arXiv:2302.00222v1 [math.NT] 1 Feb 2023

Hasse-Arf 定理的一个逆定理G. Griffith

Elder Kevin Keating 数学系 数学系 内布拉斯加大学奥马哈分校 佛罗里达大学 奥马哈，内布拉斯加州 68182 盖恩斯维尔，佛罗里达州 32611 美国 美国
elder@unomaha.edu keating@ufl.edu

2023年2月2日

摘要

设 L/K 是局部域的有限伽罗瓦扩张。Hasse-Arf 定理指出，若 Gal(L/K) 是阿贝尔群，则 L/K 的上分歧断点必须是整数。我们证明以下 Hasse-Arf 定理的逆命题：设 G 是一个非阿贝尔群，并且同构于某个剩余特征为 $p > 2$ 的局部域全分歧扩张 E/F 的伽罗瓦群。那么，存在一个剩余特征为 p 的局部域全分歧扩张 L/K，使得 Gal(L/K) $\cong G$，且 L/K 至少有一个非整数的上分歧断点。

1 引言

设 K 是一个局部域，L/K 是一个有限伽罗瓦扩张。与 L/K 相关联的是一些有理数 $u_1 \le u_2 \le \cdots \le u_n$，称为 L/K 的上分歧断点。上分歧断点提供了关于扩张 L/K 的算术信息。例如，L/K 是非平凡非分歧扩张，当且仅当 -1 是 L/K 的唯一上分歧断点；而 L/K 至多是温和分歧，当且仅当 L/K 的上分歧断点集合包含于 $\{-1, 0\}$。确定上分歧断点序列可能取值的范围，是一个经典问题。Hasse-Arf 定理 [8, 1] 指出，若 Gal(L/K) 是阿贝尔群，则 L/K 的每个上分歧断点都是整数。Hasse-Arf 定理在数论的多个领域中发挥着重要作用。例如，它用于构造 Artin 表示 [2]，也用于 Lubin 关于局部 Kronecker-Weber 定理 [10] 的证明。

本文旨在证明 Hasse-Arf 定理的逆命题。Hasse-Arf 定理的完全逆命题将表述为：若 G 是一个有限非阿贝尔群，则存在一个 G-局部域扩张，其上分歧跳跃

不是整数。事实上，Hasse-Arf 定理的逆命题并非在如此一般的情况下成立。例如，若 G 是一个非阿贝尔单群，且 L/K 是一个 G-扩张，则 K 的剩余域是无限域，且 L/K 是非分歧的，因此 L/K 唯一的上分歧跳跃是 -1。此外，若 G 是一个阶与 p 互素的非阿贝尔群，则任何剩余特征为 p 的局部域的 G-扩张 L/K 至多是温和分歧的，因此其上分歧断点包含于 $\{-1,0\}$。为排除这类例子，我们将研究范围限制在全分歧扩张上。此外，为避免空洞的情形，我们只考虑那些实际上能够作为剩余特征为 p的局部域之全分歧扩张的伽罗瓦群出现的非阿贝尔群 G 。在定理 6.2 中，我们证明，若 G 是这样的群，则对每个特征为 p 的局部域 K，都存在一个全分歧的 G-扩张 L/K，其上分歧跳跃不是整数。由 Deligne 的一个定理可进一步推出，存在一个特征 0 的局部域 F 以及一个全分歧的 G-扩张 E/F，其上分歧跳跃不是整数。

在第 2 节中，我们概述局部域伽罗瓦扩张的高阶分歧理论。我们证明 Hasse-Arf 定理逆命题的方法，是构造特征为 p 的局部域伽罗瓦扩张，使其具有非整数的上分歧跳跃。在特征为 p 的情形下进行研究的一个好处是，可以求解关于 p-扩张的嵌入问题，正如第 3 节所述。这意味着只需构造伽罗瓦群在某种意义下是极小的扩张。因此，我们在第 4 节中对极小的 p-群进行分类。在第 5 节中，我们利用第 3 节和第 4 节的结果，证明全分歧 p-扩张的 Hasse-Arf 定理逆命题。在第 6 节中，我们将证明推广到任意全分歧扩张。

在全文中，设 K 是一个关于离散赋值完备、剩余域特征为 $p>2$ 的域。设 K^{sep} 是 K 的可分闭包；对于 K^{sep}/K 的每个有限子扩张 L/K，设 v_L 是 K^{sep} 上的赋值，并将其归一化，使得 $v_L(L^\times)=\mathbb{Z}$。令 $\mathcal{O}_L$ 表示 L 的整数环，$\mathcal{M}_L$ 表示 $\mathcal{O}_L$ 的极大理想，并令 π_L 为 L 的一个素元。

2 局部域扩张中的分歧

设 L/K 是有限全分歧伽罗瓦扩张。本节定义 L/K 的下分歧跳跃和上分歧跳跃，以及 Gal(L/K) 的分歧子群。关于这些主题的更多信息，请参阅 [11] 的第 IV 章。

设 L/K 是次数为 mp^n 的全分歧伽罗瓦扩张，其中 $p\nmid m$。令 $G=\mathrm{Gal}(L/K)$。对于满足 $\sigma\neq \mathrm{id}_L$ 的 $\sigma\in G$，定义 σ 的分歧数为 $i(\sigma)=v_L(\sigma(\pi_L)-\pi_L)-1$；另定义 $i(\mathrm{id}_L)=\infty$。（注意，$i(\sigma)$ 与 $[11,\mathrm{IV}]$ 中定义的 $i_G(\sigma)$ 之间的关系为 $i_G(\sigma)=i(\sigma)+1$。）容易看出，若 $0<i(\sigma)<\infty$，则对所有 $\tau\in G$，有

$$i(\sigma^p)>i(\sigma),\quad i([\sigma,\tau])>i(\tau). \tag{2.1}$$

对于实数 $x\geq 0$，令 $G_x=\{\sigma\in G:\, i(\sigma)\geq x\}$。则 G_x 是 G的正规子群，称为 G的第 x 个下分歧群。若对所有 $\epsilon>0$，都有 $G_{b+\epsilon}\lneqq G_b$，则称 $b\geq 0$ 是 L/K 的一个下分歧断点。因此，当且仅当 $b=i(\sigma)$ 时，b 是 L/K 的一个下断点

对于某个满足 $\sigma \neq \mathrm{id}_G$ 的 $\sigma \in G$。由此可知，L/K 的每个下断点都是非负整数。此外，非负整数 b 是下分歧断点，当且仅当 $G_{b+1} \subsetneqq G_b$。

当且仅当 $|\sigma|$不是 p 的幂时，我们有 $i(\sigma) = 0$。因此，当且仅当 $m > 1$时，$b_0 = 0$ 是 L/K 的下分歧断点。若 b 是 L/K 的一个正下断点，则 $|G_b : G_{b+1}| = p^d$，其中 $d \geq 1$。在这种情况下，我们称 b 是重数为 d 的下断点。计入重数后，L/K 的正下分歧断点构成一个基数为 n 的多重集。我们用 $b_1 \leq b_2 \leq \cdots \leq b_n$ 表示 L/K 的正下断点。

设 M/K 是 L/K 的一个子扩张，并令 $H = \mathrm{Gal}(L/M)$。根据定义可知，对所有 $x \geq 0$，都有 $H_x = H \cap G_x$。因此，L/M 的下分歧断点多重集包含于 L/K 的下分歧断点多重集。换言之，分歧群 G_x 和下分歧断点在伽罗瓦群取子群时保持相容。

$G = \mathrm{Gal}(L/K)$ 的分歧群有另一种编号系统，它与模去正规子群 H 后取商群 G/H（G）的操作相容。L/K 的上分歧断点根据下断点定义如下：首先，当且仅当 $b_0 = 0$ 是一个下断点时，$u_0 = 0$ 才是 L/K 的一个上分歧断点。接着，L/K 的正上分歧断点 $u_1 \leq u_2 \leq \cdots \leq u_n$ 递归地定义为 $u_1 = b_1/m$ 和 $u_{i+1} - u_i = (b_{i+1} - b_i)/mp^i$，其中 $1 \leq i \leq n-1$。我们可以将 u_i 视为 L/K 的上分歧断点，它对应于 b_i。L/K 的上分歧断点（按重数计）构成一个多重集，记作 $\mathcal{U}_{L/K}$。注意，如果 L/K 是一个分歧的 C_p-扩张，那么 L/K 只有一个上分歧断点和一个下分歧断点 $u_1 = b_1$。因此，我们可以简单地称其为 L/K 的分歧断点。

G 的上分歧子群对实数 $x \geq 0$ 定义如下：$G^0 = G_0 = G$，$G^x = G_{b_1}$ 当 $0 < x \leq u_1$ 时，$G^x = G_{b_i}$ 当 $u_{i-1} < x \leq u_i$ 时，以及 $G^x = \{\mathrm{id}_L\}$ 当 $x > u_n$ 时。因此，$u \geq 0$ 是 L/K 的一个上分歧跳跃，当且仅当对所有 $\epsilon > 0$，都有 $G^{u+\epsilon} \subsetneqq G^u$。下述定理表明，群 G^x 与上分歧断点在伽罗瓦群取商时具有相容性：

定理 2.1（赫布兰德）。设 L/K 是一个有限全分歧伽罗瓦扩张，且 M/K 是 L/K的一个伽罗瓦子扩张。令 $G = \mathrm{Gal}(L/K)$，并令 $H = \mathrm{Gal}(L/M)$。

(a) 对于 $x \geq 0$，有 $(G/H)^x = G^x H/H$。

(b) $\mathcal{U}_{M/K} \subset \mathcal{U}_{L/K}$。

证明。（a）已在 $[11, \mathrm{IV}]$ 中作为命题14证明。（b）由（a）易得。 □

推论 2.2。设 $x \geq 0$。那么，当且仅当对所有充分小的 $\epsilon > 0$，$x \notin \mathcal{U}_{M/K}$ $G^x \leq G^{x+\epsilon}H$。

*Pr*明。由于 $G^x H = G^{x+\epsilon}H$ 当且仅当 $G^x \leq G^{x+\epsilon}H$，故结论由（a）得出 . □

我们将频繁用到以下（想必众所周知的）事实 :

引理 2.3. 设 N/K 为有限全分歧伽罗瓦扩张，并令 $G = \mathrm{Gal}(N/K)$。假设 $Z(G)$ 包含一个子群 H，使得 $H \cong C_p^2$，且令 $M = N^H$ 为 H 的不动域。设存在 $u < v$，使得 u、$v \notin \mathcal{U}_{M/K}$ 以及 $\mathcal{U}_{N/K} = \mathcal{U}_{M/K} \cup \{u, v\}$。令 $b < c$ 为与u对应的 N/K 的下分歧跳跃，v，并令 SS 表示满足 $M \subset L \subset N$ 和 $[L : M] = p$ 的域 L 的集合。那么存在 $L_0 \in SS$，具有以下性质:

(a) $\mathcal{U}_{L_0/K} = \mathcal{U}_{M/K} \cup \{u\}$ 和 N/L_0 的分歧断点为 c。

(b) 对所有满足 $L \neq L_0$ 的 $L \in SS$，我们有 $\mathcal{U}_{L/K} = \mathcal{U}_{M/K} \cup \{v\}$，且 N/L 的分歧断点为 b。

证明。首先证明 N/M 的下分歧跳跃为 b, c。由于 b 是 L/K 的一个下分歧断点，存在 $g \in G_b \setminus G_{b+1}$。由于 $u \notin \mathcal{U}_{M/K}$，由推论 2.2 可知，对于充分小的 $\epsilon > 0$，有 $G^u \leq G^{u+\epsilon}H$。由于 $G^u = G_b$且 $G^{u+\epsilon} = G_{b+1}$，由定理 2.1(a)可知 $G_b \leq G_{b+1}H$。因此，存在$g' \in G_{b+1}$ 和 $h \in H$ 使得 $g = g'h$。由此可得 $h = (g')^{-1}g \in G_b \setminus G_{b+1}$，所以有 $i(h) = b$。因此，b 是 N/M的一个下分歧断点。类似的论证表明，c 是 N/M 的一个下分歧断点。现在，由于 N/M 的下分歧跳跃为 b, c，对于每个 $L \in SS$，N/L 的分歧断点要么是 b，要么是 c。令$L_0 = N^{H_c}$ 为 $H_c = H_{b+\epsilon}$的不动域。N/L 的分歧断点为 $\geq c$当且仅当 $\mathrm{Gal}(N/L) \leq H_c$，由此可知 N/L_0 的分歧断点为 c，而对于所有满足 $L \neq L_0$的 $L \in SS$，N/L 的分歧断点为 b。

为完成证明，令 $L \in SS$ 并设 $A = \mathrm{Gal}(N/L) \leq H$。由于 c 是 N/M的最大下断点，当 $\epsilon > 0$ 充分小时，我们有

$$G^{v+\epsilon} \cap H = G_{c+1} \cap H = H_{c+1} = \{\mathrm{id}_L\}.$$

由此可知 $G^{v+\epsilon} \cap A = \{\mathrm{id}_L\}$，因此得到 $|G^{v+\epsilon}A : G^{v+\epsilon}| = |A| = p$。由于 v 是 N/K 的一个重数为 1 的上分歧跳跃，我们有 $|G^v : G^{v+\epsilon}| = p$。因此，$A \leq G^v$ 当且仅当 $G^v \leq G^{v+\epsilon}A$。由推论 2.2 可得，$v \notin \mathcal{U}_{L/K}$ 当且仅当$A \leq G^v = G_c$。因此，$v \notin \mathcal{U}_{L/K}$ 当且仅当 $A \leq G_c \cap H = H_c$。由于 $\mathcal{U}_{L/K}$ 等于 $\mathcal{U}_{M/K} \cup \{u\}$ 或 $\mathcal{U}_{M/K} \cup \{v\}$，我们得出：若 $L = L_0$，则 $\mathcal{U}_{L/K} = \mathcal{U}_{M/K} \cup \{u\}$；若 $L \neq L_0$，则$\mathcal{U}_{L/K} = \mathcal{U}_{M/K} \cup \{v\}$。 □

3 特征 p中的嵌入问题

设 K 为一个域，L/K 为有限伽罗瓦扩张，并令 $G = \mathrm{Gal}(L/K)$。设 $\widetilde{G}$ 为有限群，且 $\phi : \widetilde{G} \to G$ 为一个满同态。与 $(L/K, G, \phi)$ 相关的嵌入问题的一个解是有限扩张 M/L，满足 M在 K 上是伽罗瓦扩张，并且存在正合列的一个同构

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \text{伽罗瓦群}(M/L) & \longrightarrow & \text{伽罗瓦群}(M/K) & \longrightarrow & \text{伽罗瓦群}(L/K) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & \ker\phi & \longrightarrow & \widetilde{G} & \xrightarrow{\phi} & G & \longrightarrow & 1.
\end{array}$$

本节中，我们使用 Witt 的一个定理来证明，涉及特征为 p 的局部域的某些嵌入问题总有一个解，且该解是全分歧扩张。

回顾一下，有限 p-群 G 的秩是其 G生成集的最小大小。令 $\Phi(G)$ 表示 G的 Frattini 子群。由 Burnside 基定理可知，Frattini 商群 $G/\Phi(G)$ 是一个初等阿贝尔 p-群，且 rank(G) 等于 rank($G/\Phi(G)$)。在 [12, III], 中，Witt 证明了以下定理：

定理 3.1. 设 K 是一个特征为 p 的域，且 L/K 是一个有限伽罗瓦扩张，使得 $G = \mathrm{Gal}(L/K)$ 是一个 p-群。设 G 是一个有限 p-群，满足 rank(G) = rank(G)，并设 $\phi : G \to G$ 是一个满同态。那么存在一个扩张 M/L，它解决了与 $(L/K, G, \phi)$ 相关的嵌入问题。

我们将使用 Witt 定理的以下推论：

推论 3.2. 设 K 是一个特征为 p的局部域，且 L/K 是一个有限全分歧伽罗瓦扩张，其伽罗瓦群 G =Gal(L/K) 是一个 p-群。设 G 是一个有限 p-群，并设 ϕ: $G \to G$ 是一个满群同态。那么存在一个全分歧域扩张 M/L ，它解决了与$(L/K, G, \phi)$ 相关的嵌入问题。

证明。令 $N = \ker\phi$。只需考虑 $N \cong C_p$ 的情形。若 G 的 N 扩张 $\sim G$ 是分裂的，则 $G \cong C_p \times G$。此时，取一个分歧断点大于 L/K 的所有上分歧断点的分歧 C_p 扩张 F/K 。那么 L 和 F 在 K 上线性无关，因此 $M = LF$ 是 $\sim K$ 的全分歧伽罗瓦扩张，且 Gal(M/K) $\cong C_p \times G \cong G$。于是 M 解出了给定的嵌入问题。若 ，则 G 的 N 扩张 G 不是分裂的，我们断言 rank(G) =rank(G)。显然，我们有 rank(G) $\geq$ rank(G)。令 A 为 G 的一个生成集，使得 $|A| =$ rank(G) ，并令 $A \subset G$ 满足 $|A| = |A|$ 和 $\phi(A) = A$。若 $\langle A\rangle \neq G$ ，则 $\langle A\rangle \cong G$ 且$\sim$ $G = N \times \langle A\rangle$。这与扩张不是分裂扩张的假设矛盾，因此必有 $\langle A\rangle = G$。于是 rank(G) = rank(G)。由定理 3.1 可知，存在一个域扩张 M/L ，它解出了给定的嵌入问题。若 M/L 是非分歧的，令 F 表示 K 的 p 次非分歧扩张。于是 $F \subset M$，因此得到 $M = LF$，且 Gal(M/K) $\cong C_p \times G$。这就产生了矛盾，因此 M/L 是一个全分歧扩张。 □

4 极小非阿贝尔 p-群

我们在有限的 p-群上定义偏序：若 H 同构于 G 的商群，则 $H \preccurlyeq G$ 。我们关注非阿贝尔 p-群中 4-极小的群。我们称这样的群为极小非阿贝尔 p-群。

命题 4.1. 设 $p > 2$ 且令 G 为一个 p-群。那么 G 是一个极小非阿贝尔p-群，当且仅当 G 满足以下条件：

(i) G 是 2类幂零的。

(ii) $Z(G)$ 是阶为 p^d 的循环群，其中 $d \geq 1$。

(iii) $[G,G]$ 是 $Z(G)$ 中阶为 p 的子群。

(iv) $\overline{G} := G/Z(G)$ 是秩为 $2n$ 的初等阿贝尔 p-群，其中 $n \geq 1$，且 $[\ ,\ ]$ 在 $\overline{G}$ 上诱导一个取值于 $[G,G]$ 的非退化斜对称 $\mathbb{F}_p$-双线性形式 $(\ ,\ )_{\overline{G}}$。

证明。设 G 是一个极小非阿贝尔 p-群。由于 $Z(G)$ 非平凡，由 G 的极小性可知 $\overline{G}$ 是阿贝尔群。因此 G 是 2 类幂零群，这就得到 (i)。设 N 是 G 的一个非平凡正规子群。由 G 的极小性可知 G/N 是阿贝尔群，因此 $[G,G] \leq N$。于是 $[G,G]$ 包含于 $Z(G)$ 的所有非平凡子群中，所以 $Z(G)$ 是循环群，且 $[G,G]$ 是 $Z(G)$ 中阶为 p 的唯一子群。这就证明了 (ii) 和 (iii)。

令 z 为 $Z(G) \cong C_{p^d}$ 的一个生成元，并令 $w = z^{p^{d-1}}$。则 $[G,G] = \langle w \rangle$。对于 x, $y \in G$，我们有 $xyx^{-1} = yw^a$，其中某个 $a \in \mathbb{Z}$。因此 $xy^px^{-1} = y^pw^{pa} = y^p$，所以 $y^p \in Z(G)$。由此可知，$\overline{G}$ 是一个初等阿贝尔 p 群。令 x、y_1、$y_2 \in G$。则存在 $a_j \in \mathbb{Z}$，使得对于 $j = 1$，2，有 $xy_jx^{-1} = y_jw^{a_j}$。由此可知 $xy_1y_2x^{-1} = y_1y_2w^{a_1+a_2}$，进而得到 $[x, y_1y_2] = [x, y_1][x, y_2]$。由于 $[y, x] = [x, y]^{-1}$，我们推得 $[\ ,\ ]$ 在 $\overline{G}$ 上诱导出一个斜对称的 $\mathbb{F}_p$-双线性配对 $(\ ,\ )_{\overline{G}}$。若对所有 $y \in G$ 都有 $[x, y] = 1$，则 $x \in Z(G)$，因此该配对是非退化的。因此 $\overline{G}$ 的 $\mathbb{F}_p$-秩为偶数。这证明了 (iv)。

反过来，假设 (i)–(iv) 成立。由 (i) 或 (iii)，G是非阿贝尔群。设 N 是 G的非平凡正规子群。那么 $N \cap Z(G)$ 非平凡，因此由 (ii) 和 (iii) 可得 $[G,G] \leq N$。于是 G/N 是阿贝尔群，因此 G 是极小非阿贝尔 p群。 □

极小非阿贝尔 p群可以更明确地描述。对于 $n, d \geq 1$，我们定义一个阶为 p^{2n+d}、由 $x_1, \ldots, x_n, y_1, \ldots, y_n, z$生成的群 $H(n, d)$，其中$|x_i| = |y_i| = p$ 且 $|z| = p^d$。除 x_i和 y_i外，这些生成元两两可交换；它们满足 $[x_i, y_i] = z^{p^{d-1}}$，其中 $1 \leq i \leq n$。因此 $H(1, 1)$ 是海森堡p群，而 $H(n, 1)$ 是一个超特殊 p群。

我们定义另一个阶为 p^{2n+d}、由 $x_1, \ldots, x_n, y_1, \ldots, y_n, z$ 生成的群 $A(n, d)$。在 $A(n, d)$ 中，对于 $2 \leq i \leq n$，有 $|x_i| = p$；对于 $1 \leq i \leq n$，有 $|y_i| = p$；并且 $x_1^p = z$，其中 $|z| = p^d$。与 $H(n, d)$ 一样，除 x_i 和 y_i 外，所有生成元两两可交换，而它们满足：当 $1 \leq i \leq n$ 时，$[x_i, y_i] = z^{p^{d-1}}$。因此，$A(1, 1)$ 是阶为 p^3 的亚循环群，而 $A(n, 1)$ 是一个超特殊 p- 群。

从构造可清楚看出，群 $H(n, d)$ 和 $A(n, d)$ 满足命题 4.1 的条件 (i)–(iv)。现在我们证明其逆命题，即每个极小非阿贝尔 p-群都同构于这两个群之一。

命题 4.2. 设 $p > 2$，并设 G 是一个极小非阿贝尔 p-群。那么，对于某些 n、$d \geq 1$，要么 $G \cong H(n, d)$，要么 $G \cong A(n, d)$。

证明。由于 G 是一个极小非阿贝尔 p 群，G 满足命题 4.1 的条件 (i)–(iv)。设 z 是 $Z(G)$ 的一个生成元；于是对某个 $d \geq 1$，有 $|z| = p^d$。令 $w = z^{p^{d-1}}$，

使得 $\langle w\rangle = [G,G]$。由 (iv) 可知，对所有 $x \in G$，$x^p \in Z(G)$。对于 $x \in G$，令 $\overline{x} = xZ(G) \in \overline{G}$。

假设对所有 $x \in G$，$x^p \in Z(G)^p$。由于 $[\ ,\ ]$ 在 $\overline{G}$ 上诱导了一个非退化的 $\mathbb{F}_p$-线性配对 $(\ ,\ )_{\overline{G}}$，因此存在 $\overline{G}$ 的一个 $\mathbb{F}_p$-基 $\{\overline{x}_1,\dots,\overline{x}_n,\overline{y}_1,\dots,\overline{y}_n\}$，使得对所有 $1 \le i, j \le n$，$(\overline{x}_i,\overline{x}_j)_{\overline{G}} = (\overline{y}_i,\overline{y}_j)_{\overline{G}} = w^0$ 且 $(\overline{x}_i,\overline{y}_j)_{\overline{G}} = w^{\delta_{ij}}$。取满足 $\overline{x}_i = x_i'Z(G)$ 的 $x_i' \in G$。那么存在 $a_i \in \mathbb{Z}$ 使得 $(x_i')^p = z^{pa_i}$。因此，$x_i = x_i'z^{-a_i}$ 满足 $x_iZ(G) = \overline{x}_i$ 且 $|x_i| = p$。类似地，存在 $y_i \in G$，满足 $y_iZ(G) = \overline{y}_i$ 且 $|y_i| = p$。由此可得 $G \cong H(n,d)$。

现在假设存在 $x \in G$，使得 $x^p \notin Z(G)^p$。定义 $\phi : \overline{G} \to Z(G)/Z(G)^p$，其定义为 $\phi(xZ(G)) = x^pZ(G)^p$。显然，ϕ 定义良好。我们断言 ϕ 是一个群同态，因此也是一个 $\mathbb{F}_p$-线性映射。设 $x, y \in G$；则对某个整数 a，有 $[x,y] = z^a$。因此 $yx = xyz^{-a}$，于是得到 $(xy)^p = x^py^pz^{pb}$，其中 $b = -\frac{1}{2}(p-1)a$。因此，$\phi(xy) = \phi(x)\phi(y)$。由假设，$\phi$ 非平凡，因此 $\phi(\overline{G}) = Z(G)/Z(G)^p$ 是一个阶为 p 的循环群。令 $V =$ 为 $\ker\phi$，并令 $V^\perp$ 为相对于配对 $(\ ,\ )_{\overline{G}}$ 的 V 的正交补。那么，V 和 $V^\perp$ 是 $\overline{G}$ 的 $\mathbb{F}_p$-子空间，且 $\dim_{\mathbb{F}_p}(V) = 2n-1$，$\dim_{\mathbb{F}_p}(V^\perp) = 1$。取满足 $\overline{y}_1' = y_1'Z(G)$ 生成 $V^\perp$ 的 $y_1' \in G$。由于 $[y_1', y_1'] = w^0$，我们有 $\overline{y}_1' \in (V^\perp)^\perp = V = \ker\phi$。因此存在 $a \in \mathbb{Z}$，使得 $(y_1')^p = z^{ap}$。于是 $y_1 = y_1'z^{-a}$ 满足 $\overline{y}_1 = \overline{y}_1'$ 和 $|y_1| = p$。现在取满足 $(\overline{x}_1,\overline{y}_1)_{\overline{G}} = w^1$ 的 $x_1 \in G$。那么 $\overline{x}_1 \notin V$，因此 x_1^p 是 $Z(G)$ 的一个生成元。所以我们不妨假设 $x_1^p = z$。令 W 表示 $\overline{G}$ 中由 $\{\overline{x}_1,\overline{y}_1\}$ 张成的空间。于是，$(\ ,\ )_{\overline{G}}$ 在 W 上的限制是非退化的，因此 $V = W \oplus W^\perp$，且 $(\ ,\ )_{\overline{G}}$ 在 $W^\perp$ 上的限制是一个非退化的斜对称 $\mathbb{F}_p$-双线性形式。因此存在 $W^\perp$ 的一个基 $\{\overline{x}_2,\dots,\overline{x}_n,\overline{y}_2,\dots,\overline{y}_n\}$，使得对 $2 \le i, j \le n$，$(\overline{x}_i,\overline{x}_j)_{\overline{G}} = (\overline{y}_i,\overline{y}_j)_{\overline{G}} = w^0$ 且 $(\overline{x}_i,\overline{y}_j)_{\overline{G}} = w^{\delta_{ij}}$。取满足 $\overline{x}_i = x_i'Z(G)$ 的 $x_i' \in G$，并令 $a_i \in \mathbb{Z}$ 满足 $(x_i')^p = z^{a_i}$。由于 $2 \le i \le n$，对某个 $b_i \in \mathbb{Z}$，有 $a_i = pb_i$。因此 $x_i = x_i'z^{-b_i}$ 满足 $x_iZ(G) = \overline{x}_i$ 且 $|x_i| = p$。对于 $2 \le i \le n$，同理存在 $y_i \in G$，使得 $y_iZ(G) = \overline{y}_i$ 且 $|y_i| = p$。因此，$G \cong A(n,d)$。

□

注 4.3. 如果 p-群 G 的每个阿贝尔特征子群都是循环子群，就称其为辛型。Philip Hall 在未发表的笔记中证明，对于 $p > 2$，辛型的非阿贝尔 p-群恰好是群 $H(n,d)$ 和 $A(n,d)$，其中$n, d \ge 1$。因此，对于 $p > 2$，极小非阿贝尔 p-群与辛型的非阿贝尔 p-群相同。Hall 的结果的证明见 [7,5.4.9]。感谢 Peter Sin 指引我们查阅这一参考资料。

设 G 是一个群，N_1, N_2 是 G的子群。若 $N_1 \cup N_2$生成 G，且 N_1的每个元素都与 N_2的每个元素交换，则称 G 是 N_1和 N_2的中心积。在这种情况下，$Z(N_1) \times Z(N_2)$有一个子群 A，使得 $G \cong (N_1 \times N_2)/A$。

我们希望将极小非阿贝尔 p-群表示为中心积，其中 $H(1,1)$ 是其中一个因子。为方便起见，我们将 $H(n,d)$ 的定义扩展为令 $H(0,d) = C_{p^d}$。

P命题 4.4。（a）设 n、$d \ge 1$。则 $H(n,d)$ 是子群N_1和 N_2的中心积，其中 $N_1 \cong H(n-1,d)$ 和 $N_2 \cong H(1,1)$。更准确地说，

$$H(n,d) \cong (H(n-1,d) \times H(1,1))/B \tag{4.1}$$

对于 $Z(H(n-1,d))$ 的某个子群 $B \times Z(H(1,1))$，其阶为 p。

(b) 设 $n \geq 2$ 和 $d \geq 1$。则 $A(n,d)$ 是子群 N_1 和 N_2 的中心积，其中 $N_1 \cong A(n-1,d)$，且 $N_2 \cong H(1,1)$。更准确地说，

$$A(n,d) \cong (A(n-1,d) \times H(1,1))/B \tag{4.2}$$

对于某个子群 B， $Z(H(n-1,d)) \times Z\ H(1,1)$ 的阶为 p。

证明。(a) 设 N_1 是由 x_1、……、x_{n-1}、y_1、……、y_{n-1}、z 生成的 $H(n,d)$ 的子群，并设 N_2 是由 x_n、y_n、$z^{p^{d-1}}$ 生成的 $H(n,d)$ 的子群。则 $N_1 \cong H(n-1,d)$、$N_2 \cong H(1,1)$ 以及 N_1、N_2 满足中心积的条件。因此存在满足（4.1）的 B。由于 $|H(n,d)| = p^{2n+d}$、$|H(n-1,d)| = p^{2n+d-2}$，且 $|H(1,1)| = p^3$，我们必有 $|B| = p$。

(b) 令 N_1 为 $A(n,d)$ 由 $x_1,\ldots,x_{n-1},y_1,\ldots,y_{n-1},z$ 生成的子群，并令 N_2 为 $A(n,d)$ 由 $x_n, y_n, z^{p^{d-1}}$ 生成的子群。则 $N_1 \cong A(n-1,d)$,$N_2 \cong H(1,1)$ 和 N_1, N_2 满足中心积的条件。因此存在满足 (4.2) 的 B。由于 $|A(n,d)| = p^{2n+d}$, $|A(n-1,d)| = p^{2n+d-2}$，且 $|H(1,1)| = p^3$，我们必须有 $|B| = p$。 □

命题 4.4(b) 不适用于形如 $A(1,d)$ 的群。相反，我们使用以下描述：

命题 4.5。设 $d \geq 1$，并记 $H(1,1) = \langle x_1, y_1, z\rangle$, $C_{p^{d+1}} = \langle w\rangle$。定义 G_d 为 $H(1,1) \times C_{p^{d+1}}$ 的一个子群，使得 $G_d = \langle x_1 w, y_1, z\rangle$，并令

$$\overline{G}_d = G_d/\langle (x_1 w)^{p^d} z^{-1}\rangle = G_d/\langle w^{p^d} z^{-1}\rangle.$$

那么 $\overline{G}_d \cong A(1,d)$。

证明。我们有 $[x_1 w, y_1] = [x_1, y_1] = z$ 以及 $(x_1 w)^p = w^p$。令 $\overline{x}_1$、$\overline{y}_1$、$\overline{z}$ 分别表示 $x_1 w$、y_1、z 在 $\overline{G}_d$ 中的像。于是 $|\overline{x}_1| = p^{d+1}$、$|\overline{y}_1| = p$，以及 $[\overline{x}_1, \overline{y}_1] = \overline{z} = \overline{x}_1^{p^d}$。因此 $\overline{G}_d \cong A(1,d)$。 □

具有非整数上分歧跳跃的 5　p-扩张

设 $p > 2$，令 G 为一个非阿贝尔 p-群，并令 K 为一个特征 p、剩余域完美的局部域 k。本节证明，存在一个伽罗瓦群为 G 的全分歧伽罗瓦扩张 L/K，使得 L/K 的一个上分歧跳跃不是整数。由定理 3.1 可知，K 上仅涉及 p-群的每个嵌入问题，都能通过一个全分歧扩张求解。因此，我们只需为每个在非阿贝尔 p-群中 4-极小的 G，给出一个具有非整数上分歧跳跃的 G-扩张。这些群已在命题 4.2 中分类。

我们的证明使用一种自举论证，其基础是构造具有非整数上分歧跳跃的 $H(1,1)$-扩张。首先，我们给出一种简单的方法，利用 Artin–Schreier 扩张构造 $H(1,1)$-扩张。回顾一下，若 $\beta \in K$ 满足 $v_K(\beta) = -b$，其中 $b \geq 1$ 和 $p \nmid b$，则 $X^p - X - \beta$ 的根生成一个 K 的 C_p-扩张，其分歧断点为 b （见 $[6, \text{III}]$ 中的命题 2.5）。

引理 5.1. 设 a, b 为正整数，满足 $a > b, p \nmid a$，且 $p \nmid b$。设 $\alpha, \beta \in K$ 满足 $v_K(\alpha) = -a$ 且 $v_K(\beta) = -b$，并设 $x, y \in K^{sep}$ 满足 $x^p - x = \alpha$ 和 $y^p - y = \beta$。令 $M = K(x, y)$，并设 $\gamma \in K$。设 $z \in K^{sep}$ 满足 $z^p - z = \alpha y + \gamma$，并令 $L = M(z)$。则 L/K 是一个全分歧的 $H(1,1)$-扩张。

证明. 根据构造，M/K 是一个全分歧的 C_p^2-扩张。设 $\sigma, \tau \in \mathrm{Gal}(M/K)$ 满足 $\sigma(x) = x + 1, \sigma(y) = y, \tau(x) = x$，且 $\tau(y) = y + 1$。于是

$$(\sigma - 1)(\alpha y + \gamma) = 0$$
$$(\tau - 1)(\alpha y + \gamma) = \alpha = \wp(x).$$

由于 $x \in M$，可知 L/K 是伽罗瓦的。此外，我们可以通过设定 $\widetilde{\sigma}(z) = z$ 和 $\widetilde{\tau}(z) = z + x$，将 σ, τ 扩展为 $\widetilde{\sigma}, \widetilde{\tau} \in \mathrm{Gal}(L/K)$。容易得到 $|\widetilde{\sigma}| = |\widetilde{\tau}| = p$，$[\widetilde{\sigma}, \widetilde{\tau}] \in \mathrm{Gal}(L/M)$，且 $[\widetilde{\sigma}, \widetilde{\tau}](z) = z + 1$。最后一个公式表明，$[\widetilde{\sigma}, \widetilde{\tau}]$ 生成 $\mathrm{Gal}(L/M)$。因此 $\mathrm{Gal}(L/K) \cong H(1,1)$。

□

命题 5.2. 设 K 是特征为 $p > 2$ 的局部域，且 F/K 是一个分歧的 C_p-扩张。设 F/K 的分歧断点为 b，并设 a 是满足 $a > b$ 且 $a \not\equiv 0$、$-b$ （模 p）的整数。则存在一个全分歧扩张 L/F，使得 L/K 是一个带有 $\mathcal{U}_{L/K} = \{b, a, a + p^{-1}b\}$ 的 $H(1,1)$-扩张。特别地，L/K 具有一个不是整数的上分歧跳跃。

证明. 由 $[6, \text{III}]$ 中的命题 2.4 可知，存在 $y \in F$，使得 $F = K(y)$、$v_F(y) = -b$，且 $\beta := y^p - y \in K$。由于 $p \nmid b$，我们可以将 $a = bt + ps$ 写成 $0 \leq t < p$；根据我们关于 a 的假设，可得 $1 \leq t \leq p - 2$。令 $\alpha = \pi_K^{-ps}\beta^t$；则 $v_K(\alpha) = -a$。取满足 $x^p - x = \alpha$ 的 $x \in K^{sep}$。于是，$M := F(x) = K(x, y)$ 是 K 的一个 C_p^2-扩张，其上分歧断点为 b、a。令 $z \in K^{sep}$ 为 $t + 1$ 在 $\mathbb{F}_p^\times$ 中的逆元，取满足 $z^p - z = \alpha y + r\alpha\beta$ 的 $z \in K^{sep}$，并令 $L = M(z)$。根据引理 5.1，L/K 是一个 $H(1,1)$-扩张。此外，$\mathrm{Gal}(L/M) \cong C_p$ 是 $\mathrm{Gal}(L/K)$ 的交换子子群。因此根据（2.1），$\mathrm{Gal}(L/M)$ 是 $\mathrm{Gal}(L/K)$ 的最小非平凡分歧子群。所以根据 $[11, \text{IV}]$，中命题 3 的推论，M/K 的下分歧断点同时也是 L/K 的下分歧断点。

令 $E = F(z)$。我们无法直接计算 C_p-扩张 E/F 的分歧断点，因为 $v_F(\alpha y + r\alpha\beta) = v_F(r\alpha\beta)$ 能被 p 整除。因此，我们转而考虑阿廷 – 施赖尔方程

$$X^p - X = \alpha y + r\alpha\beta - \wp(r\pi_K^{-s} y^{t+1}).$$

由于 $r\pi_K^{-s}y^{t+1}\in F$，该方程的根生成了 E在 F上的扩张。此外，我们有

$$\begin{aligned}\alpha y+r\alpha\beta-\wp(r\pi_K^{-s}y^{t+1})&=\alpha y+r\alpha\beta+r\pi_K^{-s}y^{t+1}-(r\pi_K^{-s}y^{t+1})^p\\&=\alpha y+r\alpha\beta+r\pi_K^{-s}y^{t+1}-r\pi_K^{-ps}(y+\beta)^{t+1}\\&=\alpha y+r\alpha\beta+r\pi_K^{-s}y^{t+1}-r\pi_K^{-ps}\sum_{i=0}^{t+1}\binom{t+1}{i}\beta^{t+1-i}y^i.\end{aligned}$$

由于 $\alpha=\pi_K^{-ps}\beta^t$，和中的 $i=0$ 项为 $-r\alpha\beta$，而 $i=1$ 项为 $-\alpha y$。由此可得

$$\alpha y+r\alpha\beta-\wp(r\pi_K^{-s}y^{t+1})=r\pi_K^{-s}y^{t+1}-r\pi_K^{-ps}\sum_{i=2}^{t+1}\binom{t+1}{i}\beta^{t+1-i}y^i.$$

由于 $1\le t\le p-2$，我们得到

$$\begin{aligned}v_F\left(r\pi_K^{-ps}\binom{t+1}{2}\beta^{t-1}y^2\right)&=-p^2s-(t-1)pb-2b\\&=-pa+pb-2b.\end{aligned}$$

由于 $a>b$，我们有

$$v_F(r\pi_K^{-s}y^{t+1})=-ps-(t+1)b=-a-b>-pa+pb-2b.$$

因此

$$\begin{aligned}v_F(\alpha y+r\alpha\beta-\wp(r\pi_K^{-s}y^{t+1}))&=v_F\left(r\pi_K^{-ps}\binom{t+1}{2}\beta^{t-1}y^2\right)\\&=-pa+pb-2b,\end{aligned}$$

它不能被 p整除。因此， E/F的分歧断点为 $2b+p(a-b)$。

由于 b 是 F/K 的分歧断点，由引理 2.3 可知， M/F 的分歧断点为 $b+p(a-b)$。因此， C_p^2-扩张 L/F 的上分歧断点为 $b+p(a-b)$ $2b+p(a-b)$，下断点为 $b+p(a-b)$ $b+pa$。由于 C_p^2-扩张 M/K 的上分歧断点为 b、a，其中 $b<a$，该扩张的下断点为 b、$b+p(a-b)$。如上所述，这些也都是 L/K 的下断点。因此， L/K 的下断点为 b、$b+p(a-b)$ $b+pa$。我们得出 L/K 的上分歧跳跃为 b、a，并且

$$a+p^{-2}((b+pa)-(b+p(a-b)))=a+p^{-1}b.\qquad\square$$

引理 5.3. 设 N/K 是一个全分歧伽罗瓦扩张，且 $\mathrm{Gal}(N/K)$ 同构于 $H(n,d)$（其中 $n\ge 0$和 $d\ge 1$），或 $A(n,d)$（其中 $n,d\ge 1$）。设$G=\mathrm{Gal}(N/K)$，设 H 是 $Z(G)$ 中阶为 p的唯一子群，并设 $M\subset N$ 是 H的不动域。那么，对某个 $v\in\mathbb{Q}$，有 $\mathcal{U}_{N/K}=\mathcal{U}_{M/K}\cup\{v\}$，且对所有$w\in\mathcal{U}_{M/K}$， $v>w$ 成立。此外， $H=G^v$ 是 G中最小的非平凡分歧子群。

证明. 设 $\sigma \in G$，其中 $\sigma \notin Z(G)$。那么存在 $\tau \in G$，使得 $[\sigma,\tau]$ 生成$H \cong C_p$。因此，由 (2.1)，对于 $\rho \in H$，我们有 $i(\rho) > i(\sigma)$。假设 $\sigma \in Z(G)$，但$\sigma \notin H$。那么存在 $1 \le i \le d-1$，使得 σ^{p^i} 生成 H。再次由 (2.1)，对于所有 $\rho \in H$，我们得到 $i(\rho) > i(\sigma)$。由此可知，H 是 G中最小的非平凡分歧子群。因此 $H = G^v$，其中 v 是 N/K的最大上分歧跳跃。利用定理 2.1(b)，我们推出 $\mathcal{U}_{N/K} = \mathcal{U}_{M/K} \cup \{v\}$。□

现在我们构造至少具有一个非整数上分歧跳跃的 $H(n,d)$-扩张和 $A(n,d)$-扩张。

命题 5.4. 设 K 是特征为 $p > 2$ 的局部域，且 $n, d \ge 1$。

(a) 存在一个全分歧伽罗瓦扩张 L/K，使得 Gal$(L/K) \cong H(n,d)$，且 L/K 的最大上分歧跳跃不是整数。(b) 存在一个全分歧伽罗瓦扩张 L/K，使得 Gal$(L/K) \cong A(n,d)$，且 L/K 的最大上分歧跳跃不是整数。

证明。(a) 根据推论 3.2，存在一个全分歧 $H(n-1,d)$-扩张 N_1/K。设 v 是 N_1/K 的最大上分歧跳跃，并设 a, b 是满足 $a > b > v$, $p \nmid b$ 且 $a \not\equiv 0, -b$ (模 p) 的整数。于是，根据命题 5.2，存在一个 $H(1,1)$- 扩张 N_2/K，使得 $\mathcal{U}_{N_2/K} = \{b, a, a + p^{-1}b\}$。令 $N = N_1N_2$。由于 $\mathcal{U}_{N_1/K}$ 与 $\mathcal{U}_{N_2/K}$ 不相交，因此 $\mathcal{U}_{N/K} = \mathcal{U}_{N_1/K} \cup \mathcal{U}_{N_2/K}$，且 $N_1 \cap N_2 = K$。由此可得

$$\begin{aligned}\mathrm{Gal}(N/K) &\cong \mathrm{Gal}(N_1/K) \times \mathrm{Gal}(N_2/K)\\ &\cong H(n-1,d) \times H(1,1).\end{aligned}$$

对于 $i = 1, 2$，令 M_i 为 N_i 中由 $Z(\mathrm{Gal}(N_i/K))$ 的阶为 p 的唯一子群所固定的子域。设 $M = M_1M_2$；则 Gal$(N/M) \cong C_p^2$。由引理 5.3 可知 $\mathcal{U}_{N_1/K} = \mathcal{U}_{M_1/K} \cup \{v\}$ 且 $\mathcal{U}_{N_2/K} = \mathcal{U}_{M_2/K} \cup \{a + p^{-1}b\}$。由于 $\mathcal{U}_{M/K} = \mathcal{U}_{M_1/K} \cup \mathcal{U}_{M_2/K}$，这意味着 $\mathcal{U}_{N/K} = \mathcal{U}_{M/K} \cup \{v, a + p^{-1}b\}$。根据命题 4.4(a)，存在子群 $B \le$Gal(N/M)，使得 Gal$(N/M)/B \cong H(n,d)$。令 $L = N^B$ 为 B 的不动域；则 L/K 是一个全分歧的 $H(n,d)$-扩张。由于

$$\mathrm{Gal}(N_1M_2/K) \cong H(n-1,d) \times C_p^2 \ncong H(n,d)$$

我们有 $L \neq N_1M_2$。由于 $a + p^{-1}b > v$，且 v 是 N_1M_2/K 的最大上分歧跳跃，由引理 2.3 可知，$a + p^{-1}b \notin \mathbb{Z}$ 是 L/K 的一个上分歧跳跃。

(b) 若 $n \ge 2$，则我们按照情形 (a) 进行：设 N_1/K 是一个全分歧的 $A(n-1,d)$-扩张，其最大的上分歧跳跃为 v。由命题 5.2，存在一个 $H(1,1)$-扩张 N_2/K，使得 $\mathcal{U}_{N_2/K} = \{b, a, a + p^{-1}b\}$，其中 $a > b > v$、$p \nmid b$，且 $a \not\equiv 0$、$-b$（模 p）。令 $N = N_1N_2$，得到 $\mathcal{U}_{N/K} = \mathcal{U}_{N_1/K} \cup \mathcal{U}_{N_2/K}$、$N_1 \cap N_2 = K$，并且

$$\begin{aligned}\mathrm{Gal}(N/K) &\cong \mathrm{Gal}(N_1/K) \times \mathrm{Gal}(N_2/K)\\ &\cong A(n-1,d) \times H(1,1).\end{aligned}$$

按照证明 (a) 中的方式定义 M_i 和 M，得到 Gal$(N/M) \cong C_p^2$ 且 $\mathcal{U}_{N/K} = \mathcal{U}_{M/K} \cup \{v, a + p^{-1}b\}$。因此，由命题 4.4(b)，存在 $B \leq$ Gal(N/M)，使得 Gal$(N/K)/B \cong A(n, d)$。令 $L = N^B$，得到 Gal$(L/K) \cong A(n, d)$。由于 N_1M_2 是 M 的一个 C_p-扩张，且 v 是 N_1M_2/K 的一个上分歧跳跃，利用引理 2.3 可推出 $a + p^{-1}b$ 是 L/K 的一个上分歧跳跃。

对于每个 $d \geq 1$，还需构造一个具有非整数上分歧跳跃的 $A(1, d)$-扩张。设 N_1/K 是一个全分歧 $C_{p^{d+1}}$-扩张，并令 v 表示 N_1/K 的最大上分歧跳跃。设 F/K 是 N_1/K 的 C_p-子扩张。设 b 是 F/K 的分歧断点，并设 a 是一个整数，使得 $a > v$ 且 $a \not\equiv 0, -b$（模 p）。于是由命题 5.2，存在一个全分歧 $H(1, 1)$-扩张 N_2/K，使得 $N_1 \cap N_2 = F$ 且 $\mathcal{U}_{N_2/K} = \{b, a, a + p^{-1}b\}$。令 $N = N_1N_2$。则

$$\mathrm{Gal}(N/K) \cong \{(\sigma_1, \sigma_2) \in \mathrm{Gal}(N_1/K) \times \mathrm{Gal}(N_2/K) : \sigma_1|_F = \sigma_2|_F\}$$

同构于命题 4.5 中定义的群 G_d。设 M_1/K 是 N_1/K 的 C_{p^d}-子扩张，并设 M_2/K 是 N_2/K 的 C_p^2-子扩张。则 $M_1 \cap M_2 = F$。令 $M = M_1M_2$；则 N/M 是一个 C_p^2-扩张。由命题 4.5，存在 N/M 的一个 C_p-子扩张 L/M，使得 L/K 是一个全分歧 $A(1, d)$-扩张。另一方面，N_1M_2/M 是 N/M 的一个 C_p-子扩张，使得 N_1M_2/K 以上分歧跳跃 v。由于

$$\mathrm{Gal}(N_1M_2/K) \cong C_{p^{d+1}} \times C_p \ncong A(1, d)$$

我们有 $L \neq N_1M_2$。因此，由引理 2.3 可知，$a + p^{-1}b$ 是 L/K的一个上分歧跳跃。这就完成了证明。 □

我们现在证明 Hasse-Arf 定理对于全分歧 p-扩张的逆命题 .

定理 5.5. 设 K 是特征为 $p > 2$ 的局部域，且 G是一个有限非阿贝尔 p-群。则存在一个全分歧 G-扩张 L/K，其上分歧跳跃不是整数。

证明。由命题 4.2，G 有一个商群 $\overline{G} = G/H$，它同构于 $H(n, d)$ 或 $A(n, d)$，其中 $n, d \geq 1$。由命题 5.4，存在一个全分歧$\overline{G}$-扩张 M/K，其上分歧跳跃不是整数。由推论 3.2，存在一个扩张 L/M，使得 L/K 是一个全分歧 G-扩张。由于 $\mathcal{U}_{M/K} \subset \mathcal{U}_{L/K}$，可知 L/K 有一个非整数的上分歧跳跃。 □

推论 5.6。 设 $p > 2$，且 G 是一个有限非阿贝尔 p-群。那么存在一个特征 0 的局部域 F，其剩余特征为 p，以及一个全分歧的 G-扩张 E/F，它具有一个非整数的上分歧跳跃。

证明。设 L/K 是一个具有非整数上分歧跳跃的全分歧 G-扩张，并设 $u_{L/K}$ 是 L/K 的最大上分歧跳跃。设 F 是一个特征 0 的局部域，其剩余域与 K 相同。进一步假设 F 的绝对分歧指数 $e_F = v_F(p)$ 满足 $e_F > u_{L/K}$。由 [3] 的定理 2.8 可得，存在一个全分歧 G-扩张 E/F，其分歧断点与 L/K 相同。

□

6 G扩张的上分歧跳跃为非整数

设 G 是一个非阿贝尔群，且是某个剩余特征为 $p>2$ 的局部域全分歧扩张的伽罗瓦群。本节通过证明存在一个特征为 p 的局部域的全分歧 G-扩张，且该扩张具有非整数上分歧跳跃，从而证明全分歧扩张情形下 Hasse-Arf 定理的逆命题。

设 K 是剩余特征为 p 的局部域，且 L/K 是次数为 mp^n 的全分歧伽罗瓦扩张，其中 $p\nmid m$。令 $G=\mathrm{Gal}(L/K)$，并令 P 为 G 的野分歧子群。于是 $P\trianglelefteq G$ 且 $G/P\cong C_m$，因此对某个同态 $\psi: C_m\to \mathrm{Aut}(P)$，有 $G\cong P\rtimes_\psi C_m$。在 [5] 的注 1 中证明了：若 P 是阿贝尔群而 G 是非阿贝尔群，则 L/K 的上分歧跳跃为非整数。下面的结果给出一类更大的群 G，使得每个全分歧G扩张的上分歧跳跃都是非整数。

命题 6.1。设 K 是剩余特征为 p 的局部域，且 L/K 是次数为 mp^n 的全分歧伽罗瓦扩张，其中 $p\nmid m$。令 $G=\mathrm{Gal}(L/K)$，并按上文记 $G\cong P\rtimes_\psi C_m$。若 C_m 在 P 上的作用非平凡，则 L/K 的上分歧跳跃为非整数。

证明。令 $\Phi(P)$ 为 P 的 Frattini 子群，并令 $M=L^{\Phi(P)}$ 为 $\Phi(P)$ 的不动域。则 $\Phi(P)\trianglelefteq G$，因此 M/K 是伽罗瓦扩张。设 $\overline{P}=P/\Phi(P)$，并令$\overline{\psi}: C_m\to \mathrm{Aut}(\overline{P})$ 为由 ψ 诱导的同态。根据 Burnside 的一个定理（见 [7] 第 5 章中的定理 1.4），ψ 非平凡。因此

$$\mathrm{Gal}(M/K)\cong G/\Phi(P)\cong \overline{P}\rtimes_{\overline{\psi}} C_m$$

是非阿贝尔的。由于 $\overline{P}$ 是阿贝尔群，由 [5] 中的注 1 可知，M/K 有一个非整数的上分歧跳跃。进而由定理 2.1(b) 可知，L/K 有一个非整数的上分歧跳跃。□

现在我们来证明 Hasse-Arf 定理的逆命题：

定理 6.2。设 G 是一个有限非阿贝尔群，且是某个剩余特征为 $p>2$ 的局部域的全分歧伽罗瓦扩张的伽罗瓦群。那么存在一个剩余特征为 p 的局部域的全分歧 G-扩张 L/K，它具有一个非整数的上分歧跳跃。

证明。关于 G 的假设意味着 G 有一个正规 Sylow p-子群 P，使得 $G\cong P\rtimes_\psi C_m$，其中 m 满足 $p\nmid m$，且存在某个 $\psi: C_m\to \mathrm{Aut}(P)$。若 $\psi(C_m)$ 非平凡，则由命题 6.1 可知，剩余特征为 p 的局部域上的每个全分歧 G-扩张L/K 都具有非整数的上分歧跳跃。另一方面，若 $\psi(C_m)$ 平凡，则 $G\cong P\times C_m$，因此 P 是非阿贝尔的。于是根据定理 5.5 或推论 5.6，存在一个剩余特征为p 的局部域 F，以及一个具有非整数上分歧跳跃的全分歧 P-扩张 E/F。令 ζ_m 为一个本原 m次单位根，并设 $K=F(\zeta_m)$、$L_1=E(\zeta_m)$。于是

L_1/K是一个全分歧 P-扩张，其分歧跳跃与 E/F相同。此外，存在一个全分歧 C_m-扩张 L_2/K。设 $L = L_1L_2$。则 L/K 是一个具有非整数上分歧跳跃的全分歧 G-扩张。□

备注 6.3. 设 L/K 是一个局部域的全分歧伽罗瓦扩张，并且对于每个全分歧阿贝尔扩张 E/K， LE/K 的上分歧断点全为整数。在 [5] 中，Fesenko 证明了此时 Gal(L/K) 必为阿贝尔群。这给出了 Hasse-Arf 定理的一个逆命题，其形式与本文所述的不同。

备注 6.4. 设 K 是一个特征 2 的局部域，且 L/K 是一个全分歧伽罗瓦扩张，其伽罗瓦群是阶 8 的二面体群 D_4。文献 [4] 证明了 L/K 的上分歧断点必为整数。因此，我们在此通过构造特征 p 的局部域扩张来证明 Hasse-Arf 定理逆命题的方法，无法推广到 $p = 2$ 的情形。然而，存在若干具有非整数上分歧跳跃的全分歧 D_4 扩张 $\mathbb{Q}_2$。例如，由多项式 $X^8 + 4X^7 + 2X^4 + 4X^2 + 14$ 的一个根生成的 $\mathbb{Q}_2$ 扩张是一个 D_4 扩张，其上分歧断点为 1、2、5/2（见 [9]）。据我们所知，对于剩余特征为 2 的局部域的全分歧扩张，Hasse-Arf 定理的逆命题是否成立仍是一个未解决的问题。

注 6.5. 对于哪些局部域 K，Hasse-Arf 定理的以下更强逆命题成立，这是一个值得探究的问题：对于每个满足 K 存在一个全分歧 G-扩张的非阿贝尔群 G，都存在一个全分歧 G-扩张L/K，其上分歧跳跃不是整数。由定理 6.2 的证明可知，对于特征 $p > 2$ 的局部域，这个 Hasse-Arf 定理的逆命题成立。另一方面，注 6.4 表明，对于特征 2 的局部域，这个 Hasse-Arf 定理的逆命题并不成立。据我们所知，对于特征 0 的局部域，这个更强的 Hasse-Arf 定理逆命题是否成立，仍是一个开放问题。

参考文献

[1] C. Arf, 《关于离散赋值完美域的纯分歧扩张的研究》, J. Reine Angew. Math. 181 (1939), 1–44.[2]E. Artin, 《代数数域判别式的群论结构》, J. Reine Angew. Math. 164 (1931), 1–11.[3] P. Deligne, 《特征 p 的局部域，特征 0 局部域的极限》，载于《局部域上的约化群表示》，Hermann，巴黎，1984，119–157.[4] G. G. Elder, 《特征 p 局部域的非阿贝尔扩张的上分歧序列》，预印本。

[5] I. B. Fesenko, 《Hasse-Arf 性质与阿贝尔扩张》, 《数学消息》174 (1995), 81–87.[6] I. B. Fesenko 和 S. V. Vostokov, 《局部域及其扩张》, 美国数学会, 罗得岛州普罗维登斯, 2002.[7] D. Gorenstein, 《有限群》, 第二版, Chelsea, 纽约, 1980.[8]H. Hasse, 《关于相对阿贝尔数域的导子、判别式和分歧域》, J. Reine Angew. Math. 162 (1930), 169–184.[9] LMFDB 协作组, 《 L-函数与模形式数据库》, p-进域 2.8.22.83 的主页, `https://www.lmfdb.org/padicField/2.8.22.83`, 访问日期: 2022 年 6 月 24 日。[10] J. Lubin, 《局部 Kronecker-Weber 定理》, Trans. Amer. Math. Soc. 267 (1981), 133–138.[11] J.-P. Serre, 《局部域》, Hermann, 巴黎, 1962 年; 译本为《局部域》, 《数学讲义》67, 施普林格出版社, 1979 年。[12] E. Witt, 《构造具有给定阶 p^f 群的特征 p 伽罗瓦域》, J. Reine Angew. Math. 174 (1936), 237–245。