arXiv:2602.05284v1 [math.NT] 5 Feb 2026

不可分自同态与 Gross 格的秩二子格

Yves Aubry 和 Christelle Vincent

Abstract. 我们回答 Love 提出的一个问题：从一条超奇异椭圆曲线到其 Frobenius 基变换的同源，与其 Gross 格的秩 2 子格之间是否存在对应关系。我们将该问题改写为关于曲线不可分自同态的问题，并证明当自同态的迹为零时，这种对应关系成立；否则则未必成立。

1. Introduction

设 p 为素数， $\mathbb{F}_p$ 为含有 p 个元素的有限域， $\overline{\mathbb{F}}_p$ 为 $\mathbb{F}_p$的代数闭包。此外，设 E 为定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线，且 $B_{p为\infty}$ 在 $\mathbb{Q}$上的四元数代数，在 p 和 ∞处分歧。则 E的几何自同态环 $\mathrm{End}(E)$ 同构于B_p的∞极大理想 $\mathcal{O}$ 。对于 $\mathbb{F}_p$的 Frobenius 同态 $\varphi(z) = z^p$ ，我们记

$$E^{(p)} := E \otimes_{\mathrm{Spec}(\mathbb{F}_p),\varphi} \mathrm{Spec}(\overline{\mathbb{F}}_p)$$

对于 E 的 Frobenius 基变换。

设 $\bar{\cdot}$ 表示 $B_{p,\infty}$ 上的共轭，则我们用 $\mathrm{trd}(x) = x + \bar{x}$ 表示 $B_{p,\infty}$上的约化迹，并用 $\mathrm{nrd}(x) = x\bar{x}$ 表示约化范数。这些运算诱导出定义在$B_{p,\infty}$ 上的内积 $\frac{1}{2}\mathrm{trd}(x\bar{y})$；我们注意到 $\frac{1}{2}\mathrm{trd}(x\bar{x}) = \mathrm{nrd}(x)$。对于 $B_{p,\infty}$ 中以 $\{x_1, \ldots, x_n\}$ 为基的格 Λ，我们将其**行列式**定义为

$$\det \Lambda := \det\left(\frac{1}{2}\mathrm{trd}(x_i\bar{x}_j)\right)_{1\le i,j\le n};$$

该量与用于计算它的基的选取无关。此外，对于 $B_{p,\infty}$ 中的格 Λ，我们将其**Gross 格**定义为

$$\Lambda^T := \{2x - \mathrm{trd}(x) : x \in \Lambda\}.$$

当 $\Lambda = \mathrm{End}(E)$，其中 E 是定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线时，我们称 $\overline{\mathrm{End}}(E)^T$ 为**椭圆曲线的 Gross 格** E。

在 [Lov25]，中，Love 提出如下问题：

问题。设 ℓ为正整数， E 为定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线， $E^{(p)}$ 为其 Frobenius 基变换，$\overline{\mathrm{End}}(E)$ 为 E 的几何自同态环。是否存在次数为 ℓ 的同源$E \to E^{(p)}$ ，当且仅当 $\mathrm{End}(E)^T$ 包含一个行列式为 $4\ell p$ 的秩 2 子格?

本文将这个问题重新表述为关于超奇异椭圆曲线 E 的不可分自同态的问题（见第 2.1 节），并对这个新问题给出了部分肯定、部分否定的回答。更准确地说，我们的主要结果如下：

定理 1.1. 设 p 是一个素数， E 是定义在 $\mathbb{F}_p$上的超奇异椭圆曲线。那么，对于任意正整数 ℓ， E 存在一个次数为 ℓp 且迹为零的自同态，当且仅当 $\mathrm{End}(E)^T$包含一个行列式为 $4\ell p$的秩 2 子格。

Date: 2026年2月6日。2020 *Mathematics Subject Classification.* 11G20、14H52、11R52、14K02。
Key words and phrases. 椭圆曲线、Gross格、同源。作者感谢 Jonathan Love 富有成效的讨论，这些讨论改进了本文。此外，他们还感谢 Université de Polynésie française 的 GAATI实验室提供的款待，他们在此完成了这项工作。Aubry 获法国国家研究署通过 Barracuda项目提供的资助，资助合同编号为 ANR-21-CE39-0009-BARRACUDA。Vincent 获西蒙斯基金会数学家旅行资助。

这一主要结果推广了 [Kan89, 第 851-852], 页中的一项隐含结果。该结果指出，若超奇异椭圆曲线的 j-不变量属于 $\mathbb{F}_p$ （因此存在一个次数为 p 且迹为零的自同态），则其 Gross 格 End(E)^T 包含一个秩为 2、行列式为 $4p$的子格；此外，它也推广了 [HKTV，命题 3.1.1], 该命题证明了 Kaneko 结果的逆命题。

此外，在第4节中，我们给出一些定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线的例子，它们存在迹为 p、次数为 ℓp 的自同态；但我们证明，它们的 Gross 格不包含行列式为 $4\ell p$ 的秩 2 子格。为了说明这种情况相当常见，我们给出一个 $\ell = p$ 的例子、一个 $\ell \neq p$ 的例子（其中 ℓ 是素数），最后给出一个 ℓ 为合数的例子。

最后，鉴于命题 3.1 可能本身也具有独立的研究价值，我们在此特别指出该命题：它根据序 $\mathcal{O}$ 的一组基，给出了 $B_{p,\infty}$ 中序 $\mathcal{O}$ 的交换子理想 $[\mathcal{O}:\mathcal{O}]$ 的显式 $\mathbb{Z}$-基。

2. Preliminaries

2.1. 背景。 回想一下，在全文中， E 都是定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线。我们先将 Love 关于同源 $E \to E^{(p)}$ 的问题，改写为关于 E 的自同态的问题。设 ℓ 为正整数，且 $\alpha \in \in$End(E) 的次数为 ℓp。正如 GL25b 第 2.3.5 小节所述，定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线有唯一一个秩为 p 的子群概形，它是 Frobenius同源 $E \to E^{(p)}$ 的核，而该同源的次数为 p。因此，自同态 α 可分解为先取 Frobenius同源，再接一个次数为 ℓ 的同源 $E^{(p)} \to E$。该同源的对偶随后给出一个次数为 ℓ 的同源 $E \to E^{(p)}$。反过来，若存在一个次数为 ℓ 的同源 $E \to E^{(p)}$，其中 ℓ 为正整数，那么将它与 Verschiebung 复合（Verschiebung 是 Frobenius同源的对偶），便可得到一个次数为 ℓp 的 E 的自同态。由此可知，寻找一个次数为 ℓ 的同源 $E \to E^{(p)}$，等价于寻找一个次数为 ℓp 的 E 的自同态。我们还发现，由于当 E 为超奇异时，Verschiebung 同源是不可分的，因此超奇异椭圆曲线的不可分自同态恰好是次数可被 p 整除的自同态。

设 $\mathcal{O}$ 是$B_{p,\infty}$中的一个极大阶；则它同构于定义在$\mathbb{F}_p$上的超奇异椭圆曲线 E 的几何自同态环 End(E)。我们注意到，在此同构下，自同态的次数对应于其像的约化范数，而 End(E)上的迹与 $\mathcal{O}$上的约化迹一致。$\mathcal{O}$ 中包含约化范数可被 p 整除的元素所构成的理想，是 $\mathcal{O}$的一个双边素理想，记作 P。事实上，这是 $\mathcal{O}$ 中约化范数为 p的唯一极大双边理想。此外，设 $[\mathcal{O},\mathcal{O}]$ 是 $\mathcal{O}$的双边**交换子理想**，即由形如 $[\alpha_1,\alpha_2]$: $= \alpha_1\alpha_2 - \alpha_2\alpha_1$ （其中 $\alpha_i \in \mathcal{O}$）的元素生成的 $\mathcal{O}$ 的双边理想。众所周知（例如参见 [Voi21，第42.4节6]），对于$B_{p,\infty}$的任意极大阶， $[\mathcal{O},\mathcal{O}]$ 等于 P。最后， $P = [\mathcal{O},\mathcal{O}]$是秩为4的自由模，因为它是自由 $\mathbb{Z}$-模 $\mathcal{O}$ 的子模，且指数有限 p^2。这一事实成立是因为 $\mathcal{O}/P \cong \mathbb{F}_{p^2}$，正如 [Voi21，第42.4节6]中所论证的那样。

定义线性映射 τ: $B_{p,\infty} \to B_{p,\infty}$，使得 $\tau(x) = 2x - \mathrm{trd}(x)$；那么，格 Λ 在 τ 下的像恰好是其 Gross 格 Λ^T。正如 [GL25a 第 3 节所述，3], 若将 τ 限制在 $B_{p,\infty}$的一个序上，则 ker(τ) $= \mathbb{Z}$。在证明中，我们需要以下结果:

引理 2.1. 设 $\mathcal{O}$是 $B_{p,\infty}$中的一个序。若 $\{1,\alpha_1,\alpha_2,\alpha_3\}$是 $\mathcal{O}$的一组基，则 $\{\tau(\alpha_1)\ \tau(\alpha_2)\ \tau(\alpha_3)\}$是 $\mathcal{O}^T$的一组基。反之，若 $\{\beta_1,\beta_2,\beta_3\}$是 $\mathcal{O}^T$的一组基，则对任意满足 $\alpha_i = \tau(\beta_i)$ 的 α_i， $\{1,\alpha_1,\alpha_2,\alpha_3\}$都是 $\mathcal{O}$的一组基，其中 $i = 1$ 取值为 *2* 或 *3*。

证明。首先假设 $\{1,\alpha_1,\alpha_2,\alpha_3\}$是 $\mathcal{O}$的一组基，并令 $\beta \in \mathcal{O}^T$。那么，对于某个$\alpha \in \mathcal{O}$，有 $\beta = \tau(\alpha)$，且存在整数 a_0, a_1, a_2, a_3 使得 $\alpha = a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3$。因此，由于 τ是$\mathbb{Z}$-线性的，且$\tau(a_0) = 0$，我们有 $\beta = a_1\tau(\alpha_1) + a_2\tau(\alpha_2) + a_3\tau(\alpha_3)$，而集合 $\{\tau(\alpha_1)\ \tau(\alpha_2)\ \tau(\alpha_3)\}$生成 $\mathcal{O}^T$。此外，如果对于某些整数 a_1, a_2, a_3，有 $a_1\tau(\alpha_1) + a_2\tau(\alpha_2) + a_3\tau(\alpha_3) = 0$，那么 $a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 \in$ker($\tau$) $= \mathbb{Z}$。若将这个整数记为 a_0，则 $a_0 - a_1\alpha_1 - a_2\alpha_2 - a_3\alpha_3 = 0$。由于集合 $\{1,\alpha_1,\alpha_2,\alpha_3\}$ 线性无关，我们得出 $a_0 = a_1 = a_2 = a_3 = 0$，因此集合 $\{\tau(\alpha_1)\ \tau(\alpha_2)\ \tau(\alpha_3)\}$线性无关。

现在，设 $\{\beta_1,\beta_2,\beta_3\}$ 是 $\mathcal{O}^T$ 的一组基，满足对每个 i， $\tau(\alpha_i) = \beta_i$，且 $\alpha \in \mathcal{O}$。我们知道存在整数 a_1, a_2, a_3，使得 $\tau(\alpha) = a_1\beta_1 + a_2\beta_2 + a_3\beta_3$，因为 $\tau(\alpha) \in \mathcal{O}^T$。由于 $\tau(\alpha_i) = \beta_i$，且 τ 是 $\mathbb{Z}$-线性的，因此我们有 $\tau(\alpha) = \tau(a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3)$，从而 $\alpha - a_1\alpha_1 - a_2\alpha_2 - a_3\alpha_3 \in$ker($\tau$) $= \mathbb{Z}$。再次用 a_0 表示这个整数，我们得出 $\alpha = a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3$，且集合 $\{1,\alpha_1,\alpha_2,\alpha_3\}$ 生成 $\mathcal{O}$。此外，若 $a_0 + a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 = 0$，将 τ 应用于此等式，可得

$a_1\beta_1 + a_2\beta_2 + a_3\beta_3 = 0$。由于集合 $\{\beta_1, \beta_2, \beta_3\}$ 线性无关，因此有 $a_1 = a_2 = a_3 = 0$。由此可推得 $a_0 = 0$，所以集合 $\{1, \alpha_1, \alpha_2, \alpha_3\}$ 线性无关。□

2.2. **不可分端同态的存在性**。我们首先证明主要结果定理 1.1 的一个方向。我们注意到，[CG14] 的引理 3.4 的证明中给出了类似的论证。

命题 2.2。设 E 是定义在 $\mathbb{F}_p$ 上的超奇异椭圆曲线，且$\mathrm{End}(E)$为其几何自同态环。若$\mathrm{End}(E)^T$ 中存在行列式为 $4\ell p$ 的秩 *2* 子格，则存在 E 的次数为 ℓp 且迹为零的不可分端同态。

证明。设 Λ 是 $\mathrm{End}(E)^T$ 的行列式为 $4\ell p$的秩 2 子格，且 $\{\gamma_1, \gamma_2\}$ 是 Λ的任意一组基。考虑元素

$$\alpha := \frac{1}{2}\gamma_1\overline{\gamma}_2 - \frac{1}{4}\operatorname{trd}(\gamma_1\overline{\gamma}_2) \in B_{p,\infty}.$$

我们证明，正如 [HKTV], 中命题 3.1 的证明那样，α 属于 $\mathrm{End}(E)$，且次数为 ℓp 、迹为零。事实上，考虑 $\mathrm{End}(E)$ 中满足 $\gamma_1 = \tau(\alpha_1)$与 $\gamma_2 = \tau(\alpha_2)$的任意元素 α_1 和 α_2。于是我们有

$$\alpha = 2\alpha_1\overline{\alpha}_2 - (\operatorname{trd}(\alpha_2)\alpha_1 + \operatorname{trd}(\alpha_1)\overline{\alpha}_2) + \operatorname{trd}(\alpha_1)\operatorname{trd}(\alpha_2) - \operatorname{trd}(\alpha_1\overline{\alpha}_2)$$

由此可得 $\alpha \in \mathcal{O}$。

此外，我们有:

$$\operatorname{nrd}(\alpha) = \frac{1}{4}\left(\operatorname{nrd}(\gamma_1)\operatorname{nrd}(\gamma_2) - \frac{1}{4}\operatorname{trd}(\gamma_1\overline{\gamma}_2)^2\right) = \frac{1}{4}\det\Lambda = \ell p,$$

以及

$$\operatorname{trd}(\alpha) = \frac{1}{2}\gamma_1\overline{\gamma}_2 - \frac{1}{4}\operatorname{trd}(\gamma_1\overline{\gamma}_2) + \frac{1}{2}\gamma_2\overline{\gamma}_1 - \frac{1}{4}\operatorname{trd}(\gamma_1\overline{\gamma}_2) = \frac{1}{2}\operatorname{trd}(\gamma_1\overline{\gamma}_2) - \frac{1}{2}\operatorname{trd}(\gamma_1\overline{\gamma}_2) = 0.$$

最后我们可以得出结论：α 是不可分的，因为其次数可被 p 整除，且 E 是超奇异的。 □

3. Existence of a sublattice of rank 2

现在我们转而考虑命题 2.2 的逆命题，它具体要求：给定超奇异曲线 E 上一个次数为 ℓp 、迹为 0 的自同态 α，给出 $\mathrm{End}(E)^T$ 的一个行列式为 $4\ell p$ 的秩 2 子格。我们通过证明 $\mathrm{End}(E)^T$ 中存在线性无关的 γ_1 与 γ_2，使得

$$\alpha = \frac{1}{2}\gamma_1\overline{\gamma}_2 - \frac{1}{4}\operatorname{trd}(\gamma_1\overline{\gamma}_2).$$

事实上，若情况如此，则由命题 2.2 的证明可得：若 Λ 是由集合 $\{\gamma_1, \gamma_2\}$ 生成的格，则 $\det\Lambda = 4\mathrm{nrd}(\alpha)$，从而由 γ_1 与 γ_2 张成的 $\mathrm{End}(E)^T$ 的秩 2 子格的行列式为 $4\ell p$ （这也证明了 γ_1 与 γ_2 是线性无关的，因为 $\ell \neq 0$）。

为此，我们首先给出 $[\mathcal{O}, \mathcal{O}]$ 的一个显式 $\mathbb{Z}$-基。

命题 3.1. 设 $\mathcal{O}$ 是 B_p 的一个极大阶，∞ 是其交换子理想，且 $\{1, \alpha_1, \alpha_2, \alpha_3\}$ 是 $\mathcal{O}$ 的一组基。那么集合

$$\{[\alpha_1, \alpha_2], [\alpha_1, \alpha_3], [\alpha_2, \alpha_3], \alpha_1[\alpha_2, \alpha_3]\}$$

是 $[\mathcal{O}, \mathcal{O}]$ 的一个 $\mathbb{Z}$-基。

证明. 设 C 是由集合 $\{[\alpha_1, \alpha_2], [\alpha_1, \alpha_3], [\alpha_2, \alpha_3]\}$ 生成的 $\mathbb{Z}$-格。我们首先断言，对于所有 γ_1，γ_2 属于 $\mathcal{O}$，C 都包含 $[\gamma_1, \gamma_2]$，即 γ_1 与 γ_2 的交换子。将每个 γ_i 用基 $\{1, \alpha_1, \alpha_2, \alpha_3\}$ 表示，并显式计算交换子即可得出这一点。

根据非交换环中交换子理想和双边理想的定义，$[\mathcal{O}, \mathcal{O}]$ 中的元素具有如下形式

$$l_1[x_1, y_1]r_1 + l_2[x_2, y_2]r_2 + \cdots + l_n[x_n, y_n]r_n$$

对于任意 n 正整数以及 l_i, r_i, x_i 和 y_i，它们都是 $\mathcal{O}$ 中适用于 $i \in \{1, \ldots, n\}$的元素。因此，$[\mathcal{O}, \mathcal{O}]$ 中的元素具有如下形式

$$l_1[\alpha_{1,i}, \alpha_{1,j}]r_1 + l_2[\alpha_{2,i}, \alpha_{2,j}]r_2 + \cdots + l_n[\alpha_{n,i}, \alpha_{n,j}]r_n \tag{1}$$

其中，与前文一样，l_i 和 r_i 是 $\mathcal{O}$ 的元素，且每个 $\alpha_{i,\ j} \in \{\alpha_1, \alpha_2, \alpha_3\}$。

将每个 l_i 和 r_i 都用基 $\{1, \alpha_1, \alpha_2, \alpha_3\}$表示后，我们看到，要证明 (1) 是集合 $\{[\alpha_1, \alpha_2], [\alpha_1, \alpha_3], [\alpha_2, \alpha_3], \alpha_1[\alpha_2, \alpha_3]\}$ 中元素的 $\mathbb{Z}$-线性组合，现在只需证明，对于任意 i, j, k, ℓ，形如 $\alpha_i[\alpha_j, \alpha_k]$、$[\alpha_i, \alpha_j]\alpha_k$ 和 $\alpha_i[\alpha_j, \alpha_k]\alpha_\ell$ 的元素都是集合$\{[\alpha_1, \alpha_2], [\alpha_1, \alpha_3], [\alpha_2, \alpha_3], \alpha_1[\alpha_2, \alpha_3]\}$中元素的 $\mathbb{Z}$-线性组合。我们分几步来证明这一点。

首先，考虑形如 $\alpha_i[\alpha_j, \alpha_k]$ 的乘积。若 $i = j$ 或 $i = k$，则得到

$$\alpha_i[\alpha_i, \alpha_j] = -\alpha_i[\alpha_j, \alpha_i] = [\alpha_i, \alpha_i\alpha_j] \in C.$$

若 i，j，且 k 均互不相同，则计算得

$$\alpha_i[\alpha_j, \alpha_k] + \alpha_j[\alpha_i, \alpha_k] = [\alpha_i, \alpha_i\alpha_k] + [\alpha_i, \alpha_j\alpha_k] \in C$$

and

$$\alpha_i[\alpha_j, \alpha_k] + \alpha_k[\alpha_j, \alpha_i] = [\alpha_i\alpha_j, \alpha_k] + [\alpha_k\alpha_j, \alpha_i] \in C.$$

因此基由 $\mathcal{O}$ 中的交换子生成的左理想具有 $[\alpha_i, \alpha_j]\alpha_k$ 形式。因此，为了证明我们的结论，现在只需证明，对于任意 i，j，k，以及任意 i，$[\alpha_i, \alpha_j]\alpha_k$ 和 $\alpha_1[\alpha_2, \alpha_3]\alpha_i$ 都属于由元素 $\{[\alpha_1, \alpha_2], [\alpha_1, \alpha_3], [\alpha_2, \alpha_3], \alpha_1[\alpha_2, \alpha_3]\}$ 生成的格。

同样，若 $i = j$ 或 $i = k$，则有

$$[\alpha_i, \alpha_j]\alpha_i = -[\alpha_j, \alpha_i]\alpha_i = [\alpha_i, \alpha_j\alpha_i] \in C,$$

而若 i，j，k 均互不相同，

$$[\alpha_j, \alpha_k]\alpha_i + [\alpha_i, \alpha_k]\alpha_j = [\alpha_i, \alpha_k\alpha_j] + [\alpha_j, \alpha_k\alpha_i] \in C$$

and

$$[\alpha_j, \alpha_k]\alpha_i + [\alpha_j, \alpha_i]\alpha_k = [\alpha_j\alpha_k, \alpha_i] + [\alpha_j\alpha_i, \alpha_k] \in C.$$

此外，当然还有，

$$\alpha_1[\alpha_2, \alpha_3] - [\alpha_2, \alpha_3]\alpha_1 = [\alpha_1, [\alpha_2, \alpha_3]] \in C,$$

由此可知，对于任意的 i, j, k，每个 $[\alpha_i, \alpha_j]\alpha_k$ 都属于由元素$\{[\alpha_1, \alpha_2], [\alpha_1, \alpha_3], [\alpha_2, \alpha_3], \alpha_1[\alpha_2, \alpha_3]\}$生成的格。

最后，考虑形如 $\alpha_1[\alpha_2, \alpha_3]\alpha_i$ 的元素，我们注意到，根据上面的证明，对每个 i，乘积$[\alpha_2, \alpha_3]\alpha_i$ 都属于由元素 $\{[\alpha_1, \alpha_2], [\alpha_1, \alpha_3], [\alpha_2, \alpha_3], \alpha_1[\alpha_2, \alpha_3]\}$ 生成的格，而该格正是由 $\mathcal{O}$ 的交换子生成的左理想。因此，$\alpha_1[\alpha_2, \alpha_3]\alpha_i$ 也属于这个左理想，进而属于我们的格。因此，集合 $\{[\alpha_1, \alpha_2], [\alpha_1, \alpha_3], [\alpha_2, \alpha_3], \alpha_1[\alpha_2, \alpha_3]\}$ 生成 $[\mathcal{O}, \mathcal{O}]$。

现在，由于 $[\mathcal{O}, \mathcal{O}]$ 是秩为 4 的自由模，任何张成它的四个元素都必定线性无关。 □

以下推论与我们有关：

推论 3.2。设 $\mathcal{O}$ 是 B_p的极大阶，∞，$[\mathcal{O}, \mathcal{O}]$ 为其交换子理想，且 $\{\beta_1, \beta_2, \beta_3\}$ 是 $\mathcal{O}^T$的一组基。那么集合

$$\left\{\frac{\beta_1\beta_2 - \beta_2\beta_1}{4}, \frac{\beta_1\beta_3 - \beta_3\beta_1}{4}, \frac{\beta_2\beta_3 - \beta_3\beta_2}{4}\right\} \tag{2}$$

是 $[\mathcal{O}, \mathcal{O}]$ 中迹为零元素所成子格的 $\mathbb{Z}$-基。

证明。对于每个 $i = 1$，2，3，取 $\alpha_i \in \mathcal{O}$ 使得 $\tau(\alpha_i) = \beta_i$。由于 $\{\beta_1, \beta_2, \beta_3\}$ 是 $\mathcal{O}^T$的一组基，根据引理 2.1，集合 $\{1, \alpha_1, \alpha_2, \alpha_3\}$ 是 $\mathcal{O}$的一组基。直接计算可得

$$[\alpha_i, \alpha_j] = \alpha_i\alpha_j - \alpha_j\alpha_i = \frac{\beta_i\beta_j - \beta_j\beta_i}{4} \tag{3}$$

对于每个 i，$j \in \{1, 2, 3\}$。

交换子理想 $[\mathcal{O}, \mathcal{O}]$ 包含迹非零的元素；这是因为 $[\mathcal{O}, \mathcal{O}] = P \supset p\mathcal{O}$。由于每个 $[\alpha_i, \alpha_j]$ 的迹为零，元素 $\alpha_1[\alpha_2, \alpha_3]$ 必然具有非零的迹。因此，如果 $\alpha \in [\mathcal{O}, \mathcal{O}]$ 的迹为零，

$$\alpha = a_0[\alpha_1, \alpha_2] + a_1[\alpha_1, \alpha_3] + a_2[\alpha_2, \alpha_3] + a_3\alpha_1[\alpha_2, \alpha_3]$$

我们必须有 $a_3 = 0$。因此集合 $\{[\alpha_1, \alpha_2], [\alpha_1, \alpha_3], [\alpha_2, \alpha_3]\}$ 张成 $[\mathcal{O}, \mathcal{O}]$ 中迹为零的元素所构成的子格，并且由于它们是某个基的元素，它们是线性无关的。□

我们现在准备证明如下结果，它与命题 2.2 一起完成了定理 1.1 的证明：

定理 3.3. 设 E 是定义在 $\mathbb{F}_p$上的超奇异椭圆曲线。若 α 是 E 的一个次数为 ℓp 且迹为零的自同态，则存在 γ_1 和 γ_2 属于$\mathrm{End}(E)^T$，它们张成一个行列式为 $4\ell p$的格。

证明。 设 $\mathcal{O}$ 是B_p的一个极大阶，∞ 它与 End(E) 同构。由于 α 的范数可被 p整除且迹为零，因此 α 属于 $[\mathcal{O},\mathcal{O}]$中迹为零元素所构成的 $\mathbb{Z}$-格。于是根据推论 3.2，存在整数 a_1，a_2，a_3 使得

$$\alpha = a_1\frac{\beta_1\beta_2-\beta_2\beta_1}{4} + a_2\frac{\beta_1\beta_3-\beta_3\beta_1}{4} + a_3\frac{\beta_2\beta_3-\beta_3\beta_2}{4}.$$

我们断言，存在整数 c_{11}，c_{12}，c_{13}，c_{21}，c_{22}，c_{23} 使得

$$\begin{cases} a_1 = c_{12}c_{21} - c_{11}c_{22} \\ a_2 = c_{13}c_{21} - c_{11}c_{23} \\ a_3 = c_{13}c_{22} - c_{12}c_{23}. \end{cases}$$

事实上，若 $a_1 = a_2 = 0$，则我们有整数解 $c_{11} = c_{13} = c_{21} = c_{22} = 0$、$c_{12} = a_3$ 和 $c_{23} = -1$。否则，我们有解 $c_{11} = \gcd(a_1, a_2)$、$c_{21} = 0$、$c_{22} = -\frac{a_1}{c_{11}}$、$c_{23} = -\frac{a_2}{c_{11}}$和~~$c_{12}$~~，$c_{13}$，它们是丢番图方程的解

$$a_2c_{12} - a_1c_{13} = c_{11}a_3,$$

它们存在，因为 $\gcd(a_1, a_2)$ 整除 $c_{11}a_3$。

现在令 $\{\beta_1,\beta_2,\beta_3\}$ 为 End(E)^T 的一个 $\mathbb{Z}$-基，并设 $\gamma_1 = c_{11}\beta_1 + c_{12}\beta_2 + c_{13}\beta_3$ 和 $\gamma_2 = c_{21}\beta_1 + c_{22}\beta_2 + c_{23}\beta_3$，使得 $\gamma_1, \gamma_2 \in$ End(E)^T。经过繁琐但初等的计算可得

$$\alpha = \frac{1}{2}\gamma_1\overline{\gamma}_2 - \frac{1}{4}\,\mathrm{trd}(\gamma_1\overline{\gamma}_2).$$

如前所述，根据命题 2.2 的证明，由 γ_1 和 γ_2 张成的格 Λ 的行列式为 4 nrd(α) $= 4\ell p$。由于该值非零，集合 $\{\gamma_1,\gamma_2\}$ 线性无关，且 Λ 的秩为 2。□

4. Counter-examples when the trace is not zero

我们不妨思考一下，定理 1.1 中要求元素 $\alpha \in$End(E) 的迹为零这一条件是否必要。下面给出几个例子，说明若 End(E) 含有一个次数为 ℓp 但迹非零的元素，则未必存在 End(E)^T 的一个行列式为 $4\ell p$ 的秩 2 子格。

4.1. 当 $\ell = p$ 时的反例。考虑定义在 $\mathbb{F}_{11}$ 上、具有 j-不变量 $j = 0$ 的椭圆曲线 E；该曲线是超奇异的。在这种情况下，End(E) 含有一个范数为 $11^2 = 121$ 的自同态，但 End(E)^T 不存在行列式为 4×121 的秩 2 子格，下面对此进行说明。

设 $B_{11,\infty}$ 为在 $\mathbb{Q}$ 上的四元数代数，其恰好在 11 和 ∞ 处分歧；设 i，j，k 是 $B_{11,\infty}$ 中满足 $i^2 = -3$、$j^2 = -11$ 和 $k = ij$ 的元素。设 $\mathcal{O}$ 是 $B_{11,\infty}$ 的任意极大阶，使得 End(E) $\simeq \mathcal{O}$。

于是可以选择 $\mathcal{O}$，使其 Gross 格 $\mathcal{O}^T$ 具有由 $\{i, \frac{i+3j-k}{3}, \frac{-i-2k}{3}\}$ 给出的逐次最小基，而该基的 Gram 矩阵如下（见~~[HKTV]~~的命题 3.2.1）：

$$\begin{pmatrix} 3 & 1 & 1 \\ 1 & 15 & -7 \\ 1 & -7 & 15 \end{pmatrix}.$$

对于其他任意选取的一个与 $\mathcal{O}$ 同构的 $B_{p,\infty}$ 的极大理想 $\mathcal{O}'$，逐次最小基的 Gram 矩阵保持不变。

现在考虑 $B_{p,\infty}$ 的以下元素：

$$\alpha := \frac{11}{2} + \frac{11}{2}i;$$

我们有，α 的约化迹 trd(α) $= 11$，约化范数 nrd(α) $= 11 \times 11$。存在B_{11}的一个极大阶 $\mathcal{O}$，∞，使得 End(E) $\simeq \mathcal{O}$ 且 $\alpha \in \mathcal{O}$。我们证明 $\mathcal{O}^T$ 不包含行列式为 4×121的秩 2 子格。

事实上，设 γ_1 和 γ_2 是 $\mathcal{O}^T$ 的两个元素，且 Λ 是它们生成的格。像之前一样，若我们用$\{\beta_1,\beta_2,\beta_3\}$ 表示 $\mathcal{O}^T$ 的一组基，则 $\gamma_1 = c_{11}\beta_1 + c_{12}\beta_2 + c_{13}\beta_3$ 且 $\gamma_2 = c_{21}\beta_1 + c_{22}\beta_2 + c_{23}\beta_3$，其中 c_{ij}为整数。于是我们有

$$\mathrm{nrd}(\gamma_i) = 3c_{i1}^2 + 2c_{i1}c_{i2} + 2c_{i1}c_{i3} + 15c_{i2}^2 - 14c_{i2}c_{i3} + 15c_{i3}^2$$

以及

$$\mathrm{trd}(\gamma_1\overline{\gamma}_2) = 6c_{11}c_{21} + 2c_{11}c_{22} + 2c_{11}c_{23} + 2c_{12}c_{21} + 30c_{12}c_{22} - 14c_{12}c_{23} + 2c_{13}c_{21} - 14c_{13}c_{22} + 30c_{13}c_{23}.$$

Λ 的行列式因此为 $\mathrm{nrd}(\gamma_1)\,\mathrm{nrd}(\gamma_2) - \frac{1}{4}\mathrm{trd}(\gamma_1\overline{\gamma}_2)^2$，这是一个含 6 个变量的 4 次齐次多项式。除以 44 并进行如下变量替换后：

$$\begin{cases} x = c_{11}c_{22} - c_{12}c_{21} \\ y = c_{11}c_{23} - c_{13}c_{21} \\ z = c_{12}c_{23} - c_{13}c_{22} \end{cases} \tag{4}$$

我们得到二次型

$$Q = x^2 + y^2 + 4z^2 - xy + yz - xz.$$

接下来只需证明这个二次型不表示 11。事实上， Q 具有如下对角型：

$$Q = \left(x - \frac{y+z}{2}\right)^2 + \frac{3}{4}\left(y + \frac{z}{3}\right)^2 + \frac{11}{3}z^2,$$

因此

$$12Q = 3(2x - y - z)^2 + (3y + z)^2 + 44z^2.$$

方程 $3(2x-y-z)^2 + (3y+z)^2 + 44z^2 = 132$ 立即推出 $44z^2 \le 132$，由此得到$z^2 \le 3$，从而 $z \in \{-1, 0, 1\}$。

若 $z = 0$，则可得 $(2x-y)^2 + 3y^2 = 44$。接着 $3y^2 \le 44$，这给出 $3y^2 \in \{0, 3, 12, 27\}$，进而得到 $(2x-y)^2 \in \{44, 41, 32, 17\}$，但这些整数都不是完全平方数。因此，在 $z = 0$ 的情况下没有整数解。

若 $z = \pm 1$，我们以同样的方式继续推导，并再次得出没有整数解，因此 $\mathcal{O}^T$ 中不存在行列式为 4×121 的秩 2 子格。

4.2. 当 $\ell \neq p$ 且 ℓ 为素数时的反例。 考虑定义在 $\mathbb{F}_{31}$ 上、 j-不变量为 $j = 4$ 的超奇异椭圆曲线 E。设 $B_{31,\infty}$ 为在 31 和 ∞ 处分歧的、定义在 $\mathbb{Q}$ 上的四元数代数；设 i， j， k 为 $B_{31,\infty}$ 的元素，满足 $i^2 = -1$、 $j^2 = -31$ 和 $k = ij$；并设 $\mathcal{O}$ 为 $B_{31,\infty}$ 的极大阶，使得 $\mathrm{End}(E) \simeq \mathcal{O}$，且 $\mathcal{O}$ 包含元素

$$\alpha = \frac{31}{2} - \frac{31}{3}i - \frac{7}{6}j - \frac{2}{3}k.$$

我们有 $\mathrm{trd}(\alpha) = 31$ 且 $\mathrm{nrd}(\alpha) = 13 \times 31$。

与上面的反例类似，我们可以计算 Gross 格 $\mathcal{O}^T$ 的秩 2 子格的行列式型。使用第 4.1 小节的记号以及公式（4）的变量替换，该型等于 $124Q$ 其中 Q是

$$Q = x^2 + 2y^2 + 5z^2 - xy - xz + 2yz.$$

我们可以通过其对角型看出，型 Q 不表示 13

$$Q = \left(x - \frac{y+z}{2}\right)^2 + \frac{7}{4}\left(y + \frac{3}{7}z\right)^2 + \frac{31}{7}z^2$$

采用与第 4.1 小节中所用方法完全类似的方式。

4.3. 当 $\ell \neq p$ 且 ℓ 为合数时的反例。 这次，令 E 为定义在 $\mathbb{F}_{19}$ 上的超奇异椭圆曲线，其 j-不变量为 $j = 7$；令 $B_{19,\infty}$ 为在 19 和 ∞处分歧的 $\mathbb{Q}$ 上的四元数代数；令 i, j, k 为 $B_{19,\infty}$ 中的元素，使得 $i^2 = -1$、$j^2 = -19$和 $k = ij$。此外，取 $\mathcal{O}$ 为 $B_{19,\infty}$ 的一个极大阶，使得 End(E) $\simeq \mathcal{O}$ 且 $\mathcal{O}$ 包含元素

$$\alpha = \frac{19}{2} - \frac{19}{2}i - \frac{1}{2}j - \frac{1}{2}k$$

其约化范数为 10×19 ，约化迹为 19。

我们再次可以 证明 Gross 格 $\mathcal{O}^T$ 不包含秩 2 且行列式 t $4 \times 10 \times 19$。这一次 秩 2 子格的行列式型等于 $76Q$ ，其中

$$Q = x^2 + 2y^2 + 3z^2 - xy - xz + yz$$

具有对角型

$$Q = \left(x - \frac{y+z}{2}\right)^2 + \frac{7}{4}\left(y + \frac{z}{7}\right)^2 + \frac{19}{7}z^2.$$

由于这个 m 不表示 10，因此在 $\mathcal{O}^T$ 中不存在行列式为 $4 \times 10 \times 19$ 的秩 2 子格 .

References

[CG14] Ilya Chevyrev 和 Steven D. Galbraith。构造具有给定自同态环的超奇异椭圆曲线。*LMS Journal of Computation and Mathematics*，17：71–91，2014。[GL25a] Eyal Z. Goren 和 Jonathan R. Love。四元数代数极大序中具有指定范数的元素。*Canadian Journal of Mathematics*，77(6)：1938–1965，2025。[GL25b] Eyal Z. Goren 和 Jonathan R. Love。 *Supersingular elliptic curves, quaternion algebras and applications to cryptog-raphy*，第 66 卷，*NATO Science for Peace and Security Series - D: Information and Communication Security*，第 123–200 页。2025。[HKTV] Chenfeng He、Gaurish Korpal、Ha T. N. Tran 和 Christelle Vincent。超奇异椭圆曲线的Gross格。可见于 `https://arxiv.org/abs/2503.03478`。[Kan89] Masanobu Kaneko。超奇异 j-不变量作为模 p 的奇异模。 *Osaka J. Math.*，26(4)：849–855，1989。[Lov25] Jonathan Love。同源图的拓扑。 `https://isogeny.club`，2025 年 4 月。[Voi21] John Voight。*Quaternion algebras*，第 288 卷， *Graduate Texts in Mathematics*。Springer，Cham，2021。

(Aubry) Institut de Mathématiques de Toulon - IMATH, Université de Toulon, France
Email address: `yves.aubry@univ-tln.fr`

(Aubry) Institut de Mathématiques de Marseille - I2M, Aix Marseille Univ, UMR 7373 CNRS, France
Email address: `yves.aubry@univ-amu.fr`

(Vincent) University of Vermont, Burlington, United States of America
Email address: `christelle.vincent@uvm.edu`