 Andrews-Gordon 恒等式 [和 74] 的变形版本。

推论 8.10. 固定 $m \geq 1$。对于任意 $n \geq 1$，以及 $\lambda_1, \ldots, \lambda_m$，设它们是马尔可夫链 $\mathcal{K} = \mathcal{K}_{t,1}$ 从 $\lambda_0 = n$ 出发后依次经过的状态。那么

$$\lim_{n\to\infty} \mathbb{E}\left[t^{2\lambda_1+\cdots+2\lambda_m}\left(\frac{1-t}{1-t^{\lambda_m+1}}\right)^2\right] = (1-t)^2\sum_{k\geq 0}(-1)^k t^{\frac{(2m+1)k^2+(4m+1)k}{2}}(1+t^{k+1}) \tag{8.32}$$

$$\lim_{n\to\infty} \mathbb{E}\left[t^{2\lambda_1+\cdots+2\lambda_m}\frac{1-t}{1-t^{\lambda_m+1}}\right] = (1-t)\sum_{k\geq 0} t^{(m+1)k^2+(2m+1)k}(1-t^{2k+2}) \tag{8.33}$$

$$\lim_{n\to\infty} \mathbb{E}\left[t^{2\lambda_1+\cdots+2\lambda_m}\frac{1-t^2}{1-t^{2\lambda_m+2}}\right] = (1-t^2)\sum_{k\geq 0} t^{\frac{(2m+1)k^2+(4m+1)k}{2}}(1-t^{k+1}). \tag{8.34}$$

证明。设 $\nu_1, \ldots, \nu_m$ 是从 ∞ 出发的马尔可夫链 $\mathcal{K} = \mathcal{K}_{t,1}$ 的连续状态。当 n 趋于无穷大时，联合变量 $(\lambda_1, \ldots, \lambda_m)$ 弱收敛到 $(\nu_1, \ldots, \nu_m)$，因为马尔可夫链第一步的转移概率收敛。该弱收敛意味着

$$\lim_{n\to\infty} \mathbb{E}[t^{2\lambda_1+\cdots+2\lambda_m} f(\lambda_m)] = \mathbb{E}[t^{2\nu_1+\cdots+2\nu_m} f(\nu_m)]$$

对于推论 8.10 中出现的 f 的三种取值，结论均成立，因为在这些情况下，$t^{2\nu_1+\cdots+2\nu_m} f(\nu_m)$ 是有界函数。现在，我们对 $u = 1$ 和 $\xi = t^2$ 使用推论 8.7。注意

$$\sum_{\ell\geq 0} U^{-1}_{t,t^2}(d,\ell)F_j(\ell) = \mathbb{1}_{j=d} \tag{8.35}$$

因为函数 F_j（视为向量 $(F_j(\ell))_{\ell\in\mathbb{Z}_{\geq 0}}$）是 U_{t,t^2} 的列。因此，若推论 8.7 中的函数 f 按引理 8.8 的基 F_j 展开为

$$\frac{f(\ell)}{(t;t)_\ell (t;t)_\ell} = \sum_{j\geq 0} c_j F_j(\ell), \tag{8.36}$$

那么推论 8.7 表明

$$\begin{aligned}\mathbb{E}[t^{2\nu_1+\cdots+2\nu_m} f(\nu_m)] &= (t;t)^2_\infty \sum_{d,\ell\geq 0} U_{t,t^2}(\infty,d)E_{t,t^2}(d,d)^m U^{-1}_{t,t^2}(d,\ell)\sum_{j\geq 0} c_j F_j(\ell) \\ &= (t;t)^2_\infty \sum_{d\geq 0} U_{t,t^2}(\infty,d)E_{t,t^2}(d,d)^m c_d\end{aligned} \tag{8.37}$$

最后一行由 (8.35) 得出。我们需要证明的每种情况都对应一个不同的f，其展开系数 c_j 已在引理 8.8 中计算，而特征值$E_{t,\ t^2}(d,\ d)^m$ 是命题 8.6 中给出的 t 的显式幂。经过初等计算即可完成证明。□

9. Limiting correlation functions in low-degree extensions

本节旨在计算低次数扩张的一些特定相关函数。具体而言，我们证明定理 1.2 和定理 1.8 中的相关函数公式。利用这些结果，我们给出定理 1.10 中二次扩张内根的期望数量的精确公式，并计算 $\mathbb{Z}_p$ 中特征值数量方差的公式（推论 9.6）；这一结果未在引言中陈述。

9.1. 中的特征值 $\mathbb{Z}_p$。

在本小节中，我们讨论 $\mathbb{Z}_p$中的特征值。我们从 $\mathbb{Q}_p$中特征值的密度开始。

定理 9.1。对于所有正整数 n 以及所有 $x_1 \in \mathbb{Z}_p$，我们有 $\rho^{(n)}_{\mathbb{Q}_p}(x_1) = 1$。

证明。 在此情形下，我们有 $r = e = 1$、$\mathrm{Disc}^{K/\mathbb{Q}_p} = \#(\mathcal{O}_K : \mathbb{Z}_p[x_1]) = \#(\Lambda_E \backslash \mathrm{Mod}^{\mathbb{Z}_p[x_1]}) = 1$, 以及 $V(x_1) = \frac{1}{1-p^{-1}}$。根据引理 1.13，我们有

$$\rho^{(n)}_{\mathbb{Q}_p}(x_1) = \frac{1-p^{-n}}{1-p^{-1}} \mathbb{E}|| \det(\tilde{A})|| = 1.$$

其中， $A \in$矩阵空间$_{n-1}(\mathbb{Z}_p)$ 服从 Haar 分布，第二个等式由推论 8.5 得出。证明完毕。□

定理 9.1 和引理 1.13 导出以下推论。

推论 9.2。 对于所有 $n \geq 1$，有 $\mathbb{E}[Z_{\mathbb{Z}_p,n}] = 1$ 。

下面转而讨论 $\mathbb{Z}_p$ 上的二点相关函数。

定理 9.3。 设 x_1、$x_2 \in \mathbb{Z}_p$ 和 $m := \mathrm{val}(x_1 - x_2)$。则有

$$\rho^{(\infty)}_{\mathbb{Q}_p \times \mathbb{Q}_p}(x_1, x_2) = p^{-m} \sum_{k \geq 0} (-1)^k p^{-\frac{(2m+1)k^2+(4m+1)k}{2}} (1 + p^{-k-1}).$$

定理 9.3 可以直接由以下引理推出。

命题 9.4. 设 x_1、$x_2 \in \mathbb{Z}_p$ 和 $m := \mathrm{val}(x_1 - x_2)$。当 $A \in$ 矩阵空间$_n(\mathbb{Z}_p)$ 服从 ***Haar*** 分布时，我们有

$$\lim_{n\to\infty} \mathbb{E}||(x_1 I_n - A)(x_2 I_n - A)|| = (1-p^{-1})^2 \sum_{k \geq 0} (-1)^k p^{-\frac{(2m+1)k^2+(4m+1)k}{2}} (1 + p^{-k-1}).$$

假设命题 *9.4*，证明定理 *9.3*。根据定理 6.1 中的公式，我们有

$$\begin{aligned} \rho^{(\infty)}_{\mathbb{Q}_p \times \mathbb{Q}_p}(x_1, x_2) &= ||x_1 - x_2|| \cdot \frac{1}{(1-p^{-1})^2} \cdot \lim_{n\to\infty} \mathbb{E}||(x_1 I_n - A)(x_2 I_n - A)|| \\ &= p^{-m} \cdot \frac{1}{(1-p^{-1})^2} \cdot (1-p^{-1})^2 \sum_{k \geq 0} (-1)^k p^{-\frac{(2m+1)k^2+(4m+1)k}{2}} (1 + p^{-k-1}) \\ &= p^{-m} \sum_{k \geq 0} (-1)^k p^{-\frac{(2m+1)k^2+(4m+1)k}{2}} (1 + p^{-k-1}). \end{aligned} \tag{9.1}$$

由此得证。 □

证明命题 9.4 需要以下引理。

引理 9.5. 设 $n \geq 1$ 和 $A, B \in$ 矩阵空间$_n(\mathbb{Z}_p)$ 相互独立且服从 ***Haar*** 分布。设 x_1, x_2 是 $\mathbb{Z}_p$ 中的固定元素，且 $m := \mathrm{val}(x_1 - x_2)$。那么， $\mathbb{Z}_p$-模的联合分布

$$(\mathrm{Cok}(A - x_1 B), \mathrm{Cok}(A - x_2 B))$$

由以下方式给出。首先，随机序列

$$\begin{aligned} \mathrm{Cok}(A - x_1 B)'_1 = \lambda_1, \mathrm{Cok}(A - x_1 B)'_2 = \lambda_2, \ldots, \mathrm{Cok}(A - x_1 B)'_m = \lambda_m, \\ \mathrm{Cok}(A - x_1 B)'_{m+1} = \lambda^{(1)}_{m+1}, \mathrm{Cok}(A - x_1 B)'_{m+2} = \lambda^{(1)}_{m+2}, \ldots \end{aligned} \tag{9.2}$$

服从从状态 n 开始的定义 *8.1* 中的马尔可夫链$\mathcal{K}_{p^{-1},\,1}$ 。按上述方式确定 余核$(A - x_1 B)$ 后，对于所有 $1 \leq i \leq m$，我们有 余核$(A - x_2 B)_i =$ 余核$(A - x_1 B)_i$ ，并且随机序列

$$\mathrm{Cok}(A - x_2 B)'_{m+1} = \lambda^{(2)}_{m+1}, \mathrm{Cok}(A - x_2 B)'_{m+2} = \lambda^{(2)}_{m+2}, \ldots$$

服从以状态 λ_m 为起点的马尔可夫链 $\mathcal{K}_{p^{-1},\,1}$ 。

证明。 由于 $A \in \mathrm{Mat}_n(\mathbb{Z}_p)$ 服从 Haar 分布，且与 B 相互独立，不妨假设 $x_1 = 0$。那么，$\mathrm{Cok}(A - x_1 B) = \mathrm{Cok}(A)$ 的分布已由$\mathcal{K}_{p^{-1},\,1}$ 命题 8.3 给出。现在，给定一个固定的整数序列

$$n \geq \lambda_1 \geq \ldots \geq \lambda_m \geq \lambda_{m+1}^{(1)} \geq \ldots \geq 0, \tag{9.3}$$

我们仍需理解随机余核 $\mathrm{Cok}(A - x_2 B)$ 的分布，条件是

$$\mathrm{Cok}(A)_1' = \lambda_1, \ldots, \mathrm{Cok}(A)_m' = \lambda_m, \mathrm{Cok}(A)_{m+1}' = \lambda_{m+1}^{(1)}, \ldots \tag{9.4}$$

根据史密斯标准形，存在一列整数 $\nu_1 \geq \ldots \geq \nu_n \geq 0$，使得每个满足 (9.4) 的 $A \in \mathrm{Mat}_n(\mathbb{Z}_p)$ 都可以表示为以下形式

$$A = U_1 \,\mathrm{diag}(p^{\nu_1}, \ldots, p^{\nu_n}) U_2$$

对某个 $U_1, U_2 \in \mathrm{GL}_n(\mathbb{Z}_p)$；注意，这些完全由分拆 (9.3) 决定，因为$\nu_j = \#\{i \geq 1 : \lambda_i \geq j\}$。由于 $\mathrm{Mat}_n(\mathbb{Z}_p)$ 上的哈尔分布在 $\mathrm{GL}_n(\mathbb{Z}_p)$ 的左乘和右乘下保持不变，我们有，在条件为 A 满足 (9.4) 时，

$$\mathrm{Cok}(A - x_2 B) = \mathrm{Cok}\left(\mathrm{diag}(p^{\nu_1}, \ldots, p^{\nu_n}) - x_2 B\right) \qquad \text{in distribution.} \tag{9.5}$$

We 将分析右侧余核的分布。由于 $x_2 \in p^m \mathbb{Z}_p$，

$$\mathrm{Cok}\left(\mathrm{diag}(p^{\nu_1}, \ldots, p^{\nu_n}) - x_2 B\right)_i' = \lambda_i \qquad \text{for } 1 \leq i \leq m, \tag{9.6}$$

并且我们仍需找出 $\mathrm{Cok}\left(\mathrm{diag}(p^{\nu_1}, \ldots, p^{\nu_n}) - x_2 B\right)_i'$ 在 $i = m+1, m+2, \ldots$ 时的分布。记 $A_1 := \mathrm{diag}(p^{\nu_1}, \ldots, p^{\nu_{\lambda_m}})$，以及 $A_4 := \mathrm{diag}(p^{\nu_{\lambda_m+1}}, \ldots, p^{\nu_n})$。$A_1$ 的大小为 λ_m，其元素的赋值为 $\geq m$。A_4 的大小为 $n - \lambda_m$，其对角线元素的赋值为$< m$。记

$$B = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix},$$

其中

$$B_1 \in \mathrm{Mat}_{\lambda_m}(\mathbb{Z}_p)\ B_2 \in \mathrm{Mat}_{\lambda_m \times (n-\lambda_m)}(\mathbb{Z}_p)\ B_3 \in \mathrm{Mat}_{(n-\lambda_m) \times \lambda_m}(\mathbb{Z}_p)\ B_4 \in \mathrm{Mat}_{n-\lambda_m}(\mathbb{Z}_p)$$

均服从 Haar 分布。我们有

$$\begin{aligned} \mathrm{Cok}\left(\mathrm{diag}(p^{\nu_1}, \ldots, p^{\nu_n}) - x_2 B\right) &= \mathrm{Cok} \begin{pmatrix} A_1 - x_2 B_1 & -x_2 B_2 \\ -x_2 B_3 & A_4 - x_2 B_4 \end{pmatrix} \\ &\cong \mathrm{Cok} \begin{pmatrix} A_1 - B_0 - x_2 B_1 & -x_2 B_2 \\ 0 & A_4 - x_2 B_4 \end{pmatrix} \\ &\cong \mathrm{Cok} \begin{pmatrix} A_1 - B_0 - x_2 B_1 & 0 \\ 0 & A_4 - x_2 B_4 \end{pmatrix}, \end{aligned} \tag{9.7}$$

其中 $B_0 = x_2^2 B_2 (A_4 - x_2 B_4)^{-1} B_3 \in p^m \mathrm{Mat}_{\lambda_m}(\mathbb{Z}_p)$ 与 B_1 相互独立。因此，矩阵$A_0 := A_1 - B_0 - x_2 B_1$ 在 $\mathrm{Mat}_{\lambda_m}(p^m \mathbb{Z}_p)$ 中服从 Haar 分布。根据命题 8.3，序列

$$\mathrm{Cok}(A_0)_{m+1}', \mathrm{Cok}(A_0)_{m+2}', \ldots$$

服从以状态 λ_m 为起点的马尔可夫链$\mathcal{K}_{p^{-1},\,1}$。此外，由于 A_4 的对角线元素的赋值严格小于 m，我们推得 $\mathrm{Cok}(A_4 - x_2 B_4) \cong \mathrm{Cok}(A_4)$。因此，对所有 $1 \leq i \leq m$，都有 $\mathrm{Cok}\begin{pmatrix} A_0 & 0 \\ 0 & A_4 - x_2 B_4 \end{pmatrix}_i' = \lambda_i$；并且对所有 $i \geq 1$，都有 $\mathrm{Cok}\begin{pmatrix} A_0 & 0 \\ 0 & A_4 - x_2 B_4 \end{pmatrix}_{m+i}' = \mathrm{Cok}(A_0)_{m+i}'$。证明完毕。 □

命题 *9.4* 的证明。应用定理 5.1 和引理 5.3，我们有

$$\begin{aligned} \lim_{n\to\infty} \mathbb{E} |\det((A - x_1 I_n)(A - x_2 I_n))| &= \lim_{n\to\infty} \mathbb{E} |\det((A - x_1 B)(A - x_2 B))| \\ &= \lim_{n\to\infty} \mathbb{E}\left[\frac{1}{\#\,\mathrm{Cok}(A - x_1 B)} \cdot \frac{1}{\#\,\mathrm{Cok}(A - x_2 B)}\right], \end{aligned} \tag{9.8}$$

其中，$B \in \mathrm{Mat}_{n \times n}(\mathbb{Z}_p)$ 与 A 相互独立，且在 $\mathrm{Mat}_n(\mathbb{Z}_p)$ 上服从 Haar 分布。因此，我们只需计算最后一行中的极限。

现在，令 $n \geq 1$ 为一个固定整数。对所有 $1 \leq i \leq m$，记 $\lambda_i = \mathsf{Cok}(A - x_1 B)'_i$；对所有 $i \geq 1$ 和 $j \in \{1, 2\}$，记 $\lambda^{(j)}_{m+i} = \mathsf{Cok}(A - x_j B)'_{m+i}$。根据引理 9.5 给出的分布，我们有

$$\begin{aligned}\mathbb{E}\left[\frac{1}{\#\operatorname{Cok}(A - x_1 B)} \cdot \frac{1}{\#\operatorname{Cok}(A - x_2 B)}\right] &= \mathbb{E}\left[p^{-2(\lambda_1+\cdots+\lambda_m)-(\lambda^{(1)}_{m+1}+\lambda^{(1)}_{m+2}+\cdots)-(\lambda^{(2)}_{m+1}+\lambda^{(2)}_{m+2}+\cdots)}\right] \\ &= \mathbb{E}\Big[p^{-2(\lambda_1+\cdots+\lambda_m)} \\ &\quad \cdot \mathbb{E}[p^{-(\lambda^{(1)}_{m+1}+\lambda^{(1)}_{m+2}+\cdots)-(\lambda^{(2)}_{m+1}+\lambda^{(2)}_{m+2}+\cdots)} \mid \lambda_m]\Big] \\ &= \mathbb{E}\left[p^{-2(\lambda_1+\cdots+\lambda_m)} \cdot (\mathbb{E}[p^{-(\lambda^{(1)}_{m+1}+\lambda^{(1)}_{m+2}+\cdots)} \mid \lambda_m])^2\right] \\ &= \mathbb{E}\left[p^{-2(\lambda_1+\cdots+\lambda_m)} \cdot \frac{(1-p^{-1})^2}{(1-p^{-\lambda_m-1})^2}\right].\end{aligned} \tag{9.9}$$

这里，最后一行来自命题 8.4，而第四行成立是因为在给定 λ_m 的条件下，两个序列 $(\lambda^{(1)}_{m+1}, \lambda^{(1)}_{m+2}, \ldots\ldots)$ 和 $(\lambda^{(2)}_{m+1}, \lambda^{(2)}_{m+2}, \ldots\ldots)$ 相互独立且具有相同的分布律。应用推论 8.10，得到

$$\begin{aligned}\lim_{n\to\infty} \mathbb{E}|| \det((A - x_1 I_n)(A - x_2 I_n))|| &= \lim_{n\to\infty} \mathbb{E}\left[\frac{1}{\#\operatorname{Cok}(A - x_1 B)} \cdot \frac{1}{\#\operatorname{Cok}(A - x_2 B)}\right] \\ &= \lim_{n\to\infty} \mathbb{E}\left[p^{-2(\lambda_1+\cdots+\lambda_m)} \cdot \frac{(1-p^{-1})^2}{(1-p^{-\lambda_m-1})^2}\right] \\ &= (1-p^{-1})^2 \sum_{k\geq 0} (-1)^k p^{-\frac{(2m+1)k^2+(4m+1)k}{2}} (1 + p^{-k-1}).\end{aligned} \tag{9.10}$$

证明至此完成。 □

推论 9.6。 $\mathbb{Z}_p$ 中特征值的数量具有极限方差

$$\lim_{n\to\infty} \mathbb{E}[(Z_{\mathbb{Z}_p,n} - \mathbb{E}[Z_{\mathbb{Z}_p,n}])^2] = \lim_{n\to\infty} \mathbb{E}[Z_{\mathbb{Z}_p\times\mathbb{Z}_p,n}] = \sum_{k\geq 0} \frac{(-1)^k (1-p^{-1})(1+p^{-k-1}) p^{-\frac{k^2+k}{2}}}{1 - p^{-k^2-2k-2}}.$$

证明。 首先，回顾推论 9.2 可知，对于所有 $n \geq 1$，我们有 $\mathbb{E}[Z_{\mathbb{Z}_p,n}] = 1$。因此，我们有

$$\begin{aligned}\lim_{n\to\infty} \mathbb{E}[(Z_{\mathbb{Z}_p,n} - \mathbb{E}[Z_{\mathbb{Z}_p,n}])^2] &= \lim_{n\to\infty} \mathbb{E}[Z^2_{\mathbb{Z}_p,n}] - 1 \\ &= \lim_{n\to\infty} \mathbb{E}[Z_{\mathbb{Z}_p,n}(Z_{\mathbb{Z}_p,n} - 1)] \\ &= \lim_{n\to\infty} \mathbb{E}[Z_{\mathbb{Z}_p\times\mathbb{Z}_p,n}].\end{aligned} \tag{9.11}$$

这里，最后一行成立是因为我们总有 $Z_{\mathbb{Z}_p\times\mathbb{Z}_p,\, n} = Z_{\mathbb{Z}_p,\, n}(Z_{\mathbb{Z}_p,\, n} - 1)$，因为它们都对 $\mathbb{Z}_p$ 中的特征值有序对进行计数。接下来，对于所有 $m \geq 0$，子集

$$\mathcal{U}_m := \{(x_1, x_2) : x_1, x_2 \in \mathbb{Z}_p, \operatorname{val}(x_1 - x_2) = m\} \subset \mathbb{Z}_p \times \mathbb{Z}_p$$

具有 Haar 概率测度 $\mu_{\mathbb{Q}_p\times\mathbb{Q}_p}(\mathcal{U}_m) = (1-p^{-1})p^{-m}$。此外，根据定理 9.3，极限相关函数 $\rho^{(\infty)}_{\mathbb{Q}_p\times\mathbb{Q}_p}$ 在 $\mathcal{U}_m$ 中取值 $\rho^{(\infty)}_{\mathbb{Q}_p\times\mathbb{Q}_p}(p^m, 0)$。因此，根据定理 6.2，我们有

$$\begin{aligned}\lim_{n\to\infty} \mathbb{E}[Z_{\mathbb{Z}_p\times\mathbb{Z}_p,n}] &= \int_{\mathbb{Z}_p\times\mathbb{Z}_p} \rho^{(\infty)}_{\mathbb{Q}_p\times\mathbb{Q}_p}(x_1, x_2) dx_1 dx_2 \\ &= \sum_{m\geq 0} \rho^{(\infty)}_{\mathbb{Q}_p\times\mathbb{Q}_p}(p^m, 0) \cdot \mu_{\mathbb{Q}_p\times\mathbb{Q}_p}(\mathcal{U}_m) \\ &= \sum_{m\geq 0} (1-p^{-1}) p^{-m} \rho^{(\infty)}_{\mathbb{Q}_p\times\mathbb{Q}_p}(p^m, 0).\end{aligned} \tag{9.12}$$

最后，应用定理 9.3，我们得到

$$\begin{aligned}\sum_{m\geq 0}(1-p^{-1})p^{-m}\rho^{(\infty)}_{\mathbb{Q}_p\times\mathbb{Q}_p}(p^m,0) &= \sum_{m,k\geq 0}(-1)^k(1-p^{-1})(1+p^{-k-1})p^{-\frac{(2m+1)k^2+(4m+1)k}{2}-2m}\\ &= \sum_{k\geq 0}(-1)^k(1-p^{-1})(1+p^{-k-1})p^{-\frac{k^2+k}{2}}\sum_{m\geq 0}p^{-(k^2+2k+2)m}\\ &= \sum_{k\geq 0}\frac{(-1)^k(1-p^{-1})(1+p^{-k-1})p^{-\frac{k^2+k}{2}}}{1-p^{-k^2-2k-2}}.\end{aligned} \tag{9.13}$$

证明至此完成。 □

定理 *1.2* 的证明。 首先，给定 x， $y\in\mathbb{Z}_p$，令 $m:=\mathrm{val}(x-y)$，使得 $||x-y||=p^{-m}$。由定理 9.3，得到

$$\begin{aligned}\rho^{(\infty)}_{\mathbb{Q}_p\times\mathbb{Q}_p}(x,y) &= p^{-m}\sum_{k\geq 0}(-1)^k p^{-\frac{(2m+1)k^2+(4m+1)k}{2}}(1+p^{-k-1})\\ &= -\sum_{k\geq 1}(-1)^k p^{-\frac{(2m+1)k^2}{2}}(p^{k/2}+p^{-k/2})\\ &= 1-\sum_{k\in\mathbb{Z}}\left(\frac{1}{p^{2m+1}}\right)^{\frac{k^2}{2}}\cdot(-\sqrt{p})^k\\ &= 1-\theta_3(-\sqrt{p};||x-y||^2/p).\end{aligned} \tag{9.14}$$

因此，我们验证了 (1.4)。接下来，当 U， $V\subset\mathbb{Z}_p$ 是两个互不相交的可测集时，有$Z_{U,\ n}Z_{V,\ n}=Z_{U\times V,\ n}$，故 (1.3) 是定理 6.2 的一个特例。最后，我们回顾定理 9.1，得知对于所有 $x\in\mathbb{Z}_p$ 和 $n\geq 1$， $\rho^{(n)}_{\mathbb{Q}_p}(x)=1$。因此，我们有

$$\begin{aligned}\lim_{n\to\infty}\mathrm{Cov}(Z_{U,n},Z_{V,n}) &= \lim_{n\to\infty}(\mathbb{E}[Z_{U,n}\cdot Z_{V,n}]-\mathbb{E}[Z_{U,n}]\mathbb{E}[Z_{V,n}])\\ &= \lim_{n\to\infty}\int_{U\times V}(\rho^{(\infty)}_{\mathbb{Q}_p,\mathbb{Q}_p}(x,y)-1)dxdy\\ &= -\lim_{n\to\infty}\int_{U\times V}\theta_3(-\sqrt{p};||x-y||^2/p)dxdy.\end{aligned} \tag{9.15}$$

根据雅可比三重乘积恒等式，最后一行中的被积函数（其中 $p^{-m}=||x-y||, m\geq 0$）为

$$\prod_{i\geq 1}\left(1-\left(\frac{1}{p^{2m+1}}\right)^i\right)\left(1-\left(\frac{1}{p^{2m+1}}\right)^{i-1/2}\cdot\sqrt{p}\right)\left(1-\left(\frac{1}{p^{2m+1}}\right)^{i-1/2}\cdot\frac{1}{\sqrt{p}}\right)\geq 0, \tag{9.16}$$

so

$$\lim_{n\to\infty}\mathrm{Cov}(Z_{U,n},Z_{V,n})\leq 0. \tag{9.17}$$

这验证了 (1.5)，并完成了证明。 □

9.2. **二次扩张**。 本小节的主要目标是证明定理 1.8。我们始终在以下设定下进行讨论。设 $K/\mathbb{Q}_p$ 是一个二次扩张， $\mathcal{O}_K=\mathbb{Z}_p[x_1]$是整数子环。若 $K/\mathbb{Q}_p$ 是分歧的，则 $\mathrm{val}(x_1)=\frac{1}{2}$；若 $K/\mathbb{Q}_p$ 是非分歧的，则 $\mathrm{val}(x_1)=0$。设 $a_0,a_1\in\mathbb{Z}_p$，且 $\mathrm{val}(a_1)=m\geq 0$，并以 $Z(x)$ 表示 $a_0+a_1x_1$的最小多项式，该多项式是二次首一多项式。

在给出定理 1.8 的证明之前，我们先进行一些必要的相关计算。

命题 9.7。 设 $A\in$矩阵空间$_{n\times n}(\mathbb{Z}_p)$ 服从 *Haar* 分布。在本小节的设定下，

(1) 当 $K/\mathbb{Q}_p$ 是分歧的时，我们有

$$\lim_{n\to\infty}\mathbb{E}||\det(Z(A))|| = (1-p^{-1})\sum_{k\geq 0}p^{-(m+1)k^2-(2m+1)k}(1-p^{-2k-2}).$$

(2) 当 $K/\mathbb{Q}_p$ 为非分歧时，我们有

$$\lim_{n\to\infty}\mathbb{E}||\det(Z(A))|| = (1-p^{-2})\sum_{k\geq 0}p^{-\frac{(2m+1)k^2+(4m+1)k}{2}}(1-p^{-k-1}).$$

引理 9.8。令 $n\geq 1$ 以及 A、$B\in$ 矩阵空间$_n(\mathbb{Z}_p)$ 相互独立且服从 *Haar* 分布。则，$\mathcal{O}_K$-模 余核$(A-(a_0+a_1x_1)B)$ 的分布如下给出。

(1) 当 $K/\mathbb{Q}_p$ 为分歧时，余核$(A-(a_0+a_1x_1)B)'_{2j-1}=$ 余核$(A-(a_0+a_1x_1)B)'_{2j}$ 对于 $1\leq j\leq m$，以及随机序列

$$\mathrm{Cok}(A-(a_0+a_1x_1)B)'_1=\mathrm{Cok}(A-(a_0+a_1x_1)B)'_2=\lambda_1,\dots,$$
$$\mathrm{Cok}(A-(a_0+a_1x_1)B)'_{2m-1}=\mathrm{Cok}(A-(a_0+a_1x_1)B)'_{2m}=\lambda_m \quad (9.18)$$

其服从定义 *8.1* 中从状态 n 开始的马尔可夫链 $\mathcal{K}_{p^{-1},\,1}$。随后项的序列

$$\mathrm{Cok}(A-(a_0+a_1x_1)B)'_{2m+1}=\lambda_{m+1},\mathrm{Cok}(A-(a_0+a_1x_1)B)'_{2m+2}=\lambda_{m+2},\dots$$

其服从从状态 λ_m 开始的马尔可夫链 $\mathcal{K}_{p^{-1},\,1}$。

(2) 当 $K/\mathbb{Q}_p$ 非分歧时，随机序列

$$\mathrm{Cok}(A-(a_0+a_1x_1)B)'_1=\lambda_1,\mathrm{Cok}(A-(a_0+a_1x_1)B)'_2=\lambda_2,\dots,\mathrm{Cok}(A-(a_0+a_1x_1)B)'_m=\lambda_m$$

is distributed according to the Markov chain $\mathcal{K}_{p^{-1},1}$ of Definition 8.1 started at state n. Then, the sequence of subsequent terms

$$\mathrm{Cok}(A-(a_0+a_1x_1)B)'_{m+1}=\lambda_{m+1},\mathrm{Cok}(A-(a_0+a_1x_1)B)'_{m+2}=\lambda_{m+2},\dots$$

服从以状态 λ_m为起点的马尔可夫链$\mathcal{K}_{p^{-2},\,1}$。

证明。由于 $A\in$Mat$_n(\mathbb{Z}_p)$服从 Haar 分布，不失一般性，我们可以假设 $a_0=0$。我们先处理非分歧情形。由于 val$(a_1)=m$，对于所有 $1\leq i\leq m$，都有 Cok$(A-a_1x_1B)_i=$Cok$(A)_i$。因此，随机序列的分布

$$\mathrm{Cok}(A-a_1x_1B)'_1=\mathrm{Cok}(A)'_1,\mathrm{Cok}(A-a_1x_1B)'_2=\mathrm{Cok}(A)'_2,\dots,\mathrm{Cok}(A-a_1x_1B)'_m=\mathrm{Cok}(A)'_m$$

已由命题 8.3 给出。现在，给定一个固定的整数序列

$$n\geq\lambda_1\geq\ldots\geq\lambda_m,$$

我们希望了解后续项 Cok$(A-a_1x_1B)'_{m+i}$ 对所有 $i\geq 1$的分布律，条件是

$$\mathrm{Cok}(A)'_1=\lambda_1,\dots,\mathrm{Cok}(A)'_m=\lambda_m. \quad (9.19)$$

对于所有 $\lambda_m+1\leq j\leq n$，令 $\nu_j:=\#\{1\leq i\leq m:\ \lambda_i\geq j\}$。令 $A_1\in$ Mat$_{\lambda_m}(p^m\mathbb{Z}_p)$ 服从哈尔分布，且令 $A_4:=$diag$(p^{\nu_{\lambda_m+1}},\ \ldots\ldots,\ p^{\nu_n})$ 为一个固定矩阵。则对于所有 $1\leq i\leq m$，有 Cok$(A_4)'_i=\lambda_i$。此外，根据命题 8.3，序列

$$\mathrm{Cok}(A_1)'_{m+1},\mathrm{Cok}(A_1)'_{m+2},\dots$$

服从从状态 λ_m 开始的马尔可夫链 $\mathcal{K}_{p^{-1},\,1}$。这意味着，在给定 A 满足 (9.19) 的条件下，

$$\mathrm{Cok}(A)=\mathrm{Cok}\begin{pmatrix}A_1&0\\0&A_4\end{pmatrix},\qquad\text{in distribution.}$$

由于 $B\in$Mat$_n(\mathbb{Z}_p)$ 的哈尔分布在 GL$_n(\mathbb{Z}_p)$ 的左乘和右乘下保持不变，我们推得，在给定 A 满足 (9.19) 的条件下，

$$\mathrm{Cok}(A-a_1x_1B)=\mathrm{Cok}\left(\begin{pmatrix}A_1&0\\0&A_4\end{pmatrix}-a_1x_1B\right),\qquad\text{按分布收敛。}$$

记

$$B = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix},$$

其中

$$B_1 \in \mathrm{Mat}_{\lambda_m}(\mathbb{Z}_p), B_2 \in \mathrm{Mat}_{\lambda_m \times (n-\lambda_m)}(\mathbb{Z}_p), B_3 \in \mathrm{Mat}_{(n-\lambda_m)\times \lambda_m}(\mathbb{Z}_p), B_4 \in \mathrm{Mat}_{n-\lambda_m}(\mathbb{Z}_p)$$

均服从相互独立的 Haar 分布。我们有

$$\begin{aligned} \mathrm{Cok}\left(\begin{pmatrix} A_1 & 0 \\ 0 & A_4 \end{pmatrix} - a_1 x_1 B\right) &= \mathrm{Cok}\begin{pmatrix} A_1 - a_1x_1B_1 & -a_1x_1B_2 \\ -a_1x_1B_3 & A_4 - a_1x_1B_4 \end{pmatrix} \\ &\cong \mathrm{Cok}\begin{pmatrix} A_1 - a_1x_1B_1 - B_0 & -a_1x_1B_2 \\ 0 & A_4 - a_1x_1B_4 \end{pmatrix} \\ &\cong \mathrm{Cok}\begin{pmatrix} A_1 - a_1x_1B_1 - B_0 & 0 \\ 0 & A_4 - a_1x_1B_4 \end{pmatrix}, \end{aligned} \tag{9.20}$$

其中 $B_0 = a_1^2 x_1^2 B_2(A_4 - a_1x_1B_4)^{-1}B_3 \in p^m$ 矩阵空间$\lambda_m(\mathcal{O}_K)$ 与矩阵 $A_1 - a_1x_1B_1$ 相互独立，后者在矩阵空间$\lambda_m(p^m\mathcal{O}_K)$上服从 Haar 分布。因此，矩阵 $A_0 := A_1 - a_1x_1B_1 - B_0$ 在矩阵空间$\lambda_m(p^m\mathcal{O}_K)$上服从 Haar 分布。由命题 8.3，序列

$$\mathrm{Cok}(A_0)'_{m+1}, \mathrm{Cok}(A_0)'_{m+2}, \dots$$

服从从状态 λ_m 出发的马尔可夫链 $\mathcal{K}_{p^{-2},1}$。此外，由于 A_4 对角线上的元素的赋值严格小于 m，我们推出余核$(A_4 - a_1x_1B_4) \cong$ 余核(A_4)。因此，对所有 $1 \le i \le m$，都有余核 $\begin{pmatrix} A_0 & 0 \\ 0 & A_4 - a_1x_1B_4 \end{pmatrix}_i = \lambda_i$；并且对所有 $i \ge 1$，都有余核 $\begin{pmatrix} A_0 & 0 \\ 0 & A_4 - a_1x_1B_4 \end{pmatrix}_{m+i}' =$ 余核$($ $A_0)'_{m+i}$。

对于分歧情形，我们可以将 A 视为 $\mathrm{Mat}_n(\mathbb{Z}_p)$ 中的矩阵，也可以视为 $\mathrm{Mat}_n(\mathcal{O}_K)$ 中的矩阵。此外，对于所有 $i \ge 1$，都有 $\mathrm{Cok}_{\mathcal{O}_K}(A)'_{2i-1} = \mathrm{Cok}_{\mathcal{O}_K}(A)'_{2i} = \mathrm{Cok}_{\mathbb{Z}_p}(A)'_i$，因此随机序列的分布

$$\begin{aligned} \mathrm{Cok}(A - a_1x_1B)'_1 = \mathrm{Cok}(A - a_1x_1B)'_2 = \mathrm{Cok}_{\mathbb{Z}_p}(A)'_1, \dots, \\ \mathrm{Cok}(A - a_1x_1B)'_{2m-1} = \mathrm{Cok}(A - a_1x_1B)'_{2m} = \mathrm{Cok}_{\mathbb{Z}_p}(A)'_m \end{aligned} \tag{9.21}$$

已由命题 8.3 给出。证明的其余部分类似。 □

命题 *9.7* 的证明。 应用定理 5.1 和引理 5.3，可得

$$\begin{aligned} \lim_{n\to\infty} \mathbb{E}||\det(Z(A))|| &= \lim_{n\to\infty} \mathbb{E}||\det(A - (a_0 + a_1x_1)B)||^2 \\ &= \lim_{n\to\infty} \mathbb{E}\left[\frac{1}{\#\,\mathrm{Cok}(A - (a_0 + a_1x_1)B)}\right]. \end{aligned} \tag{9.22}$$

其中 $B \in \mathrm{Mat}_{n\times n}(\mathbb{Z}_p)$ 与 A 相互独立，且服从 Haar 分布。因此，我们只需计算最后一行的极限。

现在，令 $n \ge 1$ 为一个固定整数。当 $K/\mathbb{Q}_p$ 分歧时，对所有 $1 \le i \le m$，记 $\lambda_i := \mathrm{Cok}(A - (a_0 + a_1x_1)B)'_{2i}$，并且对所有 $i \ge 1$，记 $\lambda_{m+i} := \mathrm{Cok}(A - (a_0 + a_1x_1)B)'_{2m+i}$。根据引理 9.8 给出的分布，我们有

$$\begin{aligned} \mathbb{E}\left[\frac{1}{\#\,\mathrm{Cok}(A - (a_0 + a_1x_1)B)}\right] &= \mathbb{E}\left[p^{-2\lambda_1 - \cdots - 2\lambda_m - \lambda_{m+1} - \lambda_{m+2} - \cdots}\right] \\ &= \mathbb{E}\left[p^{-2\lambda_1 - \cdots - 2\lambda_m} \cdot \mathbb{E}[p^{-(\lambda_{m+1} + \lambda_{m+2} + \cdots)} \mid \lambda_m]\right] \\ &= \mathbb{E}\left[p^{-2\lambda_1 - \cdots - 2\lambda_m} \cdot \frac{1 - p^{-1}}{1 - p^{-\lambda_m - 1}}\right]. \end{aligned} \tag{9.23}$$

这里，最后一行来自命题 8.4。应用推论 8.10，我们有

$$\begin{aligned}\lim_{n\to\infty}\mathbb{E}\left[\frac{1}{\#\operatorname{Cok}(A-(a_0+a_1x_1)B)}\right]&=\lim_{n\to\infty}\mathbb{E}\left[p^{-2\lambda_1-\cdots-2\lambda_m}\cdot\frac{1-p^{-1}}{1-p^{-\lambda_m-1}}\right]\\&=(1-p^{-1})\sum_{k\geq 0}p^{-(m+1)k^2-(2m+1)k}(1-p^{-2k-2}).\end{aligned}\tag{9.24}$$

当 $K/\mathbb{Q}_p$ 非分歧时，对所有 $i\geq 1$，记 $\lambda_i:=\mathsf{Cok}(A-(a_0+a_1x_1)B)'_i$。根据引理 9.8 给出的分布，我们推得对于固定的 $n\geq 1$,

$$\begin{aligned}\mathbb{E}\left[\frac{1}{\#\operatorname{Cok}(A-(a_0+a_1x_1)B)}\right]&=\mathbb{E}\left[p^{-\lambda_1-\cdots-\lambda_m-\lambda_{m+1}-\lambda_{m+2}-\cdots}\right]\\&=\mathbb{E}\left[p^{-\lambda_1-\cdots-\lambda_m}\cdot\mathbb{E}[p^{-(\lambda_{m+1}+\lambda_{m+2}+\cdots)}\mid\lambda_m]\right]\\&=\mathbb{E}\left[p^{-\lambda_1-\cdots-\lambda_m}\cdot\frac{1-p^{-2}}{1-p^{-2\lambda_m-2}}\right].\end{aligned}\tag{9.25}$$

这里，最后一行来自命题 8.4。应用推论 8.10，我们得到

$$\begin{aligned}\lim_{n\to\infty}\mathbb{E}\left[\frac{1}{\#\operatorname{Cok}(A-(a_0+a_1x_1)B)}\right]&=\lim_{n\to\infty}\mathbb{E}\left[p^{-\lambda_1-\cdots-\lambda_m}\cdot\frac{1-p^{-2}}{1-p^{-2\lambda_m-2}}\right]\\&=(1-p^{-2})\sum_{k\geq 0}p^{-\frac{(2m+1)k^2+(4m+1)k}{2}}(1-p^{-k-1}).\end{aligned}\tag{9.26}$$

证明至此完成。 □

注 9.9。 我们考察命题 9.7 中计算的两个退化情形。首先，当 $m=0$ 时，我们有

$$\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||=\begin{cases}1-p^{-1} & K/\mathbb{Q}_p\text{ ramified}\\ 1-p^{-2} & K/\mathbb{Q}_p\text{ unramified,}\end{cases}$$

这与命题 5.10 一致。此外，当 m 趋于无穷大时，我们有

$$\lim_{m\to\infty}\lim_{n\to\infty}\mathbb{E}||\det(Z(A))||=(1-p^{-1})(1-p^{-2}).$$

这与推论 8.5 一致，该推论给出了 $\lim_{n\to\infty}\mathbb{E}||\det(A-a_0I)||^2=\lim_{n\to\infty}\mathbb{E}||\det(A)||^2$ 的公式，所得结果相同。

命题 9.10. 我们有

$$\#(\Lambda\backslash\operatorname{Mod}_{\mathbb{Z}_p[a_0+a_1x_1]})=\frac{1-p^{m+1}}{1-p}$$

当 $K/\mathbb{Q}_p$ 分歧时，且

$$\#(\Lambda\backslash\operatorname{Mod}_{\mathbb{Z}_p[a_0+a_1x_1]})=p^m+2p^{m-1}+2p^{m-2}+\cdots+2=\frac{1-p^m}{1-p}+\frac{1-p^{m+1}}{1-p}$$

当 $K/\mathbb{Q}_p$ 非分歧时。

证明。 注意到 $\mathbb{Z}_p[a_0+a_1x_1]=\mathbb{Z}_p+p^m\mathbb{Z}_px_1$。我们的计算依据方程 (3.60)。在 $K^\times$ 的群作用下，$\mathsf{Mod}^{\mathbb{Z}_p+p^m\mathbb{Z}_px_1}$ 中的每个轨道都有唯一一个包含 1、但不包含绝对值严格大于 1 的元素的代表元。根据定义，这样的代表元位于 $\mathcal{O}_K=\mathbb{Z}_p+\mathbb{Z}_px_1$ 内，并且由于它包含元素 1，也包含格 $\mathbb{Z}_p+p^m\mathbb{Z}_px_1$。注意， $\mathcal{O}_K/(\mathbb{Z}_p+p^m\mathbb{Z}_px_1)$ 的 $\mathbb{Z}_p$-子模 $\cong\mathbb{Z}_p/p^m\mathbb{Z}_p$ 恰好是 $p^k\mathbb{Z}_p/p^m\mathbb{Z}_p$，其中 $0\leq k\leq m$。将其提升回 $\mathsf{Mod}^{\mathbb{Z}_p+p^m\mathbb{Z}_px_1}$ 中的元素后，我们推得 $K^\times\backslash\mathsf{Mod}^{\mathbb{Z}_p[a_0+a_1x_1]}$ 的一组代表元具有如下形式

$$\mathcal{O}_K=\mathbb{Z}_p+\mathbb{Z}_px_1,\mathbb{Z}_p+p\mathbb{Z}_px_1,\ldots,\mathbb{Z}_p+p^m\mathbb{Z}_px_1.$$

对于所有 $1 \le k \le m$，我们有 $\mathrm{Aut}(\mathbb{Z}_p + p^k\mathbb{Z}_p x_1) = \mathbb{Z}_p^\times + p^k\mathbb{Z}_p x_1$，其中右侧通过乘法作用。当 $k = 0$ 时，我们有 $\mathrm{Aut}(\mathbb{Z}_p + p^k\mathbb{Z}_p x_1) = \mathcal{O}_K^\times$，其明确形式为

$$\mathcal{O}_K^\times = \mathbb{Z}_p^\times + \mathbb{Z}_p x_1$$

对于分歧情形，且

$$\mathcal{O}_K^\times = \{b_0 + b_1 x_1 \mid b_0, b_1 \text{ are not both in } p\mathbb{Z}_p\}$$

对于非分歧情形。

当 $1 \le k \le m$ 时，$\mathrm{Aut}(\mathbb{Z}_p + p^k\mathbb{Z}_p x_1) = \mathbb{Z}_p^\times + p^k\mathbb{Z}_p x_1$ 和 $\mathcal{O}_K^\times$ 都可以（作为集合）写成 $\mathbb{Z}_p$-子模 $p\mathbb{Z}_p + p^k\mathbb{Z}_p x_1 \subset \mathcal{O}_K$ 的陪集之并：

$$\mathbb{Z}_p^\times + p^k\mathbb{Z}_p x_1 = \bigsqcup_{b=1}^{p-1} b + p\mathbb{Z}_p + p^k\mathbb{Z}_p x_1, \tag{9.27}$$

and

$$\mathcal{O}_K^\times = \begin{cases} \bigsqcup_{1\le b_0\le p-1, 0\le b_1\le p^k-1} b_0 + b_1 x_1 + p\mathbb{Z}_p + p^k\mathbb{Z}_p x_1 & K/\mathbb{Q}_p \text{ ramified} \\ \bigsqcup_{\substack{0\le b_0\le p-1, 0\le b_1\le p^k-1 \\ b_0\neq 0 \text{ or } p\nmid b_1}} b_0 + b_1 x_1 + p\mathbb{Z}_p + p^k\mathbb{Z}_p x_1 & K/\mathbb{Q}_p \text{ unramified} \end{cases}. \tag{9.28}$$

因此，构成 $\mathrm{Aut}(\mathbb{Z}_p + p^k\mathbb{Z}_p x_1)$ 的陪集数为 $p-1$，而构成 $\mathcal{O}_K^\times$ 的陪集数在分歧情形下为 $(p-1)p^k$，在非分歧情形下为 $(p^2-1)p^{k-1}$。因此，对于 $0 \le k \le m$，

$$\#(\mathcal{O}_K^\times / \mathrm{Aut}(\mathbb{Z}_p + p^k\mathbb{Z}_p x_1)) = \begin{cases} 1 & k = 0 \\ p^k & k \ge 1, K/\mathbb{Q}_p \text{ ramified} \\ p^k + p^{k-1} & k \ge 1, K/\mathbb{Q}_p \text{ unramified} \end{cases}.$$

现在，应用 (3.60)，可得

$$\#(\Lambda \backslash \mathrm{Mod}_{\mathbb{Z}_p[a_0 + a_1 x_1]}) = 1 + \sum_{k=1}^{m} p^k = \frac{1 - p^{m+1}}{1 - p}$$

对于分歧情形，以及

$$\#(\Lambda \backslash \mathrm{Mod}_{\mathbb{Z}_p[a_0 + a_1 x_1]}) = 1 + \sum_{k=1}^{m} (p^k + p^{k-1}) = \frac{1 - p^m}{1 - p} + \frac{1 - p^{m+1}}{1 - p}$$

对于非分歧情形。 □

定理 *1.8* 的证明。我们有

$$||\Delta_\sigma(a_0 + a_1 x_1)||^2 = p^{-2m}||\Delta_\sigma(x_1)||^2 = p^{-2m}||\operatorname{Disc}_{K/\mathbb{Q}_p}||. \tag{9.29}$$

因此，根据定理 6.1，当 $K/\mathbb{Q}_p$ 分歧时，

$$\begin{aligned} \rho_K^{(\infty)}(a_0 + a_1 x_1) &= ||\Delta_\sigma(a_0 + a_1 x_1)|| \cdot V(a_0 + a_1 x_1) \cdot \lim_{n\to\infty} \mathbb{E}||\det(Z(A))|| \\ &= \frac{p^{-2m}||\operatorname{Disc}_{K/\mathbb{Q}_p}||}{1 - p^{-1}} \cdot \frac{1 - p^{m+1}}{1 - p} \cdot \lim_{n\to\infty} \mathbb{E}||\det(Z(A))|| \\ &= ||\operatorname{Disc}_{K/\mathbb{Q}_p}|| \frac{p^{-m}(1 - p^{-m-1})}{1 - p^{-1}} \sum_{k\ge 0} p^{-(m+1)k^2 - (2m+1)k}(1 - p^{-2k-2}). \end{aligned} \tag{9.30}$$

这里，第二行来自命题 9.10（并且我们从定义 1.6 回忆起，$V(a_0 + a_1 x_1)$会额外贡献一个 Δ_σ 项，从而得到（9.29）），第三行来自命题 9.7。非分歧情形类似可得，注意在此情形下 $||\operatorname{Disc}_{K/\mathbb{Q}_p}|| = 1$。□

对定理 1.8 中的相关函数进行积分，可得如下结果。

推论 9.11。 设 $K/\mathbb{Q}_p$ 为一个二次扩张，则有

$$\lim_{n\to\infty}\mathbb{E}[Z_{\mathcal{O}_K^{\mathrm{new}},n}]=||\operatorname{Disc}_{K/\mathbb{Q}_p}||(1-p^{-1})\sum_{k\geq 0}\frac{(1-p^{-2k-2})p^{-k^2-k}}{(1-p^{-k^2-2k-2})(1-p^{-k^2-2k-3})}$$

当 $K/\mathbb{Q}_p$ 分歧时，且

$$\lim_{n\to\infty}\mathbb{E}[Z_{\mathcal{O}_K^{\mathrm{new}},n}]=(1-p^{-1})\sum_{k\geq 0}\frac{(1-p^{-k-1})(1+p^{-k^2-2k-3})p^{-\frac{k^2+k}{2}}}{(1-p^{-k^2-2k-2})(1-p^{-k^2-2k-3})}$$

当 $K/\mathbb{Q}_p$ 非分歧时。

证明。 沿用本小节开头所述的设定，记 x_1 为 $\mathcal{O}_K$的一个生成元。对于所有 $m\geq 0$，子集

$$\mathcal{U}_m:=\{b_0+b_1x_1:b_0,b_1\in\mathbb{Z}_p,\operatorname{val}(b_1)=m\}=(\mathbb{Z}_p+p^m\mathbb{Z}_px_1)\backslash(\mathbb{Z}_p+p^{m+1}\mathbb{Z}_px_1)\subset\mathcal{O}_K$$

具有 Haar 概率测度 $\mu_K(\mathcal{U}_m)=(1-p^{-1})p^{-m}$。此外，根据定理 1.8，极限相关函数 $\rho_K^{(\infty)}$ 在 $\mathcal{U}_m$中取值 $\rho_K^{(\infty)}(p^mx_1)$。因此，根据定理 6.2，我们有

$$\begin{aligned}\lim_{n\to\infty}\mathbb{E}[Z_{\mathcal{O}_K^{\mathrm{new}},n}]&=\int_{\mathcal{O}_K}\rho_K^{(\infty)}(x)dx\\&=\sum_{m\geq 0}\rho_K^{(\infty)}(p^mx_1)\cdot\mu_K(\mathcal{U}_m)\\&=\sum_{m\geq 0}\frac{1-p^{-1}}{p^m}\rho_K^{(\infty)}(p^mx_1).\end{aligned}\tag{9.31}$$

根据定理 1.8，当 $K/\mathbb{Q}_p$ 分歧时，我们有

$$\begin{aligned}\sum_{m\geq 0}\frac{1-p^{-1}}{p^m}\rho_K^{(\infty)}(p^mx_1)&=\sum_{m,k\geq 0}||\operatorname{Disc}_{K/\mathbb{Q}_p}||\frac{(1-p^{-m-1})(1-p^{-2k-2})}{p^{(m+1)k^2+(2m+1)k+2m}}\\&=\sum_{k\geq 0}||\operatorname{Disc}_{K/\mathbb{Q}_p}||\frac{1-p^{-2k-2}}{p^{k^2+k}}\sum_{m\geq 0}\frac{1-p^{-m-1}}{p^{(k^2+2k+2)m}}\\&=\sum_{k\geq 0}||\operatorname{Disc}_{K/\mathbb{Q}_p}||\frac{1-p^{-2k-2}}{p^{k^2+k}}\left(\frac{1}{1-p^{-k^2-2k-2}}-\frac{p^{-1}}{1-p^{-k^2-2k-3}}\right)\\&=||\operatorname{Disc}_{K/\mathbb{Q}_p}||(1-p^{-1})\sum_{k\geq 0}\frac{(1-p^{-2k-2})p^{-k^2-k}}{(1-p^{-k^2-2k-2})(1-p^{-k^2-2k-3})}.\end{aligned}\tag{9.32}$$

当 $K/\mathbb{Q}_p$ 是非分歧时，我们有

$$\begin{aligned}\sum_{m\geq 0}\frac{1-p^{-1}}{p^m}\rho_K^{(\infty)}(p^mx_1)&=\sum_{m,k\geq 0}(1+p^{-1}-2p^{-m-1})(1-p^{-k-1})p^{-\frac{(2m+1)k^2+(4m+1)k}{2}-2m}\\&=\sum_{k\geq 0}(1-p^{-k-1})p^{-\frac{k^2+k}{2}}\sum_{m\geq 0}p^{-(k^2+2k+2)m}(1+p^{-1}-2p^{-m-1})\\&=\sum_{k\geq 0}(1-p^{-k-1})p^{-\frac{k^2+k}{2}}\left(\frac{1+p^{-1}}{1-p^{-k^2-2k-2}}-\frac{2p^{-1}}{1-p^{-k^2-2k-3}}\right)\\&=(1-p^{-1})\sum_{k\geq 0}\frac{(1-p^{-k-1})(1+p^{-k^2-2k-3})p^{-\frac{k^2+k}{2}}}{(1-p^{-k^2-2k-2})(1-p^{-k^2-2k-3})}.\end{aligned}\tag{9.33}$$

证明至此完成。 □

10. Estimates on repulsion of eigenvalues

自然会想到考察特征值的两点相关性。也就是说，给定两个特征值 $x_1, x_2 \in \mathbb{Z}_p$，它们是相互吸引、相互独立还是相互排斥？在定理 6.3 中，我们证明了当两个特征值 x_1, x_2 属于不同的提升子空间时，它们相互独立，即

$$\rho^{(\infty)}_{\mathbb{Q}_p[x_1]\times\mathbb{Q}_p[x_2]}(x_1, x_2) = \rho^{(\infty)}_{\mathbb{Q}_p[x_1]}(x_1)\rho^{(\infty)}_{\mathbb{Q}_p[x_2]}(x_2).$$

本节证明，当两个特征值属于同一个提升子空间时，它们会相互排斥。令

(1) $\mathcal{U}_i$ 为与次数为 $F_i = d_i$ 的 $F_i \in \mathbb{F}_p[x]$ 相对应的提升子空间。(2) $x_1, x_2 \in \mathcal{U}_i$ 为 $\mathcal{U}_i$ 中的两个元素。(3) $K_1 = \mathbb{Q}_p[x_1], K_2 = \mathbb{Q}_p[x_2]$。(4) Z_1, Z_2 分别为 x_1, x_2 的首一极小多项式。此外，我们还要求 $Z_1 \neq Z_2$，即 x_1 和 x_2 不属于同一个伽罗瓦轨道。

以下结果断言，当 p^{d_i} 较大时，$\rho^{(\infty)}_{\mathbb{Q}_p[x_1]\times\mathbb{Q}_p[x_2]}(x_1, x_2)$ 与 $\rho^{(\infty)}_{\mathbb{Q}_p[x_1]}(x_1)\rho^{(\infty)}_{\mathbb{Q}_p[x_2]}(x_2)$ 的比值约为 $||\operatorname{Res}(Z_1, Z_2)||$。

定理 10.1. 我们有

$$||\operatorname{Res}(Z_1, Z_2)||(p^{-d_i}; p^{-d_i})_\infty < \frac{\rho^{(\infty)}_{\mathbb{Q}_p[x_1]\times\mathbb{Q}_p[x_2]}(x_1, x_2)}{\rho^{(\infty)}_{\mathbb{Q}_p[x_1]}(x_1)\rho^{(\infty)}_{\mathbb{Q}_p[x_2]}(x_2)} < \frac{||\operatorname{Res}(Z_1, Z_2)||}{(p^{-d_i}; p^{-d_i})_\infty}. \tag{10.1}$$

由命题 2.6 可知，$||\operatorname{Res}(Z_1, Z_2)||$ 是 p^{-d_i} 的正整数幂。当 $||\operatorname{Res}(Z_1, Z_2)|| = p^{-kd_i}$ 且 $k \geq 2$ 时，很容易证明 (10.1) 右端小于 1。然而，当 $||\operatorname{Res}(Z_1, Z_2)|| = p^{-d_i}$ 时，这个上界仍可能大于 1，因为可以取 $p = 2, d_i = 1,$ 以及 $||\operatorname{Res}(Z_1, Z_2)|| = 1/2$。为了确切地确认 $\mathcal{U}_i$ 中的特征值彼此排斥，我们针对特殊情形 $||\operatorname{Res}(Z_1, Z_2)|| = p^{-d_i}$ 对上述估计作了小幅改进。

定理 10.2. 设 $||\operatorname{Res}(Z_1, Z_2)|| = p^{-d_i}$。那么我们有

$$p^{-d_i} < \frac{\rho^{(\infty)}_{\mathbb{Q}_p[x_1]\times\mathbb{Q}_p[x_2]}(x_1, x_2)}{\rho^{(\infty)}_{\mathbb{Q}_p[x_1]}(x_1)\rho^{(\infty)}_{\mathbb{Q}_p[x_2]}(x_2)} \leq p^{-d_i} + p^{-2d_i}.$$

本节余下部分旨在证明定理 10.1 和定理 10.2。下面的引理给出了一个有用的、关于行列式期望的初等上界。例如，我们可以取$Z = Z_1, Z = Z_2,$ 或 $Z = Z_1 Z_2$。

Lemma 10.3. 设 $Z \in \mathbb{Z}_p[x]$ 为首一多项式，其剩余是 F_i 的幂。那么我们有 *ve*

$$(p^{-d_i}; p^{-d_i})_\infty < \lim_{n\to\infty} \mathbb{E}||\det(Z(A))|| < 1.$$

证明。 命题 5.6 中的陈述意味着

$$\lim_{n\to\infty} \mathbf{P}(||\det(Z(A))|| = 1) = \lim_{n\to\infty} \mathbf{P}(Z(A) \text{ invertible}) = (p^{-d_i}; p^{-d_i})_\infty.$$

一方面，当 $Z(A)$ 不可逆时，我们总有 $||\det(Z(A))|| \leq 1/p$。这证明了上界。另一方面，存在一个非平凡有限 $\mathbb{Z}_p[x]/(Z)$-模，其在命题 5.6 中的概率严格大于零。这证明了下界。□

定理 *10.1* 的证明。由定理 6.1 可得

$$\frac{\rho^{(\infty)}_{\mathbb{Q}_p[x_1]\times\mathbb{Q}_p[x_2]}(x_1, x_2)}{\rho^{(\infty)}_{\mathbb{Q}_p[x_1]}(x_1)\rho^{(\infty)}_{\mathbb{Q}_p[x_2]}(x_2)} = ||\operatorname{Res}(Z_1, Z_2)|| \cdot \lim_{n\to\infty} \frac{\mathbb{E}||\det(Z_1(A))\det(Z_2(A))||}{\mathbb{E}||\det(Z_1(A))|| \cdot \mathbb{E}||\det(Z_2(A))||}.$$

接着应用引理 10.3。一方面,

$$\mathbb{E}||\det(Z_1(A))|| > (p^{-d_i}; p^{-d_i})_\infty$$

and

$$\mathbb{E}||\det(Z_1(A))\det(Z_2(A))|| \leq \mathbb{E}||\det(Z_2(A))||,$$

因此得到上界。另一方面,

$$\mathbb{E}||\det(Z_1(A))\det(Z_2(A))|| > (p^{-d_i}; p^{-d_i})_\infty$$

and

$$\mathbb{E}||\det(Z_1(A))||, \mathbb{E}||\det(Z_2(A))|| < 1,$$

因此得到下界。 □

下面的引理对于我们证明定理 10.2 至关重要。

引理 10.4. 若 $||\mathrm{Res}(Z_1, Z_2)|| = p^{-d_i}$, 则 $\mathbb{Z}_p[x_1] = \mathcal{O}_{K_1}$ 和 $\mathbb{Z}_p[x_2] = \mathcal{O}_{K_2}$。

证明。 由于具有对称性，我们只证明 $\mathbb{Z}_p[x_1]$的情形。只需证明以下蕴含关系

$$\mathrm{val}\, f(x_1) \geq 0 \Rightarrow f(x) \in \mathbb{Z}_p[x] \tag{10.2}$$

对于所有满足 deg $f \leq$ deg $Z_1 - 1$ 的 $f \in \mathbb{Q}_p[x]$。原因是 (10.2) 蕴含 $\{f(x_1)$: $f \in \mathbb{Q}_p[x]$, val $f(x_1) \geq 0\} \subset \mathbb{Z}_p[x_1]$, 而反向包含显然成立；根据定义，左边是 $\mathbb{Q}_p[x_1]$ 的单位球 $\mathcal{O}_{K_1}$。

由于剩余 $Z_1(x) \in \overline{\mathbb{F}}_p[x]$ 是 F_i 的幂，以下情况必有其一:

(1) deg $Z_1 = d_i$。(2) $Z_1 = Y^k + pZ_3$, 其中 $k \geq 2$, 且 $Y \in \mathbb{Z}_p[x]$ 是首一的，并且是 F_i 的一个提升。

我们将分别证明这两种情况。

若 deg $Z_1 = d_i$, 则对于任意剩余非零且 deg $f \leq d_i - 1$ 的 $f \in \mathbb{Z}_p[x]$，由命题 2.6 可得 $||\mathrm{Res}(f, Z_1)|| = 1$，这意味着 val $f(x_1) = 0$。现在设 $f \in \mathbb{Q}_p[x]$, deg $f \leq d_i - 1$ 有一个系数不属于 $\mathbb{Z}_p$。那么我们可以找到一个整数 $m \geq 1$，使得 $p^m f \in \mathbb{Z}_p[x]$ 的剩余非零，因此

$$\mathrm{val}\, f(x_1) = \mathrm{val}(p^m f(x_1)) - m = -m < 0.$$

这就验证了蕴含关系 (10.2)。

若 $Z_1 = Y^k + pZ_3$, 我们声称 Z_3 的剩余不能被 F_i整除。反设结论不成立。于是 val $Z_3(x_2) > 0$。结合 val$(Z_1(x_2)) = {}^{1}$次数 Z_2 val Res$(Z_1, Z_2) \leq 1$这一事实，可得

$$\mathrm{val}(Y^k(x_2)) = \mathrm{val}(Z_1(x_2) - pZ_3(x_2)) = \mathrm{val}(Z_1(x_2))$$

根据强三角不等式。因此， $||\mathrm{Res}(Y^k, Z_2)|| = ||\mathrm{Res}(Z_1, Z_2)|| = p^{-d_i}$。然而，$||\mathrm{Res}(Y^k, Z_2)|| = ||\mathrm{Res}(Y, Z_2)||^k$ 和 $||\mathrm{Res}(Y, Z_2)||$ 必须是 p^{-d_i}的正整数幂，这就产生了矛盾。

因此， Z_3 的剩余不能被 F_i整除，且 val $Z_3(x_1) = 0$。此外，我们有 val $Y^k(x_1) = 1 +$ val $Z_3(x_1) = 1$, 这意味着 val $Y(x_1) = 1/k$。现在，对任意剩余非零且 deg $f \leq$ deg $Z_i - 1 = kd_i - 1$ 的 $f \in \mathbb{Z}_p[x]$，我们可以将该表达式写成

$$f = Y^{k_0} Z_4 + pZ_5,$$

其中， $0 \leq k_0 < k$ 是 f的剩余在分解中出现 F_i 次的次数， $Z_4 \in \mathbb{Z}_p[x]$ 的剩余不能被 F_i整除，且 $Z_5 \in \mathbb{Z}_p[x]$。在这种情况下，我们有 val$(Y^{k_0}(x_1)Z_4(x_1)) = k_0$ val $Y(x_1) +$ val $Z_4(x_1) = k_0/k < 1$, 并且

$$\mathrm{val}\, f(x_1) = \mathrm{val}(Y^{k_0}(x_1)Z_4(x_1) + pZ_5(x_1)) = k_0/k,$$

严格小于 1。按照退化情形中相同的反证法，我们再次确认了蕴含关系 (10.2)。□

定理 *10.2* 的证明。 根据引理 10.4，我们有 $\mathbb{Z}_p[x_1] = \mathcal{O}_{K_1}$, $\mathbb{Z}_p[x_2] = \mathcal{O}_{K_2}$ 是离散赋值环，其剩余域的大小为 p^{d_i}。因此，应用定理 5.1，我们得到

$$\lim_{n\to\infty} \mathbb{E}||\det(Z_1(A))|| = \lim_{n\to\infty} \mathbb{E}||\det(Z_2(A))|| = 1 - p^{-d_i},$$

and

$$\frac{\rho^{(\infty)}_{\mathbb{Q}_p[x_1]\times\mathbb{Q}_p[x_2]}(x_1,x_2)}{\rho^{(\infty)}_{\mathbb{Q}_p[x_1]}(x_1)\rho^{(\infty)}_{\mathbb{Q}_p[x_2]}(x_2)} = p^{-d_i}\frac{\lim_{n\to\infty}\mathbb{E}||\det(Z_1(A)Z_2(A))||}{(1-p^{-d_i})^2}.$$

一方面，应用柯西-施瓦茨不等式，通过证明.....，我们得到上界

$$\begin{aligned}\lim_{n\to\infty} \mathbb{E}||\det(Z_1(A)Z_2(A))|| &\le \lim_{n\to\infty}\left(\mathbb{E}||\det(Z_1(A))||^2\right)^{1/2}\cdot\lim_{n\to\infty}\left(\mathbb{E}||\det(Z_2(A))||^2\right)^{1/2}\\ &= (1-p^{-d_i})(1-p^{-2d_i}).\end{aligned} \tag{10.3}$$

Here，第二行来自命题 5.10。另一方面，根据引理 10.3 ，

$$\begin{aligned}\lim_{n\to\infty} \mathbb{E}||\det(Z_1(A)Z_2(A))|| &> (p^{-d_i};p^{-d_i})_\infty\\ &> (1-p^{-d_i})\cdot\left(1-\sum_{k=2}^{\infty}p^{-kd_i}\right)\\ &\ge (1-p^{-d_i})^2.\end{aligned} \tag{10.4}$$

这里，第二行由广义伯努利不等式得出

$$\prod_{i=1}^{k}(1+x_i) > 1+\sum_{i=1}^{k}x_i \qquad \text{for all } x_1,\dots,x_k\in(-1,0). \tag{10.5}$$

这给出了下界。 □

11. Average numbers of eigenvalues in extensions of degree $r > 2$

设 $K/\mathbb{Q}_p$ 是一个有限扩张。本节研究落在 K 中、但不属于 K的任何真子域的特征值的期望数量级。对于次数为 1 和 2 的 K ，我们已经精确地完成了这项研究；但一般而言，当剩余次数较高时，我们仍能计算出准确的估计。我们采用 [Car22 第 4]节中的以下记号。令

(1) 设 $K/\mathbb{Q}_p$ 是一个次数为 r的有限扩张。(2) 设 $\mathcal{O}_K$ 是 K的整数环，并配备概率 Haar 测度。(3) 设 e 是 $K/\mathbb{Q}_p$的分歧次数。(4) 设 f 是 $K/\mathbb{Q}_p$的剩余次数，因此 $r = ef$，且 $\mathcal{O}_K$ 的剩余域与 $\mathbb{F}_{p^f}$同构。(5) 对所有 $d \ge 1$，令 $\mathcal{G}_d = \{\alpha \in \mathbb{F}_{p^d} \mid \mathbb{F}_{p^d} = \mathbb{F}_p[\alpha]\}$ 为 $\mathbb{F}_{p^d}$ 在 $\mathbb{F}_p$ 上的生成元集合。用 $G_d = \#\mathcal{G}_d$ 表示 $\mathcal{G}_d$的基数。(6) $\mu\colon \mathbb{Z}_{>0} \to \{0,1,-1\}$ 为莫比乌斯函数。(7) 令 $\mathcal{G}_K = \{x \in \mathcal{O}_K \mid \mathcal{O}_K = \mathbb{Z}_p[x]\}$ 为 $\mathcal{O}_K$的生成元集合。(8) 对所有 $\alpha \in \mathbb{F}_{p^f}$，令 U_α 为 $\mathcal{O}_K$ 的开子集，其在剩余域中的像为 α。(9) 令 $V = \mathcal{O}_K\backslash\mathcal{G}_K$为 $\mathcal{G}_K$在 $\mathcal{O}_K$中的补集，并且对所有 $\alpha \in \mathbb{F}_{p^f}$， $V_\alpha = V \cap U_\alpha$。

本节的目标是证明以下定理。

定理 11.1. 我们有

$$-p^{-f} \le \frac{\lim_{n\to\infty}\mathbb{E}[Z_{\mathcal{O}_K^{\mathrm{new}},n}]}{||\operatorname{Disc}_{K/\mathbb{Q}_p}||} - \sum_{d|f}\mu(\frac{f}{d})p^{d-f} < \frac{1+\tau(f)}{1-p^{-f}}p^{-f},$$

其中 $\tau(f) = \#\{d \in \mathbb{Z}_{>0} \mid d$整除 $f\}$表示 f 的正因数个数。

引理 11.2。

$$G_f = \sum_{d|f} \mu(\frac{f}{d}) p^d.$$

证明。 这是关系 $\sum_{m|f} G_m = p^f$ 的 M¨obius 反演，显然成立。 □

命题 11.3. 我们有

$$-p^{-f} \leq \frac{\int_{\mathcal{G}_K} \rho_K^{(\infty)}(x)dx}{||\operatorname{Disc}_{K/\mathbb{Q}_p}||} - \sum_{d|f} \mu(\frac{f}{d}) p^{d-f} \leq 0.$$

证明。 根据定理 6.6，我们有

$$\frac{\int_{\mathcal{G}_K} \rho_K^{(\infty)}(x)dx}{||\operatorname{Disc}_{K/\mathbb{Q}_p}||} = \int_{\mathcal{G}_K} dx = \sum_{\alpha \in \mathcal{G}_f} \int_{\mathcal{G}_K \cap U_\alpha} dx.$$

根据 [Car22，引理 4.4][10], , 对所有 $\alpha \in \mathcal{G}_f$，我们有，

$$-p^{-2f} \leq \int_{\mathcal{G}_K \cap U_\alpha} dx - p^{-f} \leq 0.$$

对所有 $\alpha \in \mathcal{G}_f$ 求和并应用引理 11.2，我们有

$$-G_f p^{-2f} \leq \sum_{\alpha \in \mathcal{G}_f} \int_{\mathcal{G}_K \cap U_\alpha} dx - \sum_{d|f} \mu(\frac{f}{d}) p^{d-f} \leq 0.$$

由平凡上界 $G_f \leq p^f$，不等式显然成立。 □

推论 11.4. 假设 $x \in \mathcal{O}_K^{\text{new}}$满足 $\mathbb{F}_p[x(\text{模 } p)] = \mathbb{F}_{p^d}$，其中 $d \mid f$。当 $x \notin \mathcal{G}_K$时，我们有 $\rho_K^{(\infty)}(x) \leq \frac{p^{-d}+2p^{-2d}}{1-p^{-f}} ||$判别式$_{K/\mathbb{Q}_p}||$。

证明。 将引理 6.5 中的估计应用于 $\rho_K^{(\infty)}(x)$ 的表达式，我们得到

$$\begin{aligned} \rho_K^{(\infty)}(x) &\leq \frac{\#(\Lambda \backslash \operatorname{Mod}_{\mathbb{Z}_p[x]})}{1-p^{-f}} ||\Delta_\sigma(x)||^2 \\ &= \frac{||\operatorname{Disc}_{K/\mathbb{Q}_p}||}{1-p^{-f}} \cdot \frac{\#(\Lambda \backslash \operatorname{Mod}_{\mathbb{Z}_p[x]})}{\#(\mathcal{O}_K/\mathbb{Z}_p[x])^2} \\ &\leq \frac{p^{-d}+2p^{-2d}}{1-p^{-f}} ||\operatorname{Disc}_{K/\mathbb{Q}_p}||. \end{aligned} \tag{11.1}$$

这里第二行是由以下事实得到的： $||\Delta_\sigma(x)||^2 = \frac{||}{||}$判别式$_{K/\mathbb{Q}_p}|| \#(\mathcal{O}_K/\mathbb{Z}_p[x])^2$，该结果在 [Car22]的第 10 页中得到证明。□

命题 11.5. 我们有

$$\sum_{\alpha \in \mathcal{G}_f} \frac{\int_{U_\alpha \backslash \mathcal{G}_K} \rho_K^{(\infty)}(x)dx}{||\operatorname{Disc}_{K/\mathbb{Q}_p}||} \leq \frac{p^{-2f}+2p^{-3f}}{1-p^{-f}}.$$

[10]按照 [Car22 中引理 4.4], 的记号，我们取 $q = p$，而 $\lambda_K = \mu_K$ 表示 $\mathcal{O}_K$上的 Haar 概率测度。

证明。 当 $x \in U_\alpha$ 对于某个 $\alpha \in \mathcal{G}_f$ 时，恒有 $\mathbb{F}_p[x(\text{模 } p)] = \mathbb{F}_{p^f}$。应用推论 11.4 中密度函数的上界，我们得到

$$\begin{aligned}\sum_{\alpha\in\mathcal{G}_f}\frac{\int_{U_\alpha\setminus\mathcal{G}_K}\rho_K^{(\infty)}(x)dx}{||\operatorname{Disc}_{K/\mathbb{Q}_p}||} &\le \frac{p^{-f}+2p^{-2f}}{1-p^{-f}}\cdot\sum_{\alpha\in\mathcal{G}_f}\int_{U_\alpha\setminus\mathcal{G}_K}dx\\ &\le \frac{p^{-f}+2p^{-2f}}{1-p^{-f}}\cdot\sum_{\alpha\in\mathcal{G}_f}p^{-2f}\\ &\le \frac{p^{-2f}+2p^{-3f}}{1-p^{-f}}.\end{aligned} \tag{11.2}$$

这里第二行来自 [Car22，引理 4.4], ，第三行成立是因为 $G_f \le p^f$。□

命题 11.6。 设 $1 \le d < f$ 是 f的一个因子。则有

$$\sum_{\alpha\in\mathcal{G}_d}\frac{\int_{U_\alpha}\rho_K^{(\infty)}(x)dx}{||\operatorname{Disc}_{K/\mathbb{Q}_p}||} \le \frac{1+2p^{-d}}{1-p^{-f}}p^{-f}.$$

证明。 应用推论 11.4 中密度函数的上界，我们有

$$\begin{aligned}\sum_{\alpha\in\mathcal{G}_d}\frac{\int_{U_\alpha}\rho_K^{(\infty)}(x)dx}{||\operatorname{Disc}_{K/\mathbb{Q}_p}||} &\le \frac{p^{-d}+2p^{-2d}}{1-p^{-f}}\cdot\sum_{\alpha\in\mathcal{G}_d}\int_{U_\alpha}dx\\ &= \frac{p^{-d}+2p^{-2d}}{1-p^{-f}}\cdot\sum_{\alpha\in\mathcal{G}_d}p^{-f}\\ &\le \frac{1+2p^{-d}}{1-p^{-f}}p^{-f}.\end{aligned} \tag{11.3}$$

这里第三行成立是因为 $G_d \le p^d$。 □

结合命题 11.3、命题 11.5 和命题 11.6 中的估计，我们可以回到定理 11.1 的证明。

定理 *11.1* 的证明。下界可直接由命题 11.3 得出。对于上界，我们有

$$\begin{aligned}\frac{\lim_{n\to\infty}\mathbb{E}[Z_{\mathcal{O}_K^{\text{new}},n}]}{||\operatorname{Disc}_{K/\mathbb{Q}_p}||} &= \frac{\int_{\mathcal{G}_K}\rho_K^{(\infty)}(x)dx}{||\operatorname{Disc}_{K/\mathbb{Q}_p}||}+\sum_{\alpha\in\mathcal{G}_f}\frac{\int_{U_\alpha\setminus\mathcal{G}_K}\rho_K^{(\infty)}(x)dx}{||\operatorname{Disc}_{K/\mathbb{Q}_p}||}+\sum_{\substack{1\le d<f\\ d|f}}\sum_{\alpha\in\mathcal{G}_d}\frac{\int_{U_\alpha}\rho_K^{(\infty)}(x)dx}{||\operatorname{Disc}_{K/\mathbb{Q}_p}||}\\ &\le \sum_{d|f}\mu(\frac{f}{d})p^{d-f}+\frac{p^{-2f}+2p^{-3f}}{1-p^{-f}}+\sum_{\substack{1\le d<f\\ d|f}}\frac{1+2p^{-d}}{1-p^{-f}}p^{-f},\end{aligned} \tag{11.4}$$

这是依次结合命题 11.3、命题 11.5 和命题 11.6 中的三个上界得到的。注意到

$$\begin{aligned}\frac{p^{-2f}+2p^{-3f}}{1-p^{-f}}+\sum_{\substack{1\le d<f\\ d|f}}\frac{1+2p^{-d}}{1-p^{-f}}p^{-f} &= \frac{p^{-f}}{1-p^{-f}}\left(\sum_{\substack{1\le d<f\\ d|f}}1+\sum_{\substack{1\le d<f\\ d|f}}2p^{-d}+p^{-f}+2p^{-2f}\right)\\ &\le \frac{p^{-f}}{1-p^{-f}}\left(\tau(f)-1+\sum_{1\le d\le 2f}2p^{-d}\right)\\ &< \frac{1+\tau(f)}{1-p^{-f}}p^{-f}.\end{aligned} \tag{11.5}$$

(11.4) 和 (11.5) 中的估计共同给出了证明。 □

定理 *1.10* 的证明。当 $K/\mathbb{Q}_p$ 是二次扩张时，极限 $\lim_{n\to\infty}\mathbb{E}[\mathbb{Z}_{\mathcal{O}_K^{\mathrm{new}},n}]$ 由推论 9.11 给出。对于更一般的情形，即 $K/\mathbb{Q}_p$ 是任意有限扩张时，估计由定理 11.1 给出。□

12. The probability that all eigenvalues are in $\mathbb{Z}_p$

记 $\mathscr{E}_n$（分别为 $\mathscr{E}_n^{\mathrm{GL}}$）为所有特征值都属于 $\mathbb{Z}_p$ 的事件，其中 A 服从 Haar 分布，$A\in \mathrm{Mat}_n(\mathbb{Z}_p)$（分别为 $A\in \mathrm{GL}_n(\mathbb{Z}_p)$）服从 Haar 分布。本节的主要结果是以下定理，它就是定理 1.12 与 $\mathrm{GL}_n(\mathbb{Z}_p)$ 对应结果的结合。

定理 12.1。我们有

$$\log_p \mathbf{P}(\mathscr{E}_n)=-\frac{n^2}{2(p-1)}-\frac{1}{2}n\log_p n+O(n),$$

and

$$\log_p \mathbf{P}(\mathscr{E}_n^{\mathrm{GL}})=-\frac{pn^2}{2(p-1)^2}-\frac{1}{2}n\log_p n+O(n).$$

这里，隐含常数取决于 p。我们滥用记号，用$\mathbf{P}$ 同时表示$\mathrm{Mat}_n(\mathbb{Z}_p)$ 上的加性 ***Haar*** 测度以及$\mathrm{GL}_n(\mathbb{Z}_p)$上的 ***Haar*** 测度。

证明定理 12.1 的主要挑战在于处理相关函数的积分；根据推论 1.3，该积分具有库仑气体的形式。幸运的是，Caruso 在 [Car22, 定理 5.8 (5)] 中证明了，在考虑随机多项式时也会出现相同的库仑气体结构。为了建立这两个随机情形之间的联系，在本节中，我们始终令 $Y_n\in\mathbb{Z}_p[x]$ 为随机多项式

$$Y_n(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0,$$

其中，$a_0,\dots,a_{n-1}$ 在 $\mathbb{Z}_p$ 中独立同分布且服从 Haar 分布。基于 Caruso 的结果，$\mathbf{P}(\mathscr{E}_n)$ 的渐近式应从$\mathbf{P}(\mathscr{E}_n^{\mathrm{poly}})$ 推出，其中 $\mathscr{E}_{\mathrm{poly}n}$ 表示 Y_n 的所有根都位于 $\mathbb{Z}_p$ 中这一事件。由于 Buhler-Goldstein-Moews-Rosenberg 已在 [BGMR06, 定理 5.1] 中求出了$\mathbf{P}(\mathscr{E}_n^{\mathrm{poly}})$ 的渐近式（在他们的论文中，他们用 r_n 表示$\mathbf{P}(\mathscr{E}_n^{\mathrm{poly}})$），因此我们能够推导出$\mathbf{P}(\mathscr{E}_n)$ 具有相同形式的渐近式。最后，我们将推导出$\mathbf{P}(\mathscr{E}_n^{\mathrm{GL}})$ 的渐近式。

下面的定义是我们在前面几节研究过的相关函数$\rho^{(n)}_{\mathbb{Q}_p^n}(x_1,\ \dots\dots,\ x_n)$的“首一 Haar 多项式”对应版本。

定义 12.2。 记 $\rho^{(n)}_{\mathbb{Q}_p^n}{}^{\mathrm{poly}}(x_1,\ \dots,\ x_n)$ 为 $Y_n(x)$ 在 ´étale 代数 $\mathbb{Q}_p^n$ 上的根相关函数。

以下命题是 [Car22，定理 5.8(5)] 的一个略有不同的版本（在原始设定中，随机多项式的所有系数，包括最高次数项的系数，均服从 Haar 分布）。

命题 12.3。 对于所有互不相同的 x_1、……、 $x_n \in \mathbb{Z}_p$，我们有

$$\rho_{\mathbb{Q}_p^n}^{(n),\mathrm{poly}}(x_1,\dots,x_n) = \prod_{1\le i<j\le n} ||x_i - x_j||.$$

命题 12.3 的证明基于以下引理，该引理是定理 3.1 的一个类似结果。

引理 12.4。 设 x_1、……、 $x_n \in \mathbb{Z}_p$ 互不相同。对于所有满足下式的元组 $s = (s_1$、……、 $s_n) \in \mathbb{N}^n$

$$s_i > n \operatorname{val}\operatorname{Disc}(x_1,\dots,x_n) = n\sum_{1\le j<k\le n} \operatorname{val}(x_j - x_k)$$

对于所有 $1 \le i \le n$，我们有

$$p^{\sum_{i=1}^n s_i} \cdot \mathbf{P}(\operatorname{val}(Y_n(x_i)) \ge s_i, \forall 1 \le i \le n) = \prod_{1\le i<j\le n} ||x_i - x_j||^{-1}.$$

基于引理 *12.4* 的命题 *12.3* 的证明。 证明所采用的论证，与第 4 节中从定理 3.1 推导定理 1.7 时所使用的论证相同。细节从略。□

引理 *12.4* 的证明。 记 Ω_{n-1} 为次数为 $\le n-1$、系数取自 $\mathbb{Z}_p$ 的多项式集合（这些多项式不必是首一的），并赋予其 Haar 概率测度。那么多项式

$$H_{n-1}(x) := Y_n(x) - (x-x_1)(x-x_2)\cdots(x-x_n)$$

服从 Ω_{n-1} 上的 Haar 测度。记

$$\Omega_{n-1}^s := \{H_{n-1} \in \Omega_{n-1} : \operatorname{val}(H_{n-1}(x_i)) \ge s_i, \forall 1 \le i \le n\},$$

它是 Ω_{n-1} 的一个 $\mathbb{Z}_p$-子模。只需证明

$$\mathbf{P}(H_{n-1} \in \Omega_{n-1}^s) = p^{-\sum_{i=1}^n s_i} \prod_{1\le i<j\le n} ||x_i - x_j||^{-1}. \tag{12.1}$$

考虑 $\mathbb{Z}_p$-模同态

$$\begin{aligned} \phi : \Omega_{n-1} &\to \mathbb{Z}_p^n \\ P(x) &\mapsto (P(x_1),\dots,P(x_n)). \end{aligned} \tag{12.2}$$

那么 $\phi(\Omega_{n-1}) = \mathbb{Z}_p[(x_1$、……、 $x_n)]$。此外，对所有 $1 \le i \le n$，都有 $s_i > \sum_{j\ne i} \operatorname{val}(x_j - x_i)$，因此多项式

$$\frac{p^{s_i}}{\prod_{j\ne i}(x_i - x_j)} \prod_{j\ne i}(x - x_j) \in \mathbb{Z}_p[x], \qquad 1 \le i \le n$$

构成 Ω_{n-1}^s 的 $\mathbb{Z}_p$-基，且 $\phi(\Omega_{n-1}^s) = \prod_{i=1}^n p^{s_i}\mathbb{Z}_p$。因此，我们有

$$\begin{aligned} \mathrm{LHS}(12.1) &= \frac{1}{\#(\Omega_{n-1} : \Omega_{n-1}^s)} \\ &= \frac{1}{\#(\phi(\Omega_{n-1}) : \phi(\Omega_{n-1}^s))} \\ &= \frac{1}{\#(\mathbb{Z}_p[(x_1,\dots,x_n)] : \prod_{i=1}^n p^{s_i}\mathbb{Z}_p)} \\ &= p^{-\sum_{i=1}^n s_i} \cdot \#(\mathbb{Z}_p^n : \mathbb{Z}_p[(x_1,\dots,x_n)]). \end{aligned} \tag{12.3}$$

最后，注意到 $\mathbb{Z}_p[(x_1,\dots,x_n)]$ 的一个基具有如下形式：$(x_1^i,\dots,x_n^i)$，其中 $0\le i\le n-1$。因此，

$$\#(\mathbb{Z}_p^n:\mathbb{Z}_p[(x_1,\dots,x_n)])=||\det\begin{pmatrix}1&\cdots&x_1^{n-1}\\ \vdots&\ddots&\vdots\\ 1&\cdots&x_n^{n-1}\end{pmatrix}||^{-1}=\prod_{1\le i<j\le n}||x_i-x_j||^{-1}.$$

证明至此完成。 □

根据命题 12.3 中相关函数的表达式，令

$$Z^{\mathrm{poly}}_{\mathbb{Z}_p^n,n}:=\#\{(x_1,\dots,x_n)\in\mathbb{Z}_p^n:x_1,\dots,x_n\text{ are distinct roots of }Y_n\}$$

表示 $\mathbb{Z}_p$ 中 Y_n 的互异根的 n-元组的数量。$Z^{\mathrm{poly}}_{\mathbb{Z}_p^n n}$, 的期望可以写成相关函数的积分

$$\mathbb{E}[Z^{\mathrm{poly}}_{\mathbb{Z}_p^n,n}]=\int_{\mathbb{Z}_p^n}\rho^{(n),\mathrm{poly}}_{\mathbb{Q}_p^n}(x_1,\dots,x_n)dx_1\cdots dx_n=\int_{\mathbb{Z}_p^n}\prod_{1\le i<j\le n}||x_i-x_j||dx_1\cdots dx_n.$$

此外，显然

$$\mathbf{P}(\mathscr{E}_n^{\mathrm{poly}})=\frac{1}{n!}\mathbb{E}[Z^{\mathrm{poly}}_{\mathbb{Z}_p^n,n}]=\frac{1}{n!}\int_{\mathbb{Z}_p^n}\prod_{1\le i<j\le n}||x_i-x_j||dx_1\cdots dx_n.$$

这将问题归结为研究 $\mathbf{P}(\mathscr{E}_n^{\mathrm{poly}})$ 的渐近性，对此我们可以引用以下结果。

定理 12.5 ([BGMR06，定理 5。1])。 存在常数 $C_1=C_1(p)$ $C_2=C_2(p)$，使得对所有 $n\ge 1$，我们有

$$C_1 n\le\log_p\mathbf{P}(\mathscr{E}_n^{\mathrm{poly}})+\frac{n^2}{2(p-1)}+\frac{1}{2}n\log_p n\le C_2 n.$$

现在，我们已准备好证明定理 12.1 中矩阵空间$_n(\mathbb{Z}_p)$的情形。

定理 *12.1* 的证明，矩阵空间$_n(\mathbb{Z}_p)$ 情形。 由定理 1.7 可知

$$\begin{aligned}\rho^{(n)}_{\mathbb{Q}_p^n}(x_1,\dots,x_n)&=\frac{(1-p^{-1})\cdots(1-p^{-n})}{(1-p^{-1})^n}\prod_{1\le i<j\le n}||x_i-x_j||\\&=\frac{(1-p^{-1})\cdots(1-p^{-n})}{(1-p^{-1})^n}\rho^{(n),\mathrm{poly}}_{\mathbb{Q}_p^n}(x_1,\dots,x_n).\end{aligned}\tag{12.4}$$

因此，我们有

$$\begin{aligned}\mathbf{P}(\mathscr{E}_n)&=\frac{1}{n!}\mathbb{E}[Z_{\mathbb{Z}_p^n,n}]\\&=\frac{(1-p^{-1})\cdots(1-p^{-n})}{(1-p^{-1})^n}\cdot\frac{1}{n!}\int_{\mathbb{Z}_p^n}\prod_{1\le i<j\le n}||x_i-x_j||dx_1\cdots dx_n\\&=\frac{(1-p^{-1})\cdots(1-p^{-n})}{(1-p^{-1})^n}\cdot\frac{1}{n!}\mathbb{E}[Z^{\mathrm{poly}}_{\mathbb{Z}_p^n,n}]\\&=\frac{(1-p^{-1})\cdots(1-p^{-n})}{(1-p^{-1})^n}\cdot\mathbf{P}(\mathscr{E}_n^{\mathrm{poly}}).\end{aligned}\tag{12.5}$$

将上述关系与定理 12.5 结合，并将项 $\log_p\frac{(1-p^{-1})\cdots(1-p^{-n})}{(1-p^{-1})^n}$代入 $O(n)$，即可完成证明。 □

现在来看$\mathbf{P}(\mathscr{E}_n^{\mathrm{GL}})$的渐近行为。以下引理将$\mathbf{P}(\mathscr{E}_{\mathrm{GL}n})$表示为$\mathbf{P}(\mathscr{E}_{\text{多项式 }b_i})$ $1\le i\le p-1$的形式，使渐近分析更容易处理。

引理 12.6。我们有

$$\mathbf{P}(\mathscr{E}_n^{\mathrm{GL}}) = \frac{1}{(1-p^{-1})^n} \sum_{b_1,\dots,b_{p-1}} \prod_{i=1}^{p-1} \left(\mathbf{P}(\mathscr{E}_{b_i}^{\mathrm{poly}}) \cdot p^{-b_i(b_i+1)/2} \right). \tag{12.6}$$

此处，求和遍历所有满足 $b_1 + \cdots + b_{p-1} = n$ 的 b_1、……、$b_{p-1} \in \mathbb{Z}_{\geq 0}$。

证明。由定理 7.3 可知

$$\rho_{\mathbb{Q}_p^n}^{(n),\mathrm{GL}}(x_1,\dots,x_n) = \frac{1}{(1-p^{-1})^n} \prod_{1\leq i<j\leq n} ||x_i - x_j||.$$

因此，我们有

$$\begin{aligned}
\mathbf{P}(\mathscr{E}_n^{\mathrm{GL}}) &= \frac{1}{(1-p^{-1})^n} \cdot \frac{1}{n!} \int_{(\mathbb{Z}_p^\times)^n} \prod_{1\leq i<j\leq n} ||x_i - x_j|| dx_1 \cdots dx_n \\
&= \frac{1}{(1-p^{-1})^n} \cdot \frac{1}{n!} \sum_{1\leq k_1,\dots,k_n\leq p-1} \int_{(k_1+p\mathbb{Z}_p)\times\cdots\times(k_n+p\mathbb{Z}_p)} \prod_{1\leq i<j\leq n} ||x_i - x_j|| dx_1 \cdots dx_n.
\end{aligned} \tag{12.7}$$

当对于给定的 i，j有 $k_i \neq k_j$ 时，我们有 $||x_i - x_j|| = 1$，因此范德蒙德式可化为对应于这些类的 $p-1$ 个范德蒙德式。给定满足 $b_1 + \cdots + b_{p-1} = n$ 的 b_1、……、$b_{p-1} \in \mathbb{Z}_{\geq 0}$，有

$$\binom{n}{b_1,\dots,b_{p-1}} = \frac{n!}{b_1!\cdots b_{p-1}!}$$

满足对于所有 $1 \leq i \leq p-1$，均有 $\#\{1 \leq j \leq n : k_j = i\} = b_i$ 的 k_1、……、$k_n \in \{1,2,\dots,p-1\}$ 的选取方式共有。因此，

$$\begin{aligned}
\mathrm{RHS}(12.7) &= \frac{1}{(1-p^{-1})^n} \sum_{b_1,\dots,b_{p-1}} \prod_{i=1}^{p-1} \frac{1}{b_i!} \int_{(p\mathbb{Z}_p)^{b_i}} \prod_{1\leq j<k\leq b_i} ||x_{j,i} - x_{k,i}|| dx_{1,i} \cdots dx_{b_i,i} \\
&= \frac{1}{(1-p^{-1})^n} \sum_{b_1,\dots,b_{p-1}} \prod_{i=1}^{p-1} \frac{p^{-b_i(b_i+1)/2}}{b_i!} \int_{\mathbb{Z}_p^{b_i}} \prod_{1\leq j<k\leq b_i} ||x_{j,i} - x_{k,i}|| dx_{1,i} \cdots dx_{b_i,i} \\
&= \frac{1}{(1-p^{-1})^n} \sum_{b_1,\dots,b_{p-1}} \prod_{i=1}^{p-1} \left(\mathbf{P}(\mathscr{E}_{b_i}^{\mathrm{poly}}) \cdot p^{-b_i(b_i+1)/2} \right).
\end{aligned} \tag{12.8}$$

此处与前文一样，求和遍历所有满足 $b_1 + \cdots + b_{p-1} = n$ 的 $b_1, \dots, b_{p-1} \in \mathbb{Z}_{\geq 0}$。证明至此完成。□

下面的引理给出了 (12.6) 右端求和项的估计。

引理 12.7。设 C_2 与定理 *12.5* 中相同。那么对于所有满足 $b_1 + \cdots + b_{p-1} = n$ 的 $b_1, \dots, b_{p-1} \in \mathbb{Z}_{\geq 0}$，我们有

$$\sum_{i=1}^{p-1} \left(\log_p \mathbf{P}(\mathscr{E}_{b_i}^{\mathrm{poly}}) - \frac{b_i(b_i+1)}{2} \right) \leq -\frac{pn^2}{2(p-1)^2} - \frac{1}{2} n \log_p n + C_2 n.$$

证明。将定理 12.5 应用于求和中的每一项，可得

$$\sum_{i=1}^{p-1} \left(\log_p \mathbf{P}(\mathscr{E}_{b_i}^{\mathrm{poly}}) - \frac{b_i(b_i+1)}{2} \right) \leq \sum_{i=1}^{p-1} \left(-\frac{pb_i^2}{2(p-1)} - \frac{1}{2} b_i \log_p b_i + (C_2 - \frac{1}{2}) b_i \right). \tag{12.9}$$

在此我们略微扩展一下约定：当 $b_i = 0$ 时，我们令 $\mathbf{P}(\mathscr{E}_{\text{多项式 }0}) = 1$，使得 $\log_p \mathbf{P}(\mathscr{E}_0^{\mathrm{poly}}) = 0$。此外，通过连续延拓，我们自然地将 $b_i \log_p b_i = 0$ 在 $b_i = 0$ 处解释为。根据这些

约定，即使某些 b_i 等于零，定理 12.5 的结论仍然成立。现在，注意到函数

$$f(b) = -\frac{pb^2}{2(p-1)} - \frac{1}{2}b\log_p b + (C_2 - \frac{1}{2})b \tag{12.10}$$

是凹函数。因此，根据詹森不等式，

$$\begin{aligned}
\mathrm{RHS}(12.9) &= \sum_{i=1}^{p-1} f(b_i) \\
&\le (p-1)f\left(\frac{\sum_{i=1}^{p-1} b_i}{p-1}\right) \\
&= (p-1)\cdot\left(-\frac{p\frac{n^2}{(p-1)^2}}{2(p-1)} - \frac{n}{2(p-1)}\log_p\frac{n}{p-1} + (C_2-\frac{1}{2})\frac{n}{p-1}\right) \\
&= -\frac{pn^2}{2(p-1)^2} - \frac{1}{2}n(\log_p n - \log_p(p-1)) + (C_2-\frac{1}{2})n \\
&\le -\frac{pn^2}{2(p-1)^2} - \frac{1}{2}n\log_p n + C_2 n.
\end{aligned} \tag{12.11}$$

□

现在，我们已准备好处理定理 12.1 中的 $\mathrm{GL}_n(\mathbb{Z}_p)$ 情形。

定理 *12.1* 的证明，$\mathrm{GL}_n(\mathbb{Z}_p)$ 情形。令 C_1, C_2 与定理 12.5 中相同。我们的目标是对 (12.6) 的右端进行初等估计。另一方面，情形

$$b_1 = \ldots = b_{n-(p-1)\lfloor\frac{n}{p-1}\rfloor} = \lfloor\frac{n}{p-1}\rfloor + 1, \quad b_{n+1-(p-1)\lfloor\frac{n}{p-1}\rfloor} = \ldots = b_{p-1} = \lfloor\frac{n}{p-1}\rfloor$$

已经给出了下界

$$\begin{aligned}
\mathrm{RHS}(12.6) &\ge \left(n-(p-1)\lfloor\frac{n}{p-1}\rfloor\right)\left(\log_p \mathbf{P}(\mathscr{E}^{\mathrm{poly}}_{\lfloor\frac{n}{p-1}\rfloor+1}) - \frac{(\lfloor\frac{n}{p-1}\rfloor+1)(\lfloor\frac{n}{p-1}\rfloor+2)}{2}\right) \\
&+ \left((p-1)(\lfloor\frac{n}{p-1}\rfloor+1)-n\right)\left(\log_p \mathbf{P}(\mathscr{E}^{\mathrm{poly}}_{\lfloor\frac{n}{p-1}\rfloor}) - \frac{\lfloor\frac{n}{p-1}\rfloor(\lfloor\frac{n}{p-1}\rfloor+1)}{2}\right) \\
&- n\log_p(1-p^{-1}) \\
&\ge (p-1)\Bigg(-\frac{(\frac{n}{p-1}+1)^2}{2(p-1)} - \frac{1}{2}\left(\frac{n}{p-1}+1\right)\log_p\left(\frac{n}{p-1}+1\right) + C_1\left(\frac{n}{p-1}+1\right) \\
&- \frac{(\frac{n}{p-1}+1)(\frac{n}{p-1}+2)}{2}\Bigg) - n\log_p(1-p^{-1}) \\
&\ge -\frac{pn^2}{2(p-1)^2} - \frac{1}{2}n\log_p n + (C_1 - 100p)n.
\end{aligned} \tag{12.12}$$

这里，将每个 $\lfloor\frac{n}{p-1}\rfloor$ 和 $\lfloor\frac{n}{p-1}\rfloor+1$ 替换为 $\frac{n}{p-1}$ ~~$+1$~~，即可得到第四行。另~~一~~方面，满足 $b_1+\cdots+b_{p-1}=n$ 的 $b_1,\ldots,b_{p-1}\in\mathbb{Z}_{\ge 0}$ 只有 $\binom{n+p-2}{p-2}$ 种选择。应用引理 12.7，可得

$$\begin{aligned}
\log_p \mathbf{P}(\mathscr{E}^{\mathrm{GL}}_n) &\le -n\log_p(1-p^{-1}) + \log_p\binom{n+p-2}{p-2} - \frac{pn^2}{2(p-1)^2} - \frac{1}{2}n\log_p n + C_2 n \\
&\le -\frac{pn^2}{2(p-1)^2} - \frac{1}{2}n\log_p n + (C_2+100p)n.
\end{aligned} \tag{12.13}$$

至此，证明完成。 □

References

[AEML22] Rida Ait El Manssour 和 Antonio Lerario。《 p进数上的概率枚举几何：完全交上的线性空间》。《{v4》，5:1329–1360，2022。（Cited on第 12 页。）[ABDF11] Gernot Akemann、Jinho Baik 和 Philippe Di Francesco。《 *The Oxford handbook of random matrix theory* 2011 Cited 2 》。牛津大学出版社，。（第 页。）[And74] George E Andrews。《奇模下罗杰斯-拉马努金恒等式的解析推广》。《 *Proceedings of the National Academy of Sciences*，71(10):4082–4085，1974。（Cited 第 60 页。）[BCFG22] Manjul Bhargava、John Cremona、Tom Fisher 和 Stevan Gajovi´c。《 $\mathbb{Z}_p$ 上次数为 n 且恰有 r 个根的多项式的密度》，2022。（Cited 第 11 和 12 页。）[Bor16] Iurie Boreico。《 *Statistics of random integral matrices*》。斯坦福大学，2016。（Cited 第 37 页。）[BC14] Alexei Borodin 和 Ivan Corwin。《 Macdonald 过程》。《 *Probability Theory and Related Fields*，158 1 2 225 Cited 14 (-)：–400，2014。（第 页。）[BS09] Alexei Borodin 和 Christopher D Sinclair。《实随机矩阵的 Ginibre 系综及其标度极限》。《 *Communications in Mathematical Physics*，291(1):177–224，2009。（Cited 第 11 页。）[Bou98] Nicolas Bourbaki。《 *Commutative algebra: chapters 1-7*》，第 1 卷。Springer Science & Business Media，1998。（Cited 第 16 页。）[BGMR06] Joe Buhler、Daniel Goldstein、David Moews 和 Joel Rosenberg。《随机首一 p 进多项式分裂的概率》。《 *Experimental Mathematics*，15(1):21–32，2006。（Cited 第 12、15、76 和 78 页。）[CT05] Richard Caron 和 Tim Traynor。《多项式的零点集》。《 *WSMR Report*，第 05–02 页，2005。（Cited 第 37 页。）[Car22] Xavier Caruso。《随机 p进多项式的零点在哪里？》。《 *Forum Math. Sigma*，10：论文编号 e55，41，2022。（Cited 第 3、12、13、15、38、40、53、54、73、74、75、76 和 77 页。）[CRV14] Xavier Caruso、David Roe 和 Tristan Vaccon。《跟踪 p 进精度》。， （A）：–。 *LMS Journal of Computation and Mathematics* 17 274 294, 2014 Cited 38 （第 页。）[CH21] Gilyoung Cheong 和 Yifeng Huang。《通过有限剩余域的完备离散赋值环上的随机矩阵研究科恩–伦斯特拉分布》。《 *Illinois Journal of Mathematics*，65(2):385–415，2021。（Cited 第 13 页。）[CH25] Gilyoung Cheong 和 Yifeng Huang。《剩余集中时随机整数矩阵的多项式推前的余核》。《 *Math. Proc. Cambridge Philos. Soc.*，178 2 229 257, ()：–。（第 页。）[CK22] Gilyoung Cheong 和 Nathan Kaplan。《Friedman 和 Washington 关于随机 p 进矩阵余核的结果的推广》。《 *Journal of Algebra*，604:636–663，2022。（Cited 第 13 页。）[CLS23] Gilyoung Cheong、Yunqi Liang 和 Michael Strand。《模素数幂整数上的矩阵多项式方程与随机矩阵的余核》。《 *Linear Algebra and its Applications*，677 1 30, 2023 Cited 13 : –。（第 页。）[CY23] Gilyoung Cheong 和 Myungjun Yu。《随机整数矩阵处多项式取值的余核分布》。《 *arXiv preprint arXiv:2303.09125*，2023 *American Journal* 。即将在《》发表。（第 *of Mathematics* Cited 3, 44, 46, 48, 49 页。）[Coh12] Henri Cohen。《 *Advanced topics in computational number theory*》，第 193 卷。Springer Science & Business Media，2012。（Cited 第 16 页。）[DC15] Daniel Delbourgo 和 Qin Chao。《关于与循环三次数域相关的 on 不变量》。《*of Computation and Mathematics* 18 1 684 698, 2015 Cited 2 *LMS Journal* ，（）：–。（第 页。）[DK23] Daniel Delbourgo 和 Heiko Knospe。《关于阿贝尔数域的 Iwasawa λ不变量与随机矩阵启发式》。《 *Mathematics of Computation*，92(342):1817–1836，2023。（Cited 第 2 页。）[Ede97] Alan Edelman。《随机实高斯矩阵具有 k 个实特征值的概率、相关分布及圆盘定律》。《 *Journal of Multivariate Analysis*，60(2):203–232，1997。（Cited 第 11 页。）[EKS94] Alan Edelman、Eric Kostlan 和 Michael Shub。《随机矩阵有多少个实特征值？》。《 *Journal of the American Mathematical Society*，7(1):247–267，1994。（Cited 第 11 页。）[EJV11] Jordan S Ellenberg、Sonal Jain 和 Akshay Venkatesh。《用 p 进随机矩阵模拟 λ不变量》。《 *Communications on pure and applied mathematics*，64(9):1243–1262，2011。（Cited on pages第 2、3、4、10 和 14 页。）[Eva06] Steven Evans。《随机 p 进多项式系统零点的期望 *Electronic Communications in Probability* 11 278 290, 2006 Cited 11 39 数》。，：–。（第 页。）[Eva02] Steven N Evans。《局部域上随机矩阵的初等因子和行列式》。《 *Stochastic processes and their applications*，102(1):89–102，2002。（Cited 第 3、14、15 和 57 页。）[FN07] Peter J Forrester 和 Taro Nagao。《实 Ginibre 系综的特征值统计》。《 *Physical review letters* 99 5 050603, 2007 Cited 11 ，（）：。（第 页。）[Ful01] Jason Fulman。《罗杰斯–拉马努金恒等式的概率证明》。《 *Bulletin of the London Mathematical Society* 33 4 397 407, 2001 Cited 3, 15, 57, 58, 59 ，（）：–。（第 页。）

[Ful02] Jason Fulman. 有限域上的随机矩阵理论。 *Bulletin of the American Mathematical Society* 39 1 51 85, 2002 Cited 14 , ( ): – 。（见第 页。）[Ful97] Jason Edward Fulman。 *Probability in the classical groups over finite fields: symmetric functions, stochastic algorithms and cycle indices* 1997 Cited 54 , 。哈佛大学, 。（见第 页。）[GWY23] Asvin G、Yifan Wei 和 John Yin。局部域上的切博塔廖夫密度定理。 *arXiv preprint arXiv:2212.00294* 2023 Cited 11 , 。（见第 页。）[Gin65] Jean Ginibre。复矩阵、四元数矩阵和实矩阵的统计系综。 *Journal of Mathematical Physics* 6 3 440 449, 1965 Cited 11 , ( ): – 。（见第 页。）[KS23] Nicholas M Katz 和 Peter Sarnak。 *Random matrices, Frobenius eigenvalues, and monodromy*, 第 45 卷。美国数学会，2023年。（Cited 见第 2 页。）[Kno24] Heiko Knospe。狄利克雷特征的特殊值、 p进 L函数与岩泽 λ不变量。 *arXiv preprint arXiv:2401.06100*，2024年。（Cited 见第 2 页。）[Kra46a] Marc Krasner。p进域的给定次数扩张的数目。, : – 。（见第 页和第 页。）[Kra46b] Marc Krasner。完备赋值域的有限可分扩张的非阿贝尔类域论：基本原理；多项式空间与变换 t；唯一性、序性和存在性定律。 *CR Acad. Sci. Paris*, 222:626–628, 1946年。（Cited 见第 21 页。）[KL21] Avinash Kulkarni 和 Antonio Lerario。 p *SIAM Journal on Applied Algebra* 进积分几何。 , ( ): – 。 *and Geometry* 5 1 28 59, 2021 Cited 12 （见第 页。）[KW24a] Debanjana Kundu 和 Lawrence C Washington。反圆分扩张的启发式。 , ( ): – 。（见第 页。）[KW24b] Debanjana Kundu 和 Lawrence C Washington。 $\mathbb{Z}_p$扩张的第一层与启发式的相容性。 *arXiv preprint arXiv:2410.06193*，2024年。（Cited 见第 2 页。）[Lee23] Jungin Lee。随机 p进矩阵余核的联合分布。 *Forum Mathematicum*,35 4 1005 1020, 2023 Cited 13 45 ( ): – 。（见第 页和第 页。）[LS91] Nils Lehmann 和 Hans-J ¨ *Physical* urgen Sommers。随机实 *review letters* 67 8 941, 1991 Cited 11 矩阵的特征值统计。, ( ): 。（见第 页。）[Mon73] Hugh L Montgomery。ζ函数零点的二点相关。载于 *Proc. Symp. Pure Math*，第 24 卷，第 1 页，1973年。（Cited 见第 2 页。）[Neu13] J ¨urgen Neukirch。 *Algebraic number theory*，第 322 卷。Springer Science & Business Media，2013年。（Cited 见第 17 页。）[RP60] Norbert Rosenzweig 和 Charles E Porter。复原子光谱中的“能级排斥”。 *Physical Review*, 120(5):1698, 1960年。（Cited 见第 11 页。）[San21] Giacomo Santato。p进 L 函数的零点：Ellenberg–Jain–Venkatesh猜想。数学 ALGANT 硕士论文，帕多瓦大学和莱顿大学，帕多瓦与莱顿，2021年。（Cited on 第 2 页。）[SW22] Will Sawin 和 Melanie Matchett Wood。范畴中随机对象的矩问题。 *arXiv preprint arXiv:2210.06279*，2022年。（Cited 见第 3、12、13、14、44、46、48 和 50 页。）[She25] Jiahe Shen。有限域上随机矩阵有理标准形的普适性。 *arXiv preprint arXiv:2510.16225* 2025 Cited 54 , 。（见第 页。）[Shm22] Roy Shmueli。p进随机 étale 代数为非分歧域的概率。 , 。（见第 页。）[Shm23] Roy Shmueli。 p *International Math-* 进数域上的根的期望数量。 *ematics Research Notices* 2023 3 2543 2571, 2023 Cited 12 , ( ): – 。（见第 页。）[Sin07] Christopher D Sinclair。Ginibre 系综中随机实矩阵的平均值。 *International Mathematics Research Notices* 2007 9 015 015, 2007 Cited 11 , ( ):rnm –rnm 。（见第 页。）[Sin22] Christopher D. Sinclair。非阿基米德静电学。载于 *p-adic analysis arithmetic and singularities* 778 *Contemp. Math.* 279 311 , , 第 卷，共 页，第 – 页。[ ], [2022] 美国数学会，罗得岛州普罗维登斯，©2022年。（Cited on 第 5 和 6 页。）[Tho13] Kelly Devine Thomas。从素数到核物理及其他领域。https://www.ias. edu/ideas/2013/primes-random-matrices，2013年。发表于 *The Institute Letter*，2013年春季。访问日期：2025-10-19。（Cited 见第 2 页。）[VP18] Roger Van Peski。局部域整数上的随机矩阵理论，2018年。本科毕业论文，普林斯顿大学。（Cited 见第 54 页。）[VP21] Roger Van Peski。 p进随机矩阵乘积的极限与涨落。 *Selecta Mathematica*, 27 5 1 71, 2021 Cited 14 ( ): – 。（见第 页。）[VZG25] Willem Veys 和 Wilson A Z ´u ˜niga-Galindo。Koba-Nielsen局部ζ函数、凸子集及广义 Selberg-Mehta-Macdonald 与 Dotsenko-Fateev型积分。 *arXiv preprint arXiv:2507.08120* 2025 Cited 6 , 。（见第 页。）[War03] S Ole Warnaar。部分 theta 函数。I. 超越遗失的笔记本。 *Proceedings of the London Mathematical Society* 87 2 363 395, 2003 Cited 9 , ( ): – 。（见第 页。）[Web21] Joe Webster。 p *p-Adic Numbers Ultrametric Analysis* 域 *and Applications* 13 1 1 43, 2021 Cited 5 中具有范数密度的对数库仑气体。 , , ( ): – 。（见第 页。）

[Web23] Joe Webster。 p *p-Adic Numbers Ultrametric* 域射影直线上的对数库仑气体。*Analysis and Applications* 15 1 59 80, 2023 Cited 5 。, , ( ): – 。（见第 页。）[Woo17] Melanie Matchett Wood。随机图沙堆群的分布。*Journal of the American Mathematical Society* 30 4 915 958, 2017 Cited 3 13 , ( ): – 。（见第 页和第 页。）[Woo19] Melanie Matchett Wood。随机整矩阵与科恩-伦斯特拉启发式。*American Journal of Mathematics* 141 2 383 398, 2019 Cited 13 , ( ): – 。（见第 页。）[Yun13] Zhiwei Yun。轨道积分与戴德金ζ函数。*arXiv preprint arXiv:1303.2420*，2013年。（Cited 见第 3、12、13、15、21、25、36、51 和 52 页。）[ZGT20] Wilson A Z ´ ˜uniga-Galindo 和 Sergii M Torba。非阿基米德库仑气体。*Journal of Mathematical Physics* 61 1 2020 Cited 6 , ( ), 。（见第 页。）[ZGZLLC22] Wilson A Z ´u ˜niga-Galindo、Brian A Zambrano-Luna 和 Edwin Le ´on-Cardenal。图、局部ζ函数、对数库仑气体与有限温度下的相变。*Journal of Mathematical Physics* 63 1 2022 Cited 6 , ( ), 。（见第 页。）