arXiv:2303.00376v1 [math.AG] 1 Mar 2023

具有第三大亏格的极大曲线的魏尔斯特拉斯半群与自同构群

PETER BEELEN、MARIA MONTANUCCI 和 LARA VICINO

Abstract. 本文明确确定了一条已知的 $\mathbb{F}_{q^2}$-极大曲线 $\mathcal{X}_3$ 在任意点处的魏尔斯特拉斯半群以及其全自同构群，该曲线具有第三大亏格。这条曲线是厄米特曲线的一个伽罗瓦子覆盖，而它的唯一性（就其亏格值而言）是一个众所周知的未解决问题。了解魏尔斯特拉斯半群或许能为解决这一问题提供关键线索。令人惊讶的是， $\mathcal{X}_3$有许多不同类型的魏尔斯特拉斯半群，且其魏尔斯特拉斯点的集合远比$\mathbb{F}_{q^2}$-有理点的集合丰富；而在所有已知魏尔斯特拉斯点的极大曲线中，情况恰恰相反。我们证明，就自同构而言，并不存在类似的例外行为：除 q较小的情形外，Aut($\mathcal{X}_3$)恰好是从厄米特曲线继承而来的自同构群。

关键词：极大曲线，魏尔斯特拉斯半群，魏尔斯特拉斯点 MSC：主要分类：11G20。次要分类：11R58，14H05，14H55

1. Introduction

亏格为 g 的 $\mathbb{F}_{q^2}$-极大曲线 $\mathcal{X}$ 是定义在 $\mathbb{F}_{q^2}$ 上的射影、几何不可约、非奇异代数曲线，其 $\mathbb{F}_{q^2}$-有理点的数量 $|\mathcal{X}(\mathbb{F}_{q^2})|$ 达到哈斯–韦伊上界，即

$$|\mathcal{X}(\mathbb{F}_{q^2})| = q^2 + 1 + 2gq.$$

$\mathbb{F}_{q^2}$-极大曲线，尤其是亏格较大的曲线，在过去几十年里受到了广泛研究；这也与基于 Goppa 方法的编码理论和密码学有关，参见例如 [13, 25]。

众所周知， $\mathbb{F}_{q^2}$-极大曲线的亏格 g 满足 $g \leq q(q-1)/2 =: g_1$，参见 [17], ；并且，当且仅当 $\mathcal{X}$ 与厄米特曲线 $\mathbb{F}_{q^2}$-同构时， $g = g_1$

$$\mathcal{H} : x^q + x = y^{q+1},$$

见 [21]。在 [8] 中证明了，要么 $g \leq \lfloor (q-1)^2/4 \rfloor =: g_2$，要么 $g = g_1$。当 q 为奇数时，$g = g_2$成立当且仅当 $\mathcal{X}$ 与方程为

$$\mathcal{X}_2 : x^q + x = y^{\frac{q+1}{2}},$$

见 [7, 定理 3.1]。当 q 为偶数时， [1]中得到了一个类似（但较弱）的结果。事实上，在附加条件——该曲线有一个特定的魏尔斯特拉斯点——成立时，亏格为 $g = g_2$ 的 $\mathbb{F}_{q^2}$-极大曲线的唯一性得以保证。若满足这一附加条件，则 [1] 中证明了， $g = q(q-2)/4$ 当且仅当 $\mathcal{X}$ 与方程为

$$\mathcal{Y}_2 : x^{\frac{q}{2}} + \ldots + x^2 + x = y^{q+1}.$$

an $\mathbb{F}_{q^2}$-极大曲线的第三大亏格的值已在 [19], 中计算得出，其中证明了以下两种情况之一成立： $g \le \lfloor (q^2 - q + 4)/6 \rfloor =: g_3$，或 $g = g_2$ 或 $g = g_1$。在 [19, 备注 3.4] 中证明了 $g \le g_3$ 是可能达到的最佳界，因为存在亏格为 g_3 的 $\mathbb{F}_{q^2}$-极大曲线，即

- $\mathcal{X}_3$： $x^{(q+1)/3} + x^{2(q+1)/3} + y^{q+1} = 0$，如果 $q \equiv 2$ （模 3）；
- $\mathcal{Y}_3$： $y^q - yx^{2(q-1)/3} + x^{(q-1)/3} = 0$，如果 $q \equiv 1$ （模 3）；以及
- $\mathcal{Z}_3$： $y^q + y + \left(\sum_{i=1}^{t} x^{q/p^i}\right)^2 = 0$，如果 $q = 3^t$。

更确切地说， $\mathcal{X}_3$、 $\mathcal{Y}_3$ 和 $\mathcal{Z}_3$ 是由这些方程给出的平面曲线的非奇异模型。上述所有例子都作为厄米特曲线$\mathcal{H}_q$的次数为 3 的伽罗瓦子覆盖出现。要理解这些曲线是否是亏格为 g_3 的唯一 $\mathbb{F}_{q^2}$-极大曲线，是一个众所周知的未解决问题。

在证明亏格为 g_1的 $\mathbb{F}_{q^2}$-极大曲线与亏格为 g_2 的 [21] -极大曲线在同构意义下的唯一性时，所谓的魏尔斯特拉斯半群和魏尔斯特拉斯点发挥了关键作用。这些对象也自然地出现在代数几何（AG）码 [25], 的研究中，是构造单点代数几何码的主要工具。

给定代数曲线 $\mathcal{X}$上的一点 P，魏尔斯特拉斯半群 $H(P)$定义为自然数 n 的集合；对于这些自然数，存在曲线 $\mathcal{X}$ 上的函数 f ，其极点因子为$(f)_\infty = nP$。根据魏尔斯特拉斯间隙定理，见 [22, 定理 1.6，集合$G(P) := \mathbb{N} \setminus H(P)$恰好包含 g个称为间隙的元素。一般而言， $H(P)$的结构会随 $P \in \mathcal{X}$ 的变化而变化。然而，已知在一般情况下，半群 $H(P)$是相同的，但 $\mathcal{X}$中可能存在有限个点，它们被称为魏尔斯特拉斯点，并具有不同的间隙集。

这些对象的内在理论意义源于 St¨ohr-Voloch 理论 [23]„ 在该理论中，魏尔斯特拉斯半群和魏尔斯特拉斯点（连同所谓的阶序列）被用来获得刻画曲线的性质。除了上述针对 g_1 和 g_2 的两种刻画外，利用魏尔斯特拉斯点、魏尔斯特拉斯半群和自同构群的重要刻画结果还可见于 [7], [9] （针对铃木曲线）和 [24]（针对 Ree 曲线）。

为了为第三大亏格的极大曲线提供类似的工具，自然会想到，是否能够完全确定亏格为 g_3 的极大曲线的魏尔斯特拉斯半群和魏尔斯特拉斯点。

在本文中，我们计算了亏格为 g_3 的曲线 $\mathcal{X}_3$ 在每一点处的魏尔斯特拉斯半群集合，其中 $q \equiv 2$ （模 3），以及其魏尔斯特拉斯点集合和完整的自同构群。

在所有已知的亏格足够大的极大曲线例子中，魏尔斯特拉斯点集合与有理点集合重合，参见例如 [3–5, 11]。为理解这一现象，先前的研究给出了极大曲线满足这一性质的充分条件，见 [10]。

与此相反，本文证明曲线 $\mathcal{X}_3$ 具有相当大的非有理魏尔斯特拉斯点集合，并且有许多不同类型的魏尔斯特拉斯半群，从而给出了首个具有这些特征的已知例子。作为上述结果的应用，我们还计算了 $\mathcal{X}_3$ 的全自同构群。

本文组织如下。第 2 节介绍代数曲线、魏尔斯特拉斯半群以及曲线 $\mathcal{X}_3$ 所需的预备结果。第 3 节介绍 $\mathbb{F}_{q^2}(\mathcal{X}_3)$ 中两族特殊函数及其关系。除 P 的少数特殊情形外，这些函数是计算 $H(P)$ 的魏尔斯特拉斯半群所用的主要工具。第 4 节和第 5 节分别证明本文的主要定理，即描述 $\mathcal{X}_3$ 上 $\mathbb{F}_{q^2}$-有理点和非 $\mathbb{F}_{q^2}$-有理点处的魏尔斯特拉斯半群。在第 6 节中，作为对所得的 $\mathcal{X}_3$ 上魏尔斯特拉斯半群结果的应用，我们计算了 $\mathcal{X}_3$ 的全自同构群。

2. Preliminaries

本节介绍全文将用到的预备概念和结果。第一小节回顾曲线 $\mathcal{X}_3$ 的定义，并着重讨论其上定义的若干特殊有理函数，计算它们的主除子。第二小节汇集正则微分方面的一些预备知识。特别地，我们计算一个典范除子，并证明推论 2.23，这一推论将在第 4 节和第 5 节中用到。

2.1. 曲线 $\mathcal{X}_3$。设 q 为一个满足 $q \equiv 2 \pmod 3$ 的素数幂，并定义 $m := \frac{q+1}{3}$。设 $\mathbb{F}_{q^2}$ 为含有 q^2 个元素的有限域，并用 p 表示 $\mathbb{F}_{q^2}$ 的特征。与前文一样，设 $\mathcal{X}_3$ 为具有如下仿射方程的平面曲线的非奇异模型

$$y^{q+1} + x^{2m} + x^m = 0. \tag{2.1}$$

函数域 $\mathbb{F}_{q^2}(\mathcal{X}_3)$ 可表示为 $\mathbb{F}_{q^2}(x, y)$，其中 $y^{q+1} + x^{2m} + x^m = 0$，不难看出 $\mathbb{F}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(x)$ 是次数为 $q+1$ 的库默尔扩张。

注 2.2. 点 (0, 0) 是由方程 (2.1) 定义的曲线的奇点。根据我们刚才对消解 $\mathcal{X}_3$ 及其函数域的观察，很容易看出，在 $\mathbb{F}_{q^2}(\mathcal{X}_3)$ 中恰有 m 个以 (0, 0) 为中心的不同位置，我们将 $\mathcal{X}_3$ 中以这些位置为中心的不同点记为 $P_0^1, \ldots, P_0^m$。平面曲线的无穷远点也是奇点。对于该点，同样恰有

m 个以它为中心的不同位置，位于 $\mathbb{F}_{q^2}(\mathcal{X}_3)$ 中。我们用 $P_\infty^1, \ldots, P_\infty^m$ 表示 $\mathcal{X}_3$ 中以这些 m 个位置为中心的不同点。

考虑厄米特曲线的 $\mathbb{F}_{q^2}$-模型 $\mathcal{H}$，其定义为

$$\mathcal{H} : u^{q+1} + v^{q+1} + 1 = 0$$

并令 $\mathbb{F}_{q^2}(\mathcal{H})$ 为 $\mathcal{H}$ 的函数域，它可表示为 $\mathbb{F}_{q^2}(u, v)$，其中 $u^{q+1} + v^{q+1} + 1 = 0$。厄米特曲线是亏格为 $g(\mathcal{H}) = q(q-1)/2$ 的非奇异平面曲线。曲线 $\mathcal{X}_3$ 是亏格为 $g(\mathcal{X}_3)$ 的 $\mathbb{F}_{q^2}$-极大曲线: $= \frac{q^2-q+4}{6}$，并且它可通过次数为 3 的态射 φ 被厄米特曲线 $\mathcal{H}$ 覆盖。更准确地说，拉回映射

$$\varphi^* : \mathbb{F}_{q^2}(\mathcal{X}_3) \longrightarrow \mathbb{F}_{q^2}(\mathcal{H})$$

定义了一个次数为 3 的伽罗瓦扩张 $\mathbb{F}_{q^2}(\mathcal{H})/\mathbb{F}_{q^2}(\mathcal{X}_3)$，其中 $x := u^3$ 且 $y := uv$。特别地，该扩张的伽罗瓦群由自同构生成

$$\tau : (u, v) \longmapsto (\zeta_3 u, \zeta_3^2 v), \tag{2.3}$$

其中，ζ_3 是 $\mathbb{F}_{q^2}$中的一个本原三次单位根。

注 2.4. 扩张 $\mathbb{F}_{q^2}(\mathcal{H})/\mathbb{F}_{q^2}(\mathcal{X}_3)$是不分歧的：事实上，由 Hurwitz 亏格公式可得

$$\deg \mathrm{Diff}(\mathbb{F}_{q^2}(\mathcal{H})/\mathbb{F}_{q^2}(\mathcal{X}_3)) = 2g(\mathcal{H}) - 2 - 3(2g(\mathcal{X}_3) - 2) = 0,$$

这恰好意味着扩张 $\mathbb{F}_{q^2}(\mathcal{H})/\mathbb{F}_{q^2}(\mathcal{X}_3)$是不分歧的。因此，若 Q 是 $\mathcal{H}$ 上位于 $\mathcal{X}_3$的点 P 之上的一个点，则对任意 $f \in \mathbb{F}_{q^2}(\mathcal{X}_3)$，有 $v_Q(f) = v_P(f)$。

为方便起见，我们定义 $\mathcal{O}_0 := \{P_0^1, \ldots, P_0^m\}$ 和 $\mathcal{O}_\infty := \{P_\infty^1, \ldots, P_\infty^m\}$。在全文中，我们用 $P_{(a,b)} \in \mathcal{X}_3(\mathbb{F}_{q^2})$表示 $\mathcal{X}_3$ 上不属于点集 $\mathcal{O}_0 \cup \mathcal{O}_\infty$的一个点，其$(x, y)$坐标为$(a, b)$。根据这一约定，特别地，此类点 $P_{(a,b)}$ 的 x坐标a 非零。类似地，我们用 $Q_{(A,B)} \in \mathcal{H}$ 表示 $\mathcal{H}$ 上一个坐标为(A, B)的点，其(u, v)坐标为(A, B)，且不位于集合 $\mathcal{O}_0 \cup \mathcal{O}_\infty$中 $\mathcal{X}_3$ 的任何一点之上。集合 $\mathcal{O}_0 \cup \mathcal{O}_\infty$ 中的点在 $\mathcal{X}_3$的全自同构群作用下属于同一轨道。事实上，该轨道为:

$$\mathcal{O} := \mathcal{O}_0 \cup \mathcal{O}_\infty \cup \mathcal{O}_m, \tag{2.5}$$

其中 $\mathcal{O}_m := \{P_{(a,0)} \mid a^m + 1 = 0\}$. 现在先确立其中一些结果会比较方便，这样我们就能高效地确定该轨道上各点的魏尔斯特拉斯半群。在第 6 节中，我们将继续研究 $\mathcal{X}_3$ 上的自同构。

引理 2.6。自同构群 Aut$(\mathcal{X}_3)$ 包含一个阶为 $2(q+1)^2$的子群 G，它同构于一个阶为 $(q+1)^2/3$ 的阿贝尔群 A 与一个 6 阶对称群的半直积。更确切地说，

$$A := \{\theta_{\gamma,\delta}(x, y) = (\gamma x, \delta y) \mid \gamma^m = \delta^{q+1} = 1\},$$

而 6 阶对称群由对合 θ_2 和阶为 3 的自同构 θ_3 生成，后者定义为

$$\theta_2(x,y)=\left(\frac{1}{x},\frac{y}{x}\right)\ and\ \theta_3(x,y)=\left(\frac{y^3}{x^2},\frac{y}{x}\right).$$

证明。通过直接计算可验证，$\langle A、\ \theta_2、\ \theta_3\rangle$ 是$\mathcal{X}_3$的一个自同构群，也就是说，引理中给出的所有映射都保持方程 $y^{q+1}+x^m+x^{2m}=0$不变。由 θ_2 和 θ_3 生成的群 T 与 6 阶对称群同构，如$\theta_2\theta_3\theta_2=\theta_3^2$所示，这可通过直接计算得出。$\theta_2$ 和 θ_3 都正规化 A，因为直接计算表明$\theta_2\theta_{\gamma,\ \delta}\theta_2=\theta_{\gamma^{-1},\ \delta\gamma^{-1}}$ 以及$\theta_3\theta_{\gamma,\ \delta}\theta_3^{-1}=\theta_{\gamma\delta^{-3},\ \gamma\delta^{-2}}$. 因此，$T$ 正规化 $A_。$ 由于 T 和 A的交为平凡交，我们由此得到 $\langle A、\ T\rangle=A\rtimes T_。\square$

接下来，我们来确定 $\mathbb{F}_{q^2}(\mathcal{X}_3)$中若干初等函数的因子。我们将该因子记为$D_\infty$

$$D_\infty:=\sum_{j=1}^{m}P_\infty^j.$$

由于 $\mathcal{X}_3$ 是 $\mathbb{F}_{q^2}$-极大的，根据基本方程 [15, 第 xix 页 (ii)]，特别可知，对于所有 $i=1、\ .....、\ m$和 $P_{(a,b)}\in\mathcal{X}_3$，存在一个函数 $f_{P_{(a,b)},\ i}\in\mathbb{F}_{q^2}(\mathcal{X}_3)$，使得

$$(f_{P_{(a,b)},i})=qP_{(a,b)}+\Phi(P_{(a,b)})-(q+1)P_\infty^i. \tag{2.7}$$

这里 Φ 表示 $\mathbb{F}_{q^2}$-弗罗贝尼乌斯映射。对于 $\mathcal{X}_3$上的一个点 $P_{(a,b)}$，我们定义函数

$$x_a:=\frac{x-a}{a},$$

正如我们稍后将看到的，它最终成为 $P_{(a,b)}$的一个局部参数。此外，令 $t_{P(a,b)}$ 为 $\mathbb{F}_{q^2}(\mathcal{X}_3)$中的以下函数

$$t_{P_{(a,b)}}:=ma^{m-1}(2a^m+1)(x-a)+b^q(y-b), \tag{2.8}$$

并令 $Q_{(A,B)}$ 为 $\mathcal{H}$ 上位于 $P_{(a,b)}$之上的一个点。注意，$t_{P_{(a,b)}}$ 是与由方程 (2.1) 定义的平面曲线上 (a,b) 处的切线相关联的函数。

按方程 (2.5) 定义 $\mathcal{O}$，对于 $P_{(a,b)}\in\mathcal{X}_3(\overline{\mathbb{F}}_{q^2})\setminus\mathcal{O}$，我们定义

$$\alpha(P_{(a,b)}):=\frac{a^m}{1+a^m}=\frac{A^{q+1}}{1+A^{q+1}}. \tag{2.9}$$

由于 $1-\alpha(P_{(a,b)})=\frac{1}{1+a^m}$，特别是 $1-\alpha(P_{(a,b)})\neq 0$，我们可以在 $\mathbb{F}_{q^2}(\mathcal{X}_3)$ 中定义以下非零函数，后文将用到：

$$f_0:=\frac{3(1-\alpha(P_{(a,b)}))}{A^{q+1}}t_{P_{(a,b)}}=(1-\alpha(P_{(a,b)}))\left(\frac{(2A^{q+1}+1)}{A^3}(x-a)+\frac{3B^q}{A}(y-b)\right), \tag{2.10}$$

其中 $A^3 = a$ 和 $AB = b$。给定一个点 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$，以及位于 $P_{(a,b)}$ 之上的 $\mathcal{H}(\overline{\mathbb{F}}_{q^2})$ 中的一个点 $Q_{(A,B)}$，下面的命题描述了函数 x_a 和 f_0 在 $Q_{(A,B)}$ 处关于局部参数 $T := \frac{u-A}{A}$ 的局部幂级数展开。在本命题及本文余下部分中，每当我们写作 $f = g + O(T^n)$，意指 $v_{P_{(a,b)}}(f - g) \geq n$。

命题 2.11. 设 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$ 和 $Q_{(A,B)}$ 为 $\mathcal{H}$ 中位于 $P_{(a,b)}$上方的一个点。考虑函数 x_a、f_0 和 $T := \frac{u-A}{A}$，它是 $Q_{(A,B)}$处的一个局部参数。则 x_a 和 f_0 在 $Q_{(A,B)}$ 处关于 T 的局部幂级数展开为

$$\begin{aligned} x_a &= 3T + 3T^2 + T^3, \\ f_0 &= 3T^2 + (\alpha(P_{(a,b)}) + 1)T^3 + O(T^q), \end{aligned} \tag{2.12}$$

其中，$\alpha(P_{(a,b)})$如方程 (2.9) 中所定义。

证明. 为方便起见，在本证明中我们将简单地用 α 代替 $\alpha(P_{(a,b)})$。我们先计算函数 $x - a$ 和 $y - b$ 关于局部参数 $T := (u - A)/A$ 在 $Q_{(A,B)}$处的局部幂级数展开。我们有：

$$x_a = \frac{x-a}{a} = \frac{x-A^3}{A^3} = \frac{u^3-A^3}{A^3} = \frac{(u-A)^3 + 3A(u-A)^2 + 3A^2(u-A)}{A^3} = 3T + 3T^2 + T^3$$

and

$$\begin{aligned} y - b = uv - AB &= (u-A)(v-B) + B(u-A) + A(v-B) - AB + AB \\ &= A(v-B)(T+1) + ABT. \end{aligned} \tag{2.13}$$

此外，由 $v^{q+1} + u^{q+1} + 1 = 0$，我们得到

$$(u-A)^{q+1} - A^{q+1} + A^q u + Au^q + (v-B)^{q+1} - B^{q+1} + B^q v + Bv^q + 1 = 0$$

或者等价地

$$A^{q+1}T^{q+1} + (v-B)^{q+1} + A^{q+1}T^q + B(v-B)^q + A^{q+1}T + B^q(v-B) = 0$$

由此得到 $v - B = -\frac{A^{q+1}}{B^q}T + O(T^q)$。将其与方程 (2.13) 结合，可得

$$\begin{aligned} y - b = A(v-B)(T+1) + ABT &= -A\frac{A^{q+1}}{B^q}T(T+1) + ABT + O(T^q) \\ &= A\left(B - \frac{A^{q+1}}{B^q}\right)T - \frac{A^{q+2}}{B^q}T^2 + O(T^q). \end{aligned}$$

现在，我们还可以计算函数 f_0 在 $Q_{(A,B)}$处关于局部参数 T的局部幂级数展开。利用方程 (2.10) 以及先前计算出的 x_a 和 $y - b$的展开式，我们得到

$$\begin{aligned} f_0 &= (1-\alpha)(3\left(A^{q+1}+1\right)T^2 + \left(2A^{q+1}+1\right)T^3) + O(T^q) \\ &= 3T^2 + (\alpha+1)T^3 + O(T^q), \end{aligned}$$

其中，在最后一个等式中，我们利用了 $\alpha = A^{q+1}/(1+A^{q+1})$。 □

命题 2.14. 在上述记号下，函数 x、x_a、y、$y-b$ 和 f_0 在 $\mathbb{F}_{q^2}(\mathcal{X}_3)$ 中的主除子为：

$$(x_a) = \begin{cases} P_{(a,b)} + \sum_{\xi^{q+1}=1,\ \xi\neq 1} P_{(a,\xi b)} - 3D_\infty & if \quad a^m \neq -1, \\ (q+1)P_{(a,0)} - 3D_\infty & if \quad a^m = -1, \end{cases} \tag{2.15}$$

and

$$\begin{aligned} (x) &= 3\sum_{i=j}^{m} P_0^j - 3D_\infty, \\ (y) &= \sum_{j=1}^{m} P_0^j + \sum_{a^m+1=0} P_{(a,0)} - 2D_\infty, \\ (y-b) &= P_{(a,b)} + E_b - 2D_\infty, \end{aligned} \tag{2.16}$$

其中 $E_b \in \mathrm{Div}(\mathcal{X}_3)$ 是次数为 $2m-1$ 的有效除子。此外，若 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$ 且 $\alpha(P_{(a,b)}) \neq -1$，则 $P_{(a,b)} \notin \mathrm{supp}(E_b)$。进一步地，对于 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$，设 f_0 为方程 (2.10) 中定义的函数。那么

$$(f_0) = 2P_{(a,b)} + E_0 - 3D_\infty, \tag{2.17}$$

其中 $E_0 \in \mathrm{Div}(\mathcal{X}_3)$ 是满足 $P_{(a,b)} \notin \mathrm{supp}(E_0)$ 的有效除子。

证明. 为了求出 x_a 和 x 的因子，注意到 $\mathbb{F}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(x)$ 是一个次数为 $q+1$ 的库默尔扩张。于是，只需注意到 x^m+1 的零点在此扩张中完全分歧，而 x 的零点和极点的分歧指数为 3。由于 $y^{q+1} = -x^m(x^m+1)$，不会发生其他分歧。这个方程也给出了 y 的因子。尚不清楚 $y-b$ 的因子是否具有命题中所述的形式，但可能出现 $P_{(a,b)} \in \mathrm{supp}(E_b)$ 的情况。在这种情况下，多项式 $f(x) := x^{2m} + x^m + b^{q+1}$ 会有一个重根 a。由于 $3f'(x) = x^{m-1}(2x^m+1)$ 和 $P_{(a,b)} \notin \mathcal{O}$，这只有在 $2a^m+1=0$ 时才可能发生。利用 $\alpha(P_{(a,b)}) + 1 = (2a^m+1)/(a^m+1)$，即可推出关于 $y-b$ 的因子的结论。

最后，由方程 (2.12) 可知 $v_{P_{(a,b)}}(f_0) = 2$；又因为 f_0 是 x_a 和 $y-b$ 的线性组合，根据三角不等式，我们还可知 $v_{P_\infty^j}(f_0) = -3$，并且 f_0 在 P_∞^j、$1 \le j \le m$ 之外没有极点。因此，方程 (2.17) 得证。□

推论 2.18。设 $\mathcal{O}$ 为方程 (2.5) 中定义的集合。那么，$|\mathcal{O}| = q+1$ 和 $\mathcal{O}$ 是引理 2.6 中定义的自同构群 G 在其对 $\mathcal{X}_3$中各点的自然作用下的一个轨道。

证明。我们注意到，扩张 $\mathbb{F}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(x)$ 的伽罗瓦群，也就是由 $(x,y) \longmapsto (x,\delta y)$ 生成的循环群，其中 δ 是一个本原 $(q+1)$ 次单位根，它逐点固定集合 $\mathcal{O}_m$，同时在集合 $\mathcal{O}_0$ 和 $\mathcal{O}_\infty$上传递地作用。引理 2.6 中定义的群 A 在集合 $\mathcal{O}_m$ 上传递地作用，因为它将 x 映射到 γx，其中 $\gamma^m = 1$。自同构 θ_2 将 x 映射到 $1/x$，因此根据方程 (2.16)，它将 G作用下的两个轨道 $\mathcal{O}_0$和 $\mathcal{O}_\infty$ 合并。另一方面，自同构 θ_3 在$\mathcal{O}_0$、 $\mathcal{O}_\infty$ 和 $\mathcal{O}_m$上作用为一个 3 阶循环。这可由方程 (2.16)以及 θ_3 将 x 映射到y^3/x^2这一事实看出。因此，在 G的作用下，所考虑的三个集合都合并为一个轨道。□

注 2.19. 设 $\bar{a} \in \mathbb{F}_{q^2}$ 满足 $\bar{a}^m = -1$。那么，基本方程 [15, Page xix (ii)] 保证，对于任意点 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{X}_3(\mathbb{F}_{q^2})$，存在一个函数 $\phi_{P_{(a,b)}} \in \mathbb{F}_{q^2}(\mathcal{X}_3)$，使得

$$(\phi_{P_{(a,b)}}) = qP_{(a,b)} + \Phi(P_{(a,b)}) - (q+1)P_{(\bar{a},0)}.$$

因此，我们可以考虑 $\mathbb{F}_{q^2}(\mathcal{X}_3)$ 中的下列函数，它将在后文中发挥作用：

$$F_{P_{(a,b)}} := \phi_{P_{(a,b)}} \cdot x_{\bar{a}}. \tag{2.20}$$

由命题 2.14，$F_{P_{(a,b)}}$ 的主除子为

$$(F_{P_{(a,b)}}) = qP_{(a,b)} + \Phi(P_{(a,b)}) - 3\sum_{j=1}^{m} P_\infty^j.$$

2.2. 正则微分与间隙。本小节中，我们回顾一个关于曲线上正则微分与曲线上一点处间隙之间关系的基本结果。具体而言，在引理 2.22 中，我们计算 $\mathcal{X}_3$ 上的一个特定典范除子；在推论 2.23 中，我们说明如何利用它确定曲线上某些点处的间隙。尤其是，推论 2.23 对第 5 节中的结果至关重要。

命题 2.21. [26, 推论 14.2.5] 设 $\mathcal{X}$ 是定义在域 $\mathbb{K}$上的亏格为 g 的代数曲线。设 P是 $\mathcal{X}$上的一个点，w是 $\mathcal{X}$上的一个正则微分。那么 $v_P(w) + 1$是 P处的一个间隙。

引理 2.22. 因子 $(q-2)D_\infty$ 是典范的。更确切地说

$$\left(\frac{ydx}{x(x^m+1)}\right) = (q-2)D_\infty.$$

证明。由 $\mathbb{F}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(x)$ 是一个次数为 $q+1$ 的库默尔扩张这一事实，可直接得出结果。事实上，正如命题 2.14 的证明中所观察到的，x^m+1 在 $\mathbb{F}_{q^2}(x)$ 中的零点在该扩张中完全分歧，x 的零点和极点的分歧指数为 3，而不是 $x^m(x^m+1)$ 零点的点则完全分裂。

因此，我们有

$$(dx) = 2\sum_{j=1}^{m} P_0^j + q \sum_{a^m+1=0} P_{(a,0)} - 4D_\infty$$

由命题 2.14 的直接计算即可得出结论。 □

推论 2.23. 设 P 是 $\mathcal{X}_3$ 上不属于 $\mathcal{O}_\infty$ 的一个点。那么对于任意 $h \in L((q-2)D_\infty)$，整数 $v_P(h)+1$ 是 P 处魏尔斯特拉斯半群的一个间隙。

证明. 根据命题 2.21 和引理 2.22，只需考虑正则微分

$$w := \frac{hydx}{x(x^m+1)}.$$

由于 $v_P(w) = v_P(h)$，推论得证。 □

3. Two families of functions in $\mathbb{F}_{q^2}(\mathcal{X}_3)$

本节旨在证明定理 3.12 和定理 3.19。这两个定理在曲线的某些点引入了两个具有给定消失阶的 $\mathbb{F}_{q^2}(\mathcal{X}_3)$ 函数族。这些函数对于计算 $\mathcal{X}_3 \setminus \mathcal{O}$ 各点处的魏尔斯特拉斯半群至关重要。

我们先给出以下定义，其中引入了一些函数，便于在定理 3.12 和定理 3.19 的证明中使用。

定义 3.1. 设 $i \in \mathbb{Z}$。此外，设 $\mathbb{F}$ 是一个特征不为三的域，并假设它包含一个本原三次单位根，记作 ζ_3。于是我们在 $\mathbb{F}(s)$ 中定义以下有理函数:

$$\mathcal{P}_i(s) := \frac{(s+\zeta_3)^{3i} - (s+\zeta_3^2)^{3i}}{3(\zeta_3-\zeta_3^2)s(s-1)}$$

and

$$\mathcal{Q}_i(s) := \frac{\left(\frac{1-\zeta_3}{3}\right)(s+\zeta_3)^{3i-1} + \left(\frac{1-\zeta_3^2}{3}\right)(s+\zeta_3^2)^{3i-1}}{s-1}.$$

严格来说，注意到并不一定要假设域 $\mathbb{F}$ 包含一个本原三次单位根。若不包含，上述定义在更大的域 $\mathbb{F}(\zeta_3)$ 上仍有意义；但实际上，可以利用初等伽罗瓦理论证明，$\mathcal{P}_i(s)$ 和 $\mathcal{Q}_i(s)$ 都属于 $\mathbb{F}(s)$。

例 3.2. 假设 $\mathbb{F} = \mathbb{Q}$。则 $\mathcal{P}_0(s) = 0$, $\mathcal{P}_1(s) = 1$, $\mathcal{P}_2(s) = 2s^3 - 3s^2 - 3s + 2$且 $\mathcal{P}_3(s) = 3s^6 - 9s^5 - 9s^4 + 33s^3 - 9s^2 - 9s + 3$。此外，$\mathcal{Q}_1(s) = s+1$, $\mathcal{Q}_2(s) = s^4+s^3-9s^2+s+1$, $\mathcal{Q}_3(s) = s^7+s^6-27s^5+29s^4+29s^3-27s^2+s+1$，且 $\mathcal{Q}_0(s) = (s^2-s+1)^{-1}$。

事实上，正如本例所示，对于正值的 i，有理函数 $\mathcal{P}_i(s)$和 $\mathcal{Q}_j(s)$都是关于 s的多项式。我们将在下面的引理中进一步探讨这一点。

引理 3.3. 设 $i \in \mathbb{Z}_{>0}$。那么 $\mathcal{P}_i(s)$是一个次数至多为 $3i-3$的非零多项式，而 $\mathcal{Q}_i(s)$是一个次数为 $3i-2$的非零多项式。

证明。容易看出，对于任意 $i \in \mathbb{Z}_{>0}$，多项式 $\tilde{\mathcal{P}}_i(s) := (s+\zeta_3)^{3i} - (s+\zeta_3^2)^{3i}$的次数至多为 $3i-1$。它不是零多项式，因为如果将 s 替换为 $-\zeta_3$，则得到

$$\tilde{\mathcal{P}}_i(-\zeta_3) = 0^{3i} - (-\zeta_3+\zeta_3^2)^{3i} = (-1+\zeta_3)^{3i}, \tag{3.4}$$

该式不为零，因为 $\zeta_3 \neq 1$. 这里用到了域 $\mathbb{F}$ 的特征不为三。˜容易看出 $\mathcal{P}_i(0) = 0$，而

$$\tilde{\mathcal{P}}_i(1) = (1+\zeta_3)^{3i} - (1+\zeta_3^2)^{3i} = (-\zeta_3^2)^{3i} - (-\zeta_3)^{3i} = (-1)^i - (-1)^i = 0.$$

我们可以得出，$\mathcal{P}_i(s)$ 是一个次数至多为 $3i-3$ 的多项式。同样，多项式 $\tilde{\mathcal{Q}}_i(s) := \frac{1-\zeta_3}{3}(s+\zeta_3)^{3i-1} + \frac{1-\zeta_3^2}{3}(s+\zeta_3^2)^{3i-1}$ 是一个次数为 $3i-1$ 且以 1 为根的多项式。因此，$\mathcal{Q}_i(s)$ 是一个次数为 $3i-2$. □的多项式

不难看出，多项式 $\mathcal{P}_i(s)$ 中 s^{3i-3} 的系数等于 $3i(\zeta_3-\zeta_3^2)$。因此，如果域 $\mathbb{F}$ 的特征为零，或不整除 i（我们已假设该特征不等于三），那么 $\mathcal{P}_i(s)$ 的次数恰好为 $3i-3$。由于我们将在有限域 $\mathbb{F}_{q^2}$ 上进行研究，其中 $q \equiv 2$ (模 3)，因此完全可能出现 $\deg\ \mathcal{P}_i(s) < 3i-3$.

下面的引理给出了刚刚介绍的有理函数之间的一个关系，该关系稍后将会派上用场。

引理 3.5. 设 i、j、$\ell \in \mathbb{Z}$。则

$$\mathcal{P}_i(s)\mathcal{P}_{\ell+j}(s) - \mathcal{P}_j(s)\mathcal{P}_{\ell+i}(s) = (s^2-s+1)^{3j}\mathcal{P}_{i-j}(s)\mathcal{P}_\ell(s) \tag{3.6}$$

and

$$\mathcal{P}_i(s)\mathcal{Q}_{\ell+j}(s) - \mathcal{P}_j(s)\mathcal{Q}_{\ell+i}(s) = (s^2-s+1)^{3j}\mathcal{P}_{i-j}(s)\mathcal{Q}_\ell(s). \tag{3.7}$$

证明。为方便起见，在本证明中，我们将用 $\mathcal{P}_i$ 和 $\mathcal{Q}_j$ 分别代替 $\mathcal{P}_i(s)$ 和 $\mathcal{Q}_i(s)$。我们只证明第二个恒等式，因为第一个恒等式的证明方法非常相似，且中间表达式更简单。首先，根据定义 3.1 并写出 $S_1 = s+\zeta_3$、$S_2 = s+\zeta_3^2$，经直接计算可得

$$3(\zeta_3-\zeta_3^2)s(s-1)^2\mathcal{P}_i\mathcal{Q}_{\ell+j} = \frac{1-\zeta_3}{3}S_1^{3i+3j+3\ell-1} + \frac{1-\zeta_3^2}{3}S_1^{3i}S_2^{3j+3\ell-1} - \frac{1-\zeta_3}{3}S_2^{3i}S_1^{3j+3\ell-1} - \frac{1-\zeta_3^2}{3}S_2^{3i+3j+3\ell-1}$$

and

$$3(\zeta_3-\zeta_3^2)s(s-1)^2\mathcal{P}_j\mathcal{Q}_{\ell+i} = \frac{1-\zeta_3}{3}S_1^{3i+3j+3\ell-1} + \frac{1-\zeta_3^2}{3}S_1^{3j}S_2^{3i+3\ell-1} - \frac{1-\zeta_3}{3}S_2^{3j}S_1^{3i+3\ell-1} - \frac{1-\zeta_3^2}{3}S_2^{3i+3j+3\ell-1}.$$

因此

$$3(\zeta_3-\zeta_3^2)s(s-1)^2(\mathcal{P}_i\mathcal{Q}_{\ell+j}-\mathcal{P}_j\mathcal{Q}_{\ell+i})=$$
$$(S_1S_2)^{3j}\left(\frac{1-\zeta_3}{3}(S_1^{3\ell+3i-3j-1}-S_2^{3i-3j}S_1^{3\ell-1})+\frac{1-\zeta_3^2}{3}(S_1^{3i-3j}S_2^{3\ell-1}-S_2^{3\ell+3i-3j-1})\right)$$
$$=(S_1S_2)^{3j}(S_1^{3(i-j)}-S_2^{3(i-j)})\left(\frac{1-\zeta_3}{3}S_1^{3\ell-1}+\frac{1-\zeta_3^2}{3}S_2^{3\ell-1}\right)$$
$$=3(\zeta_3-\zeta_3^2)s(s-1)^2(s^2-s+1)^{3j}\mathcal{P}_{i-j}\mathcal{Q}_\ell.$$

对于最后一个等式，请注意 $S_1S_2=s^2-s+1$。 □

注3.8. 对于任意 $i\in\mathbb{Z}_{>0}$，多项式 $\mathcal{P}_i(s)$ 和 $\mathcal{Q}_i(s)$ 没有公共根。事实上，当 $i=1$ 时这一点显然成立，因为 $\mathcal{P}_1(s)=1$。若 $i\geq 2$，将引理 3.5 应用于 $\ell=0$ and$j=i-1$，可得 $\mathcal{P}_i(s)\mathcal{Q}_{i-1}(s)-\mathcal{P}_{i-1}(s)\mathcal{Q}_i(s)=(s^2-s+1)^{3i-4}$。这里我们用到了$\mathcal{Q}_0(s)=(s^2-s+1)^{-1}$. 因此，$\mathcal{P}_i(s)$ 和 $\mathcal{Q}_i(s)$ 唯一可能的公共根是$-\zeta_3$或 $-\zeta_3^2$，即 s^2-s+1 的根。然而，方程 (3.4) 表明 $\mathcal{P}_i(-\zeta_3)\neq 0$，类似地可知 $\mathcal{P}_i(-\zeta_3^2)\neq 0$。

注记 3.9. 令 $\mathbb{F}=\overline{\mathbb{F}}_{q^2}$ 为 $\mathbb{F}_{q^2}$. 的代数闭包。那么对于任意 $\alpha\in\mathbb{F}\setminus\{0,1,-\zeta_3,-\zeta_3^2\}$，存在 $i>0$，使得 $\mathcal{P}_{i+1}(\alpha)=0$。事实上，对于这样的 α，有 $\mathcal{P}_{i+1}(\alpha)=0$ 当且仅当 $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{3i+3}=1$。由于 $\mathbb{F}$ 中任意非零元素都有有限乘法阶，故 i 的存在性得证。此外，由于 $\mathcal{P}_1(s)=1$，我们可知 $i>0$。

这一注记引出了以下定义：

定义 3.10. 令 $\alpha\in\overline{\mathbb{F}}_{q^2}\setminus\{0,1,-\zeta_3,-\zeta_3^2\}$。那么我们将 α 的 $\mathcal{P}$-阶定义为满足 $\mathcal{P}_{i+1}(\alpha)=0$ 的最小正整数 i。

稍后我们将在 $\alpha=\alpha(P_{(a,b)})$ 的情形下应用 $\mathcal{P}$-阶的概念。下面的引理为这一背景提供了首批信息。

引理 3.11。设 i 为正整数。满足$\alpha(P_{(a,b)})$ 的 $P_{(a,b)}\in\mathcal{X}_3(\overline{\mathbb{F}}_{q^2})\setminus\mathcal{O}$ 的个数，且其 $\mathcal{P}$-阶为 i，等于 $(q+1)^2\varphi(i+1)$，若 $\gcd(i+1,p)=1$；否则等于 0。这里，$\varphi(\cdot)$ 表示欧拉商函数。此外，$P_{(a,b)}\in\mathcal{X}_3(\overline{\mathbb{F}}_{q^2})\setminus\mathcal{O}$ 是 $\mathbb{F}_{q^2}$-有理的，当且仅当 $\alpha(P_{(a,b)})^2-\alpha(P_{(a,b)})+1=0$，或者其 $\mathcal{P}$-阶 i 满足 $i+1$ 整除 m。

证明。如果 $\alpha:=\alpha(P_{(a,b)})$ 对某个正整数 i 具有 $\mathcal{P}$-阶 i，那么 $\alpha\notin\{0,1,-\zeta_3,-\zeta_3^2\}$ 和 $P_{(a,b)}\notin\mathcal{O}$。正如注记 3.9 中所观察到的，$\mathcal{P}_{i+1}(\alpha)=0$ 当且仅当 $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{3i+3}=1$。如果特征 p 整除 $i+1$，则有 $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{3(i+1)/p}=1$，这意味着对于某个严格小于 $i+1$ 的 j，$\mathcal{P}_j(\alpha)=0$。根据 $\mathcal{P}$- 阶的定义，这是不可能的。如果 $\gcd(p,i+1)=1$，则具有 $\mathcal{P}$- 阶 i 的 α 恰好是满足 $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^3$ 为一个本原 $(i+1)$- 次单位根的那些。因此，具有 $\mathcal{P}$- 阶 i 的 α 有 $3\varphi(i+1)$ 个。由于 $\alpha=a^m/(1+a^m)$ 且 $\alpha\notin\{0,1\}$，对于每个这样的 α，有

m 个关于 a 的不同可能性。由于 $P_{(a,b)} \notin \mathcal{O}$，对于每个这样的 a，关于 b 有 $q+1$ 个不同可能性。这就证明了该引理的第一部分。

现在假设 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$ 是 $\mathbb{F}_{q^2}$-有理的，且 $\alpha^2-\alpha+1 \neq 0$。首先，我们声称在这种情况下 $\alpha \in \mathbb{F}_{q^2}$。事实上，由于 $a, b \in \mathbb{F}_{q^2}$，我们得到 $a^{3m} = a^{q+1} \in \mathbb{F}_q$ 和 $a^{2m}+a^m = -b^{q+1} \in \mathbb{F}_{q^2}$。但此时 $a^m = (a^{3m}+a^{2m}+a^m)/(a^{2m}+a^m+1) \in \mathbb{F}_{q^2}$。这里我们用到了 $a^{2m}+a^m+1 \neq 0$，这可由假设推出，即 $\alpha^2-\alpha+1 \neq 0$. 现在 $a^m \in \mathbb{F}_q$，意味着 $\alpha = a^m/(1+a^m) \in \mathbb{F}_{q^2}$。特别地，$\alpha^q = \alpha$。这意味着

$$\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^q = \frac{\alpha^q+\zeta_3^q}{\alpha^q+\zeta_3^{2q}} = \frac{\alpha+\zeta_3^2}{\alpha+\zeta_3},$$

这恰好是 $\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}$ 的逆。因此 $\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{3m} = \left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{q+1} = 1$。这表明 $i+1$ 整除 m。

反过来，若 $\alpha^2-\alpha+1=0$，则 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$ 满足 $a^{2m}+a^m+1=0$，进而推出 $b^{q+1}=1$。因此 $a, b \in \mathbb{F}_{q^2}$。若 $\alpha^2-\alpha+1 \neq 0$ 且 $i+1$ 整除 m，则 $3(i+1)$ 整除 $q+1$，并且 $\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{3(i+1)} = 1.$。因此 $\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{q+1} = 1$；清除分母后，这相当于方程 $(\alpha+\zeta_3)^{q+1} - (\alpha+\zeta_3^2)^{q+1} = 0$。这是一个关于 α 的次数为 q 的多项式，我们已经看到，该方程对所有 $\alpha \in \mathbb{F}_q$ 都成立。由此可得 $\alpha \in \mathbb{F}_{q^2}$。但此时 $a^m \in \mathbb{F}_q$，这意味着 $b^{q+1} = -a^{2m}-a^m \in \mathbb{F}_{q^2}$。由此我们也得出，在这种情况下，$P_{(a,b)}$ 是 $\mathcal{X}_3$ 的一个 $\mathbb{F}_{q^2}$-有理点。□

接下来，我们使用多项式 $\mathcal{P}_j(s)$ 和 $\mathcal{Q}_j(s)$ 来研究某些函数是否存在；这些函数将在稍后确定点 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$ 处的间隙时发挥作用。

定理 3.12. 设 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$，并假设 $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 \neq 0$。此外，设 i 为 $\alpha(P_{(a,b)})$ 的 $\mathcal{P}$ 阶。若 $i \leq m-2$，则存在一个函数 $f_i \in L((3i+3)D_\infty)$，使得 $v_{P_{(a,b)}}(f_i) = 3i+3$。此外，对于每个满足 $0 \leq j \leq \min\{i-1, m-2\}$ 的 $j \in \mathbb{Z}$，都存在一个函数 $f_j \in L((3j+3)D_\infty)$，使得 $v_{P_{(a,b)}}(f_j) = 3j+2$。

证明。在整个证明过程中，我们简化记号，用 α 代替 $\alpha(P_{(a,b)})$。同理，我们将写作 $\mathcal{P}_j$ 和 $\mathcal{Q}_j$，而不写 $\mathcal{P}_j(\alpha)$ 和 $\mathcal{Q}_j(\alpha)$。

设 $Q_{(A,B)}$ 是位于 $P_{(a,b)}$ 之上的 $\mathcal{H}$ 中的一个点，并设 $T := \frac{u-A}{A}$，它是 $Q_{(A,B)}$ 处的一个局部参数。对于每个满足 $0 \leq j \leq i$ 的 j，我们断言，存在一个函数 $f_j \in L((3j+3)D_\infty)$，使得 f_j 在 $Q_{(A,B)}$ 处相对于局部参数 T 的局部幂级数展开为

$$f_j = 3\mathcal{P}_{j+1}T^{3j+2} + \mathcal{Q}_{j+1}T^{3j+3} + O(T^q). \tag{3.13}$$

注意，根据 $\mathcal{P}$-阶的定义，这将意味着

$$f_i = \mathcal{Q}_{i+1}T^{3i+3} + O(T^q). \tag{3.14}$$

这足以证明该定理，因为正如注 2.4 中所观察到的，$v_{Q_{(A,B)}}(f_j) = v_{P_{(a,b)}}(f_j)$，且对于所有正在考虑的 j，$3j+3 < q$。

首先注意，对于 $j = 0$，我们可以取 f_0 为方程 (2.10) 中定义的函数，其关于 T 的局部幂级数展开已在方程 (2.12) 中计算得出。为证明关于 $j = 1$ 的结果，我们定义

$$f_1 := -9x_a^2 + 27f_0 - 3(\alpha-5)x_a f_0 + (\alpha^2-\alpha-5)f_0^2.$$

初等计算表明，f_1 在 $Q_{(A,B)}$ 处关于 T 的局部幂级数展开恰为

$$f_1 = 3\mathcal{P}_2 T^5 + \mathcal{Q}_2 T^6 + O(T^q).$$

对于 $j = 2$，我们定义

$$f_2 := (\alpha+1)^{-3}\left(-27\mathcal{P}_2 f_1 + 3\mathcal{P}_2^2 f_0^2 x_a - 3\mathcal{P}_2(\alpha^4+\alpha^3-4\alpha^2-4\alpha+3)f_0^3\right) + (7\alpha^2-16\alpha+7)f_1 f_0.$$

经过稍显冗长但初等的计算可知，f_2 的局部幂级数展开为

$$f_2 = 3\mathcal{P}_3 T^5 + \mathcal{Q}_3 T^6 + O(T^q).$$

对于 $3 \le j \le i$，现在假设 f_{j-1} 和 f_{j-2} 具有方程 (3.13) 中所述的形式，并按以下方式归纳构造其余函数 f_j，定义：

$$f_j := -\frac{\mathcal{P}_j f_{j-2} f_1 - \mathcal{P}_2 \mathcal{P}_{j-1} f_{j-1} f_0}{(\alpha^2-\alpha+1)^2 \mathcal{P}_{j-2}}.$$

选择函数 $f_{j-2}f_1$ 和 $f_{j-1}f_0$ 的思路在于，它们在 $Q_{(A,B)}$ 处的消失阶均为$3j+1$。因此，它们的适当线性组合将具有至少为$3j+2$的消失阶。此外，由于 $f_{j-2}f_1$ 和 $f_{j-1}f_0$ 属于 $L((3j+3)D_\infty)$，它们的线性组合也属于其中。因此，我们只需证明

$$\mathcal{P}_j f_{j-2} f_1 - \mathcal{P}_2 \mathcal{P}_{j-1} f_{j-1} f_0 = -(\alpha^2-\alpha+1)^2 \mathcal{P}_{j-2}\left(3\mathcal{P}_{j+1} T^{3j+2} + \mathcal{Q}_{j+1} T^{3j+3} + O(T^q)\right).$$

函数 $\mathcal{P}_j f_{j-2} f_1 - \mathcal{P}_2 \mathcal{P}_{j-1} f_{j-1} f_0$ 关于 T 的局部幂级数展开可由函数 $f_{j-2}f_1$ 和 $f_{j-1}f_0$的展开式得到，具体如下：

$$\begin{aligned} f_{j-2}f_1 &= \left(3\mathcal{P}_{j-1}T^{3j-4} + \mathcal{Q}_{j-1}T^{3j-3} + O(T^q)\right)\left(3\mathcal{P}_2 T^5 + \mathcal{Q}_2 T^6 + O(T^q)\right) \\ &= 9\mathcal{P}_2\mathcal{P}_{j-1}T^{3j+1} + (3\mathcal{P}_{j-1}\mathcal{Q}_2 + 3\mathcal{P}_2\mathcal{Q}_{j-1})T^{3j+2} + \mathcal{Q}_2\mathcal{Q}_{j-1}T^{3j+3} + O(T^q), \\ f_{j-1}f_0 &= \left(3\mathcal{P}_j T^{3j-1} + \mathcal{Q}_j T^{3j} + O(T^q)\right)\left(3T^2 + \mathcal{Q}_1 T^3 + O(T^q)\right) \\ &= 9\mathcal{P}_j T^{3j+1} + (3\mathcal{P}_j\mathcal{Q}_1 + 3\mathcal{Q}_j)T^{3j+2} + \mathcal{Q}_1\mathcal{Q}_j T^{3j+3} + O(T^q). \end{aligned}$$

因此，我们有

$$\mathcal{P}_j f_{j-2} f_1 - \mathcal{P}_2 \mathcal{P}_{j-1} f_{j-1} f_0 = 3(\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_2 + \mathcal{P}_2\mathcal{P}_j\mathcal{Q}_{j-1} - \mathcal{P}_2\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_1 - \mathcal{P}_2\mathcal{P}_{j-1}\mathcal{Q}_j)T^{3j+2} + \left(\mathcal{P}_j\mathcal{Q}_{j-1}\mathcal{Q}_2 - \mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1\right)T^{3j+3} + O(T^q).$$

因此，我们还需证明以下两个等式：

$$3\left(\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_2+\mathcal{P}_2\mathcal{P}_j\mathcal{Q}_{j-1}-\mathcal{P}_2\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_1-\mathcal{P}_2\mathcal{P}_{j-1}\mathcal{Q}_j\right)=-3(\alpha^2-\alpha+1)^2\mathcal{P}_{j-2}\mathcal{P}_{j+1} \tag{3.15}$$

and

$$\mathcal{P}_j\mathcal{Q}_{j-1}\mathcal{Q}_2-\mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1=-(\alpha^2-\alpha+1)^2\mathcal{P}_{j-2}\mathcal{Q}_{j+1}. \tag{3.16}$$

利用引理 3.5 可以方便地完成此事。事实上，先考虑第一个方程，并使用恒等式 (3.7)，(3.15) 得到

$$\mathcal{P}_j\mathcal{Q}_2-\mathcal{P}_2\mathcal{Q}_j=\mathcal{P}_{j-2}\mathcal{Q}_0\cdot(s^2-s+1)^6,$$

也就是说，指标为 $(j, 2, 0)$（按引理 3.5 陈述中的顺序列出）。于是，我们得到

$$\begin{aligned}\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_2-\mathcal{P}_2\mathcal{P}_{j-1}\mathcal{Q}_j&=\mathcal{P}_{j-1}(\mathcal{P}_j\mathcal{Q}_2-\mathcal{P}_2\mathcal{Q}_j)\\&=\mathcal{P}_{j-1}\cdot(\alpha^2-\alpha+1)^5\mathcal{P}_{j-2}.\end{aligned} \tag{3.17}$$

通过使用 方程 (3.7)，这次取指标 $(j-1, 1, 0)$，我们还可以将其改写为

$$\begin{aligned}\mathcal{P}_2\mathcal{P}_j\mathcal{Q}_{j-1}-\mathcal{P}_2\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_1&=\mathcal{P}_2\mathcal{P}_j\mathcal{Q}_{j-1}\mathcal{P}_1-\mathcal{P}_2\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_1\\&=-\mathcal{P}_2\mathcal{P}_j(\mathcal{P}_{j-1}\mathcal{Q}_1-\mathcal{P}_1\mathcal{Q}_{j-1})\\&=-\mathcal{P}_2\mathcal{P}_j\cdot(\alpha^2-\alpha+1)^2\mathcal{P}_{j-2}.\end{aligned} \tag{3.18}$$

然后，由方程 (3.17) 和 (3.18)，可知方程 (3.15) 等价于

$$\mathcal{P}_{j-1}\cdot(\alpha^2-\alpha+1)^5\mathcal{P}_{j-2}-\mathcal{P}_2\mathcal{P}_j\cdot(\alpha^2-\alpha+1)^2\mathcal{P}_{j-2}=-(\alpha^2-\alpha+1)^2\mathcal{P}_{j-2}\mathcal{P}_{j+1}.$$

将等式两边同时除以因子 $(\alpha^2-\alpha+1)^2\mathcal{P}_{j-2}$，并整理各项，可得

$$\mathcal{P}_{j-1}\cdot(\alpha^2-\alpha+1)^3=\mathcal{P}_2\mathcal{P}_j-\mathcal{P}_{j+1},$$

由引理 3.5 可知该式成立，因为它恰好是指标为 $(j, 1, 1)$ 的恒等式 (3.6)。

为了 证明方程 (3.16)，我们可以采用类似的方法。事实上，我们有 :

$$\begin{aligned}\mathcal{P}_j\mathcal{Q}_{j-1}\mathcal{Q}_2-\mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1&=(\mathcal{P}_j\mathcal{Q}_2-\mathcal{P}_2\mathcal{Q}_j+\mathcal{P}_2\mathcal{Q}_j)\mathcal{Q}_{j-1}-\mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1\\&=\left(\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^5+\mathcal{P}_2\mathcal{Q}_j\right)\mathcal{Q}_{j-1}-\mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1,\end{aligned}$$

其中 th 最后一个等式由带有指标 $(j, 2, 0)$ 的方程 (3.7) 得出。此外 er,

$$\begin{aligned}&\left(\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^5+\mathcal{P}_2\mathcal{Q}_j\right)\mathcal{Q}_{j-1}-\mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1=\\&\qquad\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^5\mathcal{Q}_{j-1}-\mathcal{P}_2\mathcal{Q}_j\left(\mathcal{P}_{j-1}\mathcal{Q}_1-\mathcal{P}_1\mathcal{Q}_{j-1}\right)=\\&\qquad\qquad\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^5\mathcal{Q}_{j-1}-\mathcal{P}_2\mathcal{Q}_j\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^2,\end{aligned}$$

其中，最后一个等式由带有指标 $(j-1,1,0)$ 的方程 (3.7) 得出。最后，再次利用带有指标 $(2,1,j-1)$ 的方程 (3.7)，可得

$$\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^5\mathcal{Q}_{j-1}-\mathcal{P}_2\mathcal{Q}_j\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^2=$$
$$-\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^2\left(\mathcal{P}_2\mathcal{Q}_j-\mathcal{Q}_{j-1}\cdot(\alpha^2-\alpha+1)^3\mathcal{P}_1\right)=-\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^2\mathcal{Q}_{j+1},$$

由此证明方程 (3.16)。

由此可直接得到方程 (3.13)；而观察到$\mathcal{P}_{i+1}=0$ 依假设成立，且 $\mathcal{Q}_{i+1}\neq 0$ 依注3.8成立，即可得到方程 (3.14)。由于我们已注意到，按构造，对于 $0\le j\le i$ 中所有的 j，$f_j\in L((3j+3)D_\infty)$，因此定理的证明就此完成。□

当 $\alpha^2-\alpha+1=0$ 时，定理的证明方法不再适用；不过，类似的方法仍然可行，这一点将在下面结果的证明中显现。回想一下，若 $\alpha^2-\alpha+1=0$，则对所有 $i\in\mathbb{Z}_{>0}$，α 都不是任何 $\mathcal{P}_i$ 的根。

定理 3.19. 设 $P_{(a,b)}$ 是 $\mathcal{X}_3$ 上的一个点，满足 $\alpha(P_{(a,b)})^2-\alpha(P_{(a,b)})+1=0$。那么，对于每个满足 $i\le m-2$ 的正整数 i，存在一个函数 $g_i\in L((3i+3)D_\infty)$，使得 $v_{P_{(a,b)}}(g_i)=3i+2$。

证明。与前面一样，在本证明中，我们用 α 代替 $\alpha(P_{(a,b)})$，并用 $\mathcal{P}_j$、$\mathcal{Q}_j$ 代替 $\mathcal{P}_j(\alpha)$、$\mathcal{Q}_j(\alpha)$。对于每个 $i\in\mathbb{Z}_{\ge 0}$，我们声称存在一个函数 $g_i\in L((3i+3)D_\infty)$，使得 g_i 在 $Q_{(A,B)}$ 处关于局部参数 T 的局部幂级数展开为：

$$g_i=3T^{3i+2}+(\alpha+1)T^{3i+3}+O(T^q) \tag{3.20}$$

记前一定理中构造的函数为 f_0 和 f_1，我们看到 $g_0=f_0$，而 $g_1=(2\alpha-1)f_1/9$，因为

$$(2\alpha-1)3\mathcal{P}_2\equiv 27 \pmod{\alpha^2-\alpha+1}$$

and

$$(2\alpha-1)\mathcal{Q}_2\equiv 9\alpha+9 \pmod{\alpha^2-\alpha+1}.$$

对于 $i\ge 2$，我们现在假设 g_{i-1} 和 g_{i-2} 具有方程 (3.20) 中所述的形式，并通过对下列函数作适当的线性组合，归纳地构造其余函数 g_i

$$g_{i-1},\quad g_{i-2}\cdot g_0\cdot x_a,\quad g_{i-2}\cdot g_0^2\quad\text{and}\quad g_{i-1}\cdot g_0.$$

选择这四个函数的原因在于，它们在 $Q_{(A,B)}$ 处的消失阶分别为 $3i-1$、$3i-1$、$3i$ 和 $3i+1$。因此，对它们作适当的线性组合，其消失阶至少为 $3i+2$。此外，由于这四个函数都属于 $L((3i+3)D_\infty)$，它们的任意线性组合也属于该空间。

更具体地说，如果我们令

$$g_i:=(6\alpha-3)g_{i-1}-\frac{2\alpha-1}{3}g_{i-2}g_0x_a+\frac{3\alpha-2}{3}g_{i-2}g_0^2-(\alpha-2)g_{i-1}g_0,$$

那么通过直接计算可知，方程 (3.20) 得到满足。 □

4. Weierstrass semigroups at the $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}_3$

本节中，我们计算 $\mathbb{F}_{q^2}$ 上所有 $\mathcal{X}_3$-有理点处的魏尔斯特拉斯半群。我们先确定集合 $\mathcal{O}$ 中各点处的半群，然后继续研究 $\mathcal{X}_3$ 上所有其他 $\mathbb{F}_{q^2}$- 有理点。我们假设 q 至少为 5，因此$m \geq 2$。如果 $q = 2$，则曲线 $\mathcal{X}_3$ 是一条椭圆曲线，因此在这种情况下，所有魏尔斯特拉斯半群都只是$\{0\} \cup \mathbb{Z}_{\geq 2}$。

注4.1. 根据基本方程（[15, 第 xix 页（ii）]）以及 [15, 命题 10.9]，，众所周知，在一条$\mathbb{F}_{q^2}$-极大曲线的每个 $\mathbb{F}_{q^2}$-有理点处， q 和 $q+1$ 都是非间隙。然而，在定理4.2和引理4.3中，我们针对 $\mathcal{X}_3$ 的具体情形再次证明这一事实，并通过一些简单的显式计算加以说明。

4.1. 点 $P \in \mathcal{O}$ 处的魏尔斯特拉斯半群。

定理4.2. 设 $P \in \mathcal{O}$。则 $H(P) = \langle q-2, q, q+1 \rangle$.

证明. 我们将证明

$$H(P_{(a,0)}) = \langle q-2, q, q+1 \rangle$$

对于 $P_{(a,0)} \in \mathcal{O}$ 一个满足 $a^m + 1 = 0$ 的点，因此结果将随之得出，因为根据推论 2.18，$\mathcal{O}$ 包含在 Aut($\mathcal{X}_3$) 的一个轨道中，且同一轨道中的所有点具有相同的魏尔斯特拉斯半群。

我们先证明半群 $H := \langle q-2, q, q+1 \rangle$，也就是说，由 $q-2, q$ 和 $q+1$ 生成的半群，包含于 $H(P_{(a,0)})$ 中。命题 2.14 表明，这些函数

$$\frac{1}{x-a}, \quad \frac{y}{x-a}, \quad \text{and} \quad \frac{y^3}{x(x-a)}$$

在 $\mathbb{F}_{q^2}(\mathcal{X}_3)$ 中只有一个位于 $P_{(a,0)}$ 的极点，其阶分别为 $q+1, q$ 和 $q-2$。这表明 $q-2, q, q+1 \in H(P_{(a,0)})$，从而证明了 $H \subseteq H(P_{(a,0)})$。

因此，要完成定理的证明，只需证明半群 H中的间隙数（也称为 H的亏格）等于 $g(\mathcal{X}_3)$。为此，注意到半群 H 是望远镜半群，因为序列$(a_1, a_2, a_3) := (q-2, q+1, q)$是望远镜序列。关于望远镜半群的简要讨论，参见例如 [16, 第5节4]。定义 $d_0 = 0$, $d_1 = q-2$, $d_2 =$最大公因数$(q-2, q+1) = 3$，以及 $d_3 =$最大公因数$(q-2, q, q+1) = 1$，根据 [16,命题5.35] ， H 的亏格为

$$g(H) = \frac{1}{2}\left(1 + \sum_{i=1}^{3}\left(\frac{d_{i-1}}{d_i} - 1\right)a_i\right) = g(\mathcal{X}_3).$$

□

4.2. $\mathcal{X}_3(\mathbb{F}_{q^2}) \setminus \mathcal{O}$ 中各点处的魏尔斯特拉斯半群。

引理4.3. 设 $P_{(a,b)} \in \mathcal{X}_3(\mathbb{F}_{q^2}) \setminus \mathcal{O}$。那么 $q+1$ 和 q 包含于 $H(P_{(a,b)})$中。

证明。 $q+1 \in H(P_{(a,b)})$ 这一事实直接由方程（2.7）得出。为证明 $q \in H(P_{(a,b)})$，令 $P_{(\bar{a},0)} \in \mathcal{X}_3(\mathbb{F}_{q^2})$ 满足 $\bar{a}^m + 1 = 0$，并考虑函数

$$h_q := \frac{(x-a) f_{P_{(\bar{a},0)},1}}{f_{P_{(a,b)},1}(x-\bar{a})},$$

其中函数 $f_{P_{(a,b)},\ 1}$ 和$f_{P_{(\bar{a},0)},\ 1}$ 的定义与方程（2.7）中的相同。于是，由方程（2.7）、（2.15）、（2.16），有

$$(h_q) = -qP_{(a,b)} + \sum_{\xi^{q+1}=1,\ \xi \neq 1} P_{(a,\xi b)},$$

这意味着 $q \in H(P_{(a,b)})$。 □

定理 4.4. 设 $P_{(a,b)} \in \mathcal{X}_3(\mathbb{F}_{q^2}) \setminus \mathcal{O}$ 是满足 $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 = 0$ 的一个点。那么

$$H(P_{(a,b)}) = \langle q, q+1, (q-1) + i(q-2) \mid i = 0, \ldots, m-2 \rangle.$$

证明。我们首先证明半群 $H := \langle q, q+1, (q-1) + i(q-2) \mid i = 0, \ldots, m-2 \rangle$ 包含于 $H(P_{(a,b)})$。为此，我们证明对于所有 $i = 0, \ldots, m-2$，$q, q+1, (q-1) + i(q-2)$ 都是 P 的极点数。根据引理4.3，我们已经知道$q, q+1 \in H(P_{(a,b)})$，因此只需证明对于每个$i = 0, \ldots, m-2$，$(q-1) + i(q-2)$ 都是一个极点数。我们通过考虑以下函数族来证明这一点。对于所有满足 $0 \leq i \leq m-2$ 的 i，取一点 $P_{(\bar{a},0)}$，使得 $\bar{a}^m + 1 = 0$，并定义函数

$$G_i := \frac{g_i \cdot f_{P_{(\bar{a},0)},1}^{i+1}}{f_{P_{(a,b)},1}^{i+1} \cdot (x-\bar{a})^{i+1}},$$

其中，函数 g_i 是定理 3.19 中构造的。然后利用方程 (2.7)、(2.15)、(2.16) 和定理 3.19，可得函数 G_i 的因子为

$$(G_i) = E_i - ((q-1) + i(q-2))P_{(a,b)},$$

其中 $E_i \in \mathrm{Div}(\mathcal{X}_3)$ 是一个有效除子，满足 $P_{(a,b)} \notin \mathrm{supp}(E_i)$。因此，对于所有 $i = 1, \ldots, m-2$，有 $(q-1) + i(q-2) \in H(P_{(a,b)}$。

为完成证明，我们需要证明半群 H 的亏格小于或等于 $g(\mathcal{X}_3)$。事实上，不等式 $g(H) \geq g(\mathcal{X}_3)$ 已显然成立，因为我们刚刚证明了 $H \subseteq H(P_{(a,b)})$。当然，我们知道 $0 \in H$，但我们断言，对于 $j = 1, \ldots, m-1$，$\{j(q-2) + 1, \ldots, j(q+1)\}$ 中的所有整数也都属于 H。对于 $j = 1$，这显然成立，因为$q-1, q, q+1 \in H$。如果这对某个 $j < m-1$ 成立，那么将 $q-1$ 和 $q+1$ 加到 $\{j(q-2) + 1, \ldots, j(q+1)\}$ 中的所有整数上，就表明 $\{(j+1)(q-2) + 2, \ldots, (j+1)(q+1)\}$ 中的连续整数都属于 H。由于 $(j+1)(q-2) + 1 = (q-1) + j(q-2) \in H$，我们

得出 $\{(j+1)(q-2)+1,\dots,(j+1)(q+1)\}$ 中的所有整数都属于 H。这就证明了该断言。现在注意到，$\{(m-1)(q-2)+1,\dots,(m-1)(q+1)\}$ 由 $q-2$ 个连续整数构成，且全部属于 H。将 $q-1$ 和 q 的整数倍加到这个集合中的元素上，我们得到所有大于或等于 $(m-1)(q-2)+1+q-1=(m-1)(q+1)+2$ 的整数都属于 H。这意味着 H 中的间隙数至多为

$$g(H)\le (q-2)+(q-5)+\cdots+3+1.$$

最后的 $+1$ 计数了潜在的间隙 $(m-1)$ $(q+1)$ $+1$。因此

$$g(H)\le 1+3\sum_{k=1}^{m-1}k=1+3m(m-1)/2=g(\mathcal{X}_3),$$

这正是我们需要证明的。 □

定理 4.5. 设 $P_{(a,b)}\in\mathcal{X}_3(\mathbb{F}_{q^2})\setminus\mathcal{O}$ 是一个点，使得 $\alpha(P_{(a,b)})^2-\alpha(P_{(a,b)})+1\neq 0$。此外，设 i 为 $\alpha(P_{(a,b)})$ 的 $\mathcal{P}$-阶。若 $i\le m-2$，则

$$H(P_{(a,b)})=\langle q,q+1,(q-1)+j(q-2),(q-1)+i(q-2)-1\mid j=0,\dots,i-1\rangle.$$

若 $i=m-1$，则

$$H(P_{(a,b)})=\langle q,q+1,(q-1)+j(q-2)\mid j=0,\dots,m-2\rangle.$$

证明。我们首先假设 $i\le m-2$。我们仿照定理 4.4 的证明进行，证明半群 $H:=\langle q-1,q,q+1,(q-1)+j(q-2),(q-1)+i(q-2)-1\mid j=1,\dots,i-1\rangle$ 包含于 $H(P_{(a,b)})$ 中，且至多有 $g(\mathcal{X}_3)$ 个间隙。对于所有满足$j=1$，...，$i-1$的 j，取一个满足 $\bar{a}^m+1=0$ 的点 $P_{(\bar{a},0)}$，并定义函数

$$F_j:=\frac{f_j\cdot f_{P_{(\bar{a},0)},1}^{j+1}}{f_{P_{(a,b)},1}^{j+1}\cdot(x-\bar{a})^{j+1}},$$

其中 f_j 是定理 3.12 中构造的函数。利用方程 (2.7)、(2.15) 和定理 3.19，可以看出函数 F_j 的因子为 (2.16)

$$(F_j)=E_j-((q-1)+j(q-2))P_{(a,b)}$$

其中 $E_j\in\mathrm{Div}(\mathcal{X}_3)$ 是一个有效除子，且满足 $P_{(a,b)}\notin\mathrm{supp}(E_j)$。因此，对于所有 $j=1,\dots,i-1$，都有 $(q-1)+j(q-2)\in H(P)$。类似地

$$(F_i)=E_i-((q-1)+i(q-2)-1)P_{(a,b)},$$

其中 $E_i\in\mathrm{Div}(\mathcal{X}_3)$ 是一个有效除子，且满足 $P_{(a,b)}\notin\mathrm{supp}(E_i)$。因此，我们现在已经证明了 $H\subseteq H(P_{(a,b)})$。

剩下需要证明的是，半群 H 的亏格不超过 $g(\mathcal{X}_3)$。我们知道 $0\in H$，并且如定理 4.4 的证明中一样，可以得出，对于任意 $j=1,\dots,i$，集合 $\{j(q-2)+1,\dots,j(q+1)\}$ 中的所有整数都属于 H。此外，我们已经证明

$(i+1)(q-2) \in H$，并将 $q-1$、q 和 $q+1$ 加到 $\{i(q-2)+1, \ldots, i(q+1)\}$ 中的整数上，可得 $\{(i+1)(q-2)+2, \ldots, (i+1)(q+1)\} \subseteq H$。

由于 $P_{(a,b)} \in \mathcal{X}_3(\mathbb{F}_{q^2})$，引理 3.11 表明 $i+1$ 整除 m。我们断言，对于$k = 0, \ldots, m/(i+1) - 1$ 以及所有 $j = 1, \ldots, i$，集合 $\{(k(i+1)+j)(q-2)+1, \ldots, (k(i+1)+j)(q+1)\}$ 也包含在 H 中，同时整数 $((k+1)(i+1))(q-2)$ 和集合 $\{(k+1)(i+1)(q-2)+2, \ldots, (k+1)(i+1)(q+1)\}$ 也包含在其中。到目前为止，我们已经证明了这一点对 $k = 0$ 成立。若该断言对某个 $k-1 < m/(i+1) - 1$ 成立，那么加上 $(i+1)(q-2)$ 以及$\{(i+1)(q-2)+2, \ldots, (i+1)(q+1)\}$中的整数，便可立即得出该断言对 k 也成立。由此得证该断言。对于 $k = m/(i+1) - 1$，我们得到 $\{m(q-2)+2, \ldots, m(q+1)\}$，它包含 q 个连续整数，是 H 的子集。这表明所有大于或等于 $m(q-2)+2 = (m-1)(q+1)+2$ 的整数都属于 H。现在，估算间隙数的方法与定理 4.4 的证明非常相似。该处半群的间隙数实际上与此处构造的半群 H 的间隙数完全相同：在定理的证明中，对于所有 $k = 1, \ldots, m/(i+1) - 1$，整数 $k(i+1)(q-2)$ 是一个间隙，而 $k(i+1)(q-2)+1$ 不是；而现在 $k(i+1)(q-2)$ 属于 H，且 $k(i+1)(q-2)+1$ 不属于其中。因此，$g(H) \leq g(\mathcal{X}_3)$ 再次成立。

当 $i = m-1$ 时，尚需证明该定理。采用与上文完全相同的方法，我们可以证明 $H := \langle q-1, q, q+1, (q-1)+j(q-2) \mid j = 1, \ldots, m-2 \rangle$ 包含于$H(P_{(a,b)})$。现在注意到，H 与定理 4.4 中出现的半群完全相同。因此，$g(H) \leq g(\mathcal{X}_3)$ 在这种情形下也成立。□

4.3. 关于有理魏尔斯特拉斯点的一些注记。由前两个小节可知，我们已经完全确定了其中出现的所有类型的魏尔斯特拉斯半群，以及达到给定类型的点的数量。为避免平凡情形，假设 $q \geq 5$。

定理 4.6。在 $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$ 中，不同的魏尔斯特拉斯半群 $H(P)$ 的数量恰好等于 m 的因子的数量。所出现的半群及其出现时所对应的$P \in \mathcal{X}_3(\mathbb{F}_{q^2})$如下：

- $H(P) = \langle q-2, q, q+1 \rangle$ 对于 $q+1$ 个 $P \in \mathcal{O}$。
- $H(P) = \langle q, q+1, (q-1)+j(q-2), (q-1)+i(q-2)-1 \mid j = 0, \ldots, i-1 \rangle$，其中 $1 \leq i \leq m-2$ 且 $i+1$ 整除 m；对于满足 $\alpha(P)$具有 $\mathcal{P}$阶 i的那$(q+1)^2\varphi(i+1)$个 $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$。
- $H(P) = \langle q, q+1, (q-1)+j(q-2) \mid j = 0, \ldots, m-2 \rangle$，对于满足 $\alpha(P)$具有 $\mathcal{P}$阶 $m-1$ 的那$(q+1)^2\varphi(m)$个$P \in \mathcal{X}_3(\mathbb{F}_{q^2})$，以及满足 $\alpha(P)^2 - \alpha(P) + 1 = 0$的那 $2m(q+1)$个$P \in \mathcal{X}_3(\mathbb{F}_{q^2})$。

证明。首先，定理 4.2、4.4 和 4.5 综合描述了所有可能出现在 $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$ 中的魏尔斯特拉斯半群。引理 3.11 表明，对于 $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$，唯一可能的 $\mathcal{P}$-阶 i 对应于 m 的因子 $i+1 \geq 2$。因此，可能的魏尔斯特拉斯半群总数恰好等于 m 的因子数，其中因子 1 计数半群 $\langle q-2, q, q+1 \rangle$.

至于达到某一种特定类型的 $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$ 的数量：我们知道 $|\mathcal{O}| = q+1$，而引理 3.11 则说明了有多少个 P 具有等于给定 i 的 $\mathcal{P}$-阶。剩下需要确定的点数是满足 $\alpha(P)^2 - \alpha(P) + 1 = 0$ 的那些 $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$。利用 $\alpha(P_{(a,b)}) = a^m/(1+a^m)$，我们看到，当且仅当 $a^{2m} + a^m + 1 = 0$ 且 $b^{q+1} = -1$ 时，$\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 = 0$。因此，对于恰好 $2m(q+1)$ 个 $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$，有 $\alpha(P)^2 - \alpha(P) + 1 = 0$。□

注 4.7. 不难看出，定理 4.6 中给出的生成元在所有情况下都是极小生成元集。由于 $\mathcal{X}_3$ 是 $\mathbb{F}_{q^2}$ 上的极大曲线，其 $\mathbb{F}_{q^2}$-有理点的数量等于 $q^2 + 1 + 2qg(\mathcal{X}_3) = (q+1)(q^2+q+3)$。作为合理性检查，请注意，确实有，

$$q + 1 + \sum_{i=1;i+1|m}^{m-1} (q+1)^2\varphi(i+1) + 2m(q+1) = q^2 + 1 + 2qg(\mathcal{X}_3),$$

利用方程 $\sum_{d|m} \varphi(d) = m$，其中求和遍及 m的所有因子。

利用定理 4.6，很容易确定半群的重数（即最小正元素）：除非 $P \in \mathcal{O}$，此时为 $q-2$，否则为 $q-1$。数值半群的另一个参数是其导子 c。这是使得 $\mathbb{Z}_{\geq c}$ 包含于该半群中的最小非负整数 c。由引理 2.22，$(q-2)D_\infty$ 是典范除子；由公式 (2.15)，$3D_\infty \sim (q+1)P_{(a,0)}$；并且对任意 $P \in \mathcal{X}_3$，根据基本方程 $(\mathbb{F}_{q^2})q+1(P \sim)q+1P_{(a,0)}$，可知对于所有 $P \in \mathcal{X}_3$，$(q-2)mP$都是典范除子。这意味着对于所有 $P \in \mathcal{X}_3$，$H(P)$都是对称的。特别地，对于所有 $P \in \mathcal{X}_3$，$H(P)$中的最大间隙是 $2g(\mathcal{X}_3) - 1$，这意味着$H(P)$的导子是 $2g(\mathcal{X}_3)$。

5. Weierstrass semigroups at the non-$\mathbb{F}_{q^2}$-rational points of $\mathcal{X}_3$

本节计算 $\mathcal{X}_3$ 上所有其余点处的魏尔斯特拉斯半群，即所有非 $\mathbb{F}_{q^2}$-有理点处的魏尔斯特拉斯半群。我们先计算一般情形下的半群，也就是曲线的非魏尔斯特拉斯点处的半群；最后确定非 $\mathbb{F}_{q^2}$-有理魏尔斯特拉斯点处的半群。

5.1. 一般情形。

定理 5.1. 设 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{X}_3(\mathbb{F}_{q^2})$，使得 $\mathcal{P}_j(\alpha) \neq 0$ 对所有 $j = 2, \ldots, m-1$ 均成立。那么

$$G(P_{(a,b)}) = \{jq + k \mid j = 0, \ldots, m-2,\ k = 1, \ldots, q-3j-2\} \cup \{(m-1)q+1\},$$

也就是说

$$H(P_{(a,b)}) = \{0, (j+1)(q-3)+2+k, (m-1)q+2, \ldots \mid j = 0, \ldots, m-2,\ k = 0, \ldots, 3j+1\}.$$

证明。设 $G := \{jq+k \mid j=0,\dots,m-2,\ k=1,\dots,q-3j-2\} \cup \{(m-1)q+1\}$ 为假定的间隙集。直接计算表明 $|G| = 1+\sum_{j=0}^{m-2}(q-(3j+2)) = g(\mathcal{X}_3)$。

我们需要证明，对于每个 $g \in G$，都存在一个函数 $h_g \in L((q-2)D_\infty)$，使得 $v_P(h_g) = g-1$。

令 $g = jq+k \in G$。我们区分以下几种情形。

(1) 若 $\lfloor \frac{k}{3} \rfloor \neq 0$，则定义：

$$h_g := \begin{cases} F^j_{P_{(a,b)}} \cdot f_{\lfloor \frac{k}{3} \rfloor -1} & \text{if } k \equiv 0 \pmod 3, \\ F^j_{P_{(a,b)}} \cdot (y-b) \cdot f_{\lfloor \frac{k}{3} \rfloor -1} & \text{if } k \equiv 1 \pmod 3, \\ F^j_{P_{(a,b)}} \cdot t_{P_{(a,b)}} \cdot f_{\lfloor \frac{k}{3} \rfloor -1} & \text{if } k \equiv 2 \pmod 3. \end{cases}$$

(2) 若 $\lfloor \frac{k}{3} \rfloor = 0$，则改为定义：

$$h_g := \begin{cases} F^j_{P_{(a,b)}} & \text{if } k = 1, \\ F^j_{P_{(a,b)}} \cdot (y-b) & \text{if } k = 2. \end{cases}$$

这里，函数 $f_{\lfloor \frac{k}{3} \rfloor -1}$ 是定理 3.12 中构造的函数 f_i 之一，而函数 $F_{P_{(a,b)}}$ 则按方程 (2.20) 中的定义给出。

注意到，对于 $k=3$，...，$q-3j-2$，$j=0$，...，$m-2$成立，

$$0 \le \left\lfloor \frac{k}{3} \right\rfloor - 1 \le \left\lfloor \frac{q-3j-2}{3} \right\rfloor - 1 = \frac{q-2}{3} - j - 1 = m-2-j \le m-2,$$

因此，对于任意 $i=0$，...，$m-2$ 和 $k=1$，...，$q-3j-2$，函数 h_g 都是良定义的。事实上，以这种方式定义函数 h_g 后，对于任意 $g = jq+k \in G$，我们有如下结果。情形 1：$\lfloor \frac{k}{3} \rfloor \neq 0$。

如果 $k \equiv 0$ （模 3），则

$$v_P(h_g) = jq + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1 \right) + 2 = jq + k - 1$$

and

$$(h_g)_\infty \le \left(3j + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1 + 1 \right) \right) D_\infty = (3j+k)D_\infty \le (3j+q-3j-2)D_\infty = (q-2)D_\infty.$$

若 $k \equiv 1$ （模 3），则

$$v_P(h_g) = jq + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1 \right) + 2 + 1 = jq + (k-1) - 3 + 3 = jq + k - 1$$

and

$$\begin{aligned}(h_g)_\infty &\leq \left(3j+3\left(\left\lfloor\frac{k}{3}\right\rfloor-1+1\right)+2\right)D_\infty=(3j+k+1)D_\infty\\ &\leq (3j+q-3j-4+1)D_\infty=(q-3)D_\infty,\end{aligned}$$

其中最后一个不等式由 $q-3j-2\equiv 0$（模 3）这一事实得出，因此若 $k\equiv 1$（模 3），则 $k\leq(q-3j-2)-2=q-3j-4$。

如果 $k\equiv 2$（模 3），则

$$v_P(h_g)=jq+3\left(\left\lfloor\frac{k}{3}\right\rfloor-1\right)+2+2=jq+(k-2)-3+4=jq+k-1$$

and

$$\begin{aligned}(h_g)_\infty &\leq \left(3j+3\left(\left\lfloor\frac{k}{3}\right\rfloor-1+1\right)+3\right)D_\infty=(3j+k+1)D_\infty\\ &\leq (3j+q-3j-3+1)D_\infty=(q-2)D_\infty,\end{aligned}$$

其中，最后一个不等式由以下事实得出：$q-3j-2\equiv 0$（模 3），因此如果 $k\equiv 2$（模 3），则 $k\leq(q-3j-2)-1=q-3j-3$。

情形 2：$\left\lfloor\frac{k}{3}\right\rfloor=0$。

如果 $k=1$，则

$$v_P(h_g)=jq$$

and

$$(h_g)_\infty\leq(3j)D_\infty\leq((q+1)-6)D_\infty=(q-5)D_\infty.$$

如果 $k=2$，则

$$v_P(h_g)=jq+1$$

and

$$(h_g)_\infty\leq(3j+2)D_\infty\leq((q+1)-6+2)D_\infty=(q-3)D_\infty.$$

□

由于 $\mathcal{X}_3$ 上除有限个点外的所有点处的魏尔斯特拉斯半群均如定理 5.1 所述，我们称

$$H_{gen}:=\{0,(j+1)(q-3)+2+k,(m-1)q+2,\ldots\mid j=0,\ldots,m-2,\ k=0,\ldots,3j+1\}$$

$\mathcal{X}_3$ 的一般魏尔斯特拉斯半群，并且

$$G_{gen}:=\{jq+k\mid j=0,\ldots,m-2,\ k=1,\ldots,q-3j-2\}\cup\{(m-1)q+1\}$$

$\mathcal{X}_3$的一般间隙集。

5.2. 非-$\mathbb{F}_{q^2}$-有理魏尔斯特拉斯点处的魏尔斯特拉斯半群。

定理 5.2. 设 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{X}_3(\mathbb{F}_{q^2})$，且 i 为 $\alpha(P_{(a,b)})$ 的 $\mathcal{P}$阶。假设 $i \le m-2$。则

(5.3)
$$G(P_{(a,b)}) = \left(G_{gen} \setminus \left\{ (m-2-i-\ell(i+1))q + (\ell+1)(3i+3) \mid \ell = 0, \dots, \left\lfloor \frac{m-2-i}{i+1} \right\rfloor \right\} \right) \cup \left\{ (m-2-i-\ell(i+1))q + (\ell+1)(3i+3) + 1 \mid \ell = 0, \dots, \left\lfloor \frac{m-2-i}{i+1} \right\rfloor \right\},$$

也就是说

$$H(P_{(a,b)}) = \left(H_{gen} \setminus \left\{ (m-2-i-\ell(i+1))q + (\ell+1)(3i+3) + 1 \mid \ell = 0, \dots, \left\lfloor \frac{m-2-i}{i+1} \right\rfloor \right\} \right) \cup \left\{ (m-2-i-\ell(i+1))q + (\ell+1)(3i+3) \mid \ell = 0, \dots, \left\lfloor \frac{m-2-i}{i+1} \right\rfloor \right\}.$$

证明. 令 G 为方程 (5.3) 中所述的候选间隙集。由于该集合的基数

$$\left\{ (m-2-i-\ell(i+1))q + (\ell+1)(3i+3) \mid \ell = 0, \dots, \left\lfloor \frac{m-2-i}{i+1} \right\rfloor \right\}$$

与集合的基数相同

$$\left\{ (m-2-i-\ell(i+1))q + (\ell+1)(3i+3) + 1 \mid \ell = 0, \dots, \left\lfloor \frac{m-2-i}{i+1} \right\rfloor \right\},$$

可立即得出 $|G(P_{(a,b)})| = |G_{gen}| = g(\mathcal{X}_3)$。因此，如定理 5.1 的证明中所述，接下来只需证明，对于每个 $g \in G$，存在一个函数 h_g，使得$h_g \in L((q-2)D_\infty)$ 且 $v_P(h_g) = g-1$。

对于任意 $g = jq + k$，令 $\mathfrak{c} := \left\lfloor \frac{k}{3(i+1)} \right\rfloor$。于是我们可以写成

$$\left\lfloor \frac{k}{3} \right\rfloor = \mathfrak{c}(i+1) + h,$$

其中 h 是一个满足 $0 \le h \le i$ 的整数，并且

$$k = \left\lfloor \frac{k}{3} \right\rfloor \cdot 3 + r = 3\mathfrak{c}(i+1) + 3h + r,$$

其中 r 是满足 $0 \le r \le 2$的整数。首先注意，采用这一 $\mathfrak{c}$选择后，对于所有满足 $\left\lfloor \frac{k}{3} \right\rfloor \ne \mathfrak{c}(i+1)$ 的 k，都有 $0 \le \left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1) \le i-1$。事实上，

$$\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1) \le i-1 \iff \left\lfloor \frac{k}{3} \right\rfloor - \mathfrak{c} \le i + \mathfrak{c}i,$$

因此，由于 $\left\lfloor \frac{k}{3} \right\rfloor = \mathfrak{c}(i+1) + h$，取满足 $0 \le h \le i$的整数 h，我们得到

$$\left\lfloor \frac{k}{3} \right\rfloor - \mathfrak{c} \le i + \mathfrak{c}i \quad \Longleftrightarrow \quad \mathfrak{c}(i+1) + h - \mathfrak{c} \le i + \mathfrak{c}i \quad \Longleftrightarrow \quad h \le i,$$

该条件得到满足。

现在我们区分以下几种情况。

（1）如果$\left\lfloor \frac{k}{3} \right\rfloor \neq \mathfrak{c}(i+1)$，则定义：

$$h_g := \begin{cases} F_{P_{(a,b)}}^{j} \cdot f_{\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1)} \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 0 \pmod 3, \\ F_{P_{(a,b)}}^{j} \cdot (y-b) \cdot f_{\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1)} \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 1 \pmod 3, \\ F_{P_{(a,b)}}^{j} \cdot t_{P_{(a,b)}} \cdot f_{\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1)} \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 2 \pmod 3. \end{cases}$$

（2）如果 $\left\lfloor \frac{k}{3} \right\rfloor = \mathfrak{c}(i+1)$，则改为定义：

$$h_g := \begin{cases} F_{P_{(a,b)}}^{j} \cdot (y-b) \cdot t_{P_{(a,b)}} \cdot f_{i-1} \cdot f_i^{\mathfrak{c}-1} & \text{if } k \equiv 0 \pmod 3 \text{ and } j \le m-2-i, \\ F_{P_{(a,b)}}^{j} \cdot f_{\frac{k}{3}-1} & \text{if } k \equiv 0 \pmod 3 \text{ and } j \ge m-1-i, \\ F_{P_{(a,b)}}^{j} \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 1 \pmod 3, \\ F_{P_{(a,b)}}^{j} \cdot (y-b) \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 2 \pmod 3. \end{cases}$$

事实上，对于 $g = jq + k \in G$，我们有如下情况。

情形 1：$\left\lfloor \frac{k}{3} \right\rfloor \neq \mathfrak{c}(i+1)$。

若 $k \equiv 0$（模 3），则

$$v_{P_{(a,b)}}(h_g) = jq + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1)\right) + 2 + 3\mathfrak{c}(i+1) = jq + k - 3 + 2 = jq + k - 1$$

and

$$\begin{aligned} (h_g)_\infty &\le (3j + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1) + 1\right) + 3\mathfrak{c}(i+1))D_\infty \\ &= (3j+k)D_\infty \\ &\le (3j + q - 3j - 2)D_\infty = (q-2)D_\infty, \end{aligned}$$

其中，上述最后一个不等式由 $k \le q - 3j - 2$ 这一事实得出。

若 $k \equiv 1$（模 3），则

$$v_{P_{(a,b)}}(h_g) = jq+1+3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1)\right)+2+3\mathfrak{c}(i+1) = jq+(k-1)-3+3 = jq+k-1$$

and

$$\begin{aligned}(h_g)_\infty &\le (3j+2+3\left(\left\lfloor\frac{k}{3}\right\rfloor-(\mathfrak{c}(i+1)+1)+1\right)+3\mathfrak{c}(i+1))D_\infty\\ &=(3j+k+1)D_\infty\\ &\le (3j+q-3j-3)D_\infty=(q-3)D_\infty,\end{aligned}$$

其中，最后一个不等式由 $q-3j-2\equiv 0$ （模 3）这一事实得出，因此若 $k\equiv 1$（模 3），则 $k\le (q-3j-2)-2=q-3j-4$。

若 $k\equiv 2$ （模 3），则

$$v_{P_{(a,b)}}(h_g)=jq+2+3\left(\left\lfloor\frac{k}{3}\right\rfloor-(\mathfrak{c}(i+1)+1)\right)+2+3\mathfrak{c}(i+1)=jq+(k-2)-3+4=jq+k-1$$

and

$$\begin{aligned}(h_g)_\infty &\le (3j+3+3\left(\left\lfloor\frac{k}{3}\right\rfloor-(\mathfrak{c}(i+1)+1)+1\right)+3\mathfrak{c}(i+1))D_\infty\\ &=(3j+k+1)D_\infty\\ &\le (3j+q-3j-2)D_\infty=(q-2)D_\infty,\end{aligned}$$

其中，最后一个不等式由 $q-3j-2\equiv 0$ （模 3）这一事实可得，因此，若 $k\equiv 2$（模 3），则 $k\le (q-3j-2)-1=q-3j-3$。

情形 2：$\left\lfloor\frac{k}{3}\right\rfloor=\mathfrak{c}(i+1)$。

若 $k\equiv 0$ （模 3）且 $j\le m-2-i$，则

$$v_{P_{(a,b)}}(h_g)=jq+1+2+3(i-1)+2+3(\mathfrak{c}-1)(i+1)=jq+3\mathfrak{c}(i+1)-1=jq+k-1$$

and

$$\begin{aligned}(h_g)_\infty &\le (3j+2+3+3i+3(\mathfrak{c}-1)(i+1))D_\infty\\ &=(3j+k+2)D_\infty\\ &\le (3j+q-3j-5+2)D_\infty=(q-3)D_\infty,\end{aligned}$$

因为在此情形下 $k\le q-3j-3\equiv 2$ （模 3），所以，由于 $k\equiv 0$ （模 3），则 $k\le (q-3j-3)-2=q-3j-5$。

如果 $k\equiv 0$（模 3）且 $j\ge m-1-i$，那么注意到，由于 $3j\ge q-3i-2$，因此 $k\le q-3j-2\le q-(q-3i-2)-2=3i$ 以及 $\frac{k}{3}-1\le i-1$。因此，我们有

$$v_{P_{(a,b)}}(h_g)=jq+3\left(\frac{k}{3}-1\right)+2=jq+k-1$$

and

$$\begin{aligned}(h_g)_\infty &\le (3j+3\left(\frac{k}{3}\right))D_\infty \\ &= (3j+k)D_\infty \\ &\le (3j+q-3j-2)D_\infty = (q-2)D_\infty,\end{aligned}$$

因为在这种情况下 $k \le q-3j-2$。
若 $k \equiv 1$ （模 3），则

$$v_{P_{(a,b)}}(h_g) = jq + 3\mathfrak{c}(i+1) = jq+k-1$$

由于 $3\left\lfloor \frac{k}{3} \right\rfloor = 3\mathfrak{c}$（$i+1$） $= k-1$。此外，

$$\begin{aligned}(h_g)_\infty &\le (3j+3\mathfrak{c}(i+1))D_\infty \\ &= (3j+k-1)D_\infty \\ &\le (3j+q-3j-2-1)D_\infty = (q-3)D_\infty,\end{aligned}$$

由于 $k \le q-3j-2$。
若 $k \equiv 2$ （模 3），则

$$v_{P_{(a,b)}}(h_g) = jq+1+3\mathfrak{c}(i+1) = jq+(k-2)+1 = jq+k-1$$

由于 $3\left\lfloor \frac{k}{3} \right\rfloor = 3\mathfrak{c}$（$i+1$） $= k-2$。此外，

$$\begin{aligned}(h_g)_\infty &\le (3j+2+3\mathfrak{c}(i+1))D_\infty \\ &= (3j+k)D_\infty \\ &\le (3j+q-3j-2)D_\infty = (q-2)D_\infty,\end{aligned}$$

因为 $k \le q-3j-2$。 □

5.3. 关于 $\mathcal{X}_3$ 的魏尔斯特拉斯点的最后说明。本节最后汇总关于 $\mathcal{X}_3$的魏尔斯特拉斯点的若干进一步事实。

命题 5.4. 仅当 $q \in \{2,5,8\}$ 时， $\mathcal{X}_3$ 的所有魏尔斯特拉斯点都定义在 $\mathbb{F}_{q^2}$. 上

证明。由引理 3.11 和定理 5.2 可知，当且仅当存在 i 使得 $1 \le i \le m-2$、最大公因数$(i+1,p) = 1$，且 $i+1$ 不整除 m 时，才存在非有理魏尔斯特拉斯点。由于 m 至多有 $m/3+1$ 个因子（不计其本身），且 1 到 m 之间至多有 $\lfloor m/p \rfloor$ 个 p 的倍数，因此我们看到，当 $m-2 > 1+m/3+m/p.$ 时存在非有理魏尔斯特拉斯点。由于 $p \ge 2$，且 $m-2 > 1+m/3+m/2$ 当且仅当 $q > 53$，这已经表明对所有 $q > 53$，都存在非有理魏尔斯特拉斯点。容易验证，对于 $q \in \{11,17,23,29,32,41,47,53\}$，存在满足条件的 i；而对于 $i \in \{2,5,8\}.$ □，不存在这样的 i

备注 5.5. 此时，要确定可能出现的不同魏尔斯特拉斯半群 $H(P)$ 的数量（其中 P 变化），已经相当简单。事实上，不大于 $m-1$ 的可能 $\mathcal{P}$ 阶数，就是 1 到 $m-1$ 之间满足最大公因数$(p, i+1) = 1$的 i 的数量。再计入 $P \in \mathcal{O}$ 对应的半群，便得到 $m - \lfloor m/p \rfloor$ 个不同于一般半群的可能半群。一般半群对应于 $\mathcal{X}_3$ 上那些 P 点，其 $\mathcal{P}$ 阶数至少为 m。因此，可能的半群恰有 $m - \lfloor m/p \rfloor + 1$ 个。

注 5.6. 对于 $\mathbb{F}_{q^2}$-有理点，我们确定了相应魏尔斯特拉斯半群的重数和导子。由定理 5.1 可知，在一般情形下， $H(P)$ 中最小的正非间隙是 $q-1$，而最大的间隙是 $(m-1)q+1$。因此，在一般情形下，重数为 $q-1$，导子为 $(m-1)q+2$.。若 $P \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{X}_3(\mathbb{F}_{q^2})$ 的 $\mathcal{P}$-阶为 $i \leq m-2$，那么由定理 5.2 很容易推出，最大的间隙仍为 $(m-1)q+1$，因此导子为 $(m-1)q+2$.。

重数的情形则更为复杂。我们将在下面的定理中说明具体情况。

定理 5.7。设 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{X}_3(\mathbb{F}_{q^2})$。则半群$H(P_{(a,b)})$的重数为 $q-2$ 或 $q-1$。此外，以下各项等价:

(1) $H(P_{(a,b)})$的重数为 $q-2$。(2) $\mathcal{P}$-阶 i of $\alpha(P_{(a,b)})$满足 $i+1$ 整除 $m-1$。(3) $\mathcal{P}_{m-1}(\alpha(P_{(a,b)})) = 0$。(4) (a,b)的弗罗贝尼乌斯，即 $\Phi(a,b) := (a^{q^2}, b^{q^2})$，位于平面曲线 $y^{q+1} + x^{2m} + x^m = 0$ 在 (a,b)处的切线上。

证明。比较一般情形下的间隙集与定理 5.2 所述情形下的间隙集，我们看到，唯一的区别在于某些间隙的值增加了 1。由于在一般情形下，$1, \ldots, q-2$ 都是间隙，而 $q-1$ 不是间隙，这意味着对于任意 $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{X}_3(\mathbb{F}_{q^2})$， $H(P_{(a,b)})$的重数可以是 $q-2$或 $q-1$。现在我们证明所列四项的等价性。为方便起见，记 $P = P_{(a,b)}$ 和 $\alpha = \alpha(P_{(a,b)})$。

(1) $\Rightarrow$ (2)：假设 $q-2 \in H(P)$，并令 i 为 α 的 $\mathcal{P}$ 阶。根据定理 5.2 $q-2$，可将其写成 $(m-2-i-\ell(i+1))q + (\ell+1)(3i+3)$ 的形式，其中某个 ℓ 介于 0 与 $\lfloor (m-2-i)/(i+1) \rfloor$. 之间。因此必有 $m-2-i-\ell(i+1) = 0$，这只有在 $\ell = (m-2-i)/(i+1)$ 是整数时才可能成立。故 $i+1$ 整除 $m-1$。

(2) $\Rightarrow$ (3)：根据多项式 $\mathcal{P}_{i+1}(s)$ 的定义，我们可知 $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{i+1} = 1$。若 $i+1$ 整除 $m-1$，则这意味着 $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{m-1} = 1$，进而意味着 $\mathcal{P}_{m-1}(\alpha) = 0$.

(3) $\Rightarrow$ (4)：平面曲线 $y^{q+1} + x^{2m} + x^m = 0$ 在 (a,b) 处的切线 ℓ_P 由方程 $a^{m-1}(2a^m+1)(x-a) + 3b^q(y-b) = 0$ 给出。因此， $\Phi(a,b)$ 位于 ℓ_P 上，当且仅当 $a^m(2a^m+1)(a^{q^2-1}-1) + 3b^{q+1}(b^{q^2-1}-1) = 0$。利用 $b^{q+1} = -a^{2m} - a^m$，我们可以将此方程中的所有量都用 a^m 表示，从而得到等价方程 $a^m((a^m)^{q-1}-1)^2(2(a^m)^q + (a^m)^{q-1} + a^m + 2) = 0$.。由于 $P \notin \mathcal{X}_3(\mathbb{F}_{q^2})$，我们知道 $a^m \notin \mathbb{F}_q$，并且

因此我们得出结论：

$$(a^{q^2}, b^{q^2}) \in \ell_P \Leftrightarrow 2(a^m)^q + (a^m)^{q-1} + a^m + 2 = 0.$$

利用 $a^m = \alpha/(1-\alpha)$，我们得出

$$(a^{q^2}, b^{q^2}) \in \ell_P \Leftrightarrow \alpha^{q-1} + (\alpha-1)^{q-1} + 1 = 0. \tag{5.8}$$

现在来考察我们的假设： $\mathcal{P}_{m-1}(\alpha) = 0$。这意味着

$$\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{q-2} = 1 \text{ and hence } \left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{q} = \left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{2},$$

进而得到

$$0 = (\alpha+\zeta_3)^q(\alpha+\zeta_3^2)^2 - (\alpha+\zeta_3^2)^q(\alpha+\zeta_3)^2 = (\alpha^q+\zeta_3^2)(\alpha+\zeta_3^2)^2 - (\alpha^q+\zeta_3)(\alpha+\zeta_3)^2.$$

展开所有项并除以 $\zeta_3^2 - \zeta_3$，可得

$$0 = 2\alpha^{q+1} - \alpha^q + \alpha^2 - 2\alpha = \alpha(\alpha-1)(\alpha^{q-1} + (\alpha-1)^{q-1} + 1).$$

根据方程 (5.8)，我们得到 $\Phi(a,b) \in \ell_P$。

(4) $\Rightarrow$ (1)：如果 $\Phi(a,b) \in \ell_P$，那么函数 t_P/F_P（见方程 (2.8) 和 (2.20)）在 $P_{(a,b)}$ 处有一个阶数为 $q-2$ 的极点，且没有其他极点。由于我们已经看到 $H(P)$的重数为 $q-1$ 或 $q-2$，因此重数为 $q-2$。
□

注 5.9. 令 W_q 表示魏尔斯特拉斯点的总数。我们已经看到

$$\begin{aligned} W_q &= -(q+1)^2 + (q+1) + 2(q+1)m + (q+1)^2\left(\sum_{i=0}^{m-1}\varphi(i+1) - \sum_{i=0}^{(m-1)/p-1}\varphi(p\cdot(i+1))\right) \\ &= -(q+1)^2 + (q+1) + 2(q+1)m + (q+1)^2\left(\sum_{i=1}^{m}\varphi(i) - \sum_{i=1}^{(m-1)/p}\varphi(p\cdot i)\right). \end{aligned}$$

这里， $\xi \in \mathbb{R}_{\geq 0}$ 的记号 $\sum_{i=0}^{\xi}$ 是 $\sum_{i=0}^{\lfloor \xi \rfloor}$ 的简写。

迭代地利用

$$\sum_{i=1}^{(m-1)/p}\varphi(p\cdot i) = (p-1)\sum_{i=1}^{(m-1)/p}\varphi(i) + \sum_{i=1}^{(m-1)/p^2}\varphi(p\cdot i),$$

可得

$$\sum_{i=1}^{(m-1)/p}\varphi(p\cdot i) = \sum_{e=1}^{\lfloor \log_p(m-1)\rfloor}(p-1)\sum_{i=1}^{(m-1)/p^e}\varphi(i).$$

众所周知，参见例如 $[14, \text{Thm.}330]$,，当 $N \to \infty$ 时， $\sum_{i=1}^{N}\varphi(i) = \frac{3}{\pi^2}N^2 + O(N\log(N))$ 渐近成立。

因此，我们可以看到

$$\begin{aligned}\sum_{i=1}^{(m-1)/p}\varphi(p\cdot i) &= \sum_{e=1}^{\lfloor\log_p(m-1)\rfloor}\frac{3(p-1)(m-1)^2}{\pi^2p^{2e}}+O\left(\sum_{e=1}^{\lfloor\log_p(m-1)\rfloor}\frac{m-1}{p^e}\log_p\left(\frac{m-1}{p^e}\right)\right)\\ &= \frac{3(p-1)(m-1)^2}{\pi^2}\frac{1-p^2/p^{2\lfloor\log_p(m-1)\rfloor}}{p^2-1}\\ &\qquad +O\left(\int_0^{\log_p(m-1)}\frac{m-1}{p^e}\log_p\left(\frac{m-1}{p^e}\right)de\right)\\ &= \frac{3(m-1)^2}{\pi^2(p+1)}-\frac{3p^2}{\pi^2(p+1)}\left(\frac{m-1}{p^{\lfloor\log_p(m-1)\rfloor}}\right)^2+O(q\log(q))\\ &= \frac{3(m-1)^2}{\pi^2(p+1)}+O(q\log(q)).\end{aligned}$$

回到魏尔斯特拉斯点的数量，我们可以看到

$$\begin{aligned}W_q &= (q+1)^2\left(\sum_{i=1}^{m-1}\varphi(i)-\sum_{i=1}^{(m-1)/p}\varphi(p\cdot i)\right)+O(q^2)\\ &= (q+1)^2\left(\frac{3(m-1)^2}{\pi^2}-\frac{3(m-1)^2}{\pi^2(p+1)}\right)+O(q^3\log(q))\\ &= \frac{3(m-1)^2(q+1)^2}{\pi^2}\frac{p}{p+1}+O(q^3\log(q))\\ &= \frac{q^4}{3\pi^2}\frac{p}{p+1}+O(q^3\log(q)).\end{aligned}$$

由于有理点的数量为 $O(q^3)$，这表明当 q很大时，非有理魏尔斯特拉斯点的数量远远超过有理魏尔斯特拉斯点的数量。

6. The full automorphism group X_3 的全自同构群 $\mathrm{Aut}(\mathcal{X}_3)$ of $\mathcal{X}_3$

事实证明，了解 $\mathcal{X}_3$ 上所有 $\mathbb{F}_{q^2}$-有理点的魏尔斯特拉斯半群，就能确定 $\mathcal{X}_3$ 的全自同构群 $\mathrm{Aut}(\mathcal{X}_3)$。本节将对此进行探讨。与前文一样，$q\equiv 2 \pmod 3$，我们用 p 表示 $\mathbb{F}_{q^2}$ 的特征。如第 2 节所述，函数域 $\mathbb{F}_{q^2}(\mathcal{X}_3)$ 可视为厄米函数域$\mathbb{F}_{q^2}(\mathcal{H})$的子域，且函数域扩张 $\mathbb{F}_{q^2}(\mathcal{H})/\mathbb{F}_{q^2}(\mathcal{X}_3)$ 是一个次数为 3 的无分歧伽罗瓦扩张（见注 2.4），其伽罗瓦群由自同构 τ 生成，该自同构在方程 (2.3) 中定义。构造曲线$\mathcal{X}_3$（等价地，函数域 $\mathbb{F}_{q^2}(\mathcal{X}_3)$）的自同构时，这一观察很有用。

事实上，寻找 $\mathbb{F}_{q^2}(\mathcal{X}_3)$ 的自同构的一种方法，是考察 $\mathrm{Aut}(\mathcal{H}) \cong \mathrm{PGU}(3,q)$ 中$\langle\tau\rangle$的正规化子 $N(\langle\tau\rangle)$。这样一来，理论上可以保证群 $N(\langle\tau\rangle)/\langle\tau\rangle$ 是不动域 $\mathbb{F}_{q^2}(\mathcal{X}_3)$（对应于 $\langle\tau\rangle$）的全自同构群的子群。$\mathrm{PGU}(3,q)$ 中的群$N(\langle\tau\rangle)$ 是一个众所周知的稳定自极三角形的极大子群，见[15, 定理 A.10]。其阶为 $6(q+1)^2/\gcd(3,q+1) = 2(q+1)^2$，并且同构于一个阶为 $(q+1)^2/3$ 的阿贝尔群与一个 6 阶对称群的半直积，其中包含 τ。这解释了引理 2.6 中所述自同构群的结构。

现在我们开始研究 $\mathcal{X}_3$ 的全自同构群。回忆一下，$\mathcal{O}_0 := \{P_0^1, \dots, P_0^m\}$, $\mathcal{O}_\infty := \{P_\infty^1, \dots, P_\infty^m\}$ 和 $\mathcal{O}_m = \{P_{(a,0)} \mid a^m + 1 = 0\}$。此外，$\mathcal{O} = \mathcal{O}_0 \cup \mathcal{O}_\infty \cup \mathcal{O}_m$，如方程 (2.5) 所示。

引理 6.1。 设 $\mathcal{O}$ 是方程 (2.5) 中定义的集合。则 $\mathcal{O}$ 是 $\mathrm{Aut}(\mathcal{X}_3)$ 的一个轨道 .

证明。由于 $\mathcal{X}_3$ 是 $\mathbb{F}_{q^2}$-极大的，其全自同构群 $\mathrm{Aut}(\mathcal{X}_3)$ 定义在 $\mathbb{F}_{q^2}$ 上，因此作用于集合 $\mathcal{X}_3(\mathbb{F}_{q^2})$，例如参见引理 2.4]。令 $H(P_{(a,b)})$ 和 $H(P)$ 分别为点 $P_{(a,b)} \in \mathcal{X}_3(\mathbb{F}_{q^2}) \setminus \mathcal{O}$ 处以及点 $P \in \mathcal{O}$ 处的魏尔斯特拉斯半群。由于半群 $H(P_{(a,b)})$ 和 $H(P)$ 不同（参见定理 4.2、4.4 和 4.5），$\mathrm{Aut}(\mathcal{X}_3)$ 分别作用于 $\mathcal{O}$ 和 $\mathcal{X}_3(\mathbb{F}_{q^2}) \setminus \mathcal{O}$。此外，由于根据推论 2.18 $\mathcal{O}$，$G \subseteq \mathrm{Aut}(\mathcal{X}_3)$ 的一个轨道，我们可推得 $\mathcal{O}$ 也是整个 $\mathrm{Aut}(\mathcal{X}_3)$ 的一个轨道。□

现在利用 $\mathcal{O}$ 是一个轨道这一点，开始研究 $\mathrm{Aut}(\mathcal{X}_3)$ 的 p-西罗子群。

引理 6.2. 设 $q \geq 11$。令 S_p 表示 $|\mathrm{Aut}(\mathcal{X}_3)|$的一个西罗子群。则 $|S_p| < q$。

证明。由于根据引理 6.1，S_p 作用于 $\mathcal{O}$，我们看到 S_p 至少有一个不动点 $P \in \mathcal{O}$。不妨设 $P = P_{(a,0)}$，其中 a 满足 $a^m + 1 = 0$。由于$\mathcal{X}_3$ 的 p-秩为零，S_p 在 $\mathcal{O} \setminus \{P_{(a,0)}\}$上以长轨道作用，见 [15, 引理 11.129]。这意味着 $|S_p| \leq q$。

现在假设 $|S_p| = q$。那么 $\mathrm{Aut}(\mathcal{X}_3)$ 在 $\mathcal{O}$ 上传递地二重传递，并且两个点的稳定子在此作用下是循环的，因为其阶与 p 互质（见 [15, 定理 11.49]）。此外，根据 [18, 定理 1.1],，$\mathrm{Aut}(\mathcal{X}_3)$ 有一个正则正规子群 N，除非:

- $\mathrm{Aut}(\mathcal{X}_3)$ 同构于 $\mathrm{PSL}(2,q)$、$\mathrm{PGL}(2,q)$，或
- $q = \bar{q}^3$ 且 $\mathrm{Aut}(\mathcal{X}_3)$ 同构于 $\mathrm{PSU}(3,\bar{q})$ 或 $\mathrm{PGU}(3,\bar{q})$，或
- $\mathrm{Aut}(\mathcal{X}_3)$ 同构于铃木群 $Sz(\bar{q})$，其中 $q = \bar{q}^2$。

前两种可能性可以排除，因为在这种情况下，$|\mathrm{Aut}(\mathcal{X}_3)|$ 将不会被 $2(q+1)^2$整除。此外，如果 $\mathrm{Aut}(\mathcal{X}_3)$同构于铃木群 $Sz(\bar{q})$，那么特征为 2，且 $q = \bar{q}^2$ 是 2 的偶次幂。然而，这是不可能的，因为$q \equiv 2$ (模 3)。这意味着 $\mathrm{Aut}(\mathcal{X}_3)$具有一个正则正规子群 N。于是，根据[6, 定理 1.7]6], , 我们看到 $|\mathcal{O}| = q + 1 = \ell^h$，其中 $h \in \mathbb{Z}_{>0}$ 以及某个素数ℓ。如果 q 为奇数，这不可能，因为 $q+1$ 能被 6 整除。如果 q 为偶数，我们将得到$|\mathcal{O}| = q + 1 = 2^n + 1 = \ell^h$。如果 $h = 1$, 这意味着 ℓ 是一个费马素数，而这

只有在 n 是 2 的幂时才可能。然而，由于 n 为奇数，这将推出 $n = 1$。这是不可能的，因为 $q \geq 11$。如果 $h > 1$，那么根据卡塔兰猜想（米海列斯库定理[20]），我们看到唯一的可能性是 $\ell = 3$ 和 $n = 3$。这同样不可能，因为我们假设 $q \geq 11$。因此，我们得出唯一的可能性是 $|S_2| < q$。□

接下来给出一个引理，它将帮助我们识别某些自同构 $\mathcal{X}_3$.

引理 6.3. 设 $\alpha \in \mathrm{Aut}(\mathcal{X}_3)$，并假设当把 $\alpha(x)$ 看作厄米函数域 $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ 上的函数时，它是一个立方。那么 α 可以提升为 $\mathcal{H}$的一个自同构 $\bar{\alpha}$。

证明. 由于 α是 $\mathcal{X}_3$的一个自同构，我们知道 $\alpha(y)^{q+1}+\alpha(x)^{(q+1)/3}+\alpha(x)^{2(q+1)/3} = 0$。令 $\alpha(x) = w^3$，其中 $w = w(u, v) \in \overline{\mathbb{F}}_{q^2}(\mathcal{H})$，并定义

$$\bar{\alpha}(u) = w \quad \text{and} \quad \bar{\alpha}(v) = \frac{\alpha(y)}{\bar{\alpha}(u)}.$$

Then

$$\bar{\alpha}(u)^{q+1} + \bar{\alpha}(v)^{q+1} + 1 = w^{q+1} + \frac{\alpha(y)^{q+1}}{w^{q+1}} + 1 = \frac{\alpha(x)^{2(q+1)/3} + \alpha(y)^{q+1} + \alpha(x)^{(q+1)/3}}{w^{q+1}} = 0.$$

这意味着 $\bar{\alpha}$ 保持厄米函数域的定义方程，并定义了 $\mathcal{H}$的一个自同构。□

注意，由于 $\mathcal{H}$ 的所有自同构都定义在 $\mathbb{F}_{q^2}$上，自同构 $\bar{\alpha}$ 也将定义在 $\mathbb{F}_{q^2}$上。因此，如果 $\alpha(x)$ 是 $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ 中的一个立方，那么它必然已经是 $\mathbb{F}_{q^2}(\mathcal{H})$ 中的一个立方。

6.1. $\mathcal{X}_3$ 的全自同构群 $\mathrm{Aut}(\mathcal{X}_3)$，$q$ 为奇数。我们希望利用 $\mathcal{O}$ 是 $\mathrm{Aut}(\mathcal{X}_3)$ 的一个轨道这一信息，证明对于奇数 q，若 $q = 5$ 是由（仿射）方程 $X^5 + X = Y^3$ 定义的平面曲线，则它与 $\mathcal{X}_3$ 双有理等价。相应的函数域同构描述为 $x = wX + (wX)^{-1}, y = Y/X$，其中 $w^2 = 2$。已知该曲线的自同构群同构于一个 3 阶循环群与 $\mathrm{PGL}(2, 5)$ 的半直积，参见 [15, 定理 12.11]。特别地，若 $q = 5$，则 $|\mathrm{Aut}(\mathcal{X}_3)| = 360$，其阶是引理 2.6 中所述自同构群基数的五倍。

从现在起，在本小节中我们假设 $q \geq 11$ 且 q 为奇数。事实证明，在这种情况下，$\mathcal{X}_3$ 的自同构群实际上与 G 重合。为说明这一点，我们先在关于 q 的上述假设下证明 $\mathrm{Aut}(\mathcal{X}_3)$ 是温和的，也就是说，它不包含阶为 p 的任何元素。

引理 6.4. 设 $q \geq 11$ 和 q 为奇数。那么 $|\mathrm{Aut}(\mathcal{X}_3)|$ 不被域 $\mathbb{F}_{q^2}$ 的特征 p 整除。

证明。反设 $\mathrm{Aut}(\mathcal{X}_3)$ 存在一个阶为 p^i 的 Sylow p-子群 S_p，其中 $i \geq 1$。正如我们在引理 6.2 的证明中所见，我们可以假设 S_p 固定了 $P \in \mathcal{O}$,

其中 $P = P_{(a,0)}$，对某个 a 满足 $a^m + 1 = 0$，且 S_p 在 $\mathcal{O} \setminus \{P_{(a,0)}\}$ 上具有长轨道。此外，根据引理 6.2，我们可以假设 $|S_p| < q$。

回忆一下，自同构 $\sigma : (x, y) \mapsto (x, \delta y)$ 中，δ 是一个本原的 $(q+1)$ 次单位根。它逐点固定集合 $\mathcal{O}_m$，同时在集合 $\mathcal{O}_0$ 和 $\mathcal{O}_\infty$ 上传递地作用。由此可知，σ 正规化 S_p（见 [15, 定理 11.49]），并保持包含 $\mathcal{O}_m$ 的 S_p 的轨道不变。因此，对于固定的 $\bar{a}$，有两种可能：要么包含 $P_{(\bar{a},0)}$ 的 S_p 的轨道包含于 $\mathcal{O}_m$，要么它完全包含 $\mathcal{O}_0$ 或 $\mathcal{O}_\infty$。在第二种情况下，我们会得到 $|S_p| \geq (q+1)/3 + 1$，因而有 $|S_p| = q$，这是不可能的。因此，我们可以推得，对于所有满足 $\bar{a}^m + 1 = 0$ 的 $\bar{a}$，$P_{(\bar{a},0)}$ 的 S_p-轨道都包含于 $\mathcal{O}_m$。由于 S_p 作用于 $\mathcal{O} = \mathcal{O}_m \cup \mathcal{O}_0 \cup \mathcal{O}_\infty$，$S_p$ 必须在 $\mathcal{O}_0 \cup \mathcal{O}_\infty$ 上以长轨道作用，而 $\mathcal{O}_0 \cup \mathcal{O}_\infty$ 是一个基数为 $2(q+1)/3$ 的集合。因此，我们得到了所需的矛盾，因为 $2(q+1)/3$ 不能被 p 整除。□

定理 6.5. 设 $q \geq 11$, q 为奇数。则 $\mathrm{Aut}(\mathcal{X}_3) = G$。

证明。反设 $|\mathrm{Aut}(\mathcal{X}_3)| > |G|$，则导出矛盾。设 $G_{P_{(a,0)}}$ 为 G 中 $P_{(a,0)}$ 的稳定子，其中 a 满足 $a^m + 1 = 0$。由于根据轨道-稳定子定理，$|G| = |\mathcal{O}||G_{P_{(a,0)}}|$，且根据引理 6.1，$\mathcal{O}$ 是 $\mathrm{Aut}(\mathcal{X}_3)$ 的一个轨道，因此 $\mathrm{Aut}(\mathcal{X}_3)^{P_{(a,0)}}$（$P_{(a,0)}$ 在 $\mathrm{Aut}(\mathcal{X}_3)$ 中的稳定子）包含某个额外的自同构 $\gamma \notin G_{P_{(a,0)}}$。设 C_{q+1} 为由σ 生成的循环群：$(x, y) \mapsto (x, \delta y)$，其中 δ 是一个本原的 $(q+1)$ 次单位根。于是，由于 $\mathrm{Aut}(\mathcal{X}_3)^{P_{(a,0)}}$是循环群（这是因为 $\mathrm{Aut}(\mathcal{X}_3)$ 的阶与 p互素），γ 与 C_{q+1} 交换，因此它作用于其不动点（一般而言，也作用于轨道）。这意味着 γ 作用于集合 $\mathcal{O}_m$ 和 $\mathcal{O}_0 \cup \mathcal{O}_\infty$，因为集合 $\mathcal{O}_m$ 恰好是 C_{q+1} 的不动点集合。由于 $\mathcal{O}_0$ 和 $\mathcal{O}_\infty$ 是 C_{q+1} 的长度相同的轨道，γ 要么同时固定 $\mathcal{O}_0$ 和$\mathcal{O}_\infty$，要么将它们互换。

如果 γ 同时固定 $\mathcal{O}_0$ 和 $\mathcal{O}_\infty$，那么它固定方程 (2.16) 中 x 的因子。这意味着，对于某个常数 λ，有 $\gamma(x) = \lambda x$。因此，由于 $x = u^3$ 和 λ 是常数，$\gamma(x)$ 是 $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ 中的一个立方。反之，假设 γ 交换 $\mathcal{O}_0$ 和 $\mathcal{O}_\infty$。那么，γ 将 x的因子映射为$\frac{1}{x}$的因子，这意味着存在一个常数 λ，使得 $\gamma(x) = \frac{\lambda}{x}$。因此，在所有情况下，$\alpha(x)$ 都是 $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$ 中的一个立方。

由引理 6.3，γ 可以提升为厄米特曲线 $\mathcal{H}$ 的一个自同构 $\bar{\gamma}$，其作用于位于 $\mathcal{O}$中各点之上的 $3(q+1)$ 个点的集合。这些点在几何上是厄米特曲线 $\mathcal{H}$ 与三条直线的交点，这三条直线彼此相交于 $\mathcal{H}$外的 3 个点，即构成一个自极三角形。由于这表明 γ 是由 $N(\langle\sigma\rangle)$ 所诱导的，于是 $\gamma \in G$，从而导致矛盾。□

6.2. $\mathcal{X}_3$的全自同构群，q 偶数。现在我们转而讨论 q 为偶数的情形，也就是说，当 $q = 2^n$、n 为奇数时。如果 $q = 2$，则该曲线同构于 $\mathbb{F}_4$ 上的厄米特曲线，因此其自同构群为 PGU(3, 2)，其中包含 216 个元素。这里仅考虑了定义在 $\mathbb{F}_{q^2}$ 上的自同构。因此，在这种情况下，自同构的数量是引理 2.6 中所述数量的十二倍。如果 $q = 8$,

$\mathcal{X}_3$ 的自同构群是已知的，因为在这种情况下， $\mathcal{X}_3$ 同构于 Giulietti-Korchm´aros 极大曲线（见 [12]）。例如，该曲线可以表示为具有仿射方程 $Y^9 = (X^2 + X)(X^2 + X + 1)^3$ 的平面曲线。于是，在函数域层面上的一个显式同构由 $X = \zeta_3 + (x^5 + x^4 + x^3)/y^9$ 以及 $Y = (x^5 + x^4 + x^3)/y^8$.给出。因此，对于 $q = 8$， X_3 的自同构群是一个 3 阶循环群与 PGU(3, 2) 的半直积，共有 648 个自同构，比引理 2.6 中的群多四倍。

从本小节余下部分起，我们假设 $q = 2^n$, n 为奇数且至少为五。现在我们将证明，在这种情况下， $\mathcal{X}_3$ 的自同构群与引理 2.6 中的群 G 重合。为此，我们将采用与上一小节类似的论证。当然，在这种情况下，我们无法证明 Aut($\mathcal{X}_3$) 是温和的，因为 G 本身是非温和的。事实上，我们首先证明，若 Aut($\mathcal{X}_3$) 的 Sylow 2-子群的阶大于 2，则其基数必为 $q/2$。

引理 6.6. 设 $n \geq 5$ 和 $q = 2^n$。另设 S_2 为 Aut($\mathcal{X}_3$) 的一个 Sylow 2-子群。那么，要么 $|S_2| = 2$，要么 $|S_2| = q/2$。在后一种情况下，固定点 $P_{(a,0)}$ 的 2-Sylow S_2 （其中 $a^m + 1 = 0$）在 $\mathcal{O}$ 上有以下 3 个轨道：

- $\{P_{(a,0)}\}$,
- $\mathcal{O}_1^{S_2} := \mathcal{O}_0 \cup \{P_{(\beta_1,0)} \ \dots, P_{(\beta_{(q-2)/6},0)}\}$,
- $\mathcal{O}_2^{S_2} := \mathcal{O}_\infty \cup \{P_{(\gamma_1,0)} \ \dots, \ P_{(\gamma_{(q-2)/6},0)}\}$,

其中 $\{P_{(a,0)}\}$, $\{P_{(\beta_1,0)} \ \dots, P_{(\beta_{(q-2)/6},0)}\}$ 和 $\{P_{(\gamma_1,0)} \ \dots, P_{(\gamma_{(q-2)/6},0)}\}$ 是 $\mathcal{O}_m$.的一个适当划分

证明。设 S_2 的阶为 2^i ，其中 $i \geq 1$。正如引理 6.4 的证明中一样，我们可以假设 S_2 固定 $P \in \mathcal{O}$，其中 $P = P_{(a,0)}$，对于某个 a ，使得 $a^m + 1 = 0$ ，并且 S_2在 $\mathcal{O} \setminus \{P_{(a,0)}\}$上具有长轨道。此外，根据引理 6.2，我们可以假设 $|S_2| < q$。

回忆一下，自同构 $\sigma : (x, y) \mapsto (x, \delta y)$，其中 δ是一个原始的 $(q+1)$ 次单位根，它固定 $P_{(a,0)}$ ，因此根据 [15, 定理 11.49]，正规化了 S_2。此外， σ 逐点固定集合 $\mathcal{O}_m$ ，同时在 $\mathcal{O}_0$ 和 $\mathcal{O}_\infty$上传递作用。这意味着，对于满足 $a^m + 1 = 0$的 a ， σ 保持包含 $P_{(a,0)}$的 S_2 的轨道不变。因此，对于一个固定的 a，有两种可能：要么包含 $P_{(a,0)}$ 的 S_2 的轨道包含于 $\mathcal{O}_m$中，要么它完全包含 $\mathcal{O}_0$ 或 $\mathcal{O}_\infty$。

如果第二种情形从未发生，那么 S_2 在 $\mathcal{O}_0 \cup \mathcal{O}_\infty$上半正则地作用，而 $\mathcal{O}_0 \cup \mathcal{O}_\infty$是一个基数为 $2(q + 1)/3$ 的集合。这意味着 $|S_2| = 2$。如果对于某个a发生了第二种情形，那么我们得到 $|S_2| \geq (q + 1)/3 + 1$ ，因此 $|S_2| = q/2$。注意，在这种情形下， S_2 作用于 $\mathcal{O}_m \setminus \{P_{(a,0)}\}$ 中的 q 个点时，唯一可能的轨道配置是： S_2恰有 2 个长度为 $q/2$ 的轨道：一个 $\mathcal{O}_1^{S_2}$包含 $\mathcal{O}_0$ 和 $\mathcal{O}_m$中的 $(q - 2)/6$ 个点，另一个 $\mathcal{O}_2^{S_2}$包含 $\mathcal{O}_\infty$ 以及 $\mathcal{O}_m$中剩余的 $(q - 2)/6$ 个点。□

现在我们排除引理 6.6 中的第二种情况。

引理 6.7. $|S_2| = q/2$ 这种情况不可能发生。

证明. 反设 $|S_2| = q/2$。采用引理 6.6 中的记号，我们可以假设 S_2 作用于 $\mathcal{O}$，且有三个轨道 $\{P_{(a,0)}\}$、$\mathcal{O}_1^{S_2}$和 $\mathcal{O}_2^{S_2}\}$。由 $\sigma\colon (x,y) \mapsto (x, \delta y)$ 生成的循环群 C_{q+1}，其中 δ 是一个本原的 $(q+1)$ 次单位根，它固定 $\mathcal{O}_m$中的任意点，尤其是 $P_{(a,0)}$，因此正规化 S_2。特别地，由 σ 和 S_2 中的元素生成的群 L有 $|S_2|(q+1)$ 个元素。由于两点稳定子是温和且循环的，我们得出 C_{q+1} 是点 $P_{(a,0)}$ 与任意其他 $P \in \mathcal{O}_m$.的两点稳定子

使用引理 6.6 中的记号，选取 $\gamma \in S_2$ 使得 $\gamma(P_{(\beta_1,0)}) = P_{(\beta_2,0)}$，其中$P_{(\beta_1,0)}$ $P_{(\beta_2,0)}$ $\in \mathcal{O}_1^{S_2}$互不相同。这样的 γ 存在，因为 $P_{(\beta_1,0)}$ 和 $P_{(\beta_2,0)}$ 在 S_2的作用下属于同一轨道。于是 $\gamma^{-1}\cdot\sigma\cdot\gamma$ 固定 $P_{(a,0)}$，且 $\gamma^{-1}\cdot\sigma\cdot\gamma(P_{(\beta_1,0)}) = \gamma^{-1}\cdot\sigma(P_{(\beta_2,0)}) = \gamma^{-1}(P_{(\beta_2,0)}) = P_{(\beta_1,0)}$。因此，$\gamma^{-1}\cdot\sigma\cdot\gamma$ 是一个阶为 $q+1$ 的元素，同时固定 $P_{(a,0)}$ 和$P_{(\beta_1,0)}$。因此 $\gamma^{-1}\cdot\sigma\cdot\gamma \in C_{q+1}$，更具体地说，$\gamma^{-1}\cdot\sigma\cdot\gamma = \sigma^k$，其中 $(k, q+1) = 1$。此外，由于 C_{q+1} 正规化 S_2，存在 $\tilde{\gamma} \in S_2$ 使得 $\sigma\cdot\gamma = \tilde{\gamma}\cdot\sigma$。因此 $\mathrm{id} = \gamma^{-1}\cdot\sigma\cdot\gamma\cdot\sigma^{-k} = \gamma^{-1}\tilde{\gamma}\cdot\sigma^{1-k}$。由于 $S_2 \cap C_{q+1} = \{\mathrm{id}\}$，这意味着 $k = 1$，进而 γ 和 σ 交换。

现在令 ι 为 γ 的一个适当幂，使得 ι 的阶为二。于是对任意 $P_{(\beta_j,0)} \in \mathcal{O}_1^{S_2}$，有 $\iota(P_{(\beta_j,0)}) \in \mathcal{O}_1^{S_2}$，因为 S_2 作用于 $\mathcal{O}_1^{S_2}$。另一方面，利用 σ 与 ι 交换，且 σ 固定 $\mathcal{O}_m$ 中的所有点，可得 $\sigma\cdot\iota(P_{(\beta_j,0)}) = \iota\cdot\sigma(P_{(\beta_j,0)}) = \iota(P_{(\beta_j,0)})$。因此，$\iota(P_{(\beta_j,0)})$ 是 σ的一个不动点，这意味着 $\iota(P_{(\beta_j,0)}) \in \mathcal{O}_m$。我们得出结论：$\iota(P_{(\beta_j,0)}) \in \mathcal{O}_1^{S_2} \cap \mathcal{O}_m = \{P_{(\beta_1,0)} \ldots, P_{(\beta_{(q-2)/6},0)}\}$。换言之：$\iota$ 作用于$\{P_{(\beta_1,0)} \ldots, P_{(\beta_{(q-2)/6},0)}\}$。由于 $(q-2)/6 = (q/2+1)/3$ 是奇数，这意味着除 $P_{(a,0)}$之外，ι 至少还有另一个不动点。然而，由于特征为二，根据 [15,引理 11.129]，这是不可能的。□

现在我们可以在 q 为偶数时计算 $\mathrm{Aut}(\mathcal{X}_3)$。

定理 6.8. 设 $q = 2^n$, $n \geq 5$ 为奇数。则 $\mathrm{Aut}(\mathcal{X}_3) = G$。

证明. 结合引理 6.6 和 6.7，我们得出 $|S_2| = 2$。反设 $|\mathrm{Aut}(\mathcal{X}_3)| > |G|$。令 $G_{P_{(a,0)}}$ 为 G 中 $P_{(a,0)}$ 的稳定子，其中 a 使得 $a^m + 1 = 0$。由于根据轨道-稳定子定理，$|G| = |\mathcal{O}||G_{P_{(a,0)}}|$，且根据引理 6.1，$\mathcal{O}$ 是 $\mathrm{Aut}(\mathcal{X}_3)$的一个轨道，因此 $P_{(a,0)}$ 在 $\mathrm{Aut}(\mathcal{X}_3)$中的稳定子 $\mathrm{Aut}(\mathcal{X}_3)^{P_{(a,0)}}$ 包含某个额外的自同构$\gamma \notin G_{P_{(a,0)}}$。此外，由于 $|S_2| = 2$ 且 $|G| = 2(q+1)^2$，γ 可以假设为奇数阶。

令 C_{q+1} 为由 σ 生成的循环群：$(x,y) \mapsto (x, \delta y)$，其中 δ 是一个本原的 $(q+1)$ 次单位根。由于 $\mathrm{Aut}(\mathcal{X}_3)^{P_{(a,0)}}$ 的驯分部是循环的，γ 与 C_{q+1} 交换，因此它作用于其不动点（一般情况下，也作用于轨道）。至此，证明的其余部分与定理 6.5 的证明完全相同。□

References

[1] M. Abd´on 和 F. Torres，特征二下的极大曲线，Manuscripta Math. 99 (1999), 39–53。

[2] D. Bartoli、M. Montanucci 和 F. Torres，$\mathbb{F}_{p^2}$-极大曲线若具有许多自同构，则是由厄米特曲线伽罗瓦覆盖的，Adv. Geom. 21 (2021), 325–336。[3] D. Bartoli、M. Montanucci 和 G. Zini，铃木曲线上每一点处的魏尔斯特拉斯半群，Acta Arith. 197 (2021) 1–20。[4] P. Beelen、L. Landi 和 M. Montanucci，Skabelund 极大曲线上的魏尔斯特拉斯半群，Finite Fields Appl. 72 (2021), 101811。[5] P. Beelen 和 M. Montanucci，Giulietti–Korchm´aros 曲线上的魏尔斯特拉斯半群，Finite Fields Appl. 52 (2018), 10–29。[6] N.L. Biggs 和 A.T. White，置换群与组合结构，伦敦数学会讲义丛书 33，剑桥大学出版社，剑桥—纽约，1979。[7] R. Fuhrmann、A. Garcia 和 F. Torres，关于极大曲线，J. Number Theory 67 (1997), 29–51。[8] R. Fuhrmann 和 F. Torres，具有许多有理点的有限域上曲线的亏格，Manuscripta Math. 89 (1996), 103–106。[9] R. Fuhrmann 和 F. Torres，关于魏尔斯特拉斯点与最优曲线，Rend. Circ. Mat. Palermo Suppl. 51 (1998), 25–46。[10] A. Garcia 和 F. Torres，关于具有经典魏尔斯特拉斯间隙的极大曲线。有限域上曲线的应用（西雅图，WA，1997），49–59，Contemp. Math. 245，美国数学会，普罗维登斯，RI，1999。[11] A. Garcia、P. Viana，某些非经典曲线上的魏尔斯特拉斯点，Arch. Math. 46 (1986), 315–322。[12] M. Giulietti 和 G. Korchm´aros，有限域上的一个新的极大曲线族，Math. Ann. 343 (2009), 229–245。[13] V.D. Goppa，几何与编码，Math. Appl. Kluwer，多德雷赫特，1988。[14] G.H. Hardy、E.M. Wright，数论导引，第 3 版。牛津，克拉伦登出版社，1960。[15] J.W.P. Hirschfeld、G. Korchm´aros 和 F. Torres，有限域上的代数曲线，普林斯顿应用数学丛书，普林斯顿，2008。[16] T. Høholdt、J.H. van Lint 和 R. Pellikaan，代数几何码，载于《编码理论手册》，V.S. Pless、W.C. Huffman 和 R.A. Brualdi 编。荷兰阿姆斯特丹：爱思唯尔 1 (1998), 871–961。[17] Y. I hara，关于有限域上代数曲线有理点数的一些评注，J. Fac. Sci. Tokyo 28 (1981), 721–724。[18] W.M. Kantor、M.E. O'Nan 和 G.M. Seitz，两个点的稳定子为循环群的二重传递群，J. Algebra 21 (1972), 17–50。[19] G. Korchm´aros 和 F. Torres，关于极大曲线的亏格，Math. Ann. 323 (2002), 589–608。[20] P. Mihailescu，初等分圆单位与卡塔兰猜想的证明，J. Reine Angew. Math. 572 (2004), 167–195。[21] H.G. R¨uck 和 H. Stichtenoth，有限域上厄米函数域的刻画，J. Reine Angew. Math. 457 (1994), 185–188。[22] H. Stichtenoth，代数函数域与编码，第二版。数学研究生教材，254。Springer-Verlag，柏林，2009。[23] K.O. St¨ohr 和 J.F. Voloch，魏尔斯特拉斯点与有限域上的曲线，Proc. London Math. Soc. 52 (1986), 1–19。[24] S. Tafazolian 和 F. Torres，关于 Ree 曲线，J. Pure and Appl. Alg. 223 (2019), 3831–3842。[25] M.A. Tsfasman、S. Vladut，代数几何码，Kluwer，多德雷赫特，1991。[26] G.D. Villa Salvador，代数函数域理论专题，数学：理论与应用，Birkh¨auser Boston, Inc.，波士顿，MA，2006。

Department of Applied Mathematics and Computer Science,
Technical University of Den-mark, Kongens Lyngby 2800, Denmark电子邮箱：pabe@dtu.dk

Department of Applied Mathematics and Computer Science, Technical University of Denmark, Kongens Lyngby 2800, Denmark电子邮箱：marimo@dtu.dk

Department of Applied Mathematics and Computer Science,
Technical University of Den-mark, Kongens Lyngby 2800, Denmark电子邮箱：lavi@dtu.dk