Université Grenoble Alpes

ANNALES DE L'INSTITUT FOURIER

G. Griffith Elder & Kevin Keating

Galois scaffolds for p-extensions in characteristic p

Article à paraître, mis en ligne le 5 février 2025, 27 p.

Les *Annales de l'Institut Fourier* sont membres du Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org e-ISSN : 1777-5310

Ann. Inst. Fourier, Grenoble
Article à paraître
Mis en ligne le 5 février 2025.

GALOIS SCAFFOLDS FOR p-EXTENSIONS IN CHARACTERISTIC p

by G. Griffith ELDER & Kevin KEATING

Abstract. — Let K be a local field of characteristic $p > 0$ with perfect residue field and let G be a finite p-group. In this paper we use Saltman's construction of a generic G-extension of rings of characteristic p to construct totally ramified G-extensions L/K that have Galois scaffolds. We specialize this construction to produce G-extensions L/K such that the ring of integers $\mathcal{O}_L$ is free of rank 1 over its associated order $\mathcal{A}_0$, and extensions such that $\mathcal{A}_0$ is a Hopf order in the group ring $K[G]$.

Résumé. — Soit K un corps local de caractéristique $p > 0$ de corps résiduel parfait et soit G un p-groupe fini. Dans cet article nous utilisons la construction de Saltman d'une G-extension générique d'anneaux de caractéristique p pour construire des G-extensions L/K totalement ramifiées qui ont un échafaudage galoisien. Nous spécialisons cette construction pour produire des G-extensions L/K telles que l'anneau d'entiers $\mathcal{O}_L$ soit libre de rang 1 sur son ordre associé $\mathcal{A}_0$, et des extensions telles que $\mathcal{A}_0$ soit un ordre de Hopf dans l'anneau de groupe $K[G]$.

1. Introduction

Let p be prime and let G be a group of order p^n. In [12] Saltman constructed a Galois ring extension S/R with Galois group G, where S and R are polynomial rings in n variables over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Saltman's extension is generic in the sense that every G-extension of commutative rings of characteristic p is induced by S/R. In this paper we use a slightly modified version of Saltman's construction to answer some existence questions regarding G-extensions of local fields of characteristic p.

Let K be a local field of characteristic p and let $u_1 < u_2 < \cdots < u_n$ be positive integers which are relatively prime to p. Maus [10] showed that if

Keywords: generic extensions, ramification, Galois module structure, Galois scaffold, Hopf order.
2020 *Mathematics Subject Classification:* 11S15, 11R33, 14L15, 16T05, 11S23.

$u_i > pu_{i-1}$ for $2 \leqslant i \leqslant n$ then there is a totally ramified C_{p^n}-extension L/K whose upper ramification breaks are $u_1, u_2, \ldots, u_n$. We use generic extensions to generalize Maus's result: given a p-group G and a composition series for G, there exists a constant $M \geqslant 1$ that depends only on G and the composition series, such that if $u_i > Mu_{i-1}$ for $2 \leqslant i \leqslant n$ then there is a totally ramified G-extension L/K whose upper ramification breaks are $u_1, u_2, \ldots, u_n$ (see Corollary 4.6).

Let K be a local field with residue characteristic p and let L/K be a finite totally ramified Galois extension whose Galois group $G = \mathrm{Gal}(L/K)$ is a p-group. A Galois scaffold for L/K is a set of data that facilitates computation of the Galois module structure of the ring of integers $\mathcal{O}_L$ of L and of its ideals [3]. While it seems clear that for most extensions a Galois scaffold cannot be constructed, many of the totally ramified Galois p-extensions L/K for which there is some understanding of the Galois module structure of $\mathcal{O}_L$ do in fact admit a Galois scaffold. In Theorem 5.1 we show that if $\mathrm{char}(K) = p$ then for every p-group G there exist G-extensions with Galois scaffolds. As applications we show that for every p-group G there are G-extensions L/K such that the ring of integers $\mathcal{O}_L$ of L is free of rank 1 over its associated order $\mathfrak{A}_0$ (Corollary 5.7), and there are G-extensions such that $\mathfrak{A}_0$ is a Hopf order (Corollary 5.8). Hence our constructions produce an interesting new family of Hopf orders in the group ring $K[G]$.

Throughout the paper we let K be a local field with perfect residue field; unless otherwise stated, K has characteristic p. Let K^{sep} be a separable closure of K. For each finite subextension L/K of K^{sep}/K let v_L be the valuation on K^{sep} normalized so that $v_L(L^\times) = \mathbb{Z}$ and let $\mathcal{O}_L$ be the ring of integers of L.

The authors thank Cornelius Greither for pointing them to Saltman's work on generic Galois ring extensions.

2. p-filtered groups

In this section we give the definition of p-filtered groups and record some basic facts about these objects.

Definition 2.1. — *A p-filtered group is a pair $(G, \{G_{(i)}\})$ consisting of a group G of order p^n and a composition series*

$$\{1\} = G_{(n)} < G_{(n-1)} < \cdots < G_{(1)} < G_{(0)} = G$$

for G such that $G_{(i)} \trianglelefteq G$ and $|G_{(i)}| = p^{n-i}$ for $0 \leqslant i \leqslant n$.

We often denote the p-filtered group $(G, \{G_{(i)}\})$ simply by G. If G is a p-filtered group then $G/G_{(i)}$ is also a p-filtered group, with subgroups

$$G_{(i)}/G_{(i)} < G_{(i-1)}/G_{(i)} < \cdots < G_{(1)}/G_{(i)} < G_{(0)}/G_{(i)}.$$

Let G be a p-filtered group of order p^n. Define

$$\Sigma_G = \left\{1 \leqslant i \leqslant n : \begin{array}{r}\text{The extension } G/G_{(i)} \text{ of } G/G_{(i-1)} \\ \text{by } G_{(i-1)}/G_{(i)} \text{ is split}\end{array}\right\}.$$

In addition, for $0 \leqslant i \leqslant n$ set $\Sigma_G^i = \{j \in \Sigma_G : j \leqslant i\}$.

For a finite group G we let $\Phi(G)$ denote the Frattini subgroup of G. Thus $\Phi(G)$ is the intersection of the maximal proper subgroups of G. Let G and H be finite groups. We note the following facts, which may be found in [11]:

(1) $\Phi(G \times H) = \Phi(G) \times \Phi(H)$.
(2) If G is a p-group then $\Phi(G)$ is the smallest $N \trianglelefteq G$ such that G/N is an elementary abelian p-group (Burnside's basis theorem).

The rank of the p-group G is defined to be the rank of the elementary abelian p-group $G/\Phi(G)$. It follows that $\mathrm{rank}(G)$ is equal to the cardinality of any minimal generating set for G. We will need the following elementary result:

Proposition 2.2. — *For* $1 \leqslant i \leqslant n$ *we have*

$$\mathrm{rank}(G/G_{(i)}) = \begin{cases}\mathrm{rank}(G/G_{(i-1)}) + 1 & \text{if } i \in \Sigma_G, \\ \mathrm{rank}(G/G_{(i-1)}) & \text{if } i \notin \Sigma_G.\end{cases}$$

Proof. — If $i \in \Sigma_G$ then since $G/G_{(i)}$ is a p-group and $G_{(i-1)}/G_{(i)}$ is cyclic of order p we have $G/G_{(i)} \cong (G/G_{(i-1)}) \times C_p$, and hence

$$(G/G_{(i)})/\Phi(G/G_{(i)}) \cong ((G/G_{(i-1)})/\Phi(G/G_{(i-1)})) \times C_p.$$

Therefore $\mathrm{rank}(G/G_{(i)}) = \mathrm{rank}(G/G_{(i-1)}) + 1$. If $i \notin \Sigma_G$ let A be a subset of G such that $|A| = \mathrm{rank}(G/G_{(i-1)})$ and $\{aG_{(i-1)} : a \in A\}$ generates $G/G_{(i-1)}$. Then $H = \langle aG_{(i)} : a \in A\rangle$ is a subgroup of $G/G_{(i)}$ such that $|H| \geqslant |G/G_{(i-1)}| = p^{i-1}$. If $|H| = p^{i-1}$ then $H \cap (G_{(i-1)}/G_{(i)})$ is trivial. Hence $G/G_{(i)}$ is the product of H and the central subgroup $G_{(i-1)}/G_{(i)}$, which contradicts the assumption $i \notin \Sigma_G$. Therefore $H = G/G_{(i)}$, and hence $\mathrm{rank}(G/G_{(i)}) = \mathrm{rank}(G/G_{(i-1)})$. □

Corollary 2.3. — *For* $1 \leqslant i \leqslant n$ *we have* $\mathrm{rank}(G/G_{(i)}) = |\Sigma_G^i|$. *In particular,* $\mathrm{rank}(G) = |\Sigma_G|$.

3. Generic G-extensions of commutative rings

Let G be a p-group. In this section we describe a version of Saltman's construction of a generic G-extension of commutative rings [12]. The generic G-extension S/R constructed here is somewhat more general than that given in [12], in that we don't require the Frattini subgroup of the p-group G to appear in our filtration of G. Unlike Saltman, who considers specializations of S/R to ring extensions, we only consider field extensions, since this is the case that we need for our applications.

Definition 3.1. — *Let S be a commutative ring with 1, let G be a finite group of automorphisms of S, and set*

$$R = S^G = \{x \in S : \sigma(x) = x \text{ for all } \sigma \in G\}.$$

Say that S/R is a Galois extension with group G if for every maximal ideal $M \subset S$ and every $\sigma \in G$ with $\sigma \neq 1$ there is $s \in S$ with $\sigma(s) - s \notin M$.

See [6, p. 81] for alternative characterizations of Galois extensions of rings. In general, for a ring extension S/R there may exist more than one group G of automorphisms of S such that $R = S^G$ and S/R is Galois with group G. However, if S/R is a Galois extension with group G and S, R are integral domains then by setting $E = \operatorname{Frac}(S)$ and $F = \operatorname{Frac}(R)$ we get a Galois extension of fields E/F such that $\operatorname{Gal}(E/F) \cong G$. In this case G is equal to the group of all R-automorphisms of S, so it makes sense to say that S/R is a Galois extension without specifying a group of automorphisms of S.

If R is a ring of characteristic p then the simplest nontrivial Galois p-extensions of R are Artin–Schreier extensions. Saltman gives some properties of these extensions in Theorem 1.3 of [12]:

Proposition 3.2. — *Let R be a ring of characteristic p, let $c \in R$, and set $S = R[X]/(X^p - X - c)$. Set $v = X + (X^p - X - c)$ and let σ be the unique automorphism of S which fixes R and satisfies $\sigma(v) = v + 1$. Then S/R is a Galois extension with group $\langle\sigma\rangle$.*

We will also use the following fact, which is proved as Corollary 1.3(3) in Chapter III of [6]:

Proposition 3.3. — *Let S/R be a Galois extension of rings with group G and let T be a commutative R-algebra. Then the action of G on $T \otimes_R S$ defined by $\sigma(t \otimes s) = t \otimes \sigma(s)$ makes $T \otimes_R S$ a Galois extension of T.*

Let S be a ring of characteristic p, and let G be a group of automorphisms of S such that $|G| = p^n$ and S is a Galois extension of the subring $R = S^G$ fixed by G. In Lemma 1.1 of [12] it is observed that $H^q(G,S) = 0$ for all $q \geqslant 1$. Let $\widetilde{G}$ be a group of order p^{n+1}, let $\pi : \widetilde{G} \to G$ be an onto homomorphism, and set $H = \ker(\pi)$. Let $u : G \to \widetilde{G}$ be a section of π. Then the map $g : G \times G \to H$ defined by $g(\sigma,\tau) = u(\sigma)u(\tau)u(\sigma\tau)^{-1}$ is a 2-cocycle. Let $\chi : H \to \mathbb{F}_p$ be an isomorphism; then $c(\sigma,\tau) = \chi(g(\sigma,\tau))$ is a 2-cocycle with values in $\mathbb{F}_p \subset S$. Since $H^2(G,S) = 0$ there is a cochain $(s_\sigma)_{\sigma\in G}$ with values in S such that $c(\sigma,\tau) = s_\sigma + \sigma(s_\tau) - s_{\sigma\tau}$ for all $\sigma,\tau \in G$. Let $\wp(X) = X^p - X \in \mathbb{F}_p[X]$ be the Artin–Schreier polynomial. Since $c(\sigma,\tau) \in \mathbb{F}_p$ we have $\wp(s_\sigma)+\sigma(\wp(s_\tau)) = \wp(s_{\sigma\tau})$ for all $\sigma,\tau \in G$. Thus $(\wp(s_\sigma))_{\sigma\in G}$ is a 1-cocycle with values in S. Since $H^1(G,S) = 0$ there is $d \in S$ such that $\wp(s_\sigma) = \sigma(d) - d$ for all $\sigma \in G$.

In Lemma 1.8 of [12], Saltman proved the following facts:

Lemma 3.4. — *Let S/R be a Galois extension with group G, and let $\widetilde{G}$, H, d be as above.*

1. *View $T = S[X]/(X^p - X - d)$ as an extension of S. The group G of automorphisms of S extends to a group of automorphisms of T which is isomorphic to $\widetilde{G}$ and makes T/R a Galois extension.*
2. *Suppose T' is an extension of S such that T'/R is Galois with group $\widetilde{G}$ and S is the fixed ring of H. Then for some $r \in R$ there is an isomorphism of S-algebras $T' \cong S[X]/(X^p - X - d - r)$.*
3. *If S has no nontrivial idempotents and the extension $\widetilde{G}$ of G by H is not split then $d \notin \wp(S) + R$.*

Using this lemma, we construct the generic G-extension:

Proposition 3.5. — *Let $(G, \{G_{(i)}\})$ be a p-filtered group of order p^n. Then for $1 \leqslant i \leqslant n$ there are polynomials $D_i \in \mathbb{F}_p[Y_1,\dots,Y_{i-1}]$ with the following properties:*

1. *$D_i = 0$ for $i \in \Sigma_G$, and $D_i \notin \mathbb{F}_p$ for $i \notin \Sigma_G$.*
2. *For $0 \leqslant i \leqslant n$ set $R_i = \mathbb{F}_p[X_1,\dots,X_i]$, and define $S_0, S_1,\dots,S_n$ recursively by $S_0 = \mathbb{F}_p$ and $S_i = S_{i-1}[Y_i,X_i]/(Y_i^p - Y_i - D_i - X_i)$ for $1 \leqslant i \leqslant n$. Then $S_i \cong \mathbb{F}_p[Y_1,\dots,Y_i]$ and S_i/R_i is a Galois extension.*
3. *For $1 \leqslant i \leqslant n$ let $\pi_i : \mathrm{Gal}(S_i/R_i) \to \mathrm{Gal}(S_{i-1}/R_{i-1})$ be the homomorphism induced by restriction. Then there are isomorphisms $\lambda_i : \mathrm{Gal}(S_i/R_i) \to G/G_{(i)}$ such that for $1 \leqslant i \leqslant n$ the following*

diagram commutes:

$$\begin{array}{ccc} \mathrm{Gal}(S_i/R_i) & \xrightarrow{\pi_i} & \mathrm{Gal}(S_{i-1}/R_{i-1}) \\ {\scriptstyle\lambda_i}\downarrow & & \downarrow{\scriptstyle\lambda_{i-1}} \\ G/G_{(i)} & \longrightarrow & G/G_{(i-1)} \end{array}$$

Proof. — Let $1 \leqslant i \leqslant n$ and assume that for $1 \leqslant j < i$ we have constructed D_j, S_j, λ_j satisfying the conditions of the proposition. By Lemma 3.4(1) there is $D_i \in S_{i-1}$ such that $S_{i-1}[Y_i]/(Y_i^p - Y_i - D_i)$ is Galois over R_{i-1}, with Galois group $G/G_{(i)}$. If $i \in \Sigma_G$ then the extension $G/G_{(i)}$ of $G/G_{(i-1)}$ by $G_{(i-1)}/G_{(i)}$ is split, so we may assume $D_i = 0$. On the other hand, if $i \notin \Sigma_G$ then by Lemma 3.4(3) we get $D_i \notin \mathbb{F}_p$. In either case it follows from Proposition 3.3 that $S_{i-1}[Y_i, X_i]/(Y_i^p - Y_i - D_i)$ is Galois over $R_i = R_{i-1}[X_i]$, again with Galois group $G/G_{(i)}$. Since $(\sigma - 1)(D_i + X_i) = (\sigma - 1)(D_i)$ for all

$$\sigma \in \mathrm{Gal}(S_{i-1}[X_i]/R_i) \cong \mathrm{Gal}(S_{i-1}/R_{i-1}),$$

it follows from Lemma 3.4(1) that

$$S_i = S_{i-1}[Y_i, X_i]/(Y_i^p - Y_i - D_i - X_i)$$

is Galois over R_i, and there is an isomorphism $\lambda_i : \mathrm{Gal}(S_i/R_i) \to G/G_{(i)}$ which makes the diagram in (3) commute. □

We now show that S_n/R_n is a generic G-extension, in the sense that if F is a field of characteristic p such that $F/\wp(F)$ is sufficiently large, then all G-extensions E/F are specializations of S_n/R_n.

THEOREM 3.6. — *Let $(G, \{G_{(i)}\})$ be a p-filtered group of order p^n and set $r = \mathrm{rank}(G)$. For $1 \leqslant i \leqslant n$ let $D_i \in \mathbb{F}_p[Y_1, \dots, Y_{i-1}]$ be polynomials satisfying the conditions of Proposition 3.5. Let F be a field of characteristic p such that $\dim_{\mathbb{F}_p}(F/\wp(F)) \geqslant r$.*

(1) *Let $a_1, \dots, a_n$ be elements of F such that $\{a_j + \wp(F) : j \in \Sigma_G\}$ is an $\mathbb{F}_p$-linearly independent subset of $F/\wp(F)$. Define $F_0, F_1, \dots, F_n$ recursively by $F_0 = F$ and $F_i = F_{i-1}(\alpha_i)$ for $1 \leqslant i \leqslant n$, where $\alpha_i \in F^{\mathrm{sep}}$ satisfies $\alpha_i^p - \alpha_i = d_i + a_i$ with*

$$d_i = D_i(\alpha_1, \dots, \alpha_{i-1}).$$

Then for $0 \leqslant i \leqslant n$, F_i/F is a Galois field extension and there is an isomorphism $\mu_i : \mathrm{Gal}(F_i/F) \to G/G_{(i)}$. Furthermore, the *isomorphisms* μ_i *may be chosen so that for* $1 \leqslant i \leqslant n$ *the following diagram commutes:*

$$\begin{array}{ccc} \mathrm{Gal}(F_i/F) & \longrightarrow & \mathrm{Gal}(F_{i-1}/F) \\ \Big\downarrow{\scriptstyle \mu_i} & & \Big\downarrow{\scriptstyle \mu_{i-1}} \\ G/G_{(i)} & \longrightarrow & G/G_{(i-1)}. \end{array} \tag{3.1}$$

(2) *Conversely, let* $F = F_0 \subset F_1 \subset \cdots \subset F_n$ *be a tower of Galois field extensions of* F *such that there is an isomorphism* $\mu : \mathrm{Gal}(F_n/F) \to G$ *with* $\mu(\mathrm{Gal}(F_n/F_i)) = G_{(i)}$ *for* $0 \leqslant i \leqslant n$*. Then there are* $a_j \in F$ *such that* $F_i = F(\alpha_1, \dots, \alpha_i)$ *for* $0 \leqslant i \leqslant n$*, where* α_j *are defined in terms of* a_j *as in* (1)*.*

Proof.

(1). — For $0 \leqslant i \leqslant n$ let S_i/R_i be the ring extension constructed in Proposition 3.5. Define ring homomorphisms $\psi_i : S_i \to F_i$ by $\psi_i(Y_j) = \alpha_j$ for $1 \leqslant j \leqslant i$. Then $\psi_i(X_j) = a_i$ for $1 \leqslant j \leqslant i$, so $\psi_i(R_i) \subset F$. Viewing S_{i-1} as a subring of S_i we get the compatibility conditions $\psi_i|_{S_{i-1}} = \psi_{i-1}$ for $1 \leqslant i \leqslant n$. We use induction on i. The base case $i = 0$ is trivial. Let $1 \leqslant i \leqslant n$ and assume that the statement holds for $i - 1$. We claim that $d_i + a_i \notin \wp(F_{i-1})$. By the inductive hypothesis F_{i-1}/F is Galois, with $\mathrm{Gal}(F_{i-1}/F) \cong G/G_{(i-1)}$. If $i \notin \Sigma_G$ then $G/G_{(i)}$ is a nonsplit extension of $G/G_{(i-1)}$ by $G_{(i-1)}/G_{(i)}$, so the claim follows from Lemma 3.4 (3). Suppose $i \in \Sigma_G$. By Corollary 2.3 we have $\mathrm{rank}(\mathrm{Gal}(F_{i-1}/F)) = |\Sigma_G^{i-1}|$. Since $\{a_j + \wp(F) : j \in \Sigma_G^i\}$ is an $\mathbb{F}_p$-linearly independent subset of $F/\wp(F)$, F_i/F contains an elementary abelian subextension of rank $|\Sigma_G^i| = |\Sigma_G^{i-1}| + 1$. Hence

$$\mathrm{rank}(\mathrm{Gal}(F_i/F)) > \mathrm{rank}(\mathrm{Gal}(F_{i-1}/F)).$$

It follows that $F_i \neq F_{i-1}$, so $d_i + a_i = a_i \notin \wp(F_{i-1})$. In both cases we get $[F_i : F_{i-1}] = p$, and hence $[F_i : F] = p^i$. The map $\psi_i : S_i \to F_i$ induces an onto homomorphism $F \otimes_{R_i} S_i \to F_i$. Since S_i is a free R_i-module of rank p^i, this map is an isomorphism. Hence by Proposition 3.3 we see that F_i/F is a Galois extension, with $\mathrm{Gal}(F_i/F) \cong \mathrm{Gal}(S_i/R_i)$. Therefore by Proposition 3.5 (3) there is an isomorphism $\mu_i : \mathrm{Gal}(F_i/F) \to G/G_{(i)}$ which makes the diagram (3.1) commute.

(2). — We use induction on i. Note that for $0 \leqslant i \leqslant n$, μ induces an isomorphism $\mu_i : \mathrm{Gal}(F_i/F) \to G/G_{(i)}$. Suppose we have $a_1, \dots, a_{i-1} \in F$ such that $F_{i-1} = F(\alpha_1, \dots, \alpha_{i-1})$. Set $d_i = D_i(\alpha_1, \dots, \alpha_{i-1})$. If $i \in \Sigma_G$ then $G/G_{(i)} \cong (G/G_{(i-1)}) \times C_p$ and $d_i = 0$. Hence there is $a_i \in F$ such that $F_i = F_{i-1}(\alpha_i)$, with $\alpha_i^p - \alpha_i = a_i = d_i + a_i$. Suppose $i \notin \Sigma_G$. Then by Lemma 3.4 (2) there is $a_i \in F$ such that $F_i \cong F_{i-1}[Y]/(Y^p - Y - d_i - a_i)$. Hence $F_i = F(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i)$, with α_i a root of $Y^p - Y - d_i - a_i$. □

Remark 3.7. — Saltman [12, p. 308] states that his results "can be viewed as a generalization of the theory of Witt vectors". In particular, he proves the existence of polynomials D_i which satisfy the conditions of Proposition 3.5 and Theorem 3.6. These polynomials depend only on the p-filtered group G, and not on the base field F. In the case where G is a cyclic p-group one can use Witt addition polynomials to produce D_i satisfying Saltman's conditions.

4. Ramification breaks in G-extensions

Let K be a local field of characteristic p with perfect residue field and let $(G, \{G_{(i)}\})$ be a p-filtered group of order p^n. Let $u_1 < u_2 < \cdots < u_n$ be positive integers such that $p \nmid u_i$ for $1 \leqslant i \leqslant n$. We wish to show that if this sequence grows quickly enough then there is a totally ramified G-extension L/K such that every ramification subgroup of $\mathrm{Gal}(L/K)$ is equal to $G_{(i)}$ for some i and $u_1, u_2, \ldots, u_n$ are the upper ramification breaks of L/K.

We begin by recalling some basic facts about higher ramification theory; see Chapter IV of [13] for more information on this topic. Let K be a local field and let L/K be a Galois extension. Set $G = \mathrm{Gal}(L/K)$ and let G_0 be the inertia subgroup of G. Let π_L be a uniformizer for L. We define the ramification number of $\sigma \in G$ to be $i(\sigma) = v_L(\sigma(\pi_L) - \pi_L) - 1$ if $\sigma \in G_0$, and $i(\sigma) = -1$ if $\sigma \notin G_0$. (Beware that $i_G(\sigma)$ from [13] is not the same as $i(\sigma)$: instead we have $i_G(\sigma) = i(\sigma) + 1$.) Then $i(\mathrm{id}_L) = +\infty$, and $i(\sigma)$ is a nonnegative integer for $\sigma \in G_0 \smallsetminus \{\mathrm{id}_L\}$. For $t \in \mathbb{R}$ with $t \geqslant -1$ define the tth lower ramification subgroup of G to be $G_t = \{\sigma \in G : i(\sigma) \geqslant t\}$. Say $b \geqslant -1$ is a lower ramification break of L/K if $G_b \neq G_{b+\epsilon}$ for all real $\epsilon > 0$. Thus b is a lower ramification break of L/K if and only if $b = i(\sigma)$ for some $\sigma \in G$ with $\sigma \neq \mathrm{id}_L$.

We define the Hasse–Herbrand function $\phi_{L/K} : [-1, \infty) \to [-1, \infty)$ by

$$\phi_{L/K}(x) = \int_0^x \frac{\mathrm{d}t}{|G_0 : G_t|}.$$

Then $\phi_{L/K}$ is continuous on $[-1, \infty)$ and differentiable on $(-1, \infty)$ except at the lower ramification breaks. Since $\phi_{L/K}$ is one-to-one and onto it has an inverse $\psi_{L/K} : [-1, \infty) \to [-1, \infty)$. Define the upper ramification subgroups of G by setting $G^x = G_{\psi_{L/K}(x)}$ for $x \geqslant -1$. Say that $u \geqslant -1$

is an upper ramification break of L/K if $G^u \neq G^{u+\epsilon}$ for all $\epsilon > 0$. Then $\psi_{L/K}$ is differentiable except at the upper ramification breaks of L/K, and u is an upper ramification break of L/K if and only if $\psi_{L/K}(u)$ is a lower ramification break. Let M/K be a Galois subextension of L/K and set $H = \mathrm{Gal}(L/M)$. Then by Herbrand's theorem [13, IV §3] we get $\phi_{L/K} = \phi_{M/K} \circ \phi_{L/M}$ and $\psi_{L/K} = \psi_{L/M} \circ \psi_{M/K}$. Furthermore, we have $(G/H)^x = G^x H/H$ for all $x \geqslant -1$. It follows that if u is an upper break of M/K then u is also an upper break of L/K.

Lemma 4.1. — *Let L/K be a finite Galois extension and let E/K be a ramified C_p-extension such that $E \not\subset L$. Assume that the unique (upper and lower) ramification break v of E/K is not an upper ramification break of L/K. Then the ramification break of the C_p-extension LE/L is $\psi_{L/K}(v)$.*

Proof. — Since $\psi_{LE/E} \circ \psi_{E/K} = \psi_{LE/L} \circ \psi_{L/K}$ is not differentiable at v, but $\psi_{L/K}$ is differentiable at v, we deduce that $\psi_{LE/L}$ is not differentiable at $\psi_{L/K}(v)$. Hence $\psi_{L/K}(v)$ is the unique upper break of LE/L. □

We will mainly consider totally ramified Galois extensions L/K of degree p^n with the property that for every lower ramification break b we have $|G_b : G_{b+\epsilon}| = p$. In this case there are n lower breaks $b_1 < b_2 < \cdots < b_n$ and n upper breaks $u_1 < u_2 < \cdots < u_n$. The breaks are related by the formulas $u_1 = b_1$ and $u_{i+1} - u_i = p^{-i}(b_{i+1} - b_i)$ for $1 \leqslant i \leqslant n-1$. As a result we get the following inequalities:

Lemma 4.2. — *Let $1 \leqslant i \leqslant j \leqslant n$. Then:*

(1) $b_j - b_i \leqslant p^{j-1}(u_j - u_i)$.
(2) $b_j \leqslant p^{j-1}u_j < p^j u_j$.

Proof.

(1). — If $i = j$ the claim is clear. If $i < j$ then

$$\begin{aligned} b_j - b_i &= \sum_{h=i}^{j-1}(b_{h+1} - b_h) = \sum_{h=i}^{j-1} p^h(u_{h+1} - u_h) \\ &= p^{j-1}u_j - p^i u_i + \sum_{h=i+1}^{j-1}(p^{h-1} - p^h)u_h \\ &\leqslant p^{j-1}u_j - p^i u_i + \sum_{h=i+1}^{j-1}(p^{h-1} - p^h)u_i \\ &= p^{j-1}(u_j - u_i). \end{aligned}$$

(2). — This follows from (1) by letting $i = 1$. □

The following well-known fact will often be used without comment (cf. Proposition 2.5 in [8, III]).

Lemma 4.3. — *Let K be a local field of characteristic p and let L/K be a ramified C_p-extension. Let $s \in K$ be such that L is generated over K by a root α of $X^p - X - s$. Then the following hold:*

1. *The ramification break b of L/K satisfies $b \leqslant -v_K(s)$, with equality if $p \nmid v_K(s)$.*
2. *If $b < -v_K(s)$ then there is $t \in K$ such that $v_K(s - \wp(t)) = -b$.*

Let G be a p-filtered group of order p^n, let $a_1, \ldots, a_n$ be elements of K which satisfy the hypotheses of Theorem 3.6 (1), and let K_n/K be the associated G-extension. In some cases we can compute the ramification data of K_n/K in terms of the valuations $v_K(a_1), \ldots, v_K(a_n)$:

Theorem 4.4. — *Let $(G, \{G_{(i)}\})$ be a p-filtered group of order p^n, and for $1 \leqslant i \leqslant n$ let $D_i \in \mathbb{F}_p[Y_1, \ldots, Y_{i-1}]$ be the polynomials constructed in Proposition 3.5. Let K be a local field of characteristic p with perfect residue field. Let $u_1 < u_2 < \cdots < u_n$ be positive integers such that $p \nmid u_i$, and let $a_1, \ldots, a_n$ be elements of K such that $v_K(a_i) = -u_i$ for $1 \leqslant i \leqslant n$. As in Theorem 3.6 we define $K_0, K_1, \ldots, K_n$ recursively by $K_0 = K$ and $K_i = K_{i-1}(\alpha_i)$ for $1 \leqslant i \leqslant n$, where α_i satisfies $\alpha_i^p - \alpha_i = d_i + a_i$ with $d_i = D_i(\alpha_1, \ldots, \alpha_{i-1})$. Define $b_1 < b_2 < \cdots < b_n$ recursively by $b_1 = u_1$ and $b_{i+1} - b_i = p^i(u_{i+1} - u_i)$ for $1 \leqslant i \leqslant n-1$. If the u_i are chosen so that $b_i > -p^{i-1} v_K(d_i)$ for all $i \notin \Sigma_G$ then:*

1. *K_n/K is Galois, and there is an isomorphism $\mu : \mathrm{Gal}(K_n/K) \to G$ such that $\mu(\mathrm{Gal}(K_n/K_i)) = G_{(i)}$ for $0 \leqslant i \leqslant n$.*
2. *K_n/K has upper ramification breaks $u_1, u_2, \ldots, u_n$ and lower ramification breaks $b_1, b_2, \ldots, b_n$. In addition, we have $v_K(\alpha_i) = -p^{-1} u_i$ for $0 \leqslant i \leqslant n$.*
3. *The ramification subgroups of $\mathrm{Gal}(K_n/K)$ are the subgroups of the form $\mathrm{Gal}(K_n/K_i)$ for $0 \leqslant i \leqslant n$.*

Proof. — Since the elements of $\{u_i : i \in \Sigma_G\}$ are distinct and relatively prime to p, the set $\{a_i + \wp(K) : i \in \Sigma_G\}$ is linearly independent over $\mathbb{F}_p$. Let $K_0 \subset K_1 \subset \cdots \subset K_n$ be the extensions associated to $a_1, \ldots, a_n$. Then by Theorem 3.6 (1) K_n/K is Galois, and there is an isomorphism $\mu : \mathrm{Gal}(K_n/K) \to G$ which satisfies condition (1). We use induction on i to show that $v_K(\alpha_i) = -p^{-1} u_i$ and K_i/K has upper ramification breaks $u_1, \ldots, u_i$. It then follows that $|G^{u_i}| = p^{n-i+1}$, $|G^{u_i+\epsilon}| = p^{n-i}$, and K_i/K has lower ramification breaks $b_1, \ldots, b_i$. In addition, since $\mathrm{Gal}(K_i/K) \cong$

$G/G_{(i)}$ we get

$$G_{(i)}/G_{(i)} = (G/G_{(i)})^{u_i+\epsilon} = G^{u_i+\epsilon}G_{(i)}/G_{(i)},$$

and hence $G^{u_i+\epsilon} \leqslant G_{(i)}$. Since $|G^{u_i+\epsilon}| = |G_{(i)}| = p^{n-i}$ it follows that $G_{(i)} = G^{u_i+\epsilon}$ is a ramification subgroup of $G \cong \mathrm{Gal}(K_n/K)$ for $1 \leqslant i \leqslant n$. Since $\mu(\mathrm{Gal}(K_n/K_i)) = G_{(i)}$, the $n+1$ distinct ramification subgroups of $\mathrm{Gal}(K_n/K)$ are precisely the subgroups $\mathrm{Gal}(K_n/K_i)$ for $0 \leqslant i \leqslant n$.

We have $D_1 = 0$, so the upper ramification break of K_1/K is $-v_K(a_1) = u_1$, and $v_K(\alpha_1) = p^{-1}v_K(a_1) = -p^{-1}u_1$. Let $2 \leqslant i \leqslant n$ and assume the claim holds for $i-1$. If $i \in \Sigma_G$ then $D_i = 0$ and $K(\alpha_i)/K$ is a C_p-extension with upper ramification break u_i. Since $K_i \supset K(\alpha_i)$ it follows that u_i is an upper ramification break of K_i/K. Hence by induction K_i/K has upper ramification breaks $u_1, \dots, u_{i-1}, u_i$. We also get $v_K(\alpha_i) = p^{-1}v_K(a_i) = -p^{-1}u_i$.

Suppose $i \notin \Sigma_G$, and set $d_i = D_i(\alpha_1, \dots, \alpha_{i-1})$ as in Theorem 3.6 (1). By the lower bound on b_i and Lemma 4.2 (2) we get

$$v_K(d_i) > -p^{1-i}b_i \geqslant -u_i = v_K(a_i).$$

It follows that $v_K(d_i + a_i) = v_K(a_i) = -u_i$, and hence that $v_K(\alpha_i) = -p^{-1}u_i$. Since $\wp(\alpha_i) = d_i + a_i$ we can write $\alpha_i = \alpha_i' + \alpha_i''$, with $\wp(\alpha_i') = d_i$ and $\wp(\alpha_i'') = a_i$. Let $K_i' = K_{i-1}(\alpha_i')$ and $K_i'' = K_{i-1}(\alpha_i'')$. We wish to determine the ramification breaks for the C_p-extensions K_i'/K_{i-1} and K_i''/K_{i-1}.

First consider K_i'/K_i. By Theorem 3.6 (1) we have $[K_i' : K] = p^i$. Thus $K_i' \neq K_{i-1}$ and K_i'/K_{i-1} is indeed a C_p-extension. Let b_i' be the ramification break of K_i'/K_{i-1}. Then by Lemma 4.3 (1) and the lower bound on b_i we get $b_i' \leqslant -p^{i-1}v_K(d_i) < b_i$. By Lemma 4.3 (2) there is $\ell' \in K_{i-1}$ such that $v_{K_{i-1}}(d_i - \wp(\ell')) = -b_i' > -b_i$. Now consider K_i''/K_i. Since $a_i \in K$, $K(\alpha_i'')/K$ is a C_p-extension with ramification break $-v_K(a_i) = u_i$. By Lemma 4.1 the ramification break of K_i''/K_{i-1} is

$$\psi_{K_{i-1}/K}(u_i) = \psi_{K_{i-1}/K}(u_{i-1}) + p^{i-1}(u_i - u_{i-1}) = b_{i-1} + (b_i - b_{i-1}) = b_i.$$

Hence by Lemma 4.3 (2) there is $\ell'' \in K_{i-1}$ such that $v_{K_{i-1}}(a_i - \wp(\ell'')) = -b_i$.

We have shown that $K_i'K_i''/K_{i-1}$ is a $(C_p \times C_p)$-extension with upper breaks $b_i' < b_i$. There are $p+1$ C_p-subextensions of $K_i'K_i''/K_{i-1}$, namely K_i'' and $K_{i-1}(\alpha_i' + s\alpha_i'')$ for $s \in \mathbb{F}_p$. We are interested in the ramification break for K_i/K_{i-1}, which is the $s = 1$ case. Note that $K_i = K_{i-1}(\alpha_i - \ell' - \ell'')$, with

$$\wp(\alpha_i - \ell' - \ell'') = (d_i - \wp(\ell')) + (a_i - \wp(\ell'')).$$

Since $v_{K_{i-1}}(d_i - \wp(\ell')) > v_{K_{i-1}}(a_i - \wp(\ell''))$ we get

$$v_{K_{i-1}}((d_i - \wp(\ell')) + (a_i - \wp(\ell''))) = v_{K_{k-1}}(a_i - \wp(\ell'')) = -b_i.$$

Since $p \nmid b_i$, it follows that the ramification break of K_i/K_{i-1} is b_i. Therefore b_i is a lower ramification break of K_i/K, so $\phi_{K_i/K}(b_i) = u_i$ is an upper ramification break of K_i/K. Using induction we deduce that K_i/K has upper ramification breaks $u_1, \ldots, u_{i-1}, u_i$. □

Theorem 4.4 allows us to construct G-extensions which have certain specified sequences of upper ramification breaks:

Corollary 4.5. — *Let $(G, \{G_{(i)}\})$, K, a_i, D_i, d_i, K_i, u_i, b_i be as in Theorem 4.4, and for $i \notin \Sigma_G$ let l_i denote the total degree of D_i. If $b_i > p^{i-2} l_i u_{i-1}$ for all $i \notin \Sigma_G$ then the conclusions of Theorem 4.4 hold for $K_0, K_1, \ldots, K_n$.*

Proof. — We prove by induction that $v_K(d_i + a_i) = v_K(a_i) = -u_i$, $v_K(\alpha_i) = -p^{-1}u_i$, and $b_i > -p^{i-1}v_K(d_i)$ for $1 \leqslant i \leqslant n$. This is clear for $i \in \Sigma_G$ since $d_i = 0$ in this case. Let $2 \leqslant i \leqslant n$ with $i \notin \Sigma_G$ and assume the claim holds for $1 \leqslant h < i$. Then $v_K(\alpha_h) = -p^{-1}u_h \geqslant -p^{-1}u_{i-1}$ for $1 \leqslant h < i$. Using the assumption $b_i > p^{i-2} l_i u_{i-1}$ we get $v_K(d_i) \geqslant -p^{-1} l_i u_{i-1} > -p^{1-i} b_i$, and hence $b_i > -p^{i-1} v_K(d_i)$. Lemma 4.2 (2) then gives $v_K(d_i) > -p^{1-i} b_i \geqslant -u_i = v_K(a_i)$. It follows that $v_K(d_i + a_i) = v_K(a_i)$, and hence that $v_K(\alpha_i) = -p^{-1}u_i$. Since we have shown that the hypotheses of Theorem 4.4 hold, the conclusions of the theorem hold as well. □

Let K be a local field of characteristic p. Maus [10] showed that for every sequence of positive integers $u_1, \ldots, u_n$ such that $p \nmid u_i$ for $1 \leqslant i \leqslant n$ and $u_{i+1} > pu_i$ for $1 \leqslant i \leqslant n-1$ there exists a totally ramified C_{p^n}-extension L/K whose sequence of upper ramification breaks is $u_1, \ldots, u_n$. The following corollary shows that a similar result holds with C_{p^n} replaced by an arbitrary p-filtered group.

Corollary 4.6. — *Let $(G, \{G_{(i)}\})$ be a p-filtered group of order p^n. Then there is $M \geqslant 1$, depending only on $(G, \{G_{(i)}\})$, with the following property: let K be a local field of characteristic p and let $u_1, \ldots, u_n$ be a sequence of positive integers such that $p \nmid u_i$ for $1 \leqslant i \leqslant n$ and $u_{i+1} > Mu_i$ for $1 \leqslant i \leqslant n-1$. Then there exists a totally ramified Galois extension L/K such that:*

(1) $\mathrm{Gal}(L/K) \cong G$.
(2) *The upper ramification breaks of L/K are $u_1, \ldots, u_n$.*

(3) *The ramification subgroups of* $\mathrm{Gal}(L/K) \cong G$ *are the groups* $G_{(i)}$ *in the filtration of* G*.*

Proof. — If $\Sigma_G = \{1, 2, \ldots, n\}$ set $M = 1$. Otherwise, we use the notation of Corollary 4.5 to define

$$M = \max\{p^{i-2} l_i : 1 \leqslant i \leqslant n,\ i \notin \Sigma_G\}.$$

Let $u_1, \ldots, u_n$ be positive integers such that $p \nmid u_i$ for $1 \leqslant i \leqslant n$ and $u_i > M u_{i-1}$ for $2 \leqslant i \leqslant n$. Then $u_i > u_{i-1}$, and for $i \notin \Sigma_G$ we get $b_i \geqslant u_i > p^{i-2} l_i u_{i-1}$. Therefore by Corollary 4.5 there is an extension L/K with the specified properties. □

It would be interesting to know whether Corollary 4.6 holds with $M = p$.

5. Scaffolds, Galois module structure, and Hopf orders

Let $(G, \{G_{(i)}\})$ be a p-filtered group and let K be a local field of characteristic p with perfect residue field. A Galois scaffold $(\{\Psi_i\}, \{\lambda_t\})$ for a G-extension K_n/K consists of $\Psi_i \in K[G]$ for $1 \leqslant i \leqslant n$ and $\lambda_t \in K_n$ for all $t \in \mathbb{Z}$. These are chosen so that $v_{K_n}(\lambda_t) = t$ and $\Psi_i(\lambda_t)$ can be computed up to a certain "precision" $\mathfrak{c} \geqslant 1$. Note that if a Galois scaffold $(\{\Psi_i\}, \{\lambda_t\})$ for K_n/K has precision $\mathfrak{c}$, and $1 \leqslant \mathfrak{c}' \leqslant \mathfrak{c}$, then it is also correct to say that $(\{\Psi_i\}, \{\lambda_t\})$ has precision $\mathfrak{c}'$. The existence of a Galois scaffold for K_n/K facilitates the computation of the Galois module structure of $\mathcal{O}_{K_n}$ and its ideals. For precise definitions and some basic properties of Galois scaffolds see [3].

In this section we show how the hypotheses of Theorem 4.4 can be strengthened to guarantee that the G-extension K_n/K has a Galois scaffold. This leads to sufficient conditions for $\mathcal{O}_{K_n}$ to be free over its associated order (Corollary 5.7), and sufficient conditions for the associated order of $\mathcal{O}_{K_n}$ to be a Hopf order (Corollary 5.8).

Theorem 5.1. — *Let* $(G, \{G_{(i)}\})$ *be a* p*-filtered group of order* p^n *and let* $D_1, \ldots, D_n$ *be the polynomials associated to* $(G, \{G_{(i)}\})$ *by Proposition 3.5. Let* K *be a local field of characteristic* p *with perfect residue field and let* $a \in K^\times$ *with* $p \nmid v_K(a)$*. For* $1 \leqslant i \leqslant n$ *let* $\omega_i \in K^\times$ *and set* $a_i = a\omega_i^{p^{n-1}}$*. Set* $u_i = -v_K(a_i)$ *and assume that* $0 < u_1 < \cdots < u_n$*. As in Theorem 3.6 we define* $K_0, K_1, \ldots, K_n$ *recursively by* $K_0 = K$ *and* $K_i = K_{i-1}(\alpha_i)$ *for* $1 \leqslant i \leqslant n$*, where* α_i *satisfies* $\alpha_i^p - \alpha_i = d_i + a_i$ *with*

$d_i = D_i(\alpha_1, \ldots, \alpha_{i-1})$. Define $b_1 < b_2 < \cdots < b_n$ recursively by $b_1 = u_1$ and $b_{i+1} - b_i = p^i(u_{i+1} - u_i)$ for $1 \leqslant i \leqslant n-1$. If

$$b_i > -p^{n-1}v_K(d_i) - p^{n-i}b_{i-1} + p^{n-1}u_{i-1}, \tag{5.1}$$

$$b_i > p^{n-1}u_{i-1}, \tag{5.2}$$

for all $2 \leqslant i \leqslant n$ with $i \notin \Sigma_G$ then the extensions $K_0 \subset K_1 \subset \cdots \subset K_n$ satisfy conclusions (1)–(3) of Theorem 4.4, plus the additional condition:

(4) *K_n/K admits a Galois scaffold with precision*

$$\mathfrak{c} = \min \left\{ \begin{matrix} p^{n-1}v_K(d_i) + p^{n-i}b_{i-1} + b_i - p^{n-1}u_{i-1},\ b_i - p^{n-1}u_{i-1} \\ \hfill : 2 \leqslant i \leqslant n,\ i \notin \Sigma_G \end{matrix} \right\}.$$

Furthermore, we have $\Psi_i \in K[G_{(n-i)}]$ for $1 \leqslant i \leqslant n$.

Remark 5.2. — The precision $\mathfrak{c}$ given in the theorem is equal to the minimum of the gaps in the inequalities (5.1) and (5.2).

Remark 5.3. — If $\Sigma_G = \{1, 2, \ldots, n\}$ then G is an elementary abelian p-group and our scaffold has infinite precision (cf. the characteristic-p case of Theorem 3.5 in [4]).

Proof of Theorem 5.1. — It follows from (5.1) and Lemma 4.2 (2) that for $i \notin \Sigma_G$ we have

$$b_i > -p^{n-1}v_K(d_i) - p^{n-i}b_{i-1} + p^{n-1}u_{i-1} > -p^{n-1}v_K(d_i). \tag{5.3}$$

Hence the extensions $K_0 \subset K_1 \subset \cdots \subset K_n$ satisfy the conclusions of Theorem 4.4. To prove (4) we use [4], which gives a systematic method for constructing Galois scaffolds. By our assumptions on a_i we have $p \nmid u_1$ and $u_i \equiv u_j \pmod{p^{n-1}}$ for $1 \leqslant i, j \leqslant n$. Thus $p \nmid b_1$ and $b_i \equiv b_j \pmod{p^n}$, so Assumptions 2.2 and 2.6 of [4] are satisfied. To apply Theorem 2.10 of [4] we must choose $\sigma_i \in \mathrm{Gal}(K_n/K_{i-1})$ as described in Choice 2.1 of [4], and $\mathbf{X}_j \in K_j$ as described in Choice 2.3 of [4].

As in [7], we begin by constructing $\mathbf{Y}_j \in K_j$ such that $v_{K_j}(\mathbf{Y}_j) \equiv -b_j \pmod{p^j}$. We then obtain $\mathbf{X}_j$ satisfying Choice 2.3 of [4] by multiplying $\mathbf{Y}_j$ by an appropriate element of $K^\times$. Set

$$\vec{\omega} = \begin{bmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_j \end{bmatrix} \in K^j \quad \text{and} \quad \vec{\alpha} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_j \end{bmatrix} \in (K^{\mathrm{sep}})^j.$$

Let $\phi : (K^{\mathrm{sep}})^j \to (K^{\mathrm{sep}})^j$ be the map induced by the p-Frobenius on K^{sep} and set

$$\mathbf{Y}_j = \begin{vmatrix} \alpha_1 & \omega_1^{p^{n-j}} & \cdots & \omega_1^{p^{n-2}} \\ \alpha_2 & \omega_2^{p^{n-j}} & \cdots & \omega_2^{p^{n-2}} \\ \vdots & \vdots & & \vdots \\ \alpha_j & \omega_j^{p^{n-j}} & \cdots & \omega_j^{p^{n-2}} \end{vmatrix} = \det[\vec{\alpha}, \phi^{n-j}(\vec{\omega}), \phi^{n-j+1}(\vec{\omega}), \dots, \phi^{n-2}(\vec{\omega})]. \tag{5.4}$$

For $1 \leqslant i \leqslant j$ we have $\alpha_i \in K_j$ and $\omega_i \in K$. Therefore $\mathbf{Y}_j \in K_j$.

For $1 \leqslant i \leqslant j$ set $m_i = -v_K(\omega_i)$. As in the proof of Proposition 1 of [7], we expand in cofactors along the first column to get

$$\mathbf{Y}_j = t_{1j}\alpha_1 + t_{2j}\alpha_2 + \cdots + t_{jj}\alpha_j, \tag{5.5}$$

with $t_{ij} \in K$. Since $m_1 < \cdots < m_j$, the t_{ij} satisfy

$$\begin{aligned} &v_K(t_{ij}) \\ &= v_K\left(\omega_1^{p^{n-j}}\omega_2^{p^{n-j+1}} \cdots \omega_{i-1}^{p^{n-j+i-2}}\omega_{i+1}^{p^{n-j+i-1}} \cdots \omega_j^{p^{n-2}}\right) \\ &= -p^{n-j}(m_1 + pm_2 + \cdots + p^{i-2}m_{i-1} + p^{i-1}m_{i+1} + \cdots + p^{j-2}m_j). \end{aligned} \tag{5.6}$$

It follows that for $2 \leqslant i \leqslant j$ we have

$$\begin{aligned} v_K(t_{ij}) - v_K(t_{i-1,j}) &= -p^{n-j}(p^{i-2}m_{i-1} - p^{i-2}m_i) \\ &= p^{i-j-1}(p^{n-1}m_i - p^{n-1}m_{i-1}) \\ &= p^{i-j-1}(u_i - u_{i-1}) \\ &= p^{-j}(b_i - b_{i-1}). \end{aligned}$$

Hence $v_K(t_{ij}) - v_K(t_{hj})$ is a telescoping sum for $1 \leqslant h \leqslant i \leqslant j$. Therefore we get

$$\begin{aligned} v_K(t_{ij}) - v_K(t_{hj}) &= p^{-j}(b_i - b_h), \\ v_K(t_{ij}^{p^j}) - v_K(t_{hj}^{p^j}) &= b_i - b_h. \end{aligned} \tag{5.7}$$

We claim that for $0 \leqslant i \leqslant j-1$ we have

$$\phi^i(\mathbf{Y}_j) = \det[\vec{\alpha} + \vec{d} + \cdots + \phi^{i-1}(\vec{d}), \phi^{n-j+i}(\vec{\omega}), \dots, \phi^{n-2+i}(\vec{\omega})]. \tag{5.8}$$

The case $i=0$ is given by (5.4). Let $0 \leqslant i \leqslant j-2$ and assume that (5.8) holds for i. Then

$$\begin{aligned}\phi^{i+1}(\mathbf{Y}_j) &= \phi(\det[\vec{\alpha}+\vec{d}+\cdots+\phi^{i-1}(\vec{d}),\phi^{n-j+i}(\vec{\omega}),\ldots,\phi^{n-2+i}(\vec{\omega})]) \\ &= \det[\phi(\vec{\alpha})+\phi(\vec{d})+\cdots+\phi^{i}(\vec{d}),\phi^{n-j+i+1}(\vec{\omega}),\ldots,\phi^{n-1+i}(\vec{\omega})] \\ &= \det[\vec{\alpha}+a\phi^{n-1}(\vec{\omega})+\vec{d}+\phi(\vec{d})+\cdots+\phi^{i}(\vec{d}), \\ &\qquad\qquad \phi^{n-j+i+1}(\vec{\omega}),\ldots,\phi^{n-1+i}(\vec{\omega})].\end{aligned}$$

Since $n-j+i+1 \leqslant n-1 \leqslant n-1+i$ it follows that

$$\phi^{i+1}(\mathbf{Y}_j) = \det[\vec{\alpha}+\vec{d}+\phi(\vec{d})+\cdots+\phi^{i}(\vec{d}),\phi^{n-j+i+1}(\vec{\omega}),\ldots,\phi^{n-1+i}(\vec{\omega})].$$

Hence (5.8) holds with i replaced by $i+1$.

It follows by induction that (5.8) holds for $i=j-1$. Therefore we have

$$\begin{aligned}\phi^{j}(\mathbf{Y}_j) &= \phi(\det[\vec{\alpha}+\vec{d}+\cdots+\phi^{j-2}(\vec{d}),\phi^{n-1}(\vec{\omega}),\ldots,\phi^{n+j-3}(\vec{\omega})]) \\ &= \det[\phi(\vec{\alpha})+\phi(\vec{d})+\cdots+\phi^{j-1}(\vec{d}),\phi^{n}(\vec{\omega}),\ldots,\phi^{n+j-2}(\vec{\omega})] \\ &= \det[\vec{\alpha}+a\phi^{n-1}(\vec{\omega})+\vec{d}+\phi(\vec{d})+\cdots+\phi^{j-1}(\vec{d}), \\ &\qquad\qquad \phi^{n}(\vec{\omega}),\ldots,\phi^{n+j-2}(\vec{\omega})].\end{aligned} \tag{5.9}$$

The $(i,1)$ cofactor of (5.9) is $t_{ij}^{p^j}$, where t_{ij} is the $(i,1)$ cofactor of (5.4). Since $d_1=0$ this gives

$$\mathbf{Y}_j^{p^j} = t_{1j}^{p^j}(\alpha_1+a\omega_1^{p^{n-1}}) + \sum_{i=2}^{j} t_{ij}^{p^j}\left(\alpha_i + a\omega_i^{p^{n-1}} + \sum_{h=0}^{j-1} d_i^{p^h}\right). \tag{5.10}$$

Using (5.6) we get

$$\begin{aligned}v_K(t_{1j}^{p^j}a\omega_1^{p^{n-1}}) &= v_K(a\omega_1^{p^{n-1}}) + p^j v_K(t_{1j}) \\ &= -b_1 - p^n m_2 - p^{n+1}m_3 - \cdots - p^{n+j-2}m_j.\end{aligned}$$

We claim that $v_K(\mathbf{Y}_j^{p^j}) = v_K(t_{1j}^{p^j}a\omega_1^{p^{n-1}})$. To prove this it suffices to show that the other terms in (5.10) all have K-valuation greater than $v_K(t_{1j}^{p^j}a\omega_1^{p^{n-1}})$.

Since $v_K(\alpha_i) = p^{-1}v_K(a\omega_i^{p^{n-1}}) < 0$ we have $v_K(\alpha_i) > v_K(a\omega_i^{p^{n-1}})$ for $1 \leqslant i \leqslant j$. Therefore that it suffices to prove that

$$v_K(t_{1j}^{p^j}a\omega_1^{p^{n-1}}) < v_K(t_{ij}^{p^j}a\omega_i^{p^{n-1}}) \quad (2 \leqslant i \leqslant j), \tag{5.11}$$

$$v_K(t_{1j}^{p^j}a\omega_1^{p^{n-1}}) < v_K(t_{ij}^{p^j}d_i^{p^h}) \qquad (2 \leqslant i \leqslant j,\ 0 \leqslant h \leqslant j-1). \tag{5.12}$$

We first observe that (5.11) follows from (5.7):

$$\begin{aligned} v_K(t_{ij}^{p^j} a\omega_i^{p^{n-1}}) - v_K(t_{1j}^{p^j} a\omega_1^{p^{n-1}}) &= (v_K(t_{ij}^{p^j}) - v_K(t_{1j}^{p^j})) \\ &\quad + (v_K(a\omega_i^{p^{n-1}}) - v_K(a\omega_1^{p^{n-1}})) \\ &= (b_i - b_1) + (-u_i + u_1) \\ &= b_i - u_i > 0. \end{aligned}$$

We now prove (5.12). By (5.3) we have $b_i > -p^{n-1}v_K(d_i)$. Since $h \leqslant n-1$ it follows that $b_i > -p^h v_K(d_i)$. Hence by (5.7) we get

$$\begin{aligned} v_K(t_{ij}^{p^j} d_i^{p^h}) - v_K(t_{1j}^{p^j} a\omega_1^{p^{n-1}}) &= b_i - b_1 + p^h v_K(d_i) + u_1 \\ &= b_i + p^h v_K(d_i) > 0. \end{aligned}$$

This proves (5.12), so we have

$$v_K(\mathbf{Y}_j^{p^j}) = v_K(t_{1j}^{p^j} a\omega_1^{p^{n-1}}) = v_K(t_{1j}^{p^j}) - b_1.$$

Using (5.7) we get

$$v_{K_j}(\mathbf{Y}_j) = v_K(t_{jj}^{p^j}) - b_j = v_{K_j}(t_{jj}) - b_j.$$

We have $t_{jj} \neq 0$ by (5.6), so we may define $\mathbf{X}_j = t_{jj}^{-1}\mathbf{Y}_j$. Then $v_{K_j}(\mathbf{X}_j) = -b_j$, and since $t_{jj} \in K$ we get $v_{K_j}(\mathbf{Y}_j) \equiv -b_j \pmod{p^j}$. Since $p \nmid b_j$ it follows that $K_j = K(\mathbf{X}_j) = K(\mathbf{Y}_j)$.

Now that we have constructed $\mathbf{X}_1, \dots, \mathbf{X}_n$, we need to choose $\sigma_i \in \mathrm{Gal}(K_n/K_{i-1})$ for $1 \leqslant i \leqslant n$ which satisfy the conditions of Choices 2.1 and 2.3 of [4]. Thus we need to choose $\sigma_i \in \mathrm{Gal}(K_n/K_{i-1})$ such that $\sigma_i|_{K_i}$ is a generator for $\mathrm{Gal}(K_i/K_{i-1}) \cong C_p$ and $v_{K_i}((\sigma_i - 1)\mathbf{X}_i - 1) > 0$. To satisfy these conditions it is enough to choose $\sigma_i \in \mathrm{Gal}(K_n/K_{i-1})$ such that $(\sigma_i - 1)\alpha_i = 1$. We will be imposing additional conditions on σ_i, namely that $\sigma_i(\alpha_h) = \alpha_h$ for certain h in the range $i < h \leqslant n$. The purpose of these extra conditions is to maximize the precision of the scaffold provided by [4] (see (5.18) below).

Recall from the proof of Theorem 4.4 that $K_h = K_{h-1}(\alpha_h)$, where $\alpha_h = \alpha_h' + \alpha_h''$, α_h' is a root of $Y^p - Y - d_h$, and α_h'' is a root of $Y^p - Y - a_h$. For $h \in \Sigma_G$ we have $d_h = 0$, so we may choose $\alpha_h' = 0$, and hence $\alpha_h = \alpha_h''$. For $1 \leqslant i \leqslant n$ set

$$A_i = \{\alpha_h : i < h \leqslant n,\ h \in \Sigma_G\}.$$

Then $K_i(A_i)/K_{i-1}$ is an elementary abelian p-extension of rank $|A_i| + 1$ (see Figure 5.1 (a)). Therefore there is $\rho_i \in \mathrm{Gal}(K_i(A_i)/K_{i-1})$ such that $(\rho_i - 1)\alpha_i = 1$ and $\rho_i(\alpha_h) = \alpha_h$ for all $\alpha_h \in A_i$. Since $K_i(A_i) \subset K_n$ there is $\sigma_i \in \mathrm{Gal}(K_n/K_{i-1})$ such that $\sigma_i|_{K_i(A_i)} = \rho_i$. Then $(\sigma_i - 1)\alpha_i = 1$

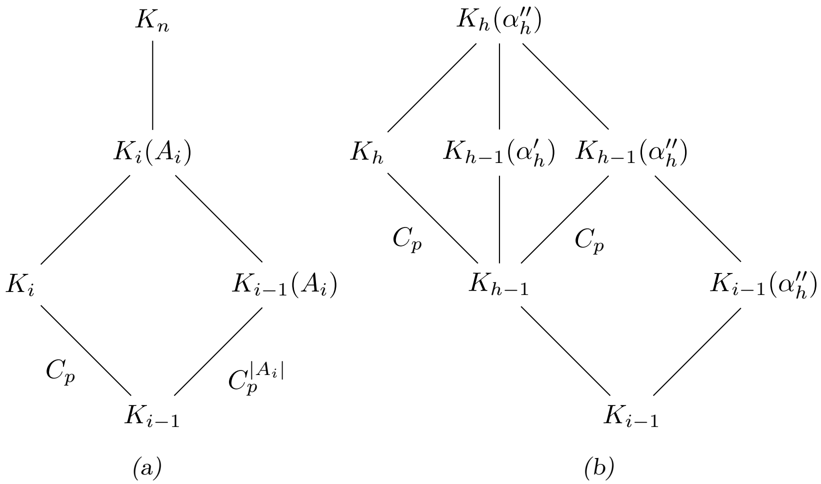

Figure 5.1. Field diagrams for Theorem 5.1

and $\sigma_i(\alpha_h) = \alpha_h$ for all $h \in \Sigma_G$ such that $h \neq i$. It follows that $\sigma_i|_{K_i}$ generates $\mathrm{Gal}(K_i/K_{i-1})$, so σ_i satisfies the conditions of Choice 2.1 of [4]. Since $\sigma_i(\alpha_h) = \alpha_h$ for $1 \leqslant h < i$, by (5.5) we get $(\sigma_i - 1)\mathbf{Y}_i = t_{ii}$ and $(\sigma_i - 1)\mathbf{X}_i = 1$. Therefore σ_i and $\mathbf{X}_i$ satisfy the conditions of Choice 2.3 of [4].

In order to apply [4] to get a Galois scaffold for K_n/K we need to look more closely at the action of $K[G]$ on K_n. Let $1 \leqslant i \leqslant j \leqslant n$. By Theorem 4.4(2) the upper ramification breaks of K_j/K are $u_1, \ldots, u_j$. Therefore the lower ramification breaks of K_j/K are $b_1, \ldots, b_j$. In particular, the lower ramification break $i(\sigma_i|_{K_j})$ of K_j/K associated to $\sigma_i|_{K_j}$ is b_i. Since $p \nmid v_{K_j}(\mathbf{X}_j)$ this implies

$$v_{K_j}((\sigma_i - 1)\mathbf{X}_j) = v_{K_j}(\mathbf{X}_j) + b_i = b_i - b_j. \tag{5.13}$$

By (5.5) we have

$$(\sigma_i - 1)\mathbf{X}_j = \mu_{ij} + \epsilon_{ij}, \tag{5.14}$$

with $\mu_{ij} = t_{ij}/t_{jj}$ and

$$\epsilon_{ij} = \frac{t_{i+1,j}}{t_{jj}}(\sigma_i - 1)\alpha_{i+1} + \cdots + \frac{t_{j-1,j}}{t_{jj}}(\sigma_i - 1)\alpha_{j-1} + (\sigma_i - 1)\alpha_j.$$

Then $\mu_{ij} \in K$ and $\epsilon_{ij} \in K_j$. Furthermore, $\mu_{ii} = 1$, $\epsilon_{ii} = 0$, and for $1 \leqslant i < j \leqslant n$ we have

$$v_{K_n}(\epsilon_{ij}) - v_{K_n}(\mu_{ij}) \geqslant \min\{v_{K_n}(t_{hj}(\sigma_i - 1)\alpha_h) : i < h \leqslant j\} - v_{K_n}(t_{ij}). \tag{5.15}$$

We view μ_{ij} as the "main term" and ϵ_{ij} as the "error term" in the decomposition (5.14) of $(\sigma_i - 1)\mathbf{X}_j$.

Motivated by Assumption 2.9 of [4] we define

$$\mathfrak{c}_0 := \min\{v_{K_n}(\epsilon_{ij}) - v_{K_n}(\mu_{ij}) - p^{n-1}u_i + p^{n-j}b_i : 1 \leqslant i < j \leqslant n\}.$$

Assume $\mathfrak{c}_0 \geqslant 1$. Since $i < j$ it follows from Lemma 4.2(2) that $-p^{n-1}u_i + p^{n-j}b_i \leqslant 0$. Hence the right side of (5.15) is positive for all $1 \leqslant i < j \leqslant n$. Thus $v_{K_j}(\mu_{ij}) < v_{K_j}(\epsilon_{ij})$, so by (5.13) we get

$$b_i - b_j = v_{K_j}((\sigma_i - 1)\mathbf{X}_j) = v_{K_j}(\mu_{ij}).$$

Therefore (5.14) satisfies the conditions of equation (5) of [4]. We can now apply Theorem 2.10 of [4] which says that K_n/K admits a Galois scaffold $(\{\Psi_i\}, \{\lambda_t\})$ with precision $\mathfrak{c}_0$. The operators Ψ_i are defined recursively in Definition 2.7 of [4] using $\mu_{ij} \in K$ and $\sigma_i \in G_{(n-i)}$. Therefore $\Psi_i \in K[G_{(n-i)}]$.

It remains to show that $\mathfrak{c}_0 \geqslant \mathfrak{c}$, where $\mathfrak{c}$ is the precision given in the statement of the theorem. Using (5.7) we get $v_{K_n}(t_{hj}) - v_{K_n}(t_{ij}) = p^{n-j}(b_h - b_i)$. Therefore we can rewrite (5.15) as

$$\begin{aligned}(5.16)\quad & v_{K_n}(\epsilon_{ij}) - v_{K_n}(\mu_{ij}) \\ & \geqslant \min\{v_{K_n}((\sigma_i - 1)\alpha_h) + p^{n-j}(b_h - b_i) : i < h \leqslant j\}.\end{aligned}$$

Set

$$(5.17)\quad \mathfrak{c}_1 = \min\{v_{K_n}((\sigma_i - 1)\alpha_h) + p^{n-j}b_h - p^{n-1}u_i : 1 \leqslant i < h \leqslant j \leqslant n\}.$$

Then by (5.16) we get $\mathfrak{c}_0 \geqslant \mathfrak{c}_1$. Hence if $\mathfrak{c}_1 \geqslant 1$ then K_n/K has a Galois scaffold with precision $\mathfrak{c}_1$. For fixed $1 \leqslant i < h \leqslant n$ the expression in (5.17) is minimized by taking $j = n$. Hence

$$\mathfrak{c}_1 = \min\{v_{K_n}((\sigma_i - 1)\alpha_h) + b_h - p^{n-1}u_i : 1 \leqslant i < h \leqslant n\}.$$

Recall that σ_i was chosen so that $(\sigma_i - 1)\alpha_h = 0$ for all $h \in \Sigma_G$. Therefore we have

$$(5.18)\quad \mathfrak{c}_1 = \min\{v_{K_n}((\sigma_i - 1)\alpha_h) + b_h - p^{n-1}u_i : 1 \leqslant i < h \leqslant n,\, h \notin \Sigma_G\}.$$

Let $1 \leqslant i < h \leqslant n$ with $h \notin \Sigma_G$. In the proof of Theorem 4.4 we saw that $K_h(\alpha_h'') = K_{h-1}(\alpha_h', \alpha_h'')$ is a $(C_p \times C_p)$-extension of K_{h-1} (see Figure 5.1(b)). Therefore $\alpha_h'' \notin K_h$. Let τ_{ih} be the (uniquely determined) element of $\mathrm{Gal}(K_h(\alpha_h'')/K_{i-1}(\alpha_h''))$ such that $\tau_{ih}|_{K_h} = \sigma_i|_{K_h}$. Since $\tau_{ih}(\alpha_h'') = \alpha_h''$ we get

$$(\sigma_i - 1)(\alpha_h) = (\tau_{ih} - 1)(\alpha_h) = (\tau_{ih} - 1)(\alpha_h').$$

Since α'_h is a root of $Y^p - Y - d_h$, it follows that $(\sigma_i - 1)(\alpha_h) = (\tau_{ih} - 1)(\alpha'_h)$ is a root of $Y^p - Y - (\sigma_i - 1)d_h$. We have

$$v_{K_{h-1}}((\sigma_i - 1)d_h) \geqslant v_{K_{h-1}}(d_h) + b_i.$$

It follows that

$$\begin{aligned} v_{K_h}((\sigma_i - 1)\alpha_h) &= v_{K_h}((\tau_{ih} - 1)\alpha'_h) \\ &\geqslant \min\{v_{K_{h-1}}((\sigma_i - 1)d_h), 0\} \\ &\geqslant \min\{v_{K_{h-1}}(d_h) + b_i, 0\} \\ &= \min\{p^{h-1}v_K(d_h) + b_i, 0\}, \end{aligned}$$

and hence that

$$v_{K_n}((\sigma_i - 1)\alpha_h) \geqslant \min\{p^{n-1}v_K(d_h) + p^{n-h}b_i, 0\}. \tag{5.19}$$

Set

$$\mathfrak{c}_2 = \min \left\{ \begin{array}{r} p^{n-1}v_K(d_h) + p^{n-h}b_i + b_h - p^{n-1}u_i,\ b_h - p^{n-1}u_i \\ : 1 \leqslant i < h \leqslant n,\ h \notin \Sigma_G \end{array} \right\}.$$

Then $\mathfrak{c}_1 \geqslant \mathfrak{c}_2$ by (5.18) and (5.19). Hence if $\mathfrak{c}_2 \geqslant 1$ then K_n/K has a Galois scaffold with precision $\mathfrak{c}_2$. Fix $2 \leqslant h \leqslant n$. Using Lemma 4.2 (1) (with $j = h - 1$) we see that the two expressions in the formula for $\mathfrak{c}_2$ are minimized by taking $i = h - 1$. Therefore

$$\mathfrak{c}_2 = \min \left\{ \begin{array}{r} p^{n-1}v_K(d_h) + p^{n-h}b_{h-1} + b_h - p^{n-1}u_{h-1},\ b_h - p^{n-1}u_{h-1} \\ : 2 \leqslant h \leqslant n,\ h \notin \Sigma_G \end{array} \right\}.$$

Thus $\mathfrak{c}_2$ is equal to the precision $\mathfrak{c}$ given in the statement of the theorem. We have $\mathfrak{c} \geqslant 1$ by assumptions (5.1) and (5.2). It now follows from Theorem 2.10 of [4] that K_n/K has a Galois scaffold with precision $\mathfrak{c}$. □

Corollary 5.4. — *Let $(G, \{G_{(i)}\})$ be a p-filtered group of order p^n, with $n \geqslant 2$. Let $D_1, \dots, D_n$ be the polynomials associated to $(G, \{G_{(i)}\})$ by Proposition 3.5, and for $i \notin \Sigma_G$ let l_i be the total degree of D_i. Choose positive integers $u_1 < \cdots < u_n$ with $p \nmid u_1$ and $u_i \equiv u_1 \pmod{p^{n-1}}$ for $2 \leqslant i \leqslant n$. Define $b_1 < b_2 < \cdots < b_n$ recursively by $b_1 = u_1$ and $b_{i+1} - b_i = p^i(u_{i+1} - u_i)$ for $1 \leqslant i \leqslant n - 1$. Assume that $u_1, \dots, u_n$ have been chosen so that*

$$b_i > p^{n-2}l_iu_{i-1} - p^{n-i}b_{i-1} + p^{n-1}u_{i-1} \tag{5.20}$$

for all $2 \leqslant i \leqslant n$ with $i \notin \Sigma_G$. Then there exists a tower of extensions $K = K_0 \subset K_1 \subset \cdots \subset K_n$ satisfying (1)–(3) of Theorem 4.4, plus the additional condition

(4) *K_n/K admits a Galois scaffold with precision*

$$\mathfrak{c}' = \min\{p^{n-i}b_{i-1} - p^{n-2}l_iu_{i-1} + b_i - p^{n-1}u_{i-1} : 2 \leqslant i \leqslant n, i \notin \Sigma_G\}. \tag{5.21}$$

Proof. — It follows from the assumptions on $u_1, \ldots, u_n$ that there are $a, \omega_i \in K^\times$ such that $v_K(a\omega_i^{p^{n-1}}) = -u_i$ for $1 \leqslant i \leqslant n$. Since $v_K(a) \equiv -u_1 \pmod{p^{n-1}}$ we have $p \nmid v_K(a)$. It follows from (5.20) and Lemma 4.2 (2) that $b_i > p^{n-2}l_iu_{i-1}$ for all $2 \leqslant i \leqslant n$ with $i \notin \Sigma_G$. Hence the proof of Corollary 4.5 shows that $p^{n-2}l_iu_{i-1} \geqslant -p^{n-1}v_K(d_i)$ for all $2 \leqslant i \leqslant n$ such that $i \notin \Sigma_G$. Therefore (5.1) follows from (5.20). Using Lemma 4.2 (2) we get $p^{i-2}l_iu_{i-1} \geqslant p^{i-2}u_{i-1} \geqslant b_{i-1}$. Hence (5.2) also follows from (5.20). Thus Theorem 5.1 gives a tower of extensions $K = K_0 \subset K_1 \subset \cdots \subset K_n$ satisfying the conditions (1)–(4) given there. The inequalities above also imply

$$\begin{aligned} -p^{n-2}l_iu_{i-1} + p^{n-i}b_{i-1} + b_i - p^{n-1}u_{i-1} &\leqslant p^{n-1}v_K(d_i) + p^{n-i}b_{i-1} \\ &\qquad + b_i - p^{n-1}u_{i-1}, \\ -p^{n-2}l_iu_{i-1} + p^{n-i}b_{i-1} + b_i - p^{n-1}u_{i-1} &\leqslant b_i - p^{n-1}u_{i-1}. \end{aligned}$$

Therefore the scaffold given by Theorem 5.1 (4) has the precision $\mathfrak{c}'$ specified in (5.21). □

Remark 5.5. — Suppose $G \cong C_{p^n}$ is cyclic. Theorem 2 of [7] gives a Galois scaffold with precision

$$\mathfrak{c}_0 = \min\{b_i - p^n u_{i-1} : 2 \leqslant i \leqslant n\},$$

under the assumption that $b_i > p^n u_{i-1}$ for $2 \leqslant i \leqslant n$. Since G is cyclic we have $\Sigma_G = \{1\}$. Furthermore, by Lemma 4 (a) of [7] we get $v_K(d_i) \geqslant -pu_i$. As in the proof of Corollary 5.4 we can apply Theorem 5.1 to produce a Galois scaffold with precision

$$\mathfrak{c}_1 = \min\{p^{n-i}b_{i-1} - p^n u_i + b_i - p^{n-1}u_{i-1} : 2 \leqslant i \leqslant n\},$$

under the assumption that $b_i > p^n u_i - p^{n-i}b_{i-1} + p^{n-1}u_{i-1}$ for $2 \leqslant i \leqslant n$. If $n \geqslant 1$ then the precision $\mathfrak{c}_1$ is strictly less than the precision $\mathfrak{c}_0$ of [7]. Furthermore, Theorem 2 of [7] allows more general choices of $a_i \in K$, namely $a_i = a\omega_i^{p^{n-1}} + e_i$ for any $e_i \in K$ such that $v_K(e_i) - v_K(a_i)$ satisfies the lower bound given in Assumption (3.3) of [7].

Remark 5.6. — It follows from Corollary 5.4 that by choosing $u_1, \ldots, u_n$ which grow quickly enough we can make $\mathfrak{c}$ arbitrarily large.

The scaffolds that we obtain from Theorem 5.1 can be used to get information about Galois module structure. Let L/K be a Galois extension with Galois group G. Recall that the associated order of $\mathcal{O}_L$ in $K[G]$ is defined to be

$$\mathfrak{A}_0 = \{\gamma \in K[G] : \gamma(\mathcal{O}_L) \subset \mathcal{O}_L\}.$$

Corollary 5.7. — *Let $(G, \{G_{(i)}\})$ be a p-filtered group of order p^n and let K_n/K be a G-extension satisfying the conditions of Theorem 5.1. Let $u_1 < \cdots < u_n$ be the upper ramification breaks of K_n/K and let $r(u_1)$ be the least nonnegative residue of u_1 modulo p^n. Assume that $r(u_1) \mid p^m - 1$ for some $1 \leqslant m \leqslant n$ and that the precision $\mathfrak{c}$ of the scaffold provided by Theorem 5.1 satisfies $\mathfrak{c} \geqslant r(u_1)$. Then $\mathcal{O}_{K_n}$ is free over its associated order $\mathfrak{A}_0$.*

Proof. — Since $u_i \equiv u_1 \pmod{p^{n-1}}$ for $1 \leqslant i \leqslant n$ we have $b_i \equiv b_1 \pmod{p^n}$. It follows that $r(b_n) = r(b_1) = r(u_1)$. Since K_n/K has a Galois scaffold with precision $\mathfrak{c} \geqslant r(u_1)$, the corollary follows from Theorem 4.8 of [3]. □

Let K be a local field with residue characteristic p. Let G be a finite group and let H be an $\mathcal{O}_K$-order in $K[G]$. Say that H is a *Hopf order* if H is a Hopf algebra over $\mathcal{O}_K$ with respect to the operations inherited from the K-Hopf algebra $K[G]$. Say that the Hopf order $H \subset K[G]$ is *realizable* if there is a G-extension L/K such that H is equal to the associated order $\mathfrak{A}_0$ of $\mathcal{O}_L$ in $K[G]$. A great deal of effort has gone into constructing and classifying Hopf orders in $K[C_p^n]$ and $K[C_{p^n}]$; see Chapter 12 of [5] for a summary. The only method known for constructing Hopf orders in $K[G]$ for an arbitrary p-group G was given by Larson [9]. However, Larson's group-theoretic approach does not give a method for finding Hopf orders which are realizable, and does not give a complete classification of Hopf orders in $K[G]$ when $|G| > p$. Therefore it is interesting that in the case where $\mathrm{char}(K) = p$ the scaffolds from Theorem 5.1 can be used to construct realizable Hopf orders in $K[G]$. Since these Hopf orders are constructed using the main result of [4], they are "truncated exponential Hopf orders" in the sense of [5, §12.9]. Thus one consequence of the following corollary is that for all p-groups G, truncated exponential Hopf orders exist in $K[G]$.

Corollary 5.8. — *Let $(G, \{G_{(i)}\})$ be a p-filtered group of order p^n and let K_n/K be a G-extension satisfying the conditions of Theorem 5.1. Let $u_1 < \cdots < u_n$ be the upper ramification breaks of K_n/K and assume that $u_1 \equiv -1 \pmod{p^n}$. Assume further that the precision $\mathfrak{c}$ of the scaffold provided by Theorem 5.1 satisfies $\mathfrak{c} \geqslant p^n - 1$. Then the associated order $\mathfrak{A}_0$ of $\mathcal{O}_{K_n}$ in $K[G]$ is a Hopf order.*

Proof. — It follows from the preceding corollary that $\mathcal{O}_{K_n}$ is free over $\mathfrak{A}_0$. The action of $K[G]$ on K_n is the regular representation, which is indecomposable since $\mathrm{char}(K) = p$. It follows that $\mathcal{O}_{K_n}$ is indecomposable as an $\mathcal{O}_K[G]$-module. Furthermore, since $b_i \equiv -1 \pmod{p^n}$ for $1 \leqslant i \leqslant n$, the different of L/K is generated by an element of K. Hence by Proposition 4.5.2 of [1] we deduce that $\mathfrak{A}_0$ is a Hopf order in $K[G]$. □

Remark 5.9. — It follows from Remark 5.6 that for every filtered p-group G there do exist G-extensions K_n/K satisfying the hypotheses of Corollary 5.8.

Remark 5.10. — Let K be a local field of characteristic 0 with residue characteristic p and let G be a finite abelian p-group. Let $H \subset K[G]$ be a Hopf order which is a local ring. In Corollary 6.5 of [2], Byott showed that H is realizable if and only if the $\mathcal{O}_K$-dual H^* of H is a local ring and a monogenic $\mathcal{O}_K$-algebra.

6. Dihedral examples

Let G be the dihedral group of order 16. Write $G = \langle \sigma, \tau \rangle$ with σ a rotation of order 8 and τ a reflection. We define a 2-filtration of G by setting $G_{(0)} = G$, $G_{(1)} = \langle \sigma^2, \tau \rangle$, $G_{(2)} = \langle \sigma^2 \rangle$, $G_{(3)} = \langle \sigma^4 \rangle$, and $G_{(4)} = \{1\}$. Then $\Phi(G) = \langle \sigma^2 \rangle = G_{(2)}$, so we have $\Sigma_G = \{1, 2\}$. Let K be a local field of characteristic $p = 2$. We will use the methods we have developed to give three examples of G-extensions K_4/K with specified properties.

We first construct a generic G-extension of rings using the results of Section 3. Since $\Sigma_G = \{1, 2\}$ we have $D_1 = D_2 = 0$. Therefore X_1, X_2 are elements of $S_2 \cong \mathbb{F}_2[Y_1, Y_2]$ defined by $X_1 = Y_1^2 - Y_1$ and $X_2 = Y_2^2 - Y_2$. To determine D_3 we use the procedure outlined in the paragraph following Proposition 3.3. Set $\overline{\sigma} = \sigma G_{(2)}$, $\overline{\tau} = \tau G_{(2)}$, $\widetilde{\sigma} = \sigma G_{(3)}$, and $\widetilde{\tau} = \tau G_{(3)}$. Then $(\overline{\sigma} - 1)Y_1 = 1$, $(\overline{\sigma} - 1)Y_2 = 0$, $(\overline{\tau} - 1)Y_1 = 0$, and $(\overline{\tau} - 1)Y_2 = 1$. Let $u : G/G_{(2)} \to G/G_{(3)}$ be the section of the projection $\pi : G/G_{(3)} \to G/G_{(2)}$ whose image is $\{\widetilde{1}, \widetilde{\sigma}, \widetilde{\tau}, \widetilde{\sigma}\widetilde{\tau}\}$, and let χ be the unique isomorphism from $G_{(2)}/G_{(3)}$ to $\mathbb{F}_2$. Then the 2-cocycle $c : (G/G_{(2)}) \times (G/G_{(2)}) \to \mathbb{F}_2$ defined by $c(g, h) = \chi(u(g)u(h)u(gh)^{-1})$ represents the class in $H^2(G/G_{(2)}, \mathbb{F}_2)$ which corresponds to the group extension $\pi : G/G_{(3)} \to G/G_{(2)}$. We find that the cochain $(s_g)_{g \in G/G_{(2)}}$ defined by $s_{\overline{1}} = 0$, $s_{\overline{\sigma}} = s_{\overline{\tau}} = Y_1$, and $s_{\overline{\sigma}\overline{\tau}} = 1$, satisfies $c(g,h) = s_g + g(s_h) - s_{gh}$ for all $g,h \in G/G_{(2)}$. We have

$$\begin{aligned}\wp(s_{\overline{1}}) &= 0 = (\overline{1}-1)(X_1(Y_1+Y_2)),\\ \wp(s_{\overline{\sigma}}) &= X_1 = (\overline{\sigma}-1)(X_1(Y_1+Y_2)),\\ \wp(s_{\overline{\tau}}) &= X_1 = (\overline{\tau}-1)(X_1(Y_1+Y_2)),\\ \wp(s_{\overline{\sigma\tau}}) &= 0 = (\overline{\sigma\tau}-1)(X_1(Y_1+Y_2)).\end{aligned}$$

Therefore we can take

$$\begin{aligned}D_3 &= X_1(Y_1+Y_2) = (Y_1^2-Y_1)(Y_1+Y_2),\\ X_3 &= Y_3^2 - Y_3 - (Y_1^2-Y_1)(Y_1+Y_2).\end{aligned}$$

A similar but more complicated computation based on the formulas $(\widetilde{\sigma}-1)Y_1 = 1$, $(\widetilde{\sigma}-1)Y_2 = 0$, $(\widetilde{\sigma}-1)Y_3 = Y_1$, $(\widetilde{\tau}-1)Y_1 = 0$, $(\widetilde{\tau}-1)Y_2 = 1$, and $(\widetilde{\tau}-1)Y_3 = Y_1$ gives

$$\begin{aligned}D_4 = X_1^3Y_1 + X_1^2X_2Y_2 + X_1^2Y_1Y_2 + X_1(Y_1^3 + Y_1Y_3 + Y_2Y_3 + Y_2)\\ + X_1X_3(Y_1+Y_2) + X_3(Y_3+Y_2).\end{aligned}$$

We can represent D_4 as a polynomial in Y_1, Y_2, Y_3 by expressing X_1, X_2, X_3 in terms of Y_1, Y_2, Y_3 using the formulas given above.

We now use the generic G-extension of rings that we have constructed to get a family of G-extensions of K. Let $a_1, a_2, a_3, a_4 \in K$ and set $u_i = -v_K(a_i)$. Assume that $0 < u_1 < u_2 < u_3 < u_4$, and that u_1, u_2, u_3, u_4 are odd. Define b_1, b_2, b_3, b_4 by $b_1 = u_1$ and $b_{i+1} = b_i + 2^i(u_{i+1} - u_i)$ for $1 \leqslant i \leqslant 3$. Set $K_4 = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, where the α_i are defined recursively by $\alpha_i^2 - \alpha_i = d_i + a_i$, with $d_1 = d_2 = 0$, $d_3 = D_3(\alpha_1, \alpha_2)$, and $d_4 = D_4(\alpha_1, \alpha_2, \alpha_3)$. Since u_1, u_2 are distinct, positive, and odd, $\{a_1 + \wp(K), a_2 + \wp(K)\}$ is linearly independent over $\mathbb{F}_p$. Therefore it follows from Theorem 3.6 that K_4/K is a G-extension. By putting additional conditions on a_1, a_2, a_3, a_4 we will get examples of G-extensions which have various interesting properties.

Example 6.1. — To satisfy the hypotheses of Theorem 4.4 we need to choose a_i so that $b_i > p^{i-1}v_K(d_i)$ for $i = 3, 4$. We first choose a_1, a_2 so that $0 < u_1 < u_2$ are odd. This gives $b_1 = u_1$, $b_2 = 2u_2 - u_1$, and $v_K(d_3) = -u_1 - \frac{1}{2}u_2$. We must choose a_3 so that u_3 is odd and $b_3 = 4u_3 - 2u_2 - u_1$ is greater than $-4v_K(d_3) = 4u_1 + 2u_2$. This is equivalent to $u_3 > \frac{5}{4}u_1 + u_2$. Under this assumption we have

$$v_K(d_4) \geqslant \min\left\{-u_1 - \tfrac{1}{2}u_2 - u_3, -\tfrac{3}{2}u_3\right\}$$

and $b_4 = 8u_4 - 4u_3 - 2u_2 - u_1$. Therefore it suffices to choose a_4 so that u_4 satisfies

$$8u_4 - 4u_3 - 2u_2 - u_1 > \max\{8u_1 + 4u_2 + 8u_3, 12u_3\}.$$

This is equivalent to

$$u_4 > \max\left\{\tfrac{9}{8}u_1 + \tfrac{3}{4}u_2 + \tfrac{3}{2}u_3,\ \tfrac{1}{8}u_1 + \tfrac{1}{4}u_2 + 2u_3\right\}.$$

If these conditions are satisfied then it follows from Theorem 4.4 that K_4/K is a G-extension whose upper ramification breaks are u_1, u_2, u_3, u_4. To get a specific example we let π_K be a uniformizer for K and set $a_1 = \pi_K^{-1}$, $a_2 = \pi_K^{-3}$, $a_3 = \pi_K^{-5}$, $a_4 = \pi_K^{-11}$. This gives a G-extension K_4/K with upper ramification breaks $1, 3, 5, 11$ and lower ramification breaks $1, 5, 13, 61$.

Example 6.2. — In order to use Theorem 5.1 to get a G-extension K_4/K with a Galois scaffold we write $a_i = a\omega_i^8$ and consider the possibilities for the ramification data of K_4/K. Choose $u_1 = b_1 = 1$. We need $u_2 > u_1$ with $u_2 \equiv u_1 \pmod 8$, so we choose $u_2 = 9$. It follows that $b_2 = 1+2(9-1) = 17$. We need $u_3 > u_2$ with $u_3 \equiv 1 \pmod 8$ such that $b_3 = 17+4(u_3-9)$ satisfies

$$b_3 > 8 \cdot \tfrac{11}{2} - 2 \cdot 17 + 8 \cdot 9 = 82,$$
$$b_3 > 8 \cdot 9 = 72.$$

We choose $u_3 = 33$, so $b_3 = 113$. Finally, we need $u_4 > u_3$ with $u_4 \equiv 1 \pmod 8$ such that $b_4 = 113 + 8(u_4 - 33)$ satisfies

$$b_4 > 8 \cdot \max\left\{1 + \tfrac{1}{2} \cdot 9 + 33, \tfrac{3}{2} \cdot 33\right\} - 113 + 8 \cdot 33 = 547,$$
$$b_4 > 8 \cdot 33 = 264.$$

We choose $u_4 = 89$, which gives $b_4 = 561$. This ramification data can be realized by taking $a = \pi_K^{-1}$, $\omega_1 = 1$, $\omega_2 = \pi_K^{-1}$, $\omega_3 = \pi_K^{-4}$, and $\omega_4 = \pi_K^{-11}$. According to Theorem 5.1 and Remark 5.2, these choices give a G-extension K_4/K which has a Galois scaffold with precision

$$\mathfrak{c} = \min\{b_3 - 82, b_3 - 72, b_4 - 547, b_4 - 264\} = 14.$$

It then follows from Corollary 5.7 that $\mathcal{O}_{K_4}$ is free over its associated order $\mathfrak{A}_0$.

Example 6.3. — We wish to use Corollary 5.8 to produce a G-extension K_4/K such that the associated order $\mathfrak{A}_0$ of $\mathcal{O}_{K_4}$ in $K[G]$ is a Hopf order. Once again we set $a_i = a\omega_i^8$. We need to determine ramification data for K_4/K that satisfies the hypotheses of Corollary 5.8. The first requirement is $u_1 \equiv -1 \pmod{16}$, so we choose $u_1 = b_1 = 15$. We need $u_2 > u_1$ with $u_2 \equiv -1 \pmod 8$. We choose $u_2 = 23$ and hence $b_2 = 31$. To apply Corollary 5.8 we need to construct an extension which has a scaffold with precision $\mathfrak{c} \geqslant 2^4 - 1 = 15$. Therefore we wish to find $u_3 \equiv -1 \pmod 8$ such that $b_3 = 31 + 4(u_3 - 23)$ makes the gaps in inequalities (5.1) and (5.2) greater than or equal to 15 (see Remark 5.2). Hence we require

$$\begin{aligned} b_3 &\geqslant 8 \cdot \tfrac{53}{2} - 2 \cdot 31 + 8 \cdot 23 + 15 = 349, \\ b_3 &\geqslant 8 \cdot 23 + 15 = 199. \end{aligned}$$

By choosing $u_3 = 103$ we get $b_3 = 351$, which satisfies both inequalities. Similarly, we need $u_4 > u_3$ with $u_4 \equiv -1 \pmod 8$ such that $b_4 = 351 + 8(u_4 - 103)$ satisfies

$$\begin{aligned} b_4 &\geqslant 8 \cdot \max\{15 + \tfrac{1}{2} \cdot 23 + 103, \tfrac{3}{2} \cdot 103\} - 351 + 8 \cdot 103 + 15 = 1724, \\ b_4 &\geqslant 8 \cdot 103 + 15 = 839. \end{aligned}$$

We choose $u_4 = 279$, which gives $b_4 = 1759$. We get a G-extension K_4/K with this ramification data by taking $a = \pi_K^{-15}$, $\omega_1 = 1$, $\omega_2 = \pi_K^{-1}$, $\omega_3 = \pi_K^{-11}$, and $\omega_4 = \pi_K^{-33}$. Using the definitions of μ_{ij} in (5.14) and t_{ij} in (5.5) we get

$$\begin{aligned} \mu_{12} &= \frac{1}{\pi_K^4}, \\ \mu_{13} &= \frac{1 + \pi_K^{20}}{\pi_K^{42}(1 + \pi_K^2)}, \\ \mu_{14} &= \frac{1 + \pi_K^{10} + \pi_K^{44} + \pi_K^{74} + \pi_K^{76} + \pi_K^{96}}{\pi_K^{109}(1 + \pi_K + \pi_K^{20} + \pi_K^{23} + \pi_K^{31} + \pi_K^{33})}, \\ \mu_{23} &= \frac{1 + \pi_K^{22}}{\pi_K^{40}(1 + \pi_K^2)}, \\ \mu_{24} &= \frac{1 + \pi_K^{11} + \pi_K^{44} + \pi_K^{99}}{\pi_K^{108}(1 + \pi_K + \pi_K^{20} + \pi_K^{23} + \pi_K^{31} + \pi_K^{33})}, \\ \mu_{34} &= \frac{1 + \pi_K + \pi_K^{64} + \pi_K^{67} + \pi_K^{97} + \pi_K^{99}}{\pi_K^{88}(1 + \pi_K + \pi_K^{20} + \pi_K^{23} + \pi_K^{31} + \pi_K^{33})}. \end{aligned}$$

Definition 2.7 of [4] gives elements $\Theta_i \in K[G]$ which are defined recursively using the "truncated exponential" $X^{[Y]} = 1 + Y(X - 1)$. In our setting these formulas give $\Theta_4 = \sigma^4$, $\Theta_3 = \sigma^2 \Theta_4^{[-\mu_{3,4}]}$, $\Theta_2 = \sigma \Theta_3^{[-\mu_{2,3}]} \Theta_4^{[-\mu_{2,4}]}$, and $\Theta_1 = \tau \Theta_2^{[-\mu_{1,2}]} \Theta_3^{[-\mu_{1,3}]} \Theta_4^{[-\mu_{1,4}]}$. For $1 \leqslant i \leqslant 4$ set $M_i = (b_i + 1)/p^i$. It follows from equation (34) of [4] that the associated order $\mathfrak{A}_0$ of $\mathcal{O}_{K_4}$ in $K[G]$ is

$$\begin{aligned} \mathfrak{A}_0 &= \mathcal{O}_K \left[\frac{\Theta_4 - 1}{\pi_K^{M_4}}, \frac{\Theta_3 - 1}{\pi_K^{M_3}}, \frac{\Theta_2 - 1}{\pi_K^{M_2}}, \frac{\Theta_1 - 1}{\pi_K^{M_1}} \right] \\ &= \mathcal{O}_K \left[\frac{\Theta_4 - 1}{\pi_K^{110}}, \frac{\Theta_3 - 1}{\pi_K^{44}}, \frac{\Theta_2 - 1}{\pi_K^{8}}, \frac{\Theta_1 - 1}{\pi_K^{8}} \right]. \end{aligned}$$

By Corollary 5.8 we see that $\mathfrak{A}_0$ is a Hopf order in $K[G]$.

BIBLIOGRAPHY

[1] M. V. Bondarko, "Local Leopoldt's problem for ideals in totally ramified p-extensions of complete discrete valuation fields", in *Algebraic number theory and algebraic geometry*, Contemporary Mathematics, vol. 300, American Mathematical Society, 2002, p. 27-57.

[2] N. P. Byott, "Monogenic Hopf orders and associated orders of valuation rings", *J. Algebra* **275** (2004), no. 2, p. 575-599.

[3] N. P. Byott, L. N. Childs & G. G. Elder, "Scaffolds and generalized integral Galois module structure", *Ann. Inst. Fourier* **68** (2018), no. 3, p. 965-1010.

[4] N. P. Byott & G. G. Elder, "Sufficient conditions for large Galois scaffolds", *J. Number Theory* **182** (2018), p. 95-130.

[5] L. N. Childs, C. Greither, K. Keating, A. Koch, T. Kohl, P. J. Truman & R. G. Underwood, *Hopf algebras and Galois module theory*, Mathematical Surveys and Monographs, vol. 260, American Mathematical Society, 2021, vii+311 pages.

[6] F. DeMeyer & E. Ingraham, *Separable algebras over commutative rings*, Lecture Notes in Mathematics, vol. 181, Springer, 1971, iv+157 pages.

[7] G. G. Elder & K. Keating, "Galois scaffolds for cyclic p^n-extensions in characteristic p", *Res. Number Theory* **8** (2022), no. 4, article no. 75 (16 pages).

[8] I. B. Fesenko & S. V. Vostokov, *Local fields and their extensions*, second ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, 2002, with a foreword by I. R. Shafarevich, xii+345 pages.

[9] R. G. Larson, "Hopf algebra orders determined by group valuations", *J. Algebra* **38** (1976), no. 2, p. 414-452.

[10] E. Maus, "On the jumps in the series of ramifications groups", *Bull. Soc. Math. Fr., Suppl., Mém.* **22** (1971), p. 127-133, Colloque de Théorie des Nombres (Univ. Bordeaux, Bordeaux, 1969).

[11] G. A. Miller, "The ϕ-subgroup of a group", *Trans. Am. Math. Soc.* **16** (1915), no. 1, p. 20-26.

[12] D. J. Saltman, "Noncrossed product p-algebras and Galois p-extensions", *J. Algebra* **52** (1978), no. 2, p. 302-314.

[13] J.-P. Serre, *Corps locaux*, Publications de l'Institut de Mathématique de l'Université de Nancago, vol. VIII, Hermann, 1962, Actualités Scientifiques et Industrielles, No. 1296, 243 pages.

Manuscrit reçu le 4 août 2023,
révisé le 8 décembre 2023,
accepté le 21 décembre 2023.

G. Griffith ELDER
Department of Mathematics
University of Nebraska Omaha
Omaha, NE 68182 (USA)
elder@unomaha.edu

Kevin KEATING
Department of Mathematics
University of Florida
Gainesville, FL 32611 (USA)
keating@ufl.edu