arXiv:2303.01984v1 [math.NT] 3 Mar 2023

特征为 p的 p^3 次非阿贝尔扩张的上分歧序列

G. GRIFFITH ELDER

Abstract. 我们对特征为 $p > 0$的局部域上的 p^3 次完全分歧非阿贝尔扩张的上分歧断点进行分类。我们发现，除了8阶二面体群外，每个 p^3阶非阿贝尔伽罗瓦群都可能出现非整数的上分歧断点。

1. Introduction

设 K 是一个局部域， L/K 是一个有限伽罗瓦扩张。Hasse-Arf定理指出，若Gal(L/K)是阿贝尔群，则 L/K的上分歧断点均为整数。但若Gal(L/K)是非阿贝尔群呢? 至少对于次数较小的非阿贝尔扩张，这些基本不变量的情况理应已得到充分了解。

本文完整描述了特征为 p的局部域上的 p^3 次完全分歧非阿贝尔扩张的上分歧断点序列。我们发现，二面体扩张的上分歧断点均为整数，而对于其他非阿贝尔群，则存在上分歧断点不是整数的扩张。在 [EH07], 中，作者与J. Hooper对包含四次单位根、特征为0且剩余特征为2的局部域上的四元数扩张进行了这一分类。

对于阿贝尔扩张，得益于包括 Miki 和 Thomas 在内的多位作者的研究，分歧断点序列已得到充分理解 [Mik81, Tho05]。

1.1. 阶为 p^3 的非阿贝尔群。

$$\begin{aligned} p = 2: \quad & Q_8 = \langle \sigma_1, \sigma_2 : \sigma_1^4 = 1, \sigma_1^2 = \sigma_2^2 = [\sigma_1, \sigma_2] \rangle, \\ & D_8 = \langle \sigma_1, \sigma_2 : \sigma_1^4 = \sigma_2^2 = 1, \sigma_1^2 = [\sigma_1, \sigma_2] \rangle, \\ p > 2: \ & H(p^3) = \langle \sigma_1, \sigma_2 : \sigma_1^p = \sigma_2^p = [\sigma_1, \sigma_2]^p = 1, [\sigma_1, \sigma_2] \in Z(H(p^3)) \rangle, \\ & M(p^3) = \langle \sigma_1, \sigma_2 : \sigma_1^{p^2} = \sigma_2^p = 1, \sigma_1^p = [\sigma_1, \sigma_2] \rangle. \end{aligned}$$

在所有情形中，阶为 p^3 的非阿贝尔群 G 都由两个元素生成，记作 σ_1、σ_2; 它们的交换子 $\sigma_3 = [\sigma_1, \sigma_2] = \sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2$ 生成该群的中心 $Z(G)$。

group-pres

备注 1.1. 将 σ_1 替换为 $\sigma_1' = \sigma_1\sigma_2^{-a}$, $a \in \mathbb{Z}$ 不会改变这些群表示中的任何一个。

Date: 2023年3月6日。

2010 *Mathematics Subject Classification.* 11S15。分歧，Hasse-Arf 定理。

前两个群分别可识别为四元数群和二面体群。第三个群是模 p 的海森堡群，可以用矩阵表示

$$H(p^3) \cong \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{F}_p \right\}$$

其元素取自 p 域。第四个群也可以用矩阵来表示

$$M(p^3) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}/(p^2), a \equiv 1 \bmod p \right\}.$$

当 $p = 2$时，请注意， $M(p^3)$ 和 D_8 的表示一致。

1.2. 局部域。本文中， K 是一个特征为 p 的域，它关于某个离散赋值是完备的，且具有完美剩余域。令K^{sep} 为 K的可分闭包；对于 K^{sep}/K的每个有限子扩张 L/K，令 v_L 为 K^{sep} 上的赋值，并将其标准化，使得 $v_L(L^\times) = \mathbb{Z}$。令 $\mathcal{O}_L$ 表示 L的整数环，令 $\mathcal{M}_L$ 表示 $\mathcal{O}_L$的极大理想，并令 π_L 为 L的一个一致化元。令 $\mathbb{F}_p$ 为含有 p 个元素的域。

1.3. 分歧断点。我们将 [Ser79，第四章] 中的内容专门应用于这样的情形： L/K 是一个次数为 p^3的完全分歧伽罗瓦扩张。定义下分歧子群 $G_i \leq G =$ 伽罗瓦群(L/K)如下：

$$G_i = \{\sigma \in \mathrm{Gal}(L/K) : v_L(\sigma(\pi_L) - \pi_L) \geq i + 1\}.$$

若 $G_b \supsetneq G_{b+1}$，则下分歧断点出现在 b。 [其他作者可能使用“跳跃”、“跳跃数”或“断点数”，而不使用“断点”。] 由于该扩张是完全分歧的，且 G 是一个 p-群，下分歧跳跃是与 p互素的正整数。若 $[G_b : G_{b+1}] = p^m$, $m \geq 1$，则称 b 以重数 $m \geq 1$出现。因此，下分歧序列中有 3 个断点 $l_1 \leq l_2 \leq l_3$。上分歧断点 $u_1 \leq u_2 \leq u_3$ 与下分歧断点之间的关系为： $u_1 = b_1$ 且 $u_i - u_{i-1} = (b_i - b_{i-1})/p^{i-1}$，其中 $i \in \{2, 3\}$。上分歧群 G^x （ $0 < x$ ）定义如下：令 $G^x = G_{b_1} = G$ （ $x \leq u_1$），$G^x = G_{b_i}$ （ $u_{i-1} < x \leq u_i$ ）， $i = 2$取 3，以及 $G^x = \{\mathrm{id}\}$ （ $u_3 < x$）。从伽罗瓦群 G 的分歧滤过转到子群 H的分歧滤过时，使用下分歧跳跃；也就是说， $H_i = G_i \cap H$。转到商群 G/H的分歧滤过时，则使用上分歧断点；也就是说，$(G/H)^i = (G^i H)/H$。

1.4. 特殊多项式。Weierstrass $\wp$-函数 $\wp(X) = X^p - X \in \mathbb{Z}[X]$ 是一个 $\mathbb{F}_p$-线性映射。回顾维特向量理论中的 Witt 多项式：

$$S(X_1, X_2) = \frac{X_1^p + X_2^p - (X_1 + X_2)^p}{p} \in \mathbb{Z}[X_1, X_2].$$

AS

1.5. Artin-Schreier扩张。在特征 p下，次数为 p 的循环扩张 L/K 都是 Artin-Schreier扩张。因此，对于某个 $x \in K^{\mathrm{sep}}$，有 $L = K(x)$，其中 $x^p - x = \kappa$，且 $\kappa \in K$。我们将 κ 称为 Artin-Schreier生成元（AS生成元）。如注记 2.1 所述，我们可以将 κ 替换为任意满足 $K^\wp = \{\wp(k) : k \in K\}$ 的 $\kappa' \in \kappa + K^\wp$，而不改变扩张 L/K。因此，由于 K是一个局部域，我们可以像在第 3 节中那样，假设 AS生成元 κ 是约化的；

也就是说， $v_K(\kappa) = $ 最大值$\{v_K(k): \ k \in \kappa + K^{\wp}\}$。若 L/K 是完全分歧的，则$b: = -v_K(\kappa) = -v_L(x) > 0$ 是 L/K的分歧断点，它与p互素。对于次数为 p 的循环扩张，上分歧断点和下分歧断点相同。结果

1.6. 主要结果。首先，我们用其阿廷–施赖尔生成元来描述这些扩张。此结果不要求 K 是局部域。

定理 1.2. 设 K 是特征为 $p > 0$ 的域。当且仅当 $L = K(x_1, x_2, x_3)$ 时，扩张 as-gen L/K 是伽罗瓦扩张，且伽罗瓦群 $\mathrm{Gal}(L/K)$ 为$\cong Q_8, D_8, H(p^3)$ 或 $M(p^3)$，其中

$$x_1^p - x_1 = \kappa_1, \qquad x_2^p - x_2 = \kappa_2, \qquad x_3^p - x_3 = \mathfrak{s}(x_1, x_2) + \kappa_3,$$

对于某个 $\kappa_i \in K$，使得 κ_1, κ_2 表示 $\mathbb{F}_p$ 上线性无关的 $K/K^{\wp}$ 的陪集，并且

$$\mathfrak{s}(x_1, x_2) = -\kappa_2 x_1 + \begin{cases} \kappa_1 x_1 + \kappa_2 x_2 & \mathrm{Gal}(L/K) \cong Q_8, \\ \kappa_1 x_1 & \mathrm{Gal}(L/K) \cong D_8, \\ 0 & \mathrm{Gal}(L/K) \cong H(p^3), \\ S(x_1, \kappa_1) & \mathrm{Gal}(L/K) \cong M(p^3). \end{cases}$$

注意，对于 $p = 2$， $S(x_1, \kappa_1) = \kappa_1 x_1$。

此外，伽罗瓦群 $\mathrm{Gal}(L/K) = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$ 由

$$(\sigma_i - 1)x_j = \delta_{ij},$$

克罗内克 δ 函数确定，对所有满足 $1 \le i, j \le 3$ 的数对 (i, j)，以下两种情况除外: $(i, j) = (1, 3)$ 和 $(2, 3)$。对于 $(i, j) = (1, 3)$，有

$$(\sigma_1 - 1)x_3 = -x_2 + \begin{cases} x_1 & \mathrm{Gal}(L/K) \cong Q_8, \\ x_1 & \mathrm{Gal}(L/K) \cong D_8, \\ 0 & \mathrm{Gal}(L/K) \cong H(p^3), \\ S(x_1, 1) & \mathrm{Gal}(L/K) \cong M(p^3). \end{cases}$$

对于 $(i, j) = (2, 3)$，有

$$(\sigma_2 - 1)x_3 = \begin{cases} x_2 & \mathrm{Gal}(L/K) \cong Q_8, \\ 0 & \mathrm{Gal}(L/K) \cong D_8, H(p^3), M(p^3). \end{cases}$$

注 1.3。定理 1.2 这样的定理可能存在，并不令人意外。Saltman 已证明，对于伽罗瓦群的阶为 p^n, $n \ge 1$ [的所有伽罗瓦扩张，都存在这样的描述[Sal78, 推论 2.5]]。定理 1.2 所做的、而 [Sal78], 中没有的，是明确描述项 $\mathfrak{s}(x_1, x_2)$。 Witt/Saltman

注 1.4。注意，对于 $p = 2$, $S(x_1, \kappa_1) = \kappa_1 x_1$ 和 $S(x_1, 1) = x_1$。因此，不出所料，关系 $\mathfrak{s}(x_1, x_2)$ 对于 D_8- 和 $M(p^3)$- 扩张的描述是一致的。注意，对于 $p > 2$, $\wp(x_i^2) = 2x_i\kappa_i + \kappa_i^2$，因此 $x_i\kappa_i \in K(x_i)^{\wp} + K$ 对于$i = 1, 2$。这意味着我们可以选择令 $\mathfrak{s}(x_1, x_2) = -\kappa_2 x_1 + \kappa_1 x_1 + \kappa_2 x_2$，对于 $\mathrm{Gal}(L/K) \cong H(p^3)$，这样 $\mathfrak{s}(x_1, x_2)$ 对于 Q_8- 和 $H(p^3)$- 扩张的描述便一致了。最后，注意 $\wp(x_1 x_2) = \kappa_2 x_1 + \kappa_1 x_2 + \kappa_1\kappa_2$。因此， $-\kappa_2 x_1 \equiv \kappa_1 x_2$ (模 $K(x_1, x_2)^{\wp} + K$)。将 x_3 替换为 $-x_3$ 后，我们可以选择令 $\mathfrak{s}(x_1, x_2) = -\kappa_1 x_2 + \kappa_1 x_1 + \kappa_2 x_2$，对于 $\mathrm{Gal}(L/K) \cong Q_8$，并选择令 $\mathfrak{s}(x_1, x_2) = -\kappa_1 x_2$，对于 $\mathrm{Gal}(L/K) \cong H(p^3)$。这些替换表明，定理 1.2 中所描述的 $Q_8, H(p^3)$ 的伽罗瓦扩张在换位作用下保持不变

换位 (1 2) 作用于下标上，正如两个群表示对群的描述保持不变一样。这是一个令人欣慰而非令人惊讶的观察。

为便于使用定理 1.2 确定分歧断点，我们将该结果特化到局部域的情形。

ram-as-gen
推论 1.5. 设 K 是特征为 $p > 0$ 的局部域。扩张 L/K 是伽罗瓦群为 $\mathrm{Gal}(L/K) \cong Q_8$, $D_8, H(p^3)$ 或 $M(p^3)$ 的全分歧伽罗瓦扩张，当且仅当定理 1.2 的内容成立，但需将陈述

- 使得“κ_1, κ_2 表示 $K/K^\wp$ 的 $\mathbb{F}_p$-线性无关陪集”

替换为另一种陈述

- “满足 $v_K(\kappa_i) = -b_i < 0$ 且 $p \nmid b_i$，并且若 $b_1 = b_2$ ，则不失一般性，κ_1, κ_2 在$\kappa_2\mathcal{O}_K/\kappa_2\mathcal{M}_K$中表示 $\mathbb{F}_p$-线性无关的陪集，”

作此替换后，定理 1.2 的结论成立。

精确界
定理 1.6. 设 K 是特征为 $p > 0$ 且剩余域完美的局部域。设 M/K 是一个完全分歧的C_p^2-扩张，其上分歧断点为$u_1 \le u_2$。因此，对某些满足 $\wp(y_i) = \beta_i$且 $v_K(\beta_i) = u_i$的 $y_1, y_2 \in K^{\mathrm{sep}}$ ，有 $M = K(y_1, y_2)$。将 M/K 嵌入伽罗瓦扩张 N/K 中，其伽罗瓦群为 $\mathrm{Gal}(N/K) = G \cong D_8, H(p^3)$ $M(p^3)$ 或 Q_8，如定理 1.2 所述。

[注：定理 1.2 中的 x_i 由伽罗瓦群的生成元确定，具体如（1）所述。 $y_i = x_i$不一定成立。参见注记 3.1。]

对于每个群 G，存在一个下界 B_G ，使得 N/K 的上分歧断点为 $u_1 \le u_2 \le u_3$ ，其中 $B_G \le u_3$ ，并且若 $B_G < u_3$ ，则 u_3 是与 p互素的整数。下面仅需描述这些下界 B_G:

$$B_{D_8} = \begin{cases} u_1 + u_2 & \text{for } u_2 = u_1 \text{ or } G_{l_2} = \langle \sigma_1^p, \sigma_2 \rangle, \\ 2u_2 & \text{for } u_2 \ne u_1 \text{ and } G_{l_2} = \langle \sigma_1 \rangle. \end{cases}$$

根据引理 3.6

$$\beta_2 = \mu_0^p + \sum_{i=1}^{p-1} \mu_i^p \beta_1^i$$

对于满足其中所述某些技术条件的某个 $\mu_i \in K$ 。令

$$r = -v_K\left(\sum_{i=1}^{p-2} \mu_i^p \beta_1^i\right), \qquad s = -v_K(\mu_{p-1}^p \beta_1^{p-1}).$$

注意， $s \equiv -u_1$模 p、 $r \ne 0$、 $-u_1$模 p，并且 $u_2 =$最大$\{r, s\}$。于是

$$B_{H(p^3)} = \max\left\{s + u_1, r + \frac{u_1}{p}\right\}.$$

若用于定义 s的 μ_{p-1}满足 $\mu_{p-1} \in -1 + \mathcal{M}_K$，则设 $\epsilon = \mu_{p-1} + 1$并

$$t = -v_K(\epsilon^p \beta_1^{p-1}).$$

Then

$$B_{M(p^3)}=\begin{cases}\max\left\{pu_1,s+u_1,r+\frac{u_1}{p}\right\} & \text{for } \mu_{p-1}\neq -1 \bmod \mathcal{M}_K, \text{ and } u_2=u_1 \text{ or } G_{l_2}=\langle\sigma_1^p,\sigma_2\rangle,\\ \max\left\{(p-1)u_1+\frac{u_1}{p},t+u_1,r+\frac{u_1}{p}\right\} & \text{for } \mu_{p-1}=-1 \bmod \mathcal{M}_K, \text{ and } u_2=u_1 \text{ or } G_{l_2}=\langle\sigma_1^p,\sigma_2\rangle,\\ pu_2 & \text{for } u_2\neq u_1 \text{ and } G_{l_2}=\langle\sigma_1\rangle.\end{cases}$$

由引理 3.6， $\beta_2\equiv\mu^p\beta_1$ 模 $\mathcal{O}_K$。若 $u_2=u_1$，则对于某个满足 $v_K(\epsilon)=e>0$ 的单位根 $\omega\in\mathcal{O}_K/\mathcal{M}_K$，有 $\mu=\omega+\epsilon$ 和 $\epsilon\in\mathcal{M}_K$。令

$$B_{Q_8}=\begin{cases}2u_2 & \text{for } u_2\neq u_1, \text{ or } u_2=u_1,\omega^3\neq 1,\\ \max\left\{\frac{3u_1}{2},2u_1-2e\right\} & \text{for } u_2=u_1,\omega^3=1.\end{cases}$$

注 1.7。Hasse-Arf 定理的结论是，上分歧断点均为整数。由于 B_{D_8} 是整数，该结论对 $G\cong D_8$仍然成立。由于对于 $G\cong Q_8$， $B_G(p^3)$ $M(p^3)$可能不是整数，因此 Hasse-Arf 定理对 $H(p^3)$ $M(p^3)$可能不成立。

1.7. 概要。§1.5 中所述的约化的阿廷-施赖尔生成元与C_p-扩张的分歧断点之间的联系，是我们用来确定这些扩张的上分歧断点的工具。因此，我们先在 §2 推导定理 1.2 和推论 1.5 中所述的阿廷-施赖尔生成元。回顾一下， $l_1\le l_2\le l_3$ 表示 N/K 的下分歧跳跃。利用 [Ser79，第四章，命题 10], ，我们将证明 $G_{l_3}=Z(G)$ $=\langle\sigma_3\rangle$。由于 $\langle\sigma_3\rangle$ 是一个分歧子群， N/M 的分歧断点就是 N/K的第三下分歧断点 l_3。这意味着，要确定 l_3，只需约化阿廷-施赖尔生成元 $\mathfrak{s}(x_1,x_2)+\kappa_3\in M$，不过，§1.5 中给出的“约化”概念对我们的目的而言略显简单。因此，在第 3 节中，我们将推广这一概念，并用它来确定某些辅助 C_p-扩张的分歧断点。接着在 §4 中，我们运用分歧理论将这些结果综合起来，以确定 $M(x_3)/M$的分歧断点。由此可得上分歧断点 $u_1\le u_2\le u_3$。最后，我们在 §5 中指出这些结果在诺丁汉群中的应用。

2. Artin-Schreier generators

设 K 是特征为 $p>0$ 的域。注意：本节的结果并不要求 K 是局部域。设嵌入 N/K 是伽罗瓦扩张，且 Gal(N/K) 为 $=\langle\sigma_1,\sigma_2\rangle\cong Q_8,D_8,H(p^3)$ 或 $M(p^3)$，采用（1）中的记号。令 $M=N^{\sigma_3}$ 满足 $\sigma_3=[\sigma_1,\sigma_2]$，表示 Gal$(N/K)$ 的中心的不变域。在每种情况下，$\langle\sigma_1,\sigma_2\rangle/\langle\sigma_3\rangle\cong C_p^2$。因此，不失一般性，我们可以假设 $M=K(x_1,x_2)$，其中某个 $x_i\in N$ 满足 $\wp(x_i)=\kappa_i$，且某些 $\kappa_i\in K$, $i=1,2$ 表示 $\mathbb{F}_p$-线性无关的 $K/K^\wp$ 的陪集，并且对于 $1\le i,j\le 2$，有 $(\sigma_i-1)x_j=\delta_{ij}$。 t echnicalities

注记 2.1. 在第 3 节应用本节的结果时，我们将假设在准备步骤中，阿廷–施赖尔生成元 κ_1,κ_2 已按此处列出的两种方式进行了调整。但由于本节其余部分不需要这一步骤，我们暂不假设已完成此调整。

(1) 注意，对于所有 $\kappa\in K$， $K(x_i)=K(x_i+\kappa)$。因此，对于所有满足 $\wp(x_i')$ $\in\kappa_i+K^\wp$ 的 $x_i'\in N$， $K(x_i)=K(x_i')$，其中 $K^\wp=\{\wp(\kappa):\kappa\in K\}$。我们可以用 $\kappa_i+K^\wp$ 中的任意元素替换 κ_i，而不改变 $M=K(x_1,x_2)$。

(2) 注意，对于 $x_2' = ax_1 + x_2$, $a \in \mathbb{Z}$, $M = K(x_1, x_2) = K(x_1, x_2')$。我们可以用 x_1' 替换 x_1，同时用 $a\kappa_1 + \kappa_2$ 替换 κ_1，而不改变 $M = K(x_1, x_2)$ 的描述。此外，如果我们用 $\sigma_1' = \sigma_1\sigma_2^{-a}$ 替换 σ_1，那么 σ_1', σ_2 对 x_1, x_2' 的作用方式，与 σ_1, σ_2 对 x_1, x_2 的作用方式相同。根据备注 1.1，用 $\sigma_1' = \sigma_1\sigma_2^{-a}$ 替换 σ_1 不会改变伽罗瓦群的表示。

我们对伽罗瓦扩张剩余部分（即 N/M）的描述取决于具体的伽罗瓦群。

2.1. Q_8。由于 N/M 是二次扩张，因此对于某个 $x_3 \in N$，有 $N = M(x_3)$，使得 $\wp(x_3) \in M$ 且 $(\sigma_3 - 1)x_3 = 1$。对于 $i = 1$，存在 $A_i \in N$ 使得 $(\sigma_i - 1)x_3 = A_i$。由于对于 $i = 1, 2$ 有 $[\sigma_i, \sigma_3] = 1$，我们发现 A_i 属于 σ_3的不变域。因此 $A_i \in M$。由于对于 $i = 1, 2$ 有 $(\sigma_i - 1)^2 = (\sigma_3 - 1)$，我们发现 $(\sigma_i - 1)A_i = 1$。因此 $A_i - x_i$ 属于 $\langle\sigma_3, \sigma_i\rangle$的不变域。换言之，

$$A_1 - x_1 \in K(x_2), \qquad A_2 - x_2 \in K(x_1).$$

存在 a、b、c、$d \in K$，使得 $A_1 = a + bx_2 + x_1$ 且 $A_2 = c + dx_1 + x_2$。将 $\sigma_1\sigma_2 = \sigma_2\sigma_1\sigma_3$ 应用于 x_3。结果为 $x_3 + A_1 + \sigma_1(A_2) = x_3 + A_2 + \sigma_2(A_1) + 1$。因此

$$(\sigma_1 - 1)A_2 = (\sigma_2 - 1)A_1 + 1.$$

由此，我们确定 $d = b + 1$。注意到 $x_3' = x_3 + dx_1x_2 + ax_1 + cx_2$满足 $\wp(x_3') \in M$, $(\sigma_3 - 1)x_3' = 1$。因此，我们可以用 x_3' 替换 x_3，从而不失一般性地得到

$$(\sigma_1 - 1)x_3 = x_1 + x_2, \qquad (\sigma_2 - 1)x_3 = x_2.$$

令 $T = \wp(x_3) \in M$。由于 $(\sigma_1 - 1)x_3 = x_1 + x_2$，我们得到 $(\sigma_1 - 1)T = \kappa_1 + \kappa_2$。由于 $(\sigma_2 - 1)x_3 = x_2$，$(\sigma_2 - 1)T = \kappa_2$。因此，$T - (\kappa_1 + \kappa_2)x_1 - \kappa_2x_2$ 同时被 σ_1 和 σ_2固定。因此，对于某个 $\kappa_3 \in K$，有 $T = (\kappa_1 + \kappa_2)x_1 + \kappa_2x_2 + \kappa_3$。

2.2. $D_8, H(p^3)$ $M(p^3)$。令 $L = N^{\sigma_2, \sigma_3}$ 为 $\langle\sigma_2, \sigma_3\rangle$的不变域，其中 $\sigma_3\rangle$是一个阶为 p^2 的正规子群。因此 $L = K(x_1)$，且 $\wp(x_1) = \kappa_1$。注意，N/L 是一个 C_p^2 扩张，并考虑 N^{σ_2}/L，一个次数为 p 的循环扩张。σ_3 的像生成伽罗瓦群 $\mathrm{Gal}(N^{\sigma_2}/L)$。因此，不失一般性，$N^{\sigma_2} = L(x_3)$，其中 $x_3 \in N$ 满足 $\wp(x_3) \in L$ 且 $(\sigma_3 - 1)x_3 = 1$。由于 $x_3 \in N^{\sigma_2}$，$(\sigma_2 - 1)x_3 = 0$。

我们还需要确定 $(\sigma_1 - 1)x_3 = A \in N$。由于 $[\sigma_1, \sigma_3] = 1$, $A \in M$。将 $\sigma_1\sigma_2 = \sigma_2\sigma_1\sigma_3$ 应用于 x_3，可得 $(\sigma_2 - 1)A = -1$。这意味着 $A + x_2$ 被 σ_2 固定，因此 $A + x_2 \in L$。接下来的讨论取决于该群。

2.2.1. $H(p^3)$。对 $A + x_2 \in L$ 应用迹 $\mathrm{Tr}^{L/K}$，并求得 $\mathrm{Tr}^{L/K}(A + x_2) = (\sigma_1^p - 1)x_3 + px_2 = 0$。因此，根据希尔伯特定理90的加法版本，存在一个 $\ell \in L$，使得 $(\sigma_1 - 1)\ell = A + x_2$。令 $x_3' = x_3 - \ell$。注意到$\wp(x_3') \in L$，$(\sigma_3 - 1)x_3' = 1$，$(\sigma_2 - 1)x_3' = 0$ 以及 $(\sigma_1 - 1)x_3' = -x_2$。因此，不失一般性，我们重新标记，使得 x_3 具有以下性质：

$$(\sigma_2 - 1)x_3 = 0, \qquad (\sigma_1 - 1)x_3 = -x_2.$$

令 $T = \wp(x_3) \in L$。由于 $(\sigma_1 - 1)x_3 = -x_2$，我们得到 $(\sigma_1 - 1)T = -\kappa_2$。因此，$T + \kappa_2x_1 \in L$ 被 σ_1固定，这意味着对于某个 $\kappa_3 \in K$，$T + \kappa_2x_1 \in K$ 和 $T = -\kappa_2x_1 + \kappa_3$。

2.2.2. $D_8, M(p^3)$。注意，当 $p=2$ 时， $S(x_1,\kappa_1)=\kappa_1 x_1$。因此， D_8 并非一个独立的情形。由于众所周知， $S(x_1,1)\ S(x_1,\kappa_1)\in L$ 满足 $\mathrm{Tr}_{L/K}S(x_1,1)=1$，且 $(\sigma_1-1)S(x_1,\kappa_1)=\wp(S(x_1,1))$，这些恒等式的验证留给读者；具体而言，

$$\mathrm{Tr}_{L/K}\left(\frac{x_1^p+1-(x_1+1)^p}{p}\right)=1,$$

$$(\sigma_1-1)\left(\frac{x_1^p+\kappa_1^p-(x_1+\kappa_1)^p}{p}\right)=\wp\left(\frac{x_1^p+1-(x_1+1)^p}{p}\right).$$

现在可以继续了。对 $A+x_2-S(x_1,1)\in L$ 应用迹 $\mathrm{Tr}^{L/K}$，并求出 $\mathrm{Tr}^{L/K}(A+x_2-S(x_1,1))=(\sigma_1^p-1)x_3+px_2-1=0$。因此，根据希尔伯特定理90的加法版本，存在一个 $\ell\in L$，使得 $(\sigma_1-1)\ell=A+x_2-S(x_1,1)$。令 $x_3'=x_3-\ell$。注意， $\wp(x_3')\in L$， $(\sigma_3-1)x_3'=1$， $(\sigma_2-1)x_3'=0$ 且 $(\sigma_1-1)x_3'=-x_2+S(x_1,1)$。因此，不失一般性，我们重新标记，使 x_3 具有这些性质：

$$(\sigma_2-1)x_3=0,\qquad (\sigma_1-1)x_3=-x_2+S(x_1,1).$$

再令 $T=\wp(x_3)\in L$。由于 $(\sigma_1-1)x_3=-x_2+S(x_1,1)$，我们得到 $(\sigma_1-1)T=-\kappa_2+(\sigma_1-1)S(x_1,\kappa_1)$。因此， $T+\kappa_2x_1-S(x_1,\kappa_1)\in L$ 被σ_1固定。我们得出结论，对于某个 $\kappa_3\in K$， $T=-\kappa_2x_1+S(x_1,\kappa_1)+\kappa_3$。

反向结论可由 [Sal78，推论 2.5] 得出。不过，鉴于这些扩张次数较小，读者可能希望看到反向结论的详细推导，因此我们给出一个概要。首先，我们引入一个引理：

反向结论

引理2.2。设 K 是一个特征为 $p>0$ 的局部域， M/K 是一个 C_p^2-扩张，且伽罗瓦群 $\mathrm{Gal}(M/K)=\langle\bar\sigma_1,\bar\sigma_2\rangle$；再设 N/M 是一个 C_p-扩张，满足 $N=M(x)$，其中某个 $x\in K^{\mathrm{sep}}$ 满足 $x^p-x=\mu$，且 $\mu\in M$。假设

$$(\bar\sigma_i-1)\mu\in M^{\wp}$$

对于 $i=1,\ 2$。则 N/K 是伽罗瓦扩张。

证明。根据假设，对于 $i=1,\ 2$，存在 $\mu_i\in M$ 使得 $\bar\sigma_i(\mu)=\mu+\wp(\mu_i)$。 $\bar\sigma_1$、 $\bar\sigma_2$ 均可扩张为同构 σ_1、 σ_2，其将 N 映入 K^{sep}。注意， $\sigma_i(x)\in K^{\mathrm{sep}}$ 是 $X^p-X=\bar\sigma_i(\mu)\in M[X]$ 的一个根。因此， $\sigma_i(x)-\mu_i$ 是 $X^p-X=\mu$ 的一个根，这意味着 $\sigma_i(x)\in N$。结论成立。□

考虑 $p>2$, $\wp(x_1)=\kappa_1$, $\wp(x_2)=\kappa_2$，且 $\wp(x_3)=-\kappa_2x_1+S(x_1,\kappa_1)+\kappa_3$ 的情形。为证明 $M(x_3)/K$ 是伽罗瓦扩张，我们使用引理2.2。将 (σ_1-1) 应用于 AS生成元 $-\kappa_2x_1+S(x_1,\kappa_1)+\kappa_3$，得到 $-\kappa_2+(\sigma_1-1)S(x_1,\kappa_1)=\wp(-x_2+S(x_1,1))\in M^{\wp}$。应用 (σ_2-1)，得到 $0\in M^{\wp}$。

既然 N/K 是伽罗瓦扩张，我们就根据 σ_1、 σ_2 在 x_3上满足的关系来确定其伽罗瓦群。由于

$$\wp((\sigma_2-1)x_3)=(\sigma_2-1)\wp(x_3)=0,$$

我们确定 $(\sigma_2-1)x_3$ 满足 $X^p-X=0$，因此 $(\sigma_2-1)x_3=c\in\mathbb{F}_p$。所以 $(\sigma_2^p-1)x_3=0$，且 $(\sigma_1-1)(\sigma_2-1)x_3=0$。我们已证明 $|\sigma_2|=p$。由于

$$\wp((\sigma_1-1)x_3)=(\sigma_1-1)\wp(x_3)=-\kappa_2+\wp(S(x_1,1)),$$

我们发现 $(\sigma_1 - 1)x_3 + x_2 - S(x_1, 1) = d \in \mathbb{F}_p$。因此 $(\sigma_1^p - 1)x_3 = (1 + \sigma_1 + \cdots \sigma_1^{p-1})S(x_1, 1) = 1$ 和 $(\sigma_2 - 1)(\sigma_1 - 1)x_3 = -1$。我们已证明 $(\sigma_2^{p^2} - 1)x_3 = 1$，因此 $|\sigma_2| = p^2$。此外，将.....放在一起

$$(\sigma_1 - 1)(\sigma_2 - 1)x_3 = 0,$$
$$(\sigma_2 - 1)(\sigma_1 - 1)x_3 = -1,$$

我们发现 $\sigma_1\sigma_2(x_3) - \sigma_2\sigma_1(x_3) = 1$，这意味着 $([\sigma_1, \sigma_2] - 1)x_3 = 1$，因此 $[\sigma_1, \sigma_2] = \sigma_2^p$。其余三种情形留给读者。

3. Reducing the Artin-Schreier generators

设 K 是特征为 $p > 0$ 的局部域，并设 N/K 是由定理 1.2 和推论 1.5 中给出的阿廷–施莱尔方程确定的、次数为 p^3 的全分歧非阿贝尔扩张。于是，伽罗瓦群 $G = \mathrm{Gal}(N/K)$ 由 σ_1、σ_2 生成，其中 $\sigma_3 = [\sigma_1, \sigma_2]$ 生成中心 $Z(G)$，其阶为 p，并固定子域 M；该子域是 K 的 C_p^2-扩张。回顾下分歧群的记号 G_i。令 $u_1 \le u_2 \le u_3$ 表示 N/K 的上分歧断点，$l_1 \le l_2 \le l_3$ 表示其下分歧断点。

在 [Ser79 的第四章命题 10], 中可以看出，如果 $\sigma \in G_i \setminus G_{i+1}$ 和 $\sigma' \in G_j \setminus G_{j+1}$，那么 $[\sigma, \sigma'] \in G_{i+j+1}$。因此，$G_{l_3}$ 中的元素属于中心 $Z(G)$，并且由于 G_{l_3} 非平凡，而中心 $Z(G)$ 的阶为 p，

$$G_{l_3} = Z(G) = \langle \sigma_3 \rangle.$$

既然我们已经证明 M 是不变域的一个分歧群的不变域，我们利用[Ser79 的第四章命题 3、推论]得出，M/K 的下分歧断点和上分歧断点分别为 $l_1 \le l_2$ 和 $u_1 \le u_2$。N/M 的分歧断点为 l_3，并且 u_3 由 $l_3 - l_2 = p^2(u_3 - u_2)$ 确定。因此，为确定上分歧序列，只需确定 C_p-扩张 $M(x_3)/M$ 的分歧断点，其中

$$\wp(x_3) = \mathfrak{s}(x_1, x_2) + \kappa_3$$

其中 $\kappa_3 \in K$ 和 $\mathfrak{s}(x_1, x_2)$ 已在定理 1.2 和推论 1.5 中描述。因此，本节的主要目的是“化简”这个 Artin-Schreier 生成元。

定义元素 $\kappa \in K$ 的 K-群赋值[1] 为陪集 $\kappa + K^\wp$, $K^\wp = \{\wp(\kappa) : \kappa \in K\}$ 中各元素所能达到的最大赋值；即，

$$g\nu_K(\kappa) = \max\{v_K(x) : x \in \kappa + K^\wp\}.$$

显然，$g\nu_K$ 在加法群 $K/K^\wp$ 上定义良好，并且 $g\nu_K(\kappa) = \infty$ 当且仅当 $\kappa \in K^\wp$，而

$$g\nu_K(\kappa_1 + \kappa_2) \ge \min\{g\nu_K(\kappa_1), g\nu_K(\kappa_2)\}$$

当 $g\nu_K(\kappa_1) \ne g\nu_K(\kappa_2)$ 时取等号。因此，一旦与指数函数 $\exp \circ g\nu_K$：$K/K^\wp \to \Re_{>0} \cup \{\infty\}$ 复合，我们便得到一个满足群赋值条件的函数；Larson 将这一概念归功于 Zassen-haus [Lar76]。群赋值需要满足四个条件，而由于加法满足交换律且 $\mathrm{char}(K) = p$，其余两个条件显然成立。

[1] 这是 1-单位 [的 *defect* 的加法类比（Wym69，第 141] 页）。

众所周知， $\mathbb{F}_p$-线性映射

wp (2)
$$\wp : \mathcal{M}_K^i/\mathcal{M}_K^{i+1} \longrightarrow \begin{cases} \mathcal{M}_K^i/\mathcal{M}_K^{i+1} & \text{for } i \geq 0, \\ \mathcal{M}_K^{pi}/\mathcal{M}_K^{pi+1} & \text{for } i < 0, \end{cases}$$

对于 $i \neq 0$，它是一个同构；而对于 $i = 0$，其核为 $\ker \wp = \mathbb{F}_p$。由此可知 $\mathcal{M}_K \subseteq K^\wp$。因此，对于 $\kappa \in \mathcal{M}_K$， $g\nu_K(\kappa) = \infty$。另一个推论是，对于 $\kappa \notin \mathcal{M}_K$， $g\nu_K(\kappa)$ 要么为零，要么等于一个与 p 互素的负整数。这一点用于证明： $K(x)/K$ 要么满足 $\wp(x) = \kappa$ 未分歧，要么分歧，此时 $p \nmid v_K(\kappa) < 0$，且 $b = -v_K(\kappa)$ 是 $K(x)/K$ 的分歧断点。

回顾注记 2.1 (1)，其中指出我们可以用任意 $x \in \kappa_i + K^\wp$ 替换 κ_i。因此，假设我们已在 §2 中进行了这种替换，从而每个 κ_i 都是 K-约化的[2]；也就是说，$v_K(\kappa_i) = g\nu_K(\kappa_i)$。由于 N/K 是完全分歧的，子扩张 $K(x_i)/K$均分歧，分歧断点为 $b_i = -v_K(\kappa_i)$。注记 2.1 (2) 指出，我们还可以用 $x_2' = ax_1 + x_2$ 替换 x_2，并用 $\sigma_1' = \sigma_1\sigma_2^{-a}$ 替换 σ_1，而不改变对 M 的描述或群的表示。随后我们可以重新标记，使得不仅 κ_1、κ_2 是约化的，且对于 $1 \leq i$、$j \leq 2$，$(\sigma_i - 1)x_j = \delta_{ij}$；而且若 $v_K(\kappa_1) = v_K(\kappa_2)$，等价地， $b_1 = b_2$，则 κ_1、κ_2 在 $\kappa_1\mathcal{O}_K/\kappa_1\mathcal{M}_K$ 中表示 $\mathbb{F}_p$-线性无关的元素。因此我们可以记为

单分歧 k (3)
$$u_1 = \min\{b_1, b_2\} \text{ and } u_2 = \max\{b_1, b_2\}$$

我们当前的记号将 M 表示为 $K(x_1, x_2)$，其中下标由伽罗瓦群确定。在 §2 中，伽罗瓦群居于核心位置，因此这种选择很自然。$\langle \sigma_2, \sigma_3 \rangle$ 的不变域是 $K(x_1)$，其中 $\wp(x_1) = \kappa_1$，且 $v_K(\kappa_1) = -b_1$。$\langle \sigma_1, \sigma_3 \rangle$ 的不变域是 $K(x_2)$，其中 $\wp(x_2) = \kappa_2$，且 $v_K(\kappa_2) = -b_2$。在本小节中，分歧居于核心位置，因此我们的记号显得不便。为此，我们令 $\{x_1, x_2\} = \{y_1, y_2\}$，使得 $\wp(y_i) = \beta_i \in K$，从而$K(y_1)/K$ 和 $K(y_2)/K$ 分别具有分歧断点 $u_1 = -v_K(\beta_1)$ $u_2 = -v_K(\beta_2)$。

x-y-switch

注记 3.1. 由于 Q_8 和 $H(p^3)$ 的群表示在换位 (1 2) 下是对称的，我们可以假设， Q_8 和 $H(p^3)$ 的群表示下标从一开始就是根据分歧滤过选定的。因此，对于这两个群，$y_1 = x_1$ 和 $y_2 = x_2$。只有对于群 D_8和 $M(p^3)$，引入 y_1, y_2 才有影响。对于这两个群，由于 (3)，当 $b_1 \leq b_2$时，我们有 $y_i = x_i$；当 $b_1 > b_2$时，我们有 $y_1 = x_2$，$y_2 = x_1$。换言之，对于 $i = 1$，我们有 $y_i = x_i$；当 $u_2 = u_1$或 $G_{l_2} = \langle \sigma_1^p$时，我们有 $2, \sigma_2\rangle$。当 $u_2 \neq u_1$ 时，我们有 $y_1 = x_2, y_2 = x_1$，并且 $G_{l_2} = \langle \sigma_1 \rangle$。

利用注记 3.1，我们将定理 1.2 中关于 $\mathfrak{s}(x_1, x_2)$ 的公式转化为关于 $y_1, y_2, \beta_1, \beta_2$ 的表达式。

s(y,y) (4)
$$\mathfrak{s}(x_1, x_2) = \begin{cases} -\beta_2 y_1 + \beta_1 y_1 + \beta_2 y_2 & \mathrm{Gal}(L/K) \cong Q_8, \\ -\beta_2 y_1 & \mathrm{Gal}(L/K) \cong H(p^3), \\ -\beta_2 y_1 + S(y_1, \beta_1) & \mathrm{Gal}(L/K) \cong D_8, M(p^3) \text{ and} \\ & \quad u_2 = u_1 \text{ or } G_{l_2} = \langle \sigma_1^p, \sigma_2 \rangle, \\ -\beta_1 y_2 + S(y_2, \beta_2) & \mathrm{Gal}(L/K) \cong D_8, M(p^3) \text{ and} \\ & \quad u_2 \neq u_1 \text{ and } G_{l_2} = \langle \sigma_1 \rangle. \end{cases}$$

[2]这是标准术语。 *e.g.* 《Tho05》第 [节中的约化 Witt 向量4]

回顾一下，对于 $p=2$, $\beta_i y_i = S(y_i,\beta_i)$，其中 $i=1$ 为 2。此外，对于伽罗瓦群$(L/K)\cong D_8, M(p^3)$。 $u_2 \neq u_1$ 和 $G_{l_2}=\langle\sigma_1\rangle$，注 1.4 说明

$$-\beta_1 y_2 = -\kappa_2 x_1 \equiv \kappa_1 x_2 = \beta_2 y_1 \pmod{M^{\wp}+K}.$$

因此，我们记录（4）的如下调整：对于 $\mathrm{Gal}(L/K)\cong D_8, M(p^3), u_2\neq u_1$ 和 $G_{l_2}=\langle\sigma_1\rangle$, 我们可以改用

(5) gD,gM-调整
gD,gM-调整

$$\mathfrak{s}(x_1,x_2) = \beta_2 y_1 + S(y_2,\beta_2).$$

现在，我们利用对 $H(p^3)$-扩张的描述来引出下一个定义。在那里我们看到 $N=M(x_3)$，其中 $x_3^p - x_3 = -\beta_2 y_1 + \kappa_3$ 对某个 $\kappa_3 \in K$成立。此外，当 κ_3 遍历 K 中的所有元素时，域 $N=M(x_3)$ 遍历所有包含 $M=K(x_1,x_2)=K(y_1,y_2)$ 的 $H(p^3)$-扩张 N/K 。对 N/K的下分歧断点/上分歧断点以及与之相关的分歧群作出的任何确定，都会刻画 C_p-扩张 N/M的分歧断点，因而必然确定 $\max\{v_M(\tau): \tau\in -\beta_2 y_1 + M^{\wp}+K\}$ 的值。然而 $-\beta_2 y_1 \in K(y_1)$，所以我们先在子域 $K(y_1)$中进行计算

$$\max\{v_{K(y_1)}(\tau): \tau \in -\beta_2 y_1 + K(y_1)^{\wp} + K\}.$$

这引出如下定义：给定一个分歧的 C_p-扩张 L/K，元素 $\ell\in L$ 的 L/K-群赋值为:

$$g\nu_{L/K}(\ell) = \max\{v_L(x): x\in \ell + L^{\wp} + K\}.$$

注意，当且仅当 $\ell \in L^{\wp}+K$ $g\nu_{L/K}(\ell)=\infty$ 且

valval (6)
$$g\nu_{L/K}(\ell+\ell') \geq \min\{g\nu_{L/K}(\ell), g\nu_{L/K}(\ell')\}$$

且当 $g\nu_{L/K}(\ell)\neq g\nu_{L/K}(\ell')$ 时等号成立。注意，若 $g\nu_{L/K}(\ell)<\infty$，则$g\nu_{L/K}(\ell)<0$。给定一个具有有限 L/K-群赋值 $g\nu_{L/K}(\ell)$ 的 $\ell\in L$，存在$l\in L$、$k\in K$，使得 $v_L(\ell+\wp(l)+k) = g\nu_{L/K}(\ell)$。我们将称这个元素为

$$\mathrm{rd}(\ell)^{\wp}_{L/K} = \ell + \wp(l) + k.$$

ℓ 的一个 L/K-约化。当然，尽管约化 $\mathrm{rd}(\ell)^{\wp}_{L/K}$ 的赋值是唯一确定的，但具有这一赋值的具体元素 $\mathrm{rd}(\ell)^{\wp}_{L/K}$ 并非唯一。若 $v_L(\ell)=v_L(\mathrm{rd}(\ell)^{\wp}_{L/K}) = g\nu_{L/K}(\ell)$，我们就称 $\ell\in L$ 是 L/K-约化的。

下一个结果是 (2) 的推广。

image
引理 3.2. 设 L/K 是一个分歧的 C_p-扩张，分歧断点为 b。因此，$L=K(y)$，其中某个 $y\in K^{\mathrm{sep}}$ 满足 $\wp(y)=\beta\in K, v_K(\beta)=-b$。设 $\phi_{L/K}\colon [0,\infty)\to[0,\infty)$ 为 Hasse-Herbrand 函数

$$\phi_{L/K}(x) = \begin{cases} x & for\ 0\leq x\leq b, \\ b+(x-b)/p & for\ b<x \end{cases}$$

其逆函数为 $\psi_{L/K}$。那么，对于与 p 互素的正整数 n，

$$\wp\colon \frac{\mathcal{M}_L^{-n}+K}{\mathcal{M}_L^{-n+1}+K} \longrightarrow \frac{\mathcal{M}_L^{-\psi_{L/K}(n)}+K}{\mathcal{M}_L^{-\psi_{L/K}(n)+1}+K}$$

是 $n\neq b$ 的同构。如果 $n=b$，那么 $\ker\wp = \mathbb{F}_p y + y\mathcal{M}_L + K$。

证明。由于 $p\nmid n$，存在唯一的一对 (i,m)，满足 $1\le i\le p-1, m\in\mathbb{Z}$，使得 $n=bi+pm$。$(\mathcal{M}_L^{-n}+K)/(\mathcal{M}_L^{-n+1}+K)$ 中的每个元素都可表示为 μy^i，其中某个 $\mu\in K$ 满足 $v_K(\mu)=-m$。由于 $\wp(\mu y^i)=\mu^p(y+\beta)^i-\mu y^i=\mu^p\binom{i}{1}\beta^{i-1}y+(\mu^p-\mu)y^i \pmod{(\mu^p\beta^{i-1}y+\mu y)\mathcal{M}_K+K}$，我们得到

$$\wp:\frac{\mathcal{M}_L^{pm-ib}+K}{\mathcal{M}_L^{pm-ib+1}+K}\longrightarrow\begin{cases}\frac{\mathcal{M}_L^{pm-ib}+K}{\mathcal{M}_L^{pm-ib+1}+K} & \text{for } pm-ib\ge -b,\\ \frac{\mathcal{M}_K^{p^2m-(i-1)pb-b}+K}{\mathcal{M}_K^{p^2m-(i-1)pb-b+1}+K} & \text{for } pm-ib<-b,\end{cases}$$

由此可得结论。 □-b

推论 3.3. 若 $\ell\in L$ 满足 $v_L(\ell)>-b$，则 $\ell\in L^\wp+K$ 且 $g\nu_{L/K}(\ell)=\infty$.-b推论 3.4. 若 $\ell\in L$ 满足 $v_L(\ell)=-b$，则对某个$\omega\in\mathcal{O}_K/\mathcal{M}_K$，有 $\ell\in\omega y+y\mathcal{M}_L$。在这种情况下，

$$\ell\in L^\wp+K \text{ and } g\nu_{L/K}(\ell)=\infty \text{ if and only if } \omega\in(\mathcal{O}_K/\mathcal{M}_K)^\wp.$$

complement

推论 3.5. 若 $\ell\in L$ 满足 $v_L(\ell)<-b$ 且满足以下任一条件

$$v_L(\ell)\not\equiv -b \bmod p \quad or \quad v_L(\ell)\equiv(p-1)b \bmod p^2,$$

于是 $g\nu_{L/K}(\ell)=v_L(\ell)$。

3.1. 对 $\mathfrak{s}(x_1,x_2)$ 中各项的 L/K-约化，其中 $D_8, H(p^3)$ $M(p^3)$。由于 $S(y_1,\beta_1)$ 和 $S(y_2,\beta_2)$ 分别与次数为 p^2 的循环扩张相关，而循环扩张中的分歧已有充分研究，本节将重点讨论 $\pm\beta_2y_1$ 的 L/K-约化。我们的第一个结果将 β_2 分解为 β_1 的幂。

子节

引理 3.6. 不失一般性，满足 $p\nmid v_K(\beta_2)\le v_K(\beta_1)<0$ 的 AS生成元 β_2 可表示为

分解

$$\beta_2=\mu_0^p+\sum_{i=1}^{p-1}\mu_i^p\beta_1^i$$

对于满足以下条件的某个 $\mu_i\in K$

a) $\mu_0\in\mathcal{O}_K/\mathcal{M}_L$ 以及以下两者之一：$\mu_0\notin\{\wp(\omega):\omega\in\mathcal{O}_K/\mathcal{M}_K\}$ 或 $\mu_0=0$; b) 对于 $1\le i\le p-1$，以下两者之一：$v_K(\mu_i^p\beta_1^i)<0$ 或 $\mu_i=0$。此外，若 $v_K(\beta_2)=v_K(\beta_1)$，我们可以假设 $\mu_1\in\mathcal{O}_M\setminus(\mathbb{F}_p+\mathcal{M}_K)$。

证明。注意到 $K^p=\{\mu^p:\mu\in K\}$ 是 K的一个子域。此外，$K=K^p(\beta_1)$ 是 K^p的一个域扩张，其次数为 p。因此，$1,\beta_1,\dots,\beta_1^{p-1}$ 是 K/K^p 的一组基，并且存在 $\mu_i\in K$ 使得

$$\beta_2=\sum_{i=0}^{p-1}\mu_i^p\beta_1^i.$$

然而，由于 β_2 是一个 AS生成元，我们只需将此陈述视为一个同余关系

(7)mu_omu

$$\beta_2\equiv\mu_0^p+\sum_{i=1}^{p-1}\mu_i^p\beta_1^i \pmod{K^\wp}.$$

考虑项 μ_0^p。若 $v_K(\mu_0^p)<0$，则由于 $\mu_0^p=\mu_0+\wp(\mu_0)$，我们可以将$\mu_0=\sum_{i=0}^{p-1}(\mu_i')^p\beta_1^i$ 表示为某个 $\mu_i'\in K$，并得到 $\beta_2\equiv(\mu_0')^p+\sum_{i=1}^{p-1}(\mu_i+\mu_i')^p\beta_1^i$

(模 $K^{\wp}$)，其中 $v_K(\mu_0') > v_K(\mu_0)$。重复此过程并重新标记，直到 $v_K(\mu_0^p) \geq 0$。现在，若 $\mu_0^p \equiv \wp(\omega)$ (模 $\mathcal{M}_K$)，其中某个 $\omega \in \mathcal{O}_K/\mathcal{M}_K$，则令 $\mu_0^p = 0$。此时，(7) 在 $\mu_0 \in \mathcal{O}_K/\mathcal{M}_K$ 的情况下成立，且满足 $\mu_0 \notin \{\wp(\omega) : \omega \in \mathcal{O}_K/\mathcal{M}_K\}$ 或 $\mu_0 = 0$。最后，由于 $\mathcal{M}_K \subset K^{\wp}$，我们注意到，若对于某个 $1 \leq i \leq p-1$，有 $v_K(\mu_i^p \beta_1^i) > 0$，则可令 $\mu_i = 0$。□

我们利用引理 3.6 和 (6) 来确定 $g\nu_{K(y_1)/K}(\beta_2 y_1)$。首先讨论 $p = 2$ 时的简单情形。

p=2

命题 3.7。设 $p = 2$，并令 $y_1, y_2, \beta_1, \beta_2$ 如上，且 β_2 如引理 3.6 中所述。则 $\beta_2 y_1$ 和 $(\beta_1 + \beta_2)y_1$ 是 $K(y_1)/K$-约化的，且

$$v_{K(y_1)}(\beta_2 y_1) = v_{K(y_1)}((\beta_1 + \beta_2)y_1) = -2u_2 - u_1.$$

类似地，$\beta_2 y_2$ 是 $K(y_2)/K$-约化的，其中 $v_{K(y_2)}(\beta_2 y_2) = -3u_2$。

证明。一旦注意到若 $v_K(\beta_1) = v_K(\beta_2)$，则有 $\mu_1 \notin \mathbb{F}_2 + \mathcal{M}_K$，从而 $v_K(\beta_1 + \beta_2) = v_K(\beta_2)$，结论便由推论 3.5 得出。□

现在我们讨论一般情形。

p>2

命题 3.8。设 $p > 2$，并令 y_1、y_2、β_1、β_2 如上，且 β_2 如引理 3.6 中所述。令

$$r = -v_K\left(\sum_{i=1}^{p-2} \mu_i^p \beta_1^i\right), \qquad s = -v_K(\mu_{p-1}^p \beta_1^{p-1}).$$

注意到 $s \equiv -u_1$ 模 p、$r \not\equiv 0$、$-u_1$ 模 p，以及 $u_2 =$ 最大$\{r, s\}$。于是

$$v_{K(y_1)}(\mathrm{rd}(\beta_2 y_1)^{\wp}_{K(y_1)/K}) = g\nu_{K(y_1)/K}(\beta_2 y_1) = -\max\{ps + u_1, pr - (p-2)u_1\}.$$

证明。令 $L = K(y_1)$。根据引理 3.6，β_2 中的各项 $\{\mu_i^p \beta_1^i\}_{i \neq 0}$ 要么为零，要么具有赋值 $v_L(\mu_i^p \beta_1^i) < 0$。将和分解为 $\sum_{i=1}^{p-2} \mu_i^p \beta_1^i = A + B$，其中 A 包含满足 $v_K(\mu_i^p \beta_1^i) \leq v_K(\beta_1)$ 的那些项，以及满足 $v_K(\beta_1) < v_K(\mu_i^p \beta_1^i) < 0$ 的非零项 B。因此

$$\beta_2 = A + \mu_{p-1}^p \beta_1^{p-1} + B + \mu_0^p.$$

由于 $v_K(\beta_2) \leq v_K(\beta_1) = -u_1$，

$$v_K(\beta_2) = \min\{v_K(A), v_K(\mu_{p-1}^p \beta^{p-1})\}.$$

$v_K(A)$ $v_K(\mu_{p-1}^p \beta_1^{p-1})$ 中至少有一个必须是 $\leq -u_1$。A、$\mu_{p-1} \in K$ 中至少有一个非零。

为确定 $g\nu_{L/K}(\beta_2 y_1)$，我们使用 (6)，并考虑以下 L/K-群赋值：

$$g\nu_{L/K}(Ay_1), \quad g\nu_{L/K}(\mu_{p-1}^p \beta_1^{p-1} y_1), \quad g\nu_{L/K}(By_1) \quad \text{and} \quad g\nu_{L/K}(\mu_0^p y_1).$$

其中两个很容易分析。

- 考虑 $g\nu_{L/K}(\mu_{p-1}^p \beta_1^{p-1} y_1)$，并假设 $\mu_{p-1} \neq 0$。那么 $v_L(\mu_{p-1}^p \beta_1^{p-1} y_1) \equiv (p-1)u_1$ 模 p^2。因此，根据推论 3.5，$\mu_{p-1}^p \beta_1^{p-1} y_1$ 是 L/K-约化的，并且

$$g\nu_{L/K}(\mu_{p-1}^p \beta_1^{p-1} y_1) = v_L(\mu_{p-1}^p \beta_1^{p-1} y_1) \leq -(p+1)u_1.$$

- 考虑 $g\nu_{L/K}(\mu_0^p y_1)$。由于 $\mu_0 \notin \{\wp(\omega) : \omega \in \mathcal{O}_K/\mathcal{M}_K\}$ 或 $\mu_0 = 0$，推论 3.4 指出

$$-u_1 \leq g\nu_{L/K}(\mu_0^p y_1).$$

其余两个 L/K-群赋值更为复杂。不过，一旦我们证明若 $A \neq 0$，则

$$g\nu_{L/K}(Ay_1) \equiv -2u_1 \bmod p \quad \text{and} \quad g\nu_{L/K}(Ay_1) \leq -2u_1,$$

当 $-2u_1 < g\nu_{L/K}(By_1)$ 时，我们便能得出

(8)目标目标

$$g\nu_{L/K}(\beta_2 y_1) = \min\{g\nu_{L/K}(\mu_{p-1}^p \beta_1^{p-1} y_1), g\nu_{L/K}(Ay_1)\}.$$

我们先假设 $\mu \neq 0$ and $1 \leq i \leq p-2$，然后展开$\wp(\mu y_1^{i+1}) = \mu^p(y_1+\beta_1)^{i+1} - \mu y_1^{i+1}$，得出

$$\wp(\mu y_1^{i+1}) = \mu^p \beta_1^{i+1} + \mu^p(i+1)\beta_1^i y_1 + \mu^p \sum_{j=2}^{i+1} \binom{i+1}{j} y_1^j \beta_1^{i+1-j} - \mu y_1^{i+1}.$$

由于 $2 \leq i+1 < p$，我们可以求解 $\mu^p \beta_1^i y_1$，得到

$$\mu^p \beta_1^i y_1 \equiv \frac{i}{2}\mu^p y_1^2 \beta_1^{i-1} - \frac{\mu y_1^{i+1}}{i+1} \pmod{\mu^p y_1^2 \beta_1^{i-1}\mathcal{M}_L + L^\wp + K}.$$

注意

$$v_K\left(\frac{i}{2}\mu^p y_1^2 \beta_1^{i-1}\right) < v_K\left(\frac{\mu y_1^{i+1}}{i+1}\right) \iff v_K(\mu^p \beta_1^i) < v_K(\beta_1).$$

因此，对于 $1 \leq i \leq p-2$ 和 $\mu \neq 0$，同时令 $\mathcal{L} = L^\wp + K$

relate

(9)

$$\mu^p \beta_1^i y_1 \equiv \begin{cases} \frac{i}{2}\mu^p y_1^2 \beta_1^{i-1} \pmod{\mu^p y_1^2 \beta_1^{i-1}\mathcal{M}_L + \mathcal{L}} & v_K(\mu^p\beta_1^i) < v_K(\beta_1), \\ \frac{\wp(\mu)}{2} y_1^2 \pmod{y_1^2 \mathcal{M}_L + \mathcal{L}} & v_K(\mu^p\beta_1^i) = v_K(\beta_1), \\ -\frac{\mu y_1^{i+1}}{i+1} \pmod{\mu y_1^{i+1}\mathcal{M}_L + \mathcal{L}} & v_K(\mu^p\beta_1^i) > v_K(\beta_1). \end{cases}$$

现在我们应用（9）。假设 $A \neq 0$ 并分情况讨论：$v_K(A) < v_K(\beta_1)$ 与 $v_K(A) = v_K(\beta_1)$。在第一种情况下 $v_K(A) < v_K(\beta_1)$，令 $\mu_i^p \beta_1^i y_1$ 为 Ay_1 的任意非零项，使得 $v_L(\mu_i^p \beta_1^i) < v_L(\beta_1)$，则根据（9），它模 $L^\wp + K$ 同余于一个赋值为 $v_L(\mu_i^p \beta_1^{i-1} y_1^2) < -2u_1$ 的项。此外，根据推论 3.5 $\mu_i^p \beta_1^{i-1} y_1^2$ 在其所表示的 $L^\wp + K$ 的陪集中具有最大的赋值。因此

$$g\nu_{L/K}(\mu_i^p \beta_1^i y_1) = v_L(\mu_i^p \beta_1^i) + (p-2)u_1 < -2u_1.$$

若存在一项使得 $v_L(\mu_i^p \beta_1^i) = v_L(\beta_1)$，则 $i = 1$ and $v_K(\mu_i) = 0$ and$\mu_i^p \beta_1^i y_1$ 模 $L^\wp + K$ 同余于一个赋值为 $-2u_1 \leq v_L(\wp(\mu_i)y_1^2)$ 的项。利用 (6)，我们得出

$$g\nu_{L/K}(Ay_1) = v_L(A) + (p-2)u_1 < -2u_1.$$

第二种情形 $v_K(A) = v_K(\beta_1)$ 出现在 A 仅有一项 $\mu_i^p \beta_1^i$，且满足 $i = 1$ 和 $v_K(\mu_i) = 0$ 时。这意味着 $v_K(A) = v_K(\beta_2)$ 并且

$$\beta_2 \equiv \mu_1^p \beta_1 \bmod \beta_1 \mathcal{M}_K.$$

由于 $u_1 = -v_K(\beta_1) = -v_K(\beta_2) = u_2$，$C_p^2$-扩张 M/K 中只有一个分歧断点，β_1 和 β_2 的每个非平凡 $\mathbb{F}_p$-线性组合都具有相同的赋值 $\mu_1 \in \mathcal{O}_K \setminus (\mathbb{F}_p + \mathcal{M}_K)$，因此 $v_K(\wp(\mu_1)) = 0$。在这种情况下，

$$g\nu_{L/K}(Ay_1) = v_L(A) + (p-2)u_1 = -2u_1.$$

最后，我们将 (9) 应用于 By_1。条件 $v_K(\mu^p\beta_1^i) > v_K(\beta_1)$ 等价于 $v_L(\mu y_1^i) > v_K(y_1) = -u_1$。因此，$By_1$ 的每一项 $\mu_i^p\beta_1^i y_1$ 模 $L^\wp + K$ 同余于一个赋值为 $v_L(-\mu y_1^{i+1})$ 的项，而该项满足 $-2u_1 < v_L(-\mu y_1^{i+1})$。所以

$$-2u_1 < g\nu_{L/K}(By_1).$$

该结果现由 (8) 及 $g\nu_{L/K}(Ay_1) = v_L(A) + (p-2)u_1$ 得出。 □

现记载涉及 $S(y_1,\beta_1)$ 或 $S(y_2,\beta_2)$ 的结果。

S(x_2)

命题 3.9。假设 $p > 2$，且 $y_1, y_2, \beta_1, \beta_2$ 如上，其中 β_2 如引理 3.6 所述。则 $S(y_2,\beta_2)$ 是 $K(y_2)/K$-约化的，且 $v_L(S(y_2,\beta_2)) = -(p^2-p+1)u_2$。令 r, s 如命题 3.8 所述。则

$$g\nu_{K(y_1)/K}(-\beta_2 y_1 + S(y_1,\beta_1)) = -\max\{(p^2-p+1)u_1, ps+u_1, pr-(p-2)u_1\},$$

除非 $\mu_{p-1}+1 \in \mathcal{M}_K$。

当 $\mu_{p-1}+1 \in \mathcal{M}_K$ 时，$s = (p-1)u_1$ 是固定的。令

$$t = -v_K((\mu_{p-1}+1)^p\beta^{p-1}) < s.$$

注意到 $t \equiv -u_1 \bmod p$。于是

$$g\nu_{K(y_1)/K}(-\beta_2 y_1 + S(y_1,\beta_1)) = -\max\{(p^2-2p+2)u_1, pt+u_1, pr-(p-2)u_1\}.$$

证明。由于 $v_{K(y_i)}(S(y_i,\beta_i)) = -(p^2-p+1)u_i$，由推论 3.5 可得 $g\nu_{K(y_i)/K}(S(y_i,\beta_i)) = -(p^2-p+1)u_i$。

现在考虑 $-\beta_2 y_1 + S(y_1,\beta_1) = C - D$，其中

$$C = -\mu_{p-1}^p\beta_1^{p-1}y_1 + S(y_1,\beta_1) = -(\mu_{p-1}^p+1)\beta_1^{p-1}y_1 - \sum_{i=1}^{p-2}\frac{1}{p}\binom{p}{i}\beta_1^i y_1^{p-i}$$

并且根据命题 3.8，已知 $D = Ay_1 + By_1 + \mu_0^p y_1$ 满足 $g\nu_{K(y_1)/K}(D) = -(pr-(p-2)u_1)$。假设 $\mu_{p-1}+1 \notin \mathcal{M}_K$。那么根据推论 3.5，

$$g\nu_{K(y_1)/K}(C) = \min\{v_{K(y_1)}(-\mu_{p-1}^p\beta_1^{p-1}y_1), v_{K(y_1)}(S(y_1,\beta_1))\} \equiv (p-1)u_1 \bmod p^2,$$

从而 $g\nu_{K(y_1)/K}(C) \neq g\nu_{K(y_1)/K}(D)$。第一条结论得证。另一方面，若 $\mu_{p-1}+1 = \tau \in \mathcal{M}_K$，则 $v_L(C) = \min\{v_L(\tau^p\beta_1^{p-1}y_1), v_L(\beta_1^{p-2}y_1^2)\} \equiv (p-1)u_1$ 或 $(2p-2)u_1 \bmod p^2$。注意到 $-(pr-(p-2)u_1) \equiv -2u_1 \bmod p$，且由于 $r \not\equiv (p-1)u_1 \bmod p$，因此 $-(pr-(p-2)u_1) \not\equiv (2p-2)u_1 \bmod p^2$。再次有 $g\nu_{K(y_1)/K}(C) \neq g\nu_{K(y_1)/K}(D)$。第二条结论得证。□

=相同于>

注 3.10。当 $p = 2$ 产生 r 的和为空和时。因此 $s = u_2$，命题 3.8 中给出的 $g\nu_{K(y_1)/K}(\beta_2 y_1)$ 的值与命题 3.7 中的值一致。命题 3.9 中给出的 $g\nu_{K(y_1)/K}(-\beta_2 y_1 + S(y_1,\beta_1))$ 和 $g\nu_{K(y_1)/K}(S(y_2,\beta_2))$ 的值也一样。它们也与命题 3.7 中的值一致。Q

-subsect

3.2. Q_8时 $\mathfrak{s}(x_1,x_2)$ 的分解与约化。在此情况下，$\mathrm{char}(K) = 2$，并且由于 $i = 1$ 的 $x_i = y_i$，2，我们也有 $u_i = -v_K(\kappa_i)$。我们将继续使用 x_i 和 κ_i（而非 y_i 和 β_i）。回想一下，$N = M(x_3)$，其中 $\wp(x_3) = (\kappa_1+\kappa_2)x_1 + \kappa_2 x_2 + \kappa_3$，对某个 κ_3 成立。事实上，当 κ_3 遍历所有 K 时，$M(x_3)$ 遍历所有 K 的全分歧四元数扩张。我们感兴趣的是

确定 $M(x_3)/M$ 的分歧断点下界。因此，我们感兴趣的是 $\max\{v_M(t):$ $t\in\mathfrak{s}'+M^{\wp}+K\}$ 对于

$$\mathfrak{s}'=\mathfrak{s}(x_1,x_2)=(\kappa_1+\kappa_2)x_1+\kappa_2x_2.$$

根据引理 3.6，我们有

(10)kappa22kappa

$$\kappa_2=\mu^2\kappa_1+\mu_0^2$$

其中 $-v_K(\mu)=m\geq 0$ 且 $\mu_0\in\mathcal{O}_K/\mathcal{M}_K$。注意到

$$u_2=u_1+2m.$$

若 $m=0$，则由于 κ_1、κ_2 在 $\kappa_1\mathcal{O}_K/\kappa_1\mathcal{M}_K$ 中线性无关，我们有$\wp(\mu)\neq 0$，这意味着 $\wp(\mu)$ 是 $\mathcal{O}_K/\mathcal{M}_K$ 中的一个单位。令

(11)X

$$X=x_2-\mu x_1$$

并注意到 $\wp(X)=-\wp(\mu)x_1+\mu_0^2$。这意味着 X 满足一个系数属于 $L=K(x_1)$ 的 Artin-Schreier 多项式。由于 $v_L(-\wp(\mu)x_1+\mu_0^2)=pv_K(\wp(\mu))-u_1\not\equiv 0 \bmod 2$，我们看到 $L(X)/L$ 是一个 C_2-扩张，其分歧断点为 $b=u_1+4m$，并且

$$v_M(X)=-(u_1+4m).$$

利用（10）和（11），将 κ_2 和 x_2 代入 $\mathfrak{s}'$，使得 $\mathfrak{s}'=\mathfrak{s}_1'+\mathfrak{s}_2'$，其中

$$\mathfrak{s}_1'=(1+\mu^2+\mu^3)\kappa_1x_1+\mu_0^2(1+\mu)x_1\in L=K(x_1),$$
$$\mathfrak{s}_2'=(\mu^2\kappa_1+\mu_0^2)X\in M=K(x_1,x_2).$$

注意到

$$v_M(\mathfrak{s}_2')=-(5u_1+12m),\quad \text{and if } m>0 \text{ then } v_L(\mathfrak{s}_1')=-(3u_1+6m),$$

但当 $m=0$时，确定 $v_L(\mathfrak{s}_1')$ 并不那么明了。

为澄清 $m=0$时的情形，我们将 $\mu^3\kappa_1x_1$ 代入 $\mathfrak{s}_1'$的表达式中，并展开 $\wp(\mu x_1X+\mu X)$，得到

$$\mu^3\kappa_1x_1\equiv\mu^4\kappa_1x_1+\mu^2\mu_0^2x_1+\mu^2\kappa_1X+\wp(\mu)x_1X+\wp(\mu)X\pmod{M^{\wp}+K}.$$

因此，$\mathfrak{s}'\equiv\mathfrak{s}$（模 $M^{\wp}+K$），其中 $\mathfrak{s}=\mathfrak{s}_1+\mathfrak{s}_2$，且

$$\mathfrak{s}_1=(1+\mu^2+\mu^4)\kappa_1x_1+\mu_0^2(1+\mu+\mu^2)x_1\in L=K(x_1),$$
$$\mathfrak{s}_2=\wp(\mu)x_1X+\wp(\mu)X+\mu_0^2X\in M=K(x_1,x_2).$$

当 $m=0$时，将 $\mu=\omega+\epsilon$ 表示为某个 $\omega\in(\mathcal{O}_K/\mathcal{M}_K)\setminus\mathbb{F}_2$ 与某个满足 $v_K(\epsilon)=e>0$的 $\epsilon\in\mathcal{M}_K$ 之和。由于 $\wp(\omega)$ 是单位元，故 $v_K(\mathfrak{s}_2)=-3u_1$。注意，若 $e\geq u_1/2$，则 $(\omega+\epsilon)^2\kappa_1\equiv\omega^2\kappa_1$ 模 $\mathcal{M}_K\subseteq K^{\wp}$；因此，由于我们只关心$\kappa_2=\mu^2\kappa+\mu_0^2$ 模 $K^{\wp}$，可以令 $\epsilon=0$。不失一般性，我们得出结论：要么 $0<e<u_1/2$，要么 $\epsilon=0$。将 μ 代入 $\mathfrak{s}_1$的表达式中：

$$\mathfrak{s}_1=(1+\omega+\omega^2)^2\kappa_1x_1+(1+\omega+\omega^2)\mu_0^2x_1+(\epsilon+\epsilon^2)^2\kappa_1x_1+(\epsilon+\epsilon^2)\mu_0^2x_1.$$

显然，$v_L(\mathfrak{s}_1)$取决于 $\omega^3\neq 1$ 还是 $\omega^3=1$。若 $\omega^3\neq 1$，则$v_L(\mathfrak{s}_1)=-3u_1$，当 $m=0$时。若 $\omega^3=1$，则

$$\mathfrak{s}_1=(\epsilon+\epsilon^2)^2\kappa_1x_1+(\epsilon+\epsilon^2)\mu_0^2x_1$$

且 $v_L(\mathfrak{s}_1) = -3u_1 + 4e$。注意，若 $\omega^3 = 1$ 且 $v_K(\epsilon) = e > u_1/2$，则 $\mathfrak{s}_1 = 0$。总之，这意味着当 $m = 0$时，

$$v_M(\mathfrak{s}_2) = -3u_1, \quad \text{and} \quad v_L(\mathfrak{s}_1) = \begin{cases} -3u_1 & \omega^3 \neq 1, \\ -3u_1 + 4e & \omega^3 = 1 \text{ and } \mathfrak{s}_1 \neq 0. \end{cases}$$

我们将这些信息归纳为一个命题。

Q8-s1-s2

命题 3.11. 设 $p = 2$。设 M/K 为一个完全分歧的 C_p^2 扩张，其上分歧数为 $u_1 \leq u_2$。令 $M = K(x_1, x_2)$，其中 $\wp(x_i) = \kappa_i$ 与$v_k(\kappa_i) = u_i$。由于 u_1、u_2 为奇数，故对某个 $\mu \in K$，有 $\kappa_2 \equiv \mu^2\kappa_1$ 模 $\mathcal{O}_M$，且 $v_K(\mu) = -m \leq 0$。若 $m = 0$，则对某个 $\omega \in \mathcal{O}_K/\mathcal{M}_K$，有 $\mu = \omega + \epsilon$，且 $\epsilon \in \mathcal{M}_K$满足 $v_K(\epsilon) = e$。令 $L = K(x_1)$。那么存在 $\mathfrak{s}_1 \in L$ 和 $\mathfrak{s}_2 \in M$，使得对于$u_2 \neq u_1$，或等价地，对于 $m > 0$,

$$v_L(\mathfrak{s}_1) = -3u_2 \text{ and } v_M(\mathfrak{s}_2) = -(6u_2 - u_1).$$

对于 $u_2 = u_1$ 或等价地对于 $m = 0$，我们有 $v_M(\mathfrak{s}_2) = -3u_1$。并且除非 $\mathfrak{s}_1 = 0$，我们有

$$v_L(\mathfrak{s}_1) = \begin{cases} -3u_1 & \text{if } \omega^3 \neq 1, \\ -3u_1 + 4e & \text{if } \omega^3 = 1 \text{ and } 0 < e < u_1/2. \end{cases}$$

注意，对于 $\mathfrak{s}_1 \neq 0$，不等式 $v_L(\mathfrak{s}_1) < -u_1$ 成立。最后，任何包含 M的 Q_8-扩张 N/K 都可以表示为 $N = M(x_3)$，其中对于某个 $\kappa_3 \in K$，有 $\wp(x_3) = \mathfrak{s}_1 + \mathfrak{s}_2 + \kappa_3$。

4. Ramification theory

linkin

g回顾一下目前的记号： N/K 是一个伽罗瓦群为 $G = \mathrm{Gal}(N/K)$ 的完全分歧非阿贝尔扩张，由 σ_1、σ_2 生成，其中 $\sigma_3 = [\sigma_1, \sigma_2]$ 固定一个子域M。当我们只关注伽罗瓦作用时，不变域 $M = N^{\sigma_3}$最初表示为 $M = K(x_1, x_2)$。现在我们需要涉及分歧断点，因此令 $M = K(y_1, y_2)$，使得对于$i = 1$、2，有 $\wp(y_i) = \beta_i$ 且 $u_i = -v_K(\beta_i)$。回顾我们已经证明：如果 $u_1 \leq u_2 \leq u_3$ 表示 N/K的上、下分歧断点，而 $l_1 \leq l_2 \leq l_3$ 表示其下分歧断点，则 M/K 的下、上分歧断点分别为 $l_1 \leq l_2$ 和 $u_1 \leq u_2$。为了确定 N/M的分歧断点 l_3，从而由 $l_3 - l_2 = p^2($ $u_3 - u_2)$ 确定 u_3，我们考察 C_p-扩张 $M(x_3)/M$，其中

$$\wp(x_3) = \mathfrak{s}(x_1, x_2) + \kappa_3$$

其中 $\mathfrak{s}(x_1, x_2)$ 首先在定理 1.5 中给出描述，随后转换/调整为 (4) 和 (5)。最后，利用第 3.1 节和第 3.2 节的结果，即命题 3.7、3.8、3.9 和 3.11，我们发现 $\mathfrak{s}(x_1, x_2)$ 模 $M^\wp + K$ 可替换为

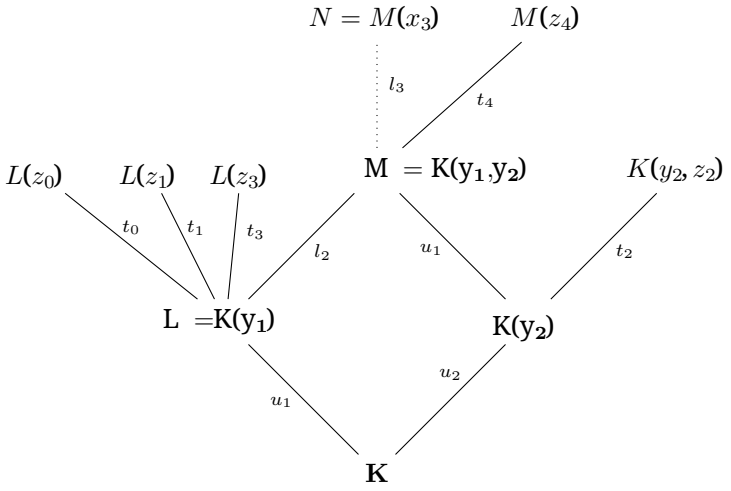
$$\mathfrak{s}(x_1, x_2) \equiv \begin{cases} -\mathrm{rd}(\beta_2 y_1)_{L/K}^{\wp} & H(p^3), \\ \mathrm{rd}(-\beta_2 y_1 + S(y_1, \beta_1))_{L/K}^{\wp} & D_8, M(p^3), (u_2 = u_1 \text{ or } G_{l_2} = \langle \sigma_1^p, \sigma_2 \rangle), \\ \mathrm{rd}(\beta_2 y_1)_{L/K}^{\wp} + S(y_2, \beta_2) & D_8, M(p^3), u_2 \neq u_1 \text{ and } G_{l_2} = \langle \sigma_1 \rangle, \\ \mathfrak{s}_1 + \mathfrak{s}_2 & Q_8. \end{cases}$$

这自然引发了人们对以下辅助 C_p-扩张的分歧断点的兴趣：

- $L(z_0)/L$ 对于 $z_0 \in K_{\mathrm{sep}}$ 使得 $\wp(z_0) = \mathrm{rd}(\beta_2 y_1)_{L/K}^{\wp}$,
- $L(z_1)/L$ 对于 $z_1 \in K_{\mathrm{sep}}$ 满足 $\wp(z_1) = \mathrm{rd}(-\beta_2 y_1 + S(y_1, \beta_1))_{L/K}^{\wp}$ 的情形,

- $K(y_2, z_2)/K(y_2)$ 对于 $z_2 \in K_{\mathrm{sep}}$ 满足 $\wp(z_2) = S(y_2, \beta_2)$ 的情形,
- $L(z_3)/L$ 对于 $z_4 \in K_{\mathrm{sep}}$ 满足 $\wp(z_3) = \mathfrak{s}_1$ 的情形，若 $\mathfrak{s}_1 \neq 0$,
- $M(z_4)/M$ 对于 $z_4 \in K_{\mathrm{sep}}$ 满足 $\wp(z_4) = \mathfrak{s}_2$的情形,

我们将其附在 M/K的图中，并且为了便于查阅，为每个C_p-子扩张标注其分歧断点。该图旨在帮助我们确定当 x_3 如 (12) 中所示时， $M(x_3)/M$ 的分歧断点。因此，我们将扩张 $M(x_3)/M$ 添加到图中，以提醒我们本练习的“目标”。



利用命题 3.7、3.8 和 3.9，可以确定分歧断点，并记录如下。注意，根据注 3.10，这些关于分歧断点的表达式对 $p = 2$ 和 $p > 2$ 均成立。

$$
\begin{aligned}
&t_0 = \max\{ps + u_1, pr - (p-2)u_1\},\\
&t_1 = \max\{(p^2 - p + 1)u_1, ps + u_1, pr - (p-2)u_1\}, \text{ or}\\
&\quad \max\{(p^2 - 2p + 2)u_1, pt + u_1, pr - (p-2)u_1\} \text{ and } s = (p-1)u_1,\\
&t_2 = (p^2 - p + 1)u_2,\\
&t_3 = 3u_2 \text{ if } u_2 \neq u_1, \text{ otherwise } t_3 > u_1,\\
&t_4 = 6u_2 - u_1 \text{ if } u_2 \neq u_1, \text{ otherwise } t_3 = 3u_1.
\end{aligned}
$$

由于元素 $\mathrm{rd}(\beta_2 y_1)^{\wp}_{L/K}$、$\mathrm{rd}(-\beta_2 y_1 + S(y_1, \beta_1))^{\wp}_{L/K}$、 $\mathfrak{s}_1$ 和 $S(y_2, \beta_2)$ 都位于 M 的真子域中，而我们关注的是这些元素的 M-群赋值，因此记录如下:

引理 4.1。以下不等式 t_0、t_1、$t_3 > l_2$ 和 $t_2 > u_1$ 均成立。

证明。通过检查以下情况证明 $t_0 > l_2 = pu_2 - (p-1)u_2$： $u_2 = r$ 和 $u_2 = s$。接下来证明 $t_1 > l_2$; 当 $t_1 = \max\{(p^2-p+1)u_1, ps+u_1, pr-(p-2)u_1\}$ 时，这一点显然。因此考虑 $t_1 = \max\{(p^2-2p+2)u_1, pt+u_1, pr-(p-2)u_1\}$且 $s = (p-1)u_1$ 的情况。如果 $u_2 = r$，则可如前所述推出 $t_1 > l_2$。另一方面，如果$u_2 = s = (p-1)u_1$，则 $l_2 = p(p-1)u_1 - (p-1)u_1 < (p^2 - 2p + 2)u_1$，由此也可得到 $t_1 > l_2$。通过检查情况 $u_2 = u_1$ 和 $u_2 > u_1$证明 $t_3 > l_2$。最后，$t_2 > u_1$，因为 $t_2 = (p^2 - p + 1)u_2 \geq 3u_2$。□

既然我们已经证明了这些不等式，接下来需要用到一个众所周知的结果。c
_p^2-breaks
引理 4.2. 设 M/L 是一个分歧的 C_p-扩张，其分歧断点为 l。设 $\alpha \in L$ 是 L-约化的： $g\nu_L(\alpha) = v_L(\alpha) = -a < 0$ 和 $p \nmid a$。假设

$$a > l.$$

设 $z \in L^{\mathrm{sep}}$ 使得 $\wp(z) = \alpha$。则 $M(z)/M$ 是一个分歧的 C_p-扩张，其分歧断点为 $pa - (p-1)l$，且

$$g\nu_M(\alpha) = -(pa - (p-1)l).$$

否则，若 $a \leq l$ 且 $M(z)/M$ 非平凡，则 $M(z)/M$ 的分歧断点小于或等于 l。虽然存在比这更精确的上界，但这已足以满足我们的目的。

证明。设 $l < a$。由于 $M(z)/L$ 是一个完全分歧的 C_p^2-扩张，其上分歧断点为 $l < a$，因此下分歧跳跃为 $l_1 = l$ 和 $l_2 = l + p(a-l)$。转至 $\mathrm{Gal}(M(z)/M)$ 的分歧滤过即可得到结论。更一般地，当 $M(z)/M$ 非平凡时， $M(z)/M$ 的分歧断点满足 $\max\{a, pa-(p-1)l\}$，且当 $a \neq l$ 时取等号。□

我们可以表示 $x_3 = \bar{x}_3 + z_5$ 其中 $\wp(z_5) = \kappa_3$ 并且

x_3
$$\bar{x}_3 = \begin{cases} -z_0 & H(p^3), \\ z_1 & D_8, M(p^3), (u_2 = u_1 \text{ or } G_{l_2} = \langle \sigma_1^p, \sigma_2 \rangle), \\ z_0 + z_2 & D_8, M(p^3), u_2 \neq u_1 \text{ and } G_{l_2} = \langle \sigma_1 \rangle, \\ z_3 + z_4 & Q_8. \end{cases} \tag{12}$$

令 s_i 表示 $M(z_i)/M$ 的分歧断点。根据引理 4.2，我们得到 $s_i = pt_i - (p-1)l_2$，其中 $i = 0, 1, 3$, $s_2 = pt_2 - (p-1)u_1$，当然还有 $s_4 = t_4$。

至此，我们已收集到确定 $M(\bar{x}_3)/M$ 的分歧断点 l_3 所需的全部信息，其中 $\bar{x}_3$ 按式 (12) 表示。考虑以下情形： $G \cong H(p^3)$，或 $G \cong D_8, M(p^3)$ 且 $G_{l_2} = \langle \sigma_1^p, \sigma_2 \rangle$。因此，对于 $i = 0, 1$，有 $\bar{l}_3 = s_i$。 $M(\bar{x}_3)/K$ 的上分歧数为 $u_1, u_2, \bar{u}_3$，其中 $\bar{u}_3 - u_2 = (\bar{l}_3 - l_2)/p^2 = (t_i - l_2)/p$。为清晰起见，将 D_8 从 $M(p^3)$ 中分离出来，由此可确立以下事实：

bar{u}_3
$$\bar{u}_3 = \begin{cases} \max\left\{s + u_1, r + \frac{u_1}{p}\right\} & H(p^3), \\ u_2 + u_1 & D_8, (u_2 = u_1 \text{ or } G_{l_2} = \langle \sigma_1^p, \sigma_2 \rangle), \\ \max\left\{pu_1, s + u_1, r + \frac{u_1}{p}\right\} & M(p^3), (u_2 = u_1 \text{ or } G_{l_2} = \langle \sigma_1^p, \sigma_2 \rangle), \\ & \quad \text{and } \mu_{p-1} \neq 1 \bmod \mathcal{M}_K \\ \max\left\{(p-1)u_1 + \frac{u_1}{p}, t + u_1, r + \frac{u_1}{p}\right\} & M(p^3), (u_2 = u_1 \text{ or } G_{l_2} = \langle \sigma_1^p, \sigma_2 \rangle), \\ & \quad \text{and } \mu_{p-1} = 1 \bmod \mathcal{M}_K. \end{cases} \tag{13}$$

现在考虑 $G \cong Q_8$，或 $G \cong D_8, M(p^3)$ 和 $u_2 \neq u_1, G_{l_2} = \langle \sigma_1 \rangle$ 的情形。在这些情形下， $\bar{x}_3$ 是两个项的和。事实上， 是 $M(z_0, z_2)$ 或 $M(z_4, z_5)$ 的一个元素。

引理 4.3. $M(z_0, z_2)$ 是一个 C_p^2-扩张，具有两个上分歧断点 $s_0 < s_2$。若 $u_2 \neq u_1$，则 $M(z_3, z_4)$ 是一个 C_p^2-扩张，其上分歧断点为 then$s_3 < s_4$。否则，若 $\mathfrak{s}_1 \neq 0$，上分歧断点为 $s_4 < s_3$。

证明。验证 $s_2 > s_0$ 由以下事实可知： $pu_2 + u_1 \geq t_0$ 和 $u_2 > u_1$。对于 $u_2 \neq u_1$，$s_3 < s_4$ 可化简为 $u_1 < u_2$。对于 $u_2 = u_1$ 和 $\mathfrak{s}_1 \neq 0$， $s_4 < s_3$ 可化简为 $e < u_1/2$。□

我们在以下情形中使用此引理：$G \cong D_8$、$M(p^3)$、$u_2 \neq u_1$ 和 $G_{l_2} = \langle \sigma_1 \rangle$，以及 $G \cong Q_8$。$M(\bar{x}_3)/M$ 的分歧断点为 $\bar{x}_3 = z_0 + z_2$ 是s_2，这也是 $M(\bar{x}_3)/K$的第三下分歧断点。$M(\bar{x}_3)/M$ 的分歧断点为 $\bar{x}_3 = z_3 + z_4$ 是 s_4，若 $u_2 \neq u_1$。另一方面，当$u_2 = u_1$ 且 $\mathfrak{s}_1 \neq 0$时，它为 s_3。若 $u_2 = u_1$ 且 $\mathfrak{s}_1 = 0$（因此 $M(z_3, z_4)$ 是一个 C_p-扩张），则它为 s_4。这些也都是 $M(\bar{x}_3)/K$的第三下分歧断点。因此我们得到：

bar{u}-2

$$\bar{u}_3 = \begin{cases} pu_2 & D_8, M(p^3), u_2 \neq u_1 \text{ and } G_{l_2} = \langle \sigma_1 \rangle, \\ 2u_2 & Q_8, u_2 \neq u_1, \text{ or } u_2 = u_1, \omega^3 \neq 1, \\ \max\left\{\frac{3u_1}{2}, 2u_1 - 2e\right\} & Q_8, u_2 = u_1, \omega^3 = 1. \end{cases} \tag{14}$$

由（13）和（14）很容易得出：要么 $\bar{u}_3$ 不是整数（因为 $p \nmid u_1$），要么 $\bar{u}_3$ 是一个模 p 同余于零的整数。现在回忆一下，无论伽罗瓦群为何， $N = M(x_3)$，其中 $x_3 = \bar{x}_3 + z_5$，且 $\wp(z_5) = \kappa_3$。不失一般性， κ_3 是 K-约化的。这意味着，除非 $\kappa_3 \in \mathfrak{O}_K$， $v_K(\kappa_3) = -b_3 < 0$ 且 $p \nmid b_3$；在这种情况下， b_3 是 $K(z_5)/K$ 的分歧断点，也是伽罗瓦扩张 $M(\bar{x}_3, z_5)/K$ 的上分歧断点，而该扩张包含 $M(x_3)/K$。$M(\bar{x}_3, z_5)/K$ 的上分歧断点也包括 $u_1 \leq u_2 < \bar{u}_3$。此外，由于 $\bar{u}_3$ 和 b_3 属于不同类型的有理数（绝不相等）， $M(x_3)/K$ 的上分歧断点为 $u_1 \leq u_2 < \max\{\bar{u}_3, b_3\}$。这些结果连同（13）和（14）中的表达式共同出现在定理 1.6 中。

5. Application

诺丁汉g正如 [BCT22]，中所解释的那样，人们对诺丁汉群的有限非阿贝尔子群的显式构造很感兴趣。作者描述了一个过程，该过程利用特征 p 下次数为 p^n 的循环扩张的维特向量描述，来产生阶为 p^n 的元素。沿用这一过程，并利用定理 1.2 中的阿廷-施赖尔描述，在诺丁汉群中确定一些阶为 p^3 的非阿贝尔子群，将会很有意义。此外，还可以利用定理 1.6 确定这些子群的上分歧序列，从而解决 [BCT22, §1.5] 中列出的一个开放问题。

References

[BCT22] Jakub Byszewski、Gunther Cornelissen 和 Djurre Tijsma, *Automata and finite order elements in the Nottingham group* **602** 2022 484 554 , 《代数学杂志》（），–。[EH07] G. Griffith Elder 和 Jeffrey J. Hooper, *On wild ramification in quaternion extensions*, 《波尔多数论杂志》（），第 – 期。MR Lar Richard Gustavus Larson, , 《代数学杂志》38（1976），第2期, 414–452。[Mik81] Hiroo Miki, *On the ramification numbers of cyclic p-extensions over local fields*, 《纯粹与应用数学杂志》328（1981），99–115。

[Sal78] David J. Saltman, *Noncrossed product p-algebras and Galois p-extensions*, 《代数学杂志》52（1978），第2期，302–314。[Ser79] Jean-Pierre Serre, *Local fields*, 《数学研究生教材》第67卷，施普林格出版社，纽约，1979年，由 Marvin Jay Greenberg 从法文译出。[Tho05] Lara Thomas, *Ramification groups in Artin-Schreier-Witt extensions*, 《波尔多数论杂志》 **17** 2005 2, 689 720 2211314 （），第 – 期。MR Wym B. Wyman, , [69] *Wildly ramified gamma extensions* 《美国数学杂志》91（1969），135–152。

Department of Mathematics, University of Nebraska at Omaha, Omaha, Nebraska, U.S.A.*Email address*: elder@unomaha.edu