Fields Institute Communications
Volume **00**, 0000

Valued fields and covers in characteristic p

David Harbater
Department of Mathematics, University of Pennsylvania
209 South 33rd Street, Philadelphia, PA 19104-6395, USA.
harbater@math.upenn.edu

Marius van der Put
Department of Mathematics, University of Groningen,
P.O.Box 800, 9700 AV Groningen, The Netherlands
mvdput@math.rug.nl

with an appendix by Robert Guralnick
Department of Mathematics, University of Southern California,
Los Angeles, CA 90089-1113
guralnic@math.usc.edu

Abstract. We consider fundamental groups of affine varieties in characteristic $p > 0$, especially in the case of complements of normal crossing divisors in projective space. In particular, we disprove a conjecture of Abhyankar concerning which finite groups can be Galois groups of covers in characteristic p, by showing that fewer groups than expected can occur. The proof uses valuation theory to establish a necessary condition for a finite group to be a Galois group, and uses group theory to show that this condition is non-trivial. We prove both local and global versions of our results.

1 Introduction

A longstanding problem is to determine the algebraic fundamental group $\pi_1(X)$ of a variety X over a field k of characteristic $p > 0$. For X irreducible, this fundamental group is defined as the inverse limit of the Galois groups of the (connected) finite étale Galois covers $Y \to X$. The set $\pi_A(X)$ of (continuous) finite quotients of $\pi_1(X)$ is precisely the set of these Galois groups, and in particular one would like to know which finite groups occur in $\pi_A(X)$. This paper considers this situation in the global case that $X = \mathbf{P}^n_k - D$, and in the local case that $X = \operatorname{Spec} k[[x_1, \ldots, x_n]] - D$,

Mathematics Subject Classification. Primary 12F12, 14E20, 12J10; Secondary 13B05, 13J05, 20D15, 20F34.

This research was undertaken at the MSRI during the fall 1999 semester on Galois groups and fundamental groups. The authors wish to thank MSRI for its hospitality. The first author also thanks NSF for its support, under research grants DMS94-00836 and DMS99-70481.

where in either case D is a normal crossings divisor and k is algebraically closed. We also discuss open subsets of the affine line over a finite field.

The above problem is rather well-understood in the case of curves over an algebraically closed field k. Let $\pi_1'(X)$ be the "prime-to-p quotient" of $\pi_1(X)$, i.e. the inverse limit of the Galois groups of only those covers of X whose degree is prime to p. Equivalently, $\pi_1'(X)$ is the inverse limit of the finite groups $G/p(G)$, where G ranges over the finite Galois groups over X, and $p(G)$ denotes the subgroup of G generated by all the elements having order a power of p. Grothendieck's comparison theorem [9], XIII, Cor. 2.12 states that for k-curves X, the group $\pi_1'(X)$ can be identified with the prime-to-p quotient of the profinite completion of the topological fundamental group of a curve over $\mathbf{C}$ having the same genus g and the same number of punctures r. In particular, if $r > 0$ (i.e. if X is an affine curve), then $\pi_1'(X)$ is the free pro-prime-to-p group on $2g + r - 1$ generators. Concerning the set $\pi_A(X)$ of all finite quotients of $\pi_1(X)$ (not just those of order prime to p), for X an affine curve, S.S. Abhyankar posed the following conjecture in his 1957 paper [1]:

Conjecture 1.1 (Abhyankar) *A finite group G is a Galois group of some finite étale Galois cover $Y \to X$ if and only if $G/p(G)$ occurs as Galois group over X, i.e., is a quotient of $\pi_1'(X)$.*

More generally, we will say that *Abhyankar's Conjecture holds* for a variety X in characteristic p if Conjecture 1.1 is satisfied by X. The original conjecture, for affine curves over an algebraically closed field, was proven in papers of M. Raynaud [23] and D. Harbater [12] (see also [13]). In [1] and later papers, Abhyankar gave examples that hinted that the conjecture should hold for higher dimensional varieties. More recently ([3], Conjectures (2.2) and (3.2)) he explicitly stated a conjecture that is equivalent to 1.1, in the formal local case and for the complement of a normal-crossings hypersurface in $\mathbf{P}^n_k$.

The first author's investigations of these higher dimensional cases brought him in contact with the second author's work on inverse Galois problems for differential and difference equations (see [21], [22], [18]). The remarkable parallelism between these theories led to the discovery that certain valued fields, which we call "fields of generalized Laurent series", can be used to show that Abhyankar's Conjecture does *not* hold in general, i.e. that the condition $G/p(G) \in \pi_A(X)$ is not sufficient to ensure that G occurs as Galois group over a higher dimensional X as above. We will make this statement more precise by stating the simplest special cases of Theorems 3.3 and 4.5.

(1) Let $X = \mathrm{Spec}(k[[x_1, x_2]][(x_1x_2)^{-1}])$. If G is the group of a connected Galois cover of X then so is $G/p(G)$. Moreover:

(i) G contains a prime-to-p subgroup $A \subset G$ which maps surjectively to $G/p(G)$ and which is itself a Galois group over X;

(ii) If $p(G) \neq 1$ then there is a non-trivial p-subgroup $P \subset G$ which is normalized by some choice of this subgroup A; and

(iii) For arbitrary G, $p(G)$ is generated by the p-subgroups P such that P is normalized by some choice of this subgroup A (depending on P).

(2) Let X be the complement in $\mathbf{P}^2_k$ of three lines in general position (i.e. not all of them passing through one point). Then any Galois group for X again has the

properties (i), (ii), and (iii) of the above statement (1).

For X in (1) or (2) above, the condition on A in (i) (i.e. that A is a finite quotient of $\pi_1'(X)$) is just that the prime-to-p group A is abelian with at most two generators. (See Proposition 3.1 and Corollary 4.2(b).) For such X, conditions (i), (ii), and (iii) are each non-trivial constraints on the group G, beyond the assumption that the prime-to-p group $G/p(G)$ is a quotient of $\pi_1'(X)$. This is shown in examples constructed by R. Guralnick, which appear in the appendix to this paper. Hence the higher dimensional version of Abhyankar's Conjecture, as posed above, does not hold. A similar situation occurs for open subsets of the affine line over a finite field. These additional constraints on Galois groups are new to the above situations; for affine curves over an algebraically closed field, the issue does not arise, because conditions (i)-(iii) are always satisfied for *any* finite group G such that $G/p(G)$ is a Galois group over X (as follows from the fact that $\pi_1'(X)$ is the prime-to-p quotient of the profinite completion of a free group).

This paper is organized as follows: Section 2 defines and studies *fields of generalized Laurent series*, a class that includes such fields as $k((x))((y))$. Section 3 applies those results to the case of Galois groups over the complement of a normal crossings divisor in the formal local case in dimension ≥ 2, in particular proving conditions (i)-(iii) above. Section 4 similarly treats the global case in dimension ≥ 2. Finally, Section 5 shows why these results imply that Abhyankar's Conjecture does not hold in these cases, and similarly why it does not hold in the one-dimensional case over a finite field. In that section we also discuss several possible variants of Abhyankar's Conjecture and discuss their relationships.

We conclude this introduction by fixing terminology for the paper. Given a finite group G, its *rank* is the size of the smallest generating set for G. If N is a normal subgroup of G, then a subgroup $H \subset G$ is a *supplement* [resp. a *complement*] to N in G if the quotient map $G \to G/N$ restricts to a surjection [resp. an isomorphism] on H. Thus H is a supplement to N if and only if H, N generate G; and H is a complement to N if and only if G is a semidirect product of N and H. For a profinite group G, we denote by $p(G)$ the closed subgroup generated by the pro-p-subgroups of G. (This agrees with the above definition of $p(G)$ for finite groups.) Equivalently, for a profinite group G, we have that $p(G) = \varprojlim p(H)$, where H runs over the finite quotients of G. A finite [resp. profinite] group G is a *quasi-p* [resp. *pro-quasi-p*] group if $p(G) = G$.

Suppose that X is a regular connected scheme and Y is a normal scheme. Then a *cover* $f : Y \to X$ is a finite generically separable morphism. A (branched) cover is *Galois* if Y is connected and if the Galois group $G = \mathrm{Gal}(Y/X)$ of automorphisms of Y preserving f acts simply transitively on a generic geometric fibre of f. The *branch locus* D of $Y \to X$ is the locus of points where the cover is not étale; this is of pure codimension 1 by Purity of Branch Locus. The cover is *tamely ramified* if the inertia group over the generic point of each irreducible component of D has order prime to p. If $X = \operatorname{Spec} R$ and $Y = \operatorname{Spec} S$ we will also say that S is *Galois* over R with Galois group G (so in particular, we are allowing ramification). As above, the *fundamental group* $\pi_1(X)$ [resp. the *prime-to-p fundamental group* $\pi_1'(X)$] is the inverse limit of the Galois groups of Galois finite étale covers of X [resp. of those whose degrees are prime to p]. We also define the *tame fundamental*

group $\pi_1^{\mathrm{t}}(X, D)$ to the the inverse limit of the Galois groups of tamely ramified Galois covers $Y \to X$ that are étale away from D. Thus $\pi_1^{\mathrm{t}}(X, D)$ is a quotient of $\pi_1(X - D)$, and $\pi_1'(X - D)$ is a quotient of $\pi_1^{\mathrm{t}}(X, D)$.

2 Fields of generalized Laurent series

In this section we study a class of valued fields that we call fields of generalized Laurent series. This class of fields includes, among others, fields of the form $k((x_1))\cdots((x_n))$. These fields, which will be used later in the paper in proving the results mentioned in the introduction, are also useful for Krull's theory of maximally complete valued fields (also called maximal fields, maximal valued fields and spherically complete valued fields; cf. [14] and [24] for more about these fields). We will develop the theory of fields of generalized Laurent series in a self-contained manner, with the exception of two references to [24].

Let k be any field and let H be an abelian group, written additively. We write $k[H]$ for its group algebra over k. Since H is additive, it is natural to introduce a (superfluous) variable z. The elements of $k[H]$ are now written as finite sums $\sum_{h\in H} c(h)z^h$ with coefficients $c(h) \in k$, and the multiplication is given by the rule $z^{h_1}z^{h_2} = z^{h_1+h_2}$. Here, we are only interested in the case where H is torsion free, i.e. H has no nontrivial elements of finite order. Then H embeds into $\mathbf{Q} \otimes H$. The latter is a vector space over $\mathbf{Q}$ and can be given a total group order. Thus H can also be given some total group order which will be denoted by o. The *field of generalized Laurent series* $k((z^{H,o}))$ is the set of formal expressions $\sum_{h\in H} c(h)z^h$, with all $c(h) \in k$, such that the support (i.e. $\{h \in H |\ c(h) \neq 0\}$) of the expression is a well ordered subset of H. (See also [24], p. 103). In $k((z^{H,o}))$ one can add and multiply in the usual way. Thus the product of two elements $\sum c(h)z^h$ and $\sum d(h)z^h$ is defined as $\sum e(h)z^h$ with $e(h) = \sum_{a+b=h} c(a)d(b)$. One easily verifies that the expression for $e(h)$ is in fact a finite sum and that $\sum e(h)z^h$ again has a well ordered support.

In order to see that $k((z^{H,o}))$ is a field one has to show (apart from trivialities) that every non zero element x has an inverse. One can write $x = c \cdot z^e \cdot (1 - r)$ with $c \in k^*$, $e \in H$ and $r = \sum_{h>0} r(h)z^h \in k((z^{H,o}))$. It suffices to show that $1 - r$ has an inverse. For $n \geq 1$ one writes $r^n = \sum_{h\in H} c(n, h)z^h$ with $c(n, h) \in k$. The verification of the following assertions is straightforward:

(i) For each $h \in H$, the number of integers $n \geq 1$ with $c(n, h) \neq 0$ is finite.
(ii) For $h \in H$ one defines $u(h) := \sum_{n\geq 1} c(n, h)$ and $u := 1 + \sum_{h\in H} u(h)z^h$. The support of the last expression is well ordered and thus $u \in k((z^{H,o}))$.
(iii) u is the inverse of $1 - r$.

For a unit $x \in k((z^{H,o}))^*$, let $v(x) \in H$ be the smallest element of the support of $x = \sum c(h)z^h$. Then the map $v : k((z^{H,o}))^* \to H$ is a valuation (in additive notation) on $k((z^{H,o}))$. Usually, one introduces a symbol ∞ which is larger than any element in H and one extends v by putting $v(0) = \infty$. The value group is clearly H. The valuation ring consists of the elements $\sum_{h\geq 0} c(h)z^h \in k((z^{H,o}))$. Its maximal ideal consists of the elements $\sum_{h>0} c(h)z^h \in k((z^{H,o}))$ and the residue field of $k((z^{H,o}))$ is k. The crucial property of $k((z^{H,o}))$ is that it has no "immediate extensions", i.e.:

Lemma 2.1 *Let $L \supset k((z^{H,o}))$ be an extension of valued fields. Suppose that L has the same value group and residue field as $k((z^{H,o}))$. Then $L = k((z^{H,o}))$.*

Proof The extension of v to L will also be called v. Take a non-zero element $x \in L$. We want to show that $x \in k((z^{H,o}))$.

We claim that we can write $x = c(h)z^h + \tilde{x}$ with $h \in H$, $c(h) \in k^*$ and either $\tilde{x} = 0$ or $v(\tilde{x}) > h = v(x)$ (with respect to the order on H). Namely, let $h = v(x)$. So $x = yh$, with $y \in L$ and $v(y) = 0$. Thus y reduces to an element $\bar{y} \in k^*$ which is a unit in the residue field. Take $c(h) = \bar{y}$. So either $y - c(h) = 0$ or $v(y - c(h)) > 0$. Let $\tilde{x} = x - c(h)h$. Then h, $c(h)$, and $\tilde{x}$ satisfy the claim.

In the notation of the claim, if $\tilde{x} = 0$ then we are done. Otherwise, the idea is to repeat the above step, inductively obtaining an expression $\sum c(h)z^h = k((z^{H,o}))$ for x. We now make this precise.

Let $D \subset H$ consist of all $d \in H$, $d \geq v(x)$ such that there exists an element $z \in k((z^{H,o}))$ with $v(x - z) > d$. The claim above shows that $v(x) \in D$; thus D is not empty. Moreover, for a given $d \in D$ there is a unique element $y_d \in k((z^{H,o}))$ with $v(x - y_d) > d$ and $y_d = \sum_{h \leq d} c(d, h)z^h$. In particular for elements $d_1 < d_2$ in D and $h \leq d_1$ one has $c(d_1, h) = c(d_2, h)$. Consider the expression $y = \sum c(h)z^h$ with $c(h) = c(d, h)$ if $h \leq d$ for some $d \in D$ and 0 otherwise. It is easily seen that the support of y is well ordered. Thus $y \in k((z^{H,o}))$. If $x \neq y$, then $v(x - y) = e \in H$ with $e \geq d$ for all $d \in D$. Write $x - y = c(e)z^e + r$ with $c(e) \in k^*$ and $r \in L$ with $v(r) > e$. Then $v(x - y - c(e)z^e) > e \geq d$ for all $d \in D$. This contradicts the definition of D. □

The lemma has the immediate consequence:

Corollary 2.2 *The field $k((z^{H,o}))$ is algebraically closed if k is algebraically closed and H is a divisible group.*

We note in passing that the definition of a maximally complete valued field F is: "F has the property of the above lemma" (shown there for $F = k((z^{H,o}))$).

Examples 2.3

(1) $k((z^{\mathbf{Z},o}))$, with o the natural ordering on $\mathbf{Z}$, is the field $k((z))$ of the formal Laurent series over k.

(2) $k((z^{\mathbf{Q},o}))$, with o the natural ordering on $\mathbf{Q}$, is a field containing the field of formal Puiseux series $\cup_{m \geq 1} k((z^{1/m}))$. The latter is the algebraic closure of $k((z))$ provided that k is algebraically closed and of characteristic 0.

For an algebraically closed field k of characteristic $p > 0$, the algebraic closure of $k((z))$ is a subfield of $k((z^{\mathbf{Q},o}))$ that is strictly larger than the field of Puiseux series. However, one can write down explicit elements of $k((z^{\mathbf{Q},o}))$ that are not in the Puiseux series field but are algebraic over the field $k((z))$. The standard example for this is the element $\sum_{n \geq 0} z^{-1/p^n} \in k((z^{\mathbf{Q},o}))$, which is a solution of the equation $t^p - t = -z^{-1}$. See also [15] for a description of this algebraic closure.

(3) On $\mathbf{Z}^2$ one can define many total group orders. Any "archimedean order" is obtained from an injective homomorphism $\mathbf{Z}^2 \to \mathbf{R}$, e.g. the map $(a, b) \mapsto a + b\alpha$ with irrational α. Let $\mathbf{R}^2$ be given the lexicographical order. Then any "non-archimedean order" on $\mathbf{Z}^2$ is obtained from an injective homomorphism $\mathbf{Z}^2 \to \mathbf{R}^2$, whose image is not contained in a one-dimensional linear subspace. We are in

particular interested in those orders o satisfying $(a,b) \geq 0 = (0,0)$ for all $a, b \geq 0$. For such o there is an embedding $k[[x,y]] \to k((z^{\mathbf{Z}^2,o}))$ with $x \mapsto z^{(1,0)}$ and $y \mapsto z^{(0,1)}$. These orders o coincide with the familiar monomial orders of Gröbner theory. Consider the non-archimedean order o defined by the canonical embedding $\mathbf{Z}^2 \to \mathbf{R}^2$, i.e., $(1,0) \mapsto (1,0)$ and $(0,1) \mapsto (0,1)$. Then, with the identifications $x = z^{(1,0)}$ and $y = z^{(0,1)}$, one has $k((z^{\mathbf{Z}^2,o})) = k((y))((x))$.

A geometric interpretation of an embedding $k[[x,y]] \subset k((z^{\mathbf{Z}^2,o}))$ is the following. The valuation of the field $k((z^{\mathbf{Z}^2,o}))$ induces a valuation on the field of fractions of $k[[x,y]]$ which is centered at the maximal ideal (x,y) (i.e., the ideal (x,y) lies in the maximal ideal of the valuation ring). The valuation defines a sequence of blowings up of $\mathrm{Spec}(k[[x,y]])$.

(4) Let an additive group H with total group order o be given and let x denote a variable. Then the field $k((z^{H,o}))((x))$ is again a generalized field of Laurent series, namely $k((z^{H',o'}))$ where $H' = H \oplus \mathbf{Z}$ and the total group order o' is given by $(h,n) > (0,0)$ (with $h \in H,\ n \in \mathbf{Z}$) if either $n > 0$ or $n = 0$ and $h > 0$.

(5) The field of fractions of the formal power series ring $k[[x_1, \ldots, x_n]]$ will be denoted, as usual, by $k((x_1, \ldots, x_n))$. We note that this is not a field of generalized Laurent series if $n > 1$. Moreover we note that the fields $k((x_1, x_2))$, $k((x_2))((x_1))$, $k((x_1))((x_2))$ are all distinct. The last two fields are fields of fields of generalized Laurent series for distinct total orders on $\mathbf{Z}^2$ (viz. the lexicographic and reverse lexicographic orders). More generally, if o is the lexicographic order on $\mathbf{Z}^n$, relative to any total order on the integers $1, \ldots, n$, then the field of generalized Laurent series $k((z^{\mathbf{Z}^n,o}))$ is a field of n-fold iterated Laurent series.

(6) More generally, let o be any total order on $\mathbf{Z}^n$ such that $(a_1, \ldots, a_n) \geq 0$ whenever $a_i \geq 0$. The embedding $k[[x_1, \ldots, x_n]] \subset k((z^{\mathbf{Z}^n,o}))$ is defined by $x_i \mapsto z^{e_i}$, where $e_1, \ldots, e_n$ is the standard basis of $\mathbf{Z}^n$. This embedding induces an embedding of fields $k((x_1, \ldots, x_n)) \subset k((z^{\mathbf{Z}^n,o}))$. We note that this is a separable field extension if k is an algebraically closed field having characteristic $p > 0$. Indeed, $\{x_1, \ldots, x_n\}$ is a p-basis of the first field and $\{z^{e_1}, \ldots, z^{e_n}\}$ is a p-basis of the second field.

Corollary 2.2 suffices for proving that the exact sequence $1 \to p(\pi_1(X)) \to \pi_1(X) \to \pi_1'(X) \to 1$ splits in the local and global cases (see Corollaries 3.4(a) and 4.7(a) below) and thus for proving the constraint (i) of the introduction. For the more refined constraints (ii) and (iii) of the introduction, we will need more information on the structure of the finite field extensions of $k((z^{H,o}))$.

Proposition 2.4 *Let K denote the field $k((z^{H,o}))$. Let $L \supset K$ be a finite extension, and let l and I denote the residue field and the value group of L.*
(1) *The valuation of K extends uniquely to a valuation of L.*
(2) *We have $[L:K] = [l:k] \cdot [I:H]$.*
(3) *Suppose that k is algebraically closed and that $L \supset K$ is a Galois extension with Galois group G. Let $H' \subset I$ be the unique subgroup of the abelian group I such that $H' \supset H$, the index $(H':H)$ is prime to p, and $(I:H')$ is a power of p. Then there is a field K' with $K \subset K' \subset L$ such that*
(a) *K' is K-isomorphic to $k((z^{H',o}))$, and $K' \supset K$ is a Galois extension with group isomorphic to H'/H.*

(b) *The Galois group of* $L \supset K'$ *is a* p*-group.*
(c) *One has* $p(G) = \mathrm{Gal}(L/K') =$ *the unique Sylow* p*-subgroup of* G*, and* $G/p(G) = \mathrm{Gal}(K'/K)$.
(d) *There is a subgroup* $A \subset G$ *which maps bijectively to* $G/p(G)$*; i.e. the exact sequence* $1 \to p(G) \to G \to G/p(G) \to 1$ *splits.*

Proof (1) This holds for L/K purely inseparable, so we may assume L/K is Galois. Let G denote its Galois group and let w be an extension of the valuation v to L. The group G operates transitively on the set of all extensions of the valuation v; see [24], Chap. F, Thm. 1, p. 166. Let $D \subset G$ denote the subgroup consisting of the elements $g \in G$ with $g(w) = w$. Then according to [24], Chap. F, Thm. 3, p. 180, the field L^D is an extension of K which has the same value group and the same residue field. By Lemma 2.1 one has $L^D = K$. Thus $D = G$ and w is the unique extension of the valuation v.

(2) (See also [24], Chap. G, Thm. 1, p. 230). We will write v for the additive valuations on K and L. Consider representatives $b_1, \ldots, b_s \in L$ of a basis of l over k and representatives $c_1, \ldots, c_t \in L$ of I/H. The collection $\{b_i c_j\}$ is certainly linearly independent over K. We have to show that it is a basis.

Consider any non-zero element $x \in L$. Then $v(x) = h + v(c_j)$ for some j and some $h \in H$. The image of $x \cdot z^{-h} c_j^{-1}$ in l is non zero. Thus we can write $x = (\sum_i y_i z^h) b_i c_j + \tilde{x}$ with all $y_i \in k$ and $v(\tilde{x}) > v(x)$. If $\tilde{x}$ happens to be 0, then we are done. If not, we have to apply the same procedure to $\tilde{x}$. By "induction" (i.e. proceeding as in the proof of Lemma 2.1), one obtains that x is a K-linear combination of the $\{b_i c_j\}$.

(3) We may consider L as a subfield of $k((z^{\mathbf{Q} \otimes H, o}))$. Choose an element $h' \in H'$ and let m be the smallest positive integer with $mh' \in H$. Write $h := mh'$. Choose $x \in L$ with $v(x) = h'$. Then $v(x^m) = h$ and x^m can be written as $c \cdot z^h \cdot (1 + s)$ with $c \in k^*$ and $s \in L$, $v(s) > 0$. The element c clearly has an m^{th} root.

We claim that $(1 + s)^{1/m}$ lies in L, and hence $z^{h'} \in L$ and $k((z^{H', o})) \subset L$. In order to prove the claim, it suffices to consider the case where $m \neq p$ is prime. The element $f = (1 + s)^{1/m}$ belongs to $k((z^{\mathbf{Q} \otimes H, o}))$ and satisfies $f^m = 1 + s$. If $f \notin L$, then $L(f)/L$ is a cyclic Galois extension of degree m. From part (2) one concludes that the value group $v(L^*)$ of L has index m in the value group of $L(f)$. Take an element $u \in L(f)$ with $v(u) \notin v(L^*)$. Then $1, u, u^2, \ldots, u^{m-1}$ is a basis of $L(f)$ over L. In particular one can write $f = a_0 u^0 + a_1 u + \cdots + a_{m-1} u^{m-1}$ with all $a_i \in L$. The values $v(a_i u^i)$ for the non zero terms are distinct. Thus $v(a_0) = 0$ and $v(a_i u^i) > 0$ for $i \neq 0$. Let $j \geq 1$ be such that $v(a_j u^j)$ is the smallest element of $\{v(a_1 u), \ldots, v(a_{m-1} u^{m-1})\}$. Then $1 + s = a_0^m + m a_0^{m-1} a_j u^j + r$ where $v(r) > v(a_j u^j)$. Thus $v(a_j u^j) = v(1 + s - a_0^m)$. This contradicts $v(u) \notin v(L^*)$, and thereby proves the claim.

The extension $k((z^{H, o})) \subset k((z^{H', o}))$ is clearly Galois with group isomorphic to the prime-to-p group H'/H. This proves (a) of (3). By (2) the degree $[L : k((z^{H', o}))]$ is equal to $[I : H']$, which is a power of p. Thus (b) and (c) and are proved. Finally, since the groups $p(G)$ and $G/p(G)$ have relatively prime order, the exact sequence $1 \to p(G) \to G \to G/p(G) \to 1$ splits [11], Thm. 15.2.2. Thus the required A of part (d) exists. □

Remarks 2.5 (a) A more explicit way to arrive at the required subgroup $A \subset G$ in the above proof is again to consider L as a subfield of $k((z^{\mathbf{Q}\otimes H,o}))$. For every homomorphism $\mu : \mathbf{Q} \otimes H/H \to k^*$ one defines the automorphism σ_μ of the field extension $k((z^{\mathbf{Q}\otimes H,o})) \supset k((z^{H,o}))$ by the formula

$$\sigma_\mu(\sum_{h\in\mathbf{Q}\otimes H} c(h)z^h) = \sum_{h\in\mathbf{Q}\otimes H} \mu(h)c(h)z^h.$$

For every Galois extension $K \subset F$ with F contained in $k((z^{\mathbf{Q}\otimes H,o}))$, the map $\mu \mapsto \sigma_\mu|_F$ is a homomorphism $\mathrm{Hom}(\mathbf{Q} \otimes H/H, k^*) \to \mathrm{Gal}(F/K)$. For the field $F = k((z^{H',o}))$ this homomorphism is clearly surjective. Let A denote the image of $\mathrm{Hom}(\mathbf{Q} \otimes H/H, k^*) \to \mathrm{Gal}(L/K) = G$. Then A maps surjectively to $G/p(G)$. The map is injective since A has no elements of order p.

(b) By Remark (a), a generalized field of Laurent series $k((z^{H,o}))$ has explicit automorphisms! Let $\mu : H \to k^*$ be a group homomorphism. We associate to μ the automorphism σ_μ of $k((z^{H,o}))$ given by the formula $\sigma_\mu(\sum_h c(h)z^h) = \sum_h \mu(h)c(h)z^h$.

We apply the above remark to the field of generalized Laurent series $F := k((z^{\mathbf{Q}^n,o}))$, where k is an algebraically closed field of characteristic $p > 0$ and where the total group order o satisfies $(a_1, \ldots, a_n) \geq (0, \ldots, 0)$ if $a_1, \ldots, a_n \in \mathbf{Q}$ and all $a_i \geq 0$. Let $\mathcal{A}$ be the group of the automorphisms of F consisting of the σ_μ such that the homomorphism $\mu : \mathbf{Q}^n \to k^*$ is trivial on $\mathbf{Z}^n$. By definition, $\mathcal{A} \approx \mathrm{Hom}(\mathbf{Q}/\mathbf{Z}, k^*)^n$. Since k is algebraically closed and has characteristic $p > 0$, one can identify $\mathrm{Hom}(\mathbf{Q}/\mathbf{Z}, k^*)$ with $\widehat{\mathbf{Z}}'$, i.e., the prime-to-p quotient of the profinite completion $\widehat{\mathbf{Z}}$ of $\mathbf{Z}$. In this way $\mathcal{A}$ is identified with $(\widehat{\mathbf{Z}}')^n$.

Applying this to Example 2.3(5), we may choose o so that $k((z^{\mathbf{Z}^n,o}))$ equals $k((x_1))\cdots((x_n)) \subset F$, and we obtain:

Corollary 2.6 *Let k be algebraically closed of characteristic p, write K for the field $k((x_1))\cdots((x_n))$, let $K' = K[x_i^{1/m} \mid 1 \leq i \leq n;\ (m,p) = 1]$, and let K^{sep} be the separable closure of K. Then the surjective homomorphism of groups $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Gal}(K'/K) \approx (\widehat{\mathbf{Z}}')^n$ has a section.*

Proof By Corollary 2.2, $F = k((z^{\mathbf{Q}^n,o}))$ is algebraically closed and hence contains K^{sep}. Any $\sigma_u \in \mathcal{A}$ preserves the property of an element being separably algebraic over K, i.e. leaves K^{sep} invariant as a set. So we have a surjection $\mathcal{A} \to \mathrm{Gal}(K^{\mathrm{sep}}/K)$, whose composition with $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Gal}(K'/K) \approx (\widehat{\mathbf{Z}}')^n$ is an isomorphism on $\mathcal{A}$. The inverse of this isomorphism is the desired section. □

Remarks 2.7 (a) While the above presentation is elementary, Proposition 2.4 and Corollary 2.6 can also be understood in terms of ramification theory of valued fields. Namely, suppose K is a valued field with algebraically closed residue field and with no immediate extensions (as in the above results, by Lemma 2.1). Then K is its own inertia field. Also, the ramification field is an abelian pro-prime-to-p Galois extension of the inertia field, and the separable closure is a Galois pro-p extension of the ramification field; cf. [16], §5. The conclusions of Proposition 2.4(d) and Corollary 2.6 follow from these properties.

(b) See also [19] and [20], §1, Proposition 1, for related results about iterated Laurent series fields.

3 Local covers

In this section we study Galois groups of covers of "local spaces", over an algebraically closed field k of characteristic p. That is, we consider Galois étale covers of $\operatorname{Spec} k[[x_1,\dots,x_n]][(x_1\cdots x_n)^{-1}]$, or equivalently Galois branched covers of $\operatorname{Spec} k[[x_1,\dots,x_n]]$ that are branched only over the locus of $(x_1\cdots x_n)$. The case of tame covers is handled in the following classical result (cf. [10], Theorem 2.3.2, or [2]):

Proposition 3.1 *If $\operatorname{Spec} R \to \operatorname{Spec} k[[x_1,\dots,x_n]]$ is a tamely ramified Galois cover with branch locus contained in the locus of $(x_1\cdots x_r)$ for some $r \le n$, then R is contained in $k[[x_1,\dots,x_n]][x_1^{1/m},\dots,x_r^{1/m}]$ for some integer $m \ge 1$, not divisible by p. The Galois group of the given cover is abelian, of order prime to p, and of rank at most r.*

Proof Let $X = \operatorname{Spec} k[[x_1,\dots,x_n]]$ and let $Y = \operatorname{Spec} R$. Let m be the greatest common divisor of the ramification indices of $Y \to X$ over the divisors (x_i), for $i = 1,\dots,r$; here m is prime to p by the tameness hypothesis. Let $X' = \operatorname{Spec} k[[x_1,\dots,x_n]][x_1^{1/m},\dots,x_r^{1/m}] = \operatorname{Spec} k[[x_1^{1/m},\dots,x_r^{1/m}]]$ and let Y' be the normalization of $Y \times_X X'$. Then X' is regular, and $Y' \to X'$ is étale in codimension 1 by Abhyankar's Lemma. By Purity of Branch Locus, $Y' \to X'$ is étale everywhere. But $k[[x_1^{1/m},\dots,x_r^{1/m}]]$ is a complete local ring with algebraically closed residue field; so Hensel's Lemma implies that Y' is a trivial cover of X' (i.e. a disjoint union of copies of X'). Hence R is contained in $k[[x_1,\dots,x_n]][x_1^{1/m},\dots,x_r^{1/m}]$. The Galois group of the given cover is as claimed, since it is a quotient of that of $X' \to X$, viz. a product of r copies of a cyclic group of order m. □

In particular, the above proposition shows that such a tamely ramified cover has degree prime to p.

We now turn to the more general case, in which wild ramification is permitted — i.e. in which the orders of the inertia groups over the (x_i) can be divisible by p. We first prove a lemma.

Lemma 3.2 *Let E be a field, let $A \supset E[[x]]$ be a finite Galois extension of discrete valuation rings with group G, and let E' be a separable field extension of E (not necessarily algebraic over E). Let A' be the compositum of A and $E'[[x]]$ in an algebraic closure of $E'((x))$, and let $G' = \operatorname{Gal}(A'/E'[[x]])$.*

(a) If $y \in A$ is a uniformizer for A, then y is a uniformizer for A'.

(b) Under the natural inclusion $G' \hookrightarrow G$, the inertia subgroup of G' maps isomorphically onto the inertia subgroup of G.

Proof The ring $B := A \otimes_{E[[x]]} E'[[x]]$ is a complete semi-local ring, since it is finite over $E'[[x]]$. Here B is equal to a product $B_1 \times \cdots \times B_s$ of complete local domains B_i; and the total ring of fractions of B is of the form $L = L_1 \times \cdots \times L_s$, with L_i the field of fractions of B_i. The ring L is an extension of $E'((x))$, and the action of G on B extends to an action on L such that $L^G = E'((x))$. Thus G acts transitively on the components of $\operatorname{Spec}(B)$, i.e. on the factors B_i, or equivalently on the minimal prime ideals $\underline{P_i}$ of B (where $\underline{P_i}$ corresponds to B_i).

Let y generate the maximal ideal of A and put $E_1 := A/(y)$. Then $B/(y) \cong E_1 \otimes_E E'$ since $x \in (y)$. Since E' is a separable extension of E, it follows that $E_1 \otimes_E E'$ is reduced [17], 27.D. Thus $E_1 \otimes_E E'$ is a product of fields $F_1 \times \cdots \times F_s$,

where F_i can be identified with the residue field of B_i. Let $y_i \in B_i$ denote the image of y under the projection $B \to B_i$. Then $B_i/(y_i) = F_i$ and therefore B_i is a complete discrete valuation ring with uniformizer y_i. Each of the B_i can be identified with A', the compositum of A and $E'[[x]]$ in an algebraic closure of $E'((x))$. This proves part (a).

Now identify A' with B_1. The subgroup G' of G consists of the $\sigma \in G$ such that σ fixes $\underline{P}_1$. Let σ be an element of the inertia group of $G = \mathrm{Gal}(A/E[[x]])$. Then σ is the identity modulo (y) and induces the identity on $B/(y)$. In particular $\underline{P}_1$ is fixed under σ and thus σ belongs to the inertia group of G'. Hence G and G' have the same inertia groups. This proves part (b). □

Theorem 3.3 *Suppose that G is the Galois group of a Galois branched cover of* $\mathrm{Spec}\, k[[x_1, \ldots, x_n]]$ *that is branched only over $(x_1 \cdots x_r)$, where $1 \le r \le n$.*

(a) Then $p(G)$ has an abelian supplement of order prime to p and rank $\le r$.

(b) If I is an inertia group over some (x_i), then the abelian supplement A may be chosen so as to normalize the p-group $p(I)$. Hence if p divides the order of G, then A may be chosen so as to normalize a non-trivial p-subgroup of G.

(c) The subgroup $p(G)$ is generated by the collection of p-subgroups that are normalized by such supplements.

Proof The given branched cover corresponds to a finite extension R of the ring $R_0 := k[[x_1, \ldots, x_n]]$. Here R is an integrally closed domain, and $R[(x_1 \cdots x_r)^{-1}]$ is étale over $R_0[(x_1 \cdots x_r)^{-1}]$. Moreover the fraction field of R is a Galois extension, with group G, of the fraction field $F := k((x_1, \ldots, x_n))$ of R_0. By Proposition 3.1, the corresponding $G/p(G)$-extension $\tilde{R} = R^{p(G)}$ of R_0 is contained in the ring $R_0[x_1^{1/m}, \ldots, x_r^{1/m}]$ for some integer $m \ge 1$ not divisible by p. Also $G/p(G)$ is abelian, of order prime to p, and of rank $\le r$, by 3.1.

If the order of G is prime to p, then $p(G) = 1$ and the assertion is immediate from Proposition 3.1. So assume p divides the order of G. We begin by proving parts (a) and (b); and after reordering the x_i's we may assume that $i = 1$.

Let $\phi : F \hookrightarrow K := k((x_n))((x_{n-1})) \cdots ((x_1))$ be the natural embedding given by $\phi(x_i) = x_i$. In the terminology of Section 2, the field K may be identified with the generalized Laurent series field $k((z^{\mathbf{Z}^n, o}))$, where o is the lexicographic order on $\mathbf{Z}^n$, and where x_j is identified with z^{e_j} for $j = 1, \ldots, n$. Let v be the discrete valuation on F associated to (x_1), and let w be a discrete valuation on R (or its fraction field) over v, for which I is an inertia group. The completion of the local ring of R_0 at v is $E[[x_1]]$, where $E = k((x_2, \ldots, x_n))$. Let $\hat{R}_w$ denote the completion of the local ring of R at w, and let L_w denote its field of fractions. Then the inertia group of $\hat{R}_w$ over $E[[x_1]]$ is also I.

Let L be the compositum of L_w and K (as extensions of $E((x_1))$) in an algebraic closure $\bar{K}$ of K. (Thus L can also be viewed as the compositum of R and K in $\bar{K}$.) The extension $K \subset L$ is a finite Galois extension whose Galois group G' is identified with a subgroup of G. Write $E' := k((x_n))((x_{n-1})) \cdots ((x_2))$; this is the generalized Laurent series field $k((z^{\mathbf{Z}^{n-1}, o'}))$, where o' is the lexicographic order on $\mathbf{Z}^{n-1}$. The integral closure of $E'[[x_1]]$ in L is the unique discrete valuation ring of L lying over the discrete valuation of $E'((x_1)) = K$. By Example 2.3(6), E' is separable over E. So viewing G' as a subgroup of G, it follows from Lemma 3.2(b) that the inertia group of G' is the same as that of G over (x_1).

Consider the compositum $\tilde{L}$ of K and $\tilde{R}$. Then $\tilde{L}$ is a subfield of L, and is a Galois extension of K with Galois group $G/p(G)$, since $\tilde{R}$ is linearly disjoint from K over R_0 (because $R_0[x_1^{1/m}, \ldots, x_r^{1/m}]$ is, and $\tilde{R} \subset R_0[x_1^{1/m}, \ldots, x_r^{1/m}]$). So G' maps surjectively to $G/p(G)$, and the map $G'/p(G') \to G/p(G)$ is surjective. Part 3 of Proposition 2.4 asserts that $p(G')$ is a p-group, and provides a prime-to-p abelian subgroup $A_0 \subset G'$ which is a supplement to $p(G')$ in G' and hence to $p(G)$ in G. Since $G/p(G)$ is abelian of rank $\leq r$, there is a subgroup $A \subset A_0$ which is of rank $\leq r$ and is still a supplement to $p(G)$ in G. Since I is normal in G', the subgroup $A \subset G'$ normalizes I and hence its characteristic subgroup $p(I)$. Since $p(G')$ is a p-group, and since $I \subset G'$, it follows that $p(I)$ is a p-group. This proves part (a) and the first part of (b). The second part of (b) follows from Proposition 3.1, since that implies that if p divides the order of G then the cover is not tamely ramified; i.e. some $p(I)$ is non-trivial.

For part (c), let N be the normal subgroup of G generated by the groups $p(I)$, where I ranges over all the inertia groups over the various (x_i)'s. Each $p(I)$ is a p-group contained in $p(G)$, and so $N \subset p(G)$. Now the subcover corresponding to $N \subset G$ is tamely ramified, since N contains each $p(I)$; hence this cover is of degree prime-to-p by Proposition 3.1. So the index of N in G is prime-to-p. Hence $N = p(G)$, i.e. $p(G)$ is generated by the p-groups $p(I)$. The assertion now follows from part (b). □

Corollary 3.4 *Let $X = \operatorname{Spec} k[[x_1, \ldots, x_n]][(x_1 \ldots x_r)^{-1}]$, with $1 \leq r \leq n$.*
(a) Then $\pi_1'(X)$ is isomorphic to $\hat{\mathbf{Z}}'^r$, and the exact sequence

$$1 \to p(\pi_1(X)) \to \pi_1(X) \to \pi_1'(X) \to 1 \text{ splits.} \qquad (*)$$

(b) The group $p(\pi_1(X))$ is generated by the collection of pro-p-subgroups P such that P is normalized by the image of some splitting of the exact sequence.

Proof Let $R_0 = k[[x_1, \ldots, x_n]]$, let $S_0 = R_0[(x_1 \ldots x_r)^{-1}]$, and let S [resp. S'] be the maximal unramified [resp. maximal pro-prime-to-p unramified] extension of S_0. By Proposition 3.1, S' is the union of the rings $S_0[x_1^{1/m}, \ldots, x_r^{1/m}]$, as m ranges over positive integers prime to p. The Galois group of this extension is $\hat{\mathbf{Z}}'^r$, so the first part of (a) follows.

Let R be the integral closure of R_0 in S, let $1 \leq i \leq r$, and let I be an inertia group of R over the ideal (x_i) of R_0. Consider the following

Claim: The subgroup $p(I) \subset I$ is a pro-p-group, and there is a splitting $\sigma : \pi_1'(X) \to \pi_1(X)$ of $(*)$ whose image normalizes $p(I)$.

Once this is proven, the second part of (a) is automatic, and part (b) also follows because the various inertia groups I generate $\pi_1(X)$ (since $\operatorname{Spec} R_0$ has no unramified covers). So it remains to prove the claim.

For each normal subgroup $N \subset \pi_1(X)$ of finite index, let $G_N = \pi_1(X)/N$, let $I_N = I/(I \cap N)$, and let Σ_N be the set of prime-to-p abelian supplements A_N to $p(G_N)$ in G_N that are of rank $\leq r$ and that normalize $p(I_N)$. Then I_N is an inertia group over (x_i) for a G_N-Galois cover of X, and so $p(I_N)$ is a p-group. Thus $I = \varprojlim I_N$ is a pro-p-group. By Theorem 3.3(b), Σ_N is a non-empty set (which is finite, since G_N is). Since the inverse limit of a non-empty family of non-empty finite sets is non-empty, we have that $\Sigma := \varprojlim \Sigma_N$ is non-empty. Let $A \in \Sigma$. Then A is an abelian pro-prime-to-p subgroup of $\pi_1(X)$ which is topologically generated

by a set of $m \leq r$ elements and which normalizes $p(I)$. Moreover A is a supplement to $p(\pi_1(X))$, i.e. A surjects onto $\pi_1'(X) \approx \hat{\mathbf{Z}}'^r$. Since $m \leq r$, it follows that $A \approx \hat{\mathbf{Z}}'^r$ and the surjection $A \to \pi_1'(X)$ is an isomorphism. So the inverse of this isomorphism is a splitting $\sigma : \pi_1'(X) \to A \subset \pi_1(X)$ of $(*)$ whose image normalizes $p(I)$. This proves the claim, and hence the Corollary. □

Remark 3.5 A splitting in Corollary 3.4 can be described explicitly, in terms of the group $\mathcal{A} \subset \mathrm{Aut}(J/K)$ described at the end of Section 2, where $K = k((z^{\mathbf{Z}^n,o}))$ and $J = k((z^{\mathbf{Q}^n,o}))$. For simplicity take $r = n$. The natural embedding of $F = k((x_1,\ldots,x_n))$ into K extends to an embedding $\phi : F^{\mathrm{sep}} \hookrightarrow J$. Consider the infinite intermediate Galois extensions $F \subset L_1 \subset L_2 \subset F^{\mathrm{sep}}$ corresponding to the groups $\pi_1'(X)$ and $\pi_1(X)$. By linear disjointness (as in the proof of Theorem 3.3), the Galois group of $\phi(L_1)K/K$ is again $\pi_1'(X)$. The Galois group H of the Galois extension $\phi(L_2)K/K$ is a subgroup of $\pi_1(X)$. The group $\mathcal{A}$, which is isomorphic to $\hat{\mathbf{Z}}'^n$, leaves the fields $\phi(L_1)$ and $\phi(L_2)$ setwise invariant. The actions of $\mathcal{A}$ on $\phi(L_1)$ and $\phi(L_2)$ induce continuous homomorphisms $\mathcal{A} \to \pi_1'(X)$ and $\mathcal{A} \to H \subset \pi_1(X)$, where the former is an isomorphism. The composition $\mathcal{A} \to \pi_1(X) \to \pi_1'(X)$ is a continuous isomorphism which yields the required splitting.

The natural embedding of $F = k((x_1,\ldots,x_n))$ into $K = k((z^{\mathbf{Z}^n,o}))$ gives us an inclusion $\mathrm{Gal}(K^{\mathrm{sep}}/K) \hookrightarrow \mathrm{Gal}(F^{\mathrm{sep}}/F)$. The natural surjection $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Gal}(K'/K) \approx \hat{\mathbf{Z}}'^n$ (where K' is as in Corollary 2.6) is the composition of the above inclusion and the natural surjection $\mathrm{Gal}(F^{\mathrm{sep}}/F) \to \hat{\mathbf{Z}}'^n$. Moreover this latter surjection factors through the surjection $\pi_1(X) \to \pi_1'(X)$ in Corollary 3.4. So by Corollary 2.6 we obtain:

Corollary 3.6 *Let $X = \mathrm{Spec}\, k[[x_1,\ldots,x_n]][(x_1\cdots x_r)^{-1}]$ and let F be the function field of X. Then the natural surjection $\mathrm{Gal}(F^{\mathrm{sep}}/F) \to \pi_1'(X) \approx \hat{\mathbf{Z}}'^n$ has a section which lifts a section of $\pi_1(X) \to \pi_1'(X)$ in Corollary 3.4(a).*

4 Coverings of the complement of a hypersurface in a projective space

We now turn to covers of "global spaces" over an algebraically closed field k of characteristic p. In particular, we consider spaces X that are of the form $\mathbf{P}^n_k - D$, where D is a divisor in $\mathbf{P}^n_k$. Here, we require D to have only normal crossings as singularities (or for short, to be a "normal crossings divisor"). That is, for every point Q on D, we require that the ideal of D in the complete local ring $\hat{\mathcal{O}}_{\mathbf{P}^n,Q}$ of Q is generated by an element of the form $y_1\cdots y_t$, where $\{y_1,\ldots,y_n\}$ is a basis of the maximal ideal of $\hat{\mathcal{O}}_{\mathbf{P}^n,Q}$ and $1 \leq t \leq n$. (There is also a more restrictive notion of "strong normal crossing", which requires that each irreducible component of D be smooth; but we allow the more general notion here.)

Theorem 4.1 [Abhyankar, Fulton] *Let $n > 1$, and let D be a divisor with normal crossings in $\mathbf{P}^n_k$. Let G be the Galois group of a Galois branched cover of $\mathbf{P}^n$ that is at most tamely ramified over D and is étale elsewhere. Then G is abelian.*

Proof The inertia group along any irreducible component of the ramification locus is cyclic, since the cover is tamely ramified. Also, since $\mathbf{P}^n_k$ has no unramified covers (by applying Bertini's Theorem to reduce to the well-known case of $n = 1$), the inertia groups of the components of the ramification locus together generate G.

If two components of the ramification locus meet at a point Q_1 of the cover over a point $Q \in \mathbf{P}^n$, then their inertia groups are contained in the inertia group at Q_1. Passing to the complete local rings at Q and Q_1, it follows from Proposition 3.1 that the inertia group at Q_1 is abelian and hence the inertia groups of the two components commute. So to prove the theorem, it suffices to prove that any two components of the ramification locus meet; and this in turn follows from the following

Claim. There is only one irreducible component of the ramification locus over each irreducible component of the branch locus.

We now prove the claim. Let $D = \sum D_j$ be the branch locus of the tamely ramified cover $f : Y \to \mathbf{P}^n$, where D is a divisor with normal crossings. We want to show that $E_j := f^{-1}(D_j)$ is irreducible. Let $g : \tilde{D}_j \to D_j \subset \mathbf{P}^n$ be the normalization of D_j, and let $\tilde{E}_j = \tilde{D}_j \times_{\mathbf{P}^n} E_j$. Thus $\tilde{D}_j$ is smooth.

A local analysis shows that $\tilde{E}_j$ is also smooth. Namely, suppose that a point P on D_j is an r-fold normal crossing on D, and a t-fold normal crossing on D_j (with $t \leq r$). After a change of variables, we may assume that locally near P (i.e. in the complete local ring at P), the divisor D is given by $x_1 \cdots x_r = 0$, and D_j is given by $x_1 \cdots x_t = 0$. Replacing Y by a cover, we may assume by Proposition 3.1 that Y is given locally by $y_i^{m_i} = x_i$, with $i = 1, \ldots, r$, and that E_j is given locally by $y_1 \cdots y_t = 0$. So locally, $\tilde{E}_j$ is the disjoint union of the loci $y_i = 0$, for $i = 1, \ldots, t$; and this is smooth.

So to prove that E_j is irreducible, it suffices to show that $\tilde{E}_j$ is connected. This follows from the Fulton-Hansen connectedness theorem [7], which says that V is an irreducible projective variety of dimension $> n$, and $F : V \to \mathbf{P}^n \times \mathbf{P}^n$ is finite, then $F^{-1}(\Delta)$ is connected, where Δ is the diagonal. Here, taking $V = \tilde{D}_j \times Y$, and taking $F = g \times f$, we have that V is of dimension $2n-1$ (which is $> n$ since $n > 1$). So $\tilde{E}_j = \tilde{D}_j \times_{\mathbf{P}^n} E_j = F^{-1}(\Delta)$ is irreducible, as asserted, proving the claim. □

Corollary 4.2 [Abhyankar, Fulton] *Let $n > 1$, and let D be a divisor with normal crossings in $\mathbf{P}^n$, having irreducible components $D_1, \ldots, D_r$ of degrees $d_1, \ldots, d_r$. Let q be the largest power of p that divides all the d_i, and let $d_i' = d_i/q$.*

(a) Let $Y \to \mathbf{P}^n$ be a tamely ramified Galois cover branched only at D. Then for some integer $m \geq 1$, Y is dominated by a cover of the form $y_i^m = f_i$ (for $i = 1, \ldots r$), where f_i defines D_i on the complement of a hyperplane. If the cover is cyclic of degree m prime to p, then it is given by an equation of the form $y^m = \prod f_i^{a_i}$, for some integers $a_i \geq 0$ such that $\sum a_i d_i \equiv 0 \pmod m$.

(b) $\pi_1^{\mathrm{t}}(\mathbf{P}^n, D) = \pi_1'(\mathbf{P}^n - D) = \hat{\mathbf{Z}}'^r/(d_1, \ldots, d_r)\hat{\mathbf{Z}}' = \hat{\mathbf{Z}}'^r/(d_1', \ldots, d_r')\hat{\mathbf{Z}}'$, with the ith coordinate vector of $\hat{\mathbf{Z}}'^r$ mapping to a generator of the unique inertia group over D_i.

Proof (a) After a change of variables we may assume that no D_i is the hyperplane H at infinity where $x_{n+1} = 0$. Working in affine coordinates on $\mathbf{A}^n = \mathbf{P}^n - H$, let D_i be given by the polynomial $f_i \in k[x_1, \ldots, x_n]$. First consider a cyclic tamely ramified cover $Y \to \mathbf{P}^n$, say of degree m. If p divides m, then Y has a tamely ramified subcover of degree p; a contradiction, since that cover would have to be unramified over $\mathbf{P}^n$, which is simply connected. So m is prime to p. By Kummer theory, the function field of Y is given by $F[f^{1/m}]$, where $F = k(x_1, \ldots, x_n)$ and $f \in k[x_1, \ldots, x_n]$ is of the form $\prod f_i^{a_i}$, with $a_i \geq 0$. Since the cover is unramified

over the hyperplane at infinity, we have that $\sum a_i d_i \equiv 0 \pmod m$. By the above, a cyclic tame cover is dominated by a cover of the form $y_i^m = f_i$, where $i = 1, \dots r$. Hence the same follows for all abelian tamely ramified covers.

(b) Let $F^* := F[x_i^{1/m} \,|\, 1 \le i \le r; (m,p) = 1]$ and let $\tilde{F}$ be the maximal subextension of F^* that is unramified over H, the hyperplane at infinity. By (a), the function fields of tamely ramified covers of $\mathbf{P}^n$ branched at D are precisely the finite subextensions of $\tilde{F}$ over F. Now $\mathrm{Gal}(F^*/F) = \hat{\mathbf{Z}}'^r$, with the ith coordinate vector generating inertia over D_i. Also, $\tilde{F}$ is the fixed field of $\{(a_1, \dots, a_r) \,|\, \sum d_i a_i = 0\}$. So $\mathrm{Gal}(\tilde{F}/F) = \hat{\mathbf{Z}}'^r/(d_1, \dots, d_r)\hat{\mathbf{Z}}' = \hat{\mathbf{Z}}'^r/(d_1', \dots, d_r')\hat{\mathbf{Z}}'$, which is a pro-prime-to-p group. So $\pi_1^{\mathrm{t}}(\mathbf{P}^n, D) = \pi_1'(\mathbf{P}^n - D) = \mathrm{Gal}(\tilde{F}/F)$, and (b) is shown. □

Remark 4.3 The above results were stated in [2], but the claim in the proof of Theorem 4.1 was proven in [2] only in the case of *strong* normal crossings (i.e. assuming also that each component of D is smooth). See also [25] for a brief presentation of Abhyankar's proof in that case. Later, Fulton ([6], cf. also Deligne [5]) proved the claim without the hypothesis of smooth components; but the proof there was given only for $n = 2$. The proof extends to general $n \ge 2$, though; and that is what we have given above. (Fulton also says in [6] that the result with $n = 2$ can be used to deduce the following assertion in dimension $n > 2$: If $Y \to \mathbf{P}^n$ is a tamely ramified Galois cover whose branch locus D has the property that a generic plane section of D is a curve with only normal crossings, then the Galois group is abelian.)

The above results have the following consequence:

Corollary 4.4 *Let $n > 1$, and let D be a normal crossing divisor in $\mathbf{P}_k^n$ with irreducible components $D_1, \dots, D_{n+1}$. Let Q be a point of $\mathbf{P}^n$ lying in $D_1 \cap \cdots \cap D_n$, and suppose that the degree of D_{n+1} is a power of p. Then any tamely ramified Galois branched cover of $\mathbf{P}^n$ that is étale away from D is totally ramified over Q.*

Proof Let G be the Galois group and let d_i be the degree of D_i. Thus $d_{n+1} = p^u$ for some $u \ge 0$. By Corollary 4.2, the natural surjection $\pi : \hat{\mathbf{Z}}'^{n+1} \to G$, which maps the ith coordinate vector to a generator of inertia over D_i, has the property that its kernel contains $(d_1, \dots, d_n, p^u)$. Choose an integer m such that $mp^u \equiv 1$ modulo the order of the Galois group G. Then the kernel of π also contains $(md_1, \dots, md_n, mp^u)$ and hence contains $(md_1, \dots, md_n, 1)$. Thus the inertia group over D_{n+1} is contained in the subgroup of G generated by the inertia groups over the other D_i. Since the inertia groups together generate G (because $\mathbf{P}^n$ is simply connected), the result follows. □

We now come to the key result:

Theorem 4.5 *Let $n > 1$, and let D be a reduced hypersurface in $\mathbf{P}_k^n$ with irreducible components $D_1, \dots, D_r$ of degrees $d_1, \dots, d_r$, and with $r \le n+1$. Suppose that D has only normal crossings. Let $X = \mathbf{P}_k^n - D$ and let $Y \to X$ be a Galois finite étale cover of X with group G.*

(a) Suppose either that $r \le n$, or that some d_i is a pth power. Then there is an abelian supplement $A \subset G$ to $p(G)$ having rank at most $\max(r, n)$, and having order prime to p.

(b) Suppose either that $r \leq n$ and $p(G) \neq 1$, or that d_i is a pth power and D_j is wildly ramified for some pair $i \neq j$. Then A may be chosen to normalize a non-trivial p-subgroup of G.

(c) Suppose either that $r \leq n$, or that at least two d_i's are pth powers, or that some d_i is a pth power and the corresponding D_i is tamely ramified. Then $p(G)$ is generated by the set of p-subgroups $P \subset G$ such that P is normalized by some choice of A.

Proof By Corollary 4.2(b), the group $G/p(G)$ has a generating set of at most $\max(r, n)$ elements (using that some d_i is a pth power, in the case that $r = n+1$). So if A is any abelian supplement to $p(G)$ in G that has order prime to p and normalizes some subgroup $P \subset G$, then A contains a subgroup A_0 that is generated by at most $\max(r, n)$ elements and also has the other properties of A. So it suffices to prove the result without the condition on the rank of A. In the remainder of this proof, this is what we do.

(a) The first case (i.e. $r \leq n$) reduces to the second case, since if $r \leq n$ we may adjoin lines $D_{r+1}, \ldots, D_{n+1}$ such that the enlarged divisor still has normal crossings. So assume we are in that case. After reordering the components, we may assume that d_{n+1} is a power of p, say p^u with $u \geq 0$. Take a point Q in the intersection $D_1 \cap \cdots \cap D_n$. Let $Y_2 \to Y_1 \to \mathbf{P}^n$ denote the branched covers corresponding to G and $G/p(G)$. By Corollary 4.4, $Y_1 \to \mathbf{P}^n$ is totally ramified over Q; let $Q_1 \in Y_1$ be the unique point over Q. Choose a point $Q_2 \in Y_2$ above Q_1. Then the stabilizer $G' \subset G$ of Q_2 maps surjectively to $G/p(G)$. That is, $G'/p(G') \to G/p(G)$ is an isomorphism, and so every supplement to $p(G')$ in G' is also a supplement to $p(G)$ in G. After completing the two local rings at Q and Q_2, and using that D has normal crossings, one obtains from the above a finite extension $k[[x_1, \ldots, x_n]] \subset R$ where R is an integrally closed domain; its field of fractions is a Galois extension, with group G', of the field of fractions $F := k((x_1, \ldots, x_n))$ of $R_0 := k[[x_1, \ldots, x_n]]$; and $R_0[(x_1 \cdots x_n)^{-1}] \subset R[(x_1 \cdots x_n)^{-1}]$ is étale. By Theorem 3.3(a), there is an abelian prime-to-p supplement A to $p(G')$ in G'. Any such A is a supplement to $p(G)$ in G.

(b) Again we may assume that we are in the second case. Namely, in the first case, some D_j (with $j \leq r$) is wildly ramified (by Theorem 4.1), and we may adjoin lines $D_{r+1}, \ldots, D_{n+1}$ as in (a), with $d_i = 1$, a power of p, for $r < i \leq n+1$. This reduces us to the latter case, and after renumbering the components of G, we may assume that $i = n + 1$.

Retaining the notation from the proof of (a), we have that $Y_2 \to \mathbf{P}^1$ is wildly ramified over Q, since it is wildly ramified over D_j. Thus the order of G' is divisible by p. So by the second part of Theorem 3.3(b) applied to G', the group A above may be chosen to normalize a non-trivial p-subgroup of $G' \subset G$.

(c) By adding extra lines, the first case reduces to the third. The second and third cases are subsumed by the hypothesis that for every component D_i of D that is wildly ramified, there is a $j \neq i$ such that d_j is a pth power. So assume that condition. Since every tamely ramified cover is of degree prime-to-p by Corollary 4.2, it suffices to show that if D_i is wildly ramified and if I is an inertia group over D_i, there is a choice of A in (a) that normalizes $p(I)$ (which is a p-group since I is an inertia group over the generic point of a divisor). After reordering the components of D, we may assume that $i = 1$ and that d_{n+1} is a pth power. Let D_1' be a component of the ramification locus of $Y_2 \to \mathbf{P}^1$, lying over D_1, and having

inertia group I. With notation as in (a), choose Q_2 such that D_1' passes through Q_2. So by the first part of Theorem 3.3(b) applied to G', the group A in (a) may be chosen to normalize $p(I)$. □

Corollary 4.6 *Let $n > 1$ and $0 \leq r \leq n$, let $D \subset \mathbf{P}^n$ be the locus of $x_0 \cdots x_r = 0$, and let $X = \mathbf{P}^n - D$. Then the Galois group of any Galois étale cover of X satisfies these properties:*

(i) There is an abelian supplement $A \subset G$ to $p(G)$ having rank at most r, and having order prime to p.

(ii) The group A in (i) may be chosen to normalize a non-trivial p-subgroup of G, if p divides the order of G.

(iii) $p(G)$ is generated by the set of p-subgroups $P \subset G$ such that P is normalized by some choice of A in (i).

Proof Apart from the assertion on rank, this is a special case of Theorem 4.5. But $G/p(G)$ has rank r by Corollary 4.2, since each component of D has degree 1. So as in the comments at the beginning of the proof of Theorem 4.5, we may replace A by a subgroup A_0 of rank $\leq r$, which has the same properties. □

Corollary 4.7 *Let $n > 1$, and let D be a normal crossings hypersurface in $\mathbf{P}^n_k$ having at most $n+1$ irreducible components. Let $X = \mathbf{P}^n - D$.*

(a) If $r \leq n$ or the degree of some irreducible component of D is a pth power, then the exact sequence

$$1 \to p(\pi_1(X)) \to \pi_1(X) \to \pi_1'(X) \to 1$$

splits. This splitting may be chosen so that its image normalizes a non-trivial pro-p-subgroup of $\pi_1(X)$.

(b) If $r \leq n$ or at least two irreducible components of D have degrees that are pth powers, then $p(\pi_1(X))$ is generated by the set of pro-p-subgroups $P \subset \pi_1(X)$ such that P is normalized by the image of some choice of section.

Proof This follows from Theorem 4.5 in the same way that Corollary 3.4 followed from Theorem 3.3, and using in the second part of (a) above the fact that there exist covers that are wildly ramified over every component of D. □

In particular, Corollary 4.7 applies if $D = (x_0 \cdots x_r = 0)$, a union of coordinate hyperplanes. In this situation $\pi_1'(X)$ is isomorphic to $\hat{\mathbf{Z}}'^r$ by Corollary 4.2(b), so $\pi_1(X)$ is a split extension of a free abelian pro-prime-to-p group of rank r by a pro-quasi-p group. Moreover the possible splittings satisfy the extra normalizing condition of 4.7(b).

5 Which groups are Galois groups of covers?

We return to the problem of finding $\pi_A(X)$, the class of finite Galois groups over X, in either the local or the global case. We would like to describe $\pi_A(X)$ in terms of the (known) class of prime-to-p groups in $\pi_A(X)$. We show here that the results of Sections 3 and 4, which provide additional necessary conditions for a group to be in $\pi_A(X)$, contradict the higher dimensional case of Abhyankar's Conjecture 1.1. (The fact that these conditions are really new restrictions is group-theoretic, and follows from the Appendix to this paper.) We also show that Abhyankar's Conjecture fails in general for curves over finite fields, because of similar extra conditions there. In

all these situations, the extra conditions suggest possible variations on Abhyankar's Conjecture which would generalize the classical case of curves over an algebraically closed field, and which may possibly apply more generally.

Let X be a variety over a field k of characteristic p. For any finite group G, let $\mathcal{S}(G)$ be the set of prime-to-p supplements H to $p(G) \subset G$ such that $H \in \pi_A(X)$. Also, let $\mathcal{P}(G)$ be the set of p-subgroups $P \subset G$ that are normalized by some $H \in \mathcal{S}(G)$ (which can depend on P). We then have six classes of finite groups, viz. those satisfying each of these (progressively stronger) conditions in turn:

(1) $G/p(G) \in \pi_A(X)$.
(2) $\mathcal{S}(G)$ (or equivalently, $\mathcal{P}(G)$) is nonempty.
(3) $\mathcal{P}(G)$ contains a nontrivial p-group, or $p(G) = 1 \in \mathcal{P}(G)$.
(4) The groups in $\mathcal{P}(G)$ together generate $p(G)$.
(5) $p(G)$ is the normal closure of some P in $\mathcal{P}(G)$.
(6) $\mathcal{P}(G)$ contains a Sylow p-subgroup of G.

(By definition of $\mathcal{S}(G)$ and $\mathcal{P}(G)$, the condition $p(G) = 1 \in \mathcal{P}(G)$ in (3) is equivalent to saying that $p(G) = 1$ and $G \in \pi_A(X)$.)

Condition (1) is trivially necessary in order for G to be a Galois group over X. In several situations, Abhyankar has conjectured that (1) is also sufficient. We consider several key cases, over a field k of characteristic p:

Example 5.1 Let X be an affine k-curve, with k algebraically closed. Thus X is obtained by deleting $r \geq 1$ points from a smooth projective curve of genus $g \geq 0$. Then Abhyankar's Conjecture holds for X, i.e. condition (1) is necessary and sufficient for a finite group G to lie in $\pi_A(X)$. In this situation, a prime-to-p group is in $\pi_A(X)$ if and only if it can be generated by a set of $2g+r-1$ elements or fewer; i.e. if and only if the group is a quotient of the free group on $2g + r - 1$ generators. Because of this freeness, conditions (1)-(6) are all equivalent to each other, and to the condition that $G \in \pi_A(X)$. Indeed, in [12], Abhyankar's Conjecture was shown by proving that every group that satisfies (6) in this situation must be a Galois group over X, and then observing that conditions (1) and (6) are equivalent here.

Example 5.2 Let $X = \operatorname{Spec} k[[x_1, \ldots, x_n]][(x_1 \cdots x_r)^{-1}]$, where $n > 1$ and $1 \leq r \leq n$, and where k is algebraically closed. By Theorem 3.3, in order for G to be a Galois group over X, not only is condition (1) necessary, but (2), (3), and (4) are as well. In this situation, a prime-to-p group is in $\pi_A(X)$ if and only if it is abelian and can be generated by a set of r elements or fewer.

Consider in particular the case of $r = 2$. Then conditions (1)-(6) are inequivalent, by the Appendix. (Namely, Theorem 6.1 of the Appendix shows that conditions (F1)-(F6) there are distinct for the class of prime-to-p abelian groups of rank ≤ 2, i.e. to conditions (1)-(6) above.) Thus Abhyankar's local conjecture in higher dimensions does not hold — e.g. any group that satisfies (1) but not (2) will not occur. Moreover, conditions (2) and (3) are also insufficient to imply that a group is in $\pi_A(X)$. One might ask whether condition (4) is both necessary and sufficient, or perhaps whether one of the two strictly stronger conditions (5) or (6) is. This remains open.

On the other hand, if $r = 1$, then conditions (1)-(6) are all equivalent. It is thus natural in this case to expect Abhyankar's Conjecture to hold in that case —

i.e. that these conditions are necessary and sufficient for a finite group G to be a Galois group over X. But this too remains open.

Example 5.3 Let X be the complement of a normal crossings divisor D in $\mathbf{P}^n_k$, with $n > 1$, and where k is algebraically closed. Say D has irreducible components $D_1, \dots, D_r$, with D_i of degree d_i. By Corollary 4.2, a prime-to-p group is in $\pi_A(X)$ if and only if G is abelian and has generators $g_1, \dots, g_r$ such that $\prod g_i^{d_i} = 1$. If some d_i is a pth power, then this condition is equivalent to the group being abelian and generated by $r-1$ or fewer elements (since the ith generator can be omitted). In this situation, conditions (1)-(6) are the same as in the previous example, but with $r-1$ instead of r. Thus the conditions are again strictly increasing in strength, by the Appendix. By Theorem 4.5(a) and (b), any finite group in $\pi_A(X)$ satisfies conditions (2) and (3). If at least two d_i's are pth powers, then any finite group in $\pi_A(X)$ satisfies condition (4), by Theorem 4.5(c). So this holds if all $d_i = 1$.

In particular, consider the case of $r = 3$ and all $d_i = 1$, i.e. X is the complement of three coordinate hyperplanes in $\mathbf{P}^n$ (with $n \geq 2$). By the above, any Galois group over X satisfies condition (4). The Appendix shows that (4) is strictly stronger then (1), and so Abhyankar's Conjecture does not hold here. That is, condition (1) is insufficient to guarantee that a group is in $\pi_A(X)$. Again, one can ask whether one of (4), (5), and (6) is both necessary and sufficient. This too is open.

On the other hand, if $r \leq 2$ then again the six conditions are equivalent to each other. Moreover, in these situations, Abhyankar's Conjecture does hold for X; i.e. these conditions are necessary and sufficient for a group G to be a Galois group over X. Namely, (1) is necessary, as always. In the other direction, note that (1) is equivalent to $G = p(G)$ if $r = 1$, and is equivalent to $G/p(G)$ being cyclic if $r = 2$. Since $X \approx \mathbf{A}^1 \times \mathbf{P}^{n-1}$ if $r = 1$, and $X \approx (\mathbf{A}^1 - \{0\}) \times \mathbf{P}^{n-1}$ if $r = 2$, sufficiency follows from Abhyankar's Conjecture for $\mathbf{A}^1$ [23] and for $\mathbf{A}^1 - \{0\}$ [12].

Example 5.4 Let k be a finite field of characteristic p, and let X be an affine open subset of $\mathbf{P}^1_k$, say with $r \geq 1$ points missing. Let $\bar{k}$ be an algebraic closure of k and let $\bar{X} = X \times_k \bar{k}$. We have the fundamental exact sequence

$$1 \to \pi_1(\bar{X}) \to \pi_1(X) \to G_k \to 1$$

where $G_k = \mathrm{Gal}(\bar{k}/k)$. Since G_k is pro-cyclic and $\pi_1'(\bar{X})$ is free pro-prime-to-p of rank $r-1$, it follows that any finite prime-to-p group in $\pi_A(X)$ must be an extension of a cyclic group by a group of rank $\leq r-1$. (This disproves a recent suggestion by Abhyankar that *any* finite group G is a Galois group over X if $G/p(G)$ has rank $\leq r$.)

In particular take $r = 2$ and $X = \mathbf{A}^1_k - \{0\}$. If G is the Galois group of an étale cover $Y \to X$, then $G/p(G)$ is metacyclic (i.e. cyclic-by-cyclic). Let $K = k((x))$, the fraction field of the complete local ring of $\mathbf{P}^1_k$ at $x = 0$. Let $\hat{X} = \mathrm{Spec}\, K$ and let $\hat{Y}$ be a connected component of the pullback $Y \times_X \hat{X}$. Then $\hat{Y} \to \hat{X}$ corresponds to a Galois field extension of K, with group $H \subset G$. Here $Y \to X$ extends to a cover of $\mathbf{P}^1_k$ branched at $\{0, \infty\}$, and H is the decomposition group at some point over 0 (corresponding to the choice of connected component $\hat{Y}$). Since k is a finite field of characteristic p, the inertia group $I \subset H$ has a unique Sylow p-subgroup P; the subgroup P is normal in the decomposition group H; and H/P is metacyclic. By [12], Lemma 5.3 (or by the Schur-Zassenhaus Theorem [8]), $p(H)$ has a prime-to-p supplement $E \subset H$ that normalizes a given Sylow p-subgroup of H. Thus E is also

a supplement to $p(G)$ in G. Now the composition $E \hookrightarrow H \to H/P$ is injective, since E is prime-to-p whereas the kernel of $H \to H/P$ is a p-group. So E is metacyclic.

The above may be done in turn for each of the points over 0, and we may similarly proceed with the points over ∞. The p-groups $p(D)$, where D ranges over all the decomposition groups of $Y \to X$ over 0 and ∞, together generate $p(G)$; while $p(D)$ is generated by the Sylow p-subgroups of D. Thus we have proven

Theorem 5.5 *Let k be a finite field of characteristic p, and let G be the Galois group of a Galois finite étale cover of $X = \mathbf{A}^1_k - \{0\}$. Then $p(G)$ has a prime-to-p metacyclic supplement $A \subset G$. Moreover, this supplement may be chosen to normalize a non-trivial p-subgroup of G provided $p(G) \neq 1$; and the set of p-subgroups that can be normalized by such supplements together generate $p(G)$.*

This result is an analog of Theorems 3.3 and 4.5. The above proof is also analogous to the proofs of those results, using $k((x))$ here rather than the fields of generalized Laurent series there.

Example 1a of Section 6.4 of the Appendix now shows that Abhyankar's Conjecture does not hold for $X = \mathbf{A}^1_k - \{0\}$; i.e. that there are finite groups G such that $G/p(G)$ is in $\pi_A(X)$ but G is not in $\pi_A(X)$. Namely, take any pair of distinct odd primes r, p such that r divides $p-1$ (so that k contains a primitive rth root of unity). Let $A = (\mathbf{Z}/r\mathbf{Z})^2$. Then A is a Galois group of a Galois étale cover $Y \to X$, viz. Y is given over k' by $y^r = x$, where k'/k is the field extension of degree r. Example 1a of Section 6.4 of the Appendix gives a group G such that $G/p(G) \approx A$ but such that $p(G)$ has no prime-to-p metacyclic supplement in G; and so Theorem 5.5 shows that G is not a Galois group over X.

On the other hand, for the affine line $\mathbf{A}^1_k$, Abhyankar's Conjecture remains open. In this case, the conjecture says that π_A consists of the cyclic-by-quasi-p groups, with the cyclic part corresponding to Frobenius. As in the case $r = 1$ of Example 5.2 and the case $r = 2$ of Example 5.3, conditions (1)-(6) are all equivalent here, suggesting that the conjecture holds in this situation.

At the other extreme, there is the Inverse Galois Problem over $k(x)$; this can be viewed as the case in which every point of $\mathbf{A}^1_k$ is permitted to be in the branch locus. The expectation is that every finite group occurs over $k(x)$; and this expectation is equivalent to Abhyankar's Conjecture 1.1 over $k(x)$ if every finite *prime-to-p* group is a Galois group over $k(x)$. Whether that latter property holds is open in general, but it is known to hold if $p = 2$ (since every odd ordered group is solvable by the Feit-Thompson Theorem, and every solvable group is a Galois group over the global field $k(x)$ by Shafarevich's Theorem). But by the Appendix, conditions (1)-(6) are all equivalent if π'_A is the class of all finite prime-to-p groups. So this suggests that the Inverse Galois Problem should have an affirmative answer for $k(x)$, with k a finite field of characteristic p, at least if $p = 2$.

6 Supplements in p' by quasi p-groups

Appendix by Robert Guralnick. [1]

6.1 Introduction. This appendix considers several group-theoretic conditions that are motivated by the preceding paper, and proves results that are used in Section 5 of that paper.

[1]The author thanks MSRI for its hospitality during the Fall 1999 semester and acknowledges the support of NSF grant DMS 9970305.

We first recall some notation. If X and Y are subsets of a group G, we let XY denote the set of products xy, $x \in X, y \in Y$. If X is a normal subgroup and Y is a subgroup, then $XY = YX$ is a subgroup of G. If $G = XY$, we say that Y is a *supplement* to X in G. If, in addition, $X \cap Y = 1$, we say that Y is a *complement* to X. If X is normal and Y is a complement to X, then G is a semidirect product of X and Y.

Let $\mathcal{C}$ be a class of finite groups. Motivated by the previous article, we consider the general problem of given a finite group G with a normal subgroup Q such that G/N is in $\mathcal{C}$, when does there exist a subgroup H of G such that $G = QH$ with H in $\mathcal{C}$. Note that if this is the case, then G is the homomorphic image of a semidirect product QJ with $J \cong H$. Thus, one may be able to reduce questions about extensions to split extensions.

Now fix a prime p. More precisely, we focus on the case when $Q = p(G)$ is the subgroup generated by all the Sylow p-subgroups of G (and so G/Q is a p'-group, i.e. a group whose order is not divisible by p). A group H is said to be a *quasi p-group* if $H = p(H)$.

Recall that a group is *metacyclic* if it is cyclic-by-cyclic (i.e an extension of a cyclic group by a cyclic group). If $\mathcal{C}$ is any class of abelian groups closed under quotients containing a rank 2 p'-group or is the class of metacyclic groups (or metacyclic p'-groups), we show that there are five additional properties that may be considered (each stronger than the previous) which are distinct. In particular, the classes given by the properties (F1)-(F6) below are distinct for $\mathcal{C}$ the class of all abelian groups, abelian p'-groups or rank 2 abelian or abelian p'-groups. We do show that for many classes of groups the classes (F1) - (F6) coincide.

We now fix a prime p and a class $\mathcal{C}$ of finite groups. For a finite group G, let $\mathcal{S}(G)$ be the set of supplements H to $p(G)$ such that $H \in \mathcal{C}$. Also, let $\mathcal{P}(G)$ be the set of p-subgroups P of G that are normalized by some $H \in \mathcal{S}(G)$. We then have six classes of finite groups – those satisfying each of the conditions listed below. Note that (F($i+1$)) implies (Fi) for $i = 2, 3, 4, 5$, and (F2) implies (F1) if $\mathcal{C}$ is closed under quotients.

(F1) $G/p(G)$ is in $\mathcal{C}$.
(F2) $\mathcal{S}(G)$ is nonempty.
(F3) $\mathcal{P}(G)$ contains a nontrivial p-group, or $p(G) = 1$ and $G \in \mathcal{C}$.
(F4) The groups in $\mathcal{P}(G)$ together generate $p(G)$.
(F5) $p(G)$ is the normal closure of some P in $\mathcal{P}(G)$.
(F6) $\mathcal{P}(G)$ contains a Sylow p-subgroup of G.

Let $\mathcal{S}'(G)$ denote the set of prime-to-p supplements to Q in $\mathcal{C}$. It is easy to see that if $\mathcal{C}$ is also closed under subgroups, then $H \in \mathcal{S}(G)$ implies that there is a p'-subgroup H_1 of H in $\mathcal{S}'(G)$. See Lemma 6.6. Thus, under the natural condition that $\mathcal{C}$ is closed under subgroups, we may replace $\mathcal{C}$ by the set of p'-groups in $\mathcal{C}$ in each of the conditions (Fi). If we let (Fi)$'$ denote this condition, then (Fi) and (Fi)$'$ are equivalent. In the setting we are working in, it is more natural to consider classes of p'-groups and also to consider classes which are closed under quotients. Our first main result is:

Theorem 6.1 *If $\mathcal{C}$ is any class of abelian groups containing a rank 2 elementary abelian subgroup of order prime to p or $\mathcal{C}$ is the class of metacyclic groups or metacyclic p'-groups, then the families* (Fi), $1 \leq i \leq 6$ *are distinct.*

The second main result deals with general classes $\mathcal{C}$. We say a class $\mathcal{C}$ is *closed under Frattini extensions* if it satisfies the following property: if N is normal in G and is contained in the Frattini subgroup, and if G/N is in $\mathcal{C}$, then G is in $\mathcal{C}$. Similarly, we say $\mathcal{C}$ is *closed under central Frattini extensions* if it satisfies: if N is central in G and is contained in the Frattini subgroup, and if G/N is in $\mathcal{C}$, then G is in $\mathcal{C}$.

See below for the definition of the Frattini subgroup and some basic properties. Some examples of such classes are the collection of nilpotent groups, π-groups (groups whose order is product of primes all in π for π some set of primes), solvable groups and d-generated groups. Also, note that if we have several classes closed under Frattini extensions, so is the intersection. So for example the family of d-generated nilpotent groups, for d a positive integer, is also such a class.

Theorem 6.2 *If $\mathcal{C}$ is a class of finite groups closed under Frattini extensions, then* (F1) *implies all* (Fi). *If, in addition, $\mathcal{C}$ is closed under quotients, then the families* (F1)-(F6) *coincide.*

We remark that if $\mathcal{C}$ is any class of nilpotent groups, then closure under Frattini extensions is equivalent to closure under central Frattini extensions. In fact, the previous theorem is valid for any normal subgroup of G, not just $p(G)$ — see Theorem 6.7. Moreover, if Q contains $p(G)$, then of course all quotients are p'-groups. If $\mathcal{C}$ is a class closed under Frattini extensions, then so is the class $\mathcal{C}_\pi$, the set of π-groups in $\mathcal{C}$. Thus if the previous result applies to $\mathcal{C}$ then it applies to the subclass of p'-groups of $\mathcal{C}$ as well; i.e. (F1)-(F6) still coincide even if we restrict attention just to p'-supplements. Below we also prove at least a partial converse to the previous theorem. In the next result, we need to assume that our classes are closed under quotients and normal subgroups (for example any class of finite groups defined by identities). We suspect that a variation on our methods will show that Theorem 6.1 holds for the classes considered in the next result (i.e. (F1)-(F6) are all distinct).

Theorem 6.3 *If $\mathcal{C}$ is a class of p'-groups closed under normal subgroups and quotient groups but not closed under central Frattini extensions, then there exists a finite group G such that $G/p(G)$ is in $\mathcal{C}$ with $\mathcal{S}(G)$ empty. In particular* (F1) *and* (F2) *are distinct.*

The appendix is organized as follows. In the next section, we consider classes closed under Frattini extensions and prove Theorem 6.2. In the following section, we prove Theorem 6.3. In the last section, we give several more examples to prove Theorem 6.1.

6.2 Classes closed under Frattini extensions. We prove Theorem 6.2 in this section. Let G be a finite group. Recall that the Frattini subgroup $\Phi(G)$ is the intersection of all the maximal subgroups of G.

We recall some easy properties of $\Phi(G)$. See [4], Chapter 8 or [8], Chapter 5. We will use a special case of the so-called Frattini argument – if N is normal in G and R is a Sylow r-subgroup of N, then $G = NN_G(R)$. This follows from the fact that all conjugates of R in G are already conjugate in N (by Sylow's theorem).

Lemma 6.4 1. *If $G = \langle X, \Phi(G)\rangle$, then $G = \langle X\rangle$.*
2. *$\Phi(G)$ is nilpotent.*

3. *G is nilpotent if and only if $G/\Phi(G)$ is nilpotent if and only if $G/\Phi(G)$ is abelian of squarefree exponent.*

Proof The first statement is by definition of the Frattini subgroup. We prove the second and third statements as special cases of the following: if N is normal in G and contains $\Phi(G)$, then $N/\Phi(G)$ nilpotent implies that N is nilpotent. (The second assertion is the case $N = \Phi(G)$ while the third assertion is the case $N = G$ together with the elementary observation that if G is nilpotent, then $G/\Phi(G)$ is abelian of squarefree exponent.)

Recall that a finite group is nilpotent if and only if each of its Sylow subgroups is normal and hence characteristic. Let R be a Sylow r-subgroup of N. Then $R\Phi(G)/\Phi(G)$ is characteristic in the nilpotent group $N/\Phi(G)$ and so is normal in $G/\Phi(G)$. Thus, $R\Phi(G)$ is normal in G. By the Frattini argument, $G = N_G(R)R\Phi(G) = N_G(R)\Phi(G) = N_G(R)$. Thus, R is normal in G (and so in N as well). Hence N is nilpotent. □

We give some examples of classes which are closed under Frattini extensions.

Lemma 6.5 *The following classes of finite groups are closed under Frattini extensions:*

1. *d-generated groups;*
2. *nilpotent groups;*
3. *solvable groups;*
4. *π-groups.*

Proof Since any set which generates modulo the Frattini subgroup, generates, the property of d-generation clearly is closed under Frattini extensions. Solvability is closed under extensions and since the Frattini subgroup is nilpotent, solvability is closed under Frattini extensions. If G/N is nilpotent, the result follows by the previous lemma. Finally, we consider the family of π-groups.

Suppose that L is a normal subgroup of G and G/L is a π-group and L is a π'-group (π' denotes the complementary set of primes to π). By the Schur-Zassenhaus Theorem (cf [8]), $G = LH$ with H a complement (and π-group). If M is a maximal subgroup containing H, then M cannot contain L (for $G = LH = LM$ and so $G = M$). Thus, L is not contained in the Frattini subgroup of G.

Now let N be any normal subgroup of G contained in $\Phi(G)$. Let R be a Sylow r-subgroup of N for some prime r dividing $|N|$. Since N is nilpotent, R is characteristic in N and normal in G. Thus, by the previous paragraph, G/R is not an r'-group, whence neither is G/N (since $|G : R| = |G : N||N : R|$ and r does not divide $|N : R|$). So the only primes dividing $|G|$ are those dividing $|G/N|$, yielding the result. □

It is clear that abelian groups and metacyclic groups are closed under quotients and subgroups but are not closed under central Frattini extensions.

Lemma 6.6 *Let G be a finite group, Q a normal subgroup and P a Sylow p-subgroup of Q.*

1. *If H is minimal among supplements to Q, then $H \cap Q \leq \Phi(H)$ and $H \cap Q$ is nilpotent.*
2. *There exists a subgroup $H \leq N_G(P)$ such that $G = QH$ and $H \cap Q$ is contained in the Frattini subgroup of H (and is in particular nilpotent).*

3. *If G/Q is a π-group and $G = HQ$, then H contains a supplement H_1 to Q in G which is a π-group.*

Proof We prove 1. If $H \cap Q$ is not contained in the Frattini subgroup of H, then $H = M(H \cap Q)$ for M a maximal subgroup of H not containing Q. Thus, $G = QH = QM$, contradicting the minimality of H.

By the Frattini argument, $G = QN_G(P)$. Let H be a minimal supplement to Q in G contained in $N_G(P)$. This proves 2.

For the final result, take H_1 to be a minimal supplement to Q contained in H. Then H_1 is a Frattini extension of the π-group $G/Q \cong H_1/(Q \cap H_1)$. Since π-groups are closed under Frattini extensions, the result follows. □

Theorem 6.7 *Let G be a finite group and Q a normal subgroup. Let P be a Sylow p-subgroup of Q. Let $\mathcal{C}$ denote a class of finite groups closed under Frattini extensions.*

1. *If $G/Q \in \mathcal{C}$, then there exists a subgroup A of $N_G(P)$ in $\mathcal{C}$ with $G = QA$ and $A \cap Q$ nilpotent and contained in the Frattini subgroup of A.*
2. *G is the homomorphic image of a semidirect product QH with $H \in \mathcal{C}$ and H normalizing P.*

Proof We prove the first statement. Let A be a minimal supplement to Q contained in $N_G(P)$ (note that $N_G(P)$ is a supplement and so A exists). By the previous lemma, $A \cap Q$ is contained in the Frattini subgroup of A. Since $A/(A \cap Q) \cong G/Q \in \mathcal{C}$, this implies that $A \in \mathcal{C}$ and normalizes P.

We now show that the first statement implies the second. Let H be any supplement to Q in G with $H \in \mathcal{C}$ (and normalizing P). Let J be the semidirect product QH (given by the action of H on Q). Consider the multiplication map $m : J \to G$ given by $xh \in J \mapsto xh \in G$. It is straightforward to see that this is a surjective homomorphism. □

Since the intersection of any two classes of finite groups closed under Frattini extensions is also closed under Frattini extensions, we may replace $\mathcal{C}$ in the above theorem by any class containing G/Q and closed under Frattini extensions. In particular, if G/Q is a π-group, we may replace $\mathcal{C}$ by the set of π-groups in $\mathcal{C}$ (which is also a class closed under Frattini extensions).

Note the previous theorem immediately yields Theorem 6.2, by taking $Q = p(G)$ to obtain that (F1) implies (F6), and using the comment just before the statement of (F1)-(F6) for the other implications.

6.3 Classes not closed under Frattini extensions. If $\mathcal{C}$ is a class of finite groups not closed under Frattini extensions, it is clear that we cannot always find a supplement in $\mathcal{C}$ to a normal subgroup N with quotient in $\mathcal{C}$ — just take G not in $\mathcal{C}$ with G/Q in $\mathcal{C}$ with Q contained in the Frattini subgroup. If $G = QH$, then $H = G$. We need to work harder if we insist that $Q = p(G)$. In this section, we show that it is possible to construct such an example if $\mathcal{C}$ is closed under quotients and normal subgroups but not closed under central Frattini extensions.

Observe that if $\mathcal{C}$ is a class of r-groups for some prime r or more generally a class of nilpotent groups, then closure under Frattini extensions is precisely the same as closure under central Frattini extensions.

We start with two lemmas.

Lemma 6.8 *If $\mathcal{C}$ is not closed under Frattini extensions, then exists a finite group H not in $\mathcal{C}$ and a minimal normal subgroup N such that H/N is in $\mathcal{C}$. If $\mathcal{C}$ is not closed under central Frattini extensions, then exists a finite group H not in $\mathcal{C}$ and minimal central subgroup N such that H/N is in $\mathcal{C}$.*

Proof Let H be a finite group and N a normal subgroup with H/N in $\mathcal{C}$ but H not in $\mathcal{C}$ where N is contained in the Frattini subgroup (and for the second part, N also central in H). Assume that $|H||N|$ is minimal.

If N is not a minimal normal subgroup, there exists a nontrivial proper normal subgroup L of H contained in N. If H/L is in $\mathcal{C}$, the pair (H, L) is also an example with $|L| < |N|$, a contradiction to the minimality of $|H||N|$. If H/L is not in $\mathcal{C}$, consider the pair $(H/L, N/L)$. □

If H is a group, we let H' denote the commutator subgroup of H.

Lemma 6.9 *Let r be a prime and N an r-subgroup of the Frattini subgroup of H. If N is normal in G and $x \in N$, then $x = h^r y$ for some $h \in H$ and $y \in H'$. Moreover, $N = \langle \Phi(T) \cap N \mid T \in \mathrm{Syl}_r(H) \rangle$.*

Proof If U is an r-group, we note that $\Phi(U) = \langle U', u^r | u \in U \rangle$. Since a product of rth powers is an rth power modulo H', we see that the second result implies the first.

We first show that $N \cap \Phi(T)$ is nontrivial. Assume the contrary. Thus, $T' \cap N = 1$. In particular, N is abelian (and indeed is elementary abelian since any rth power of an element of N would be in $\Phi(T)$).

Since $1 \to N \to H \to H/N \to 1$ is nonsplit (as N is contained in the Frattini subgroup of G), the same is true when we restrict this sequence to T (since the index $|H : T| = |H/N : T/N|$ is prime to p and N is a p-group, the restriction map from $H^2(H/N, N) \to H^2(T/N, N)$ is injective).

Let M be a subgroup of T such that $T = \langle M, N, \Phi(T) \rangle$ and $M \cap N \leq \Phi(T)$ (since $T/\Phi(T)$ is an elementary abelian r-group, this is easily done). Then $T = MN$ (because this true modulo $\Phi(T)$) and $M \cap N \leq M \cap N \cap \Phi(T) = 1$. Thus, the sequence $1 \to N \to T \to T/N \to 1$ splits, a contradiction and so $N \cap \Phi(T) \neq 1$ as asserted.

We now complete the proof. Let $N_0 = \langle N \cap \Phi(T) | T \in \mathrm{Syl}_r(G) \rangle$. Then N_0 is nontrivial and normal in G. Now pass to G/N_0. Then $\Phi(T/N_0) = N_0\Phi(T)/N_0$ and so $\Phi(T/N_0) \cap N/N_0 = (N_0\Phi(T) \cap N)/N_0 = N_0(\Phi(T) \cap N)/N_0 = 1$. On the other hand, the argument above shows that $\Phi(T/N_0) \cap N/N_0 \neq 1$ unless $N/N_0 = 1$. Thus, $N = N_0$ as required. □

We will use the following standard easy commutator identities. See [4] or [8].

Lemma 6.10 *If H is a group and $[x, y] = z$ with z central in H, then $[x^e, y] = [x, y^e] = z^e$ and $(xy)^e = x^e y^e [x, y]^{e(e-1)/2}$ for any positive integer e. If H' is contained in $Z(H)$, then $[a, bc] = [a, b][a, c]$.*

The following group will be necessary for our construction. Let r be any prime distinct from p. Let V and W be vector spaces over the field of r elements, each of dimension d. We construct the group $R = R(d, r)$ which is generated by V and W subject only to the relations that the commutator subgroup R' is contained in $Z(R)$, the center of R. In particular, R is nilpotent of class 2. Since V and W each have exponent r, this implies that $[v, w]^r = [v^r, w] = 1$ for $v \in V$ and $w \in W$. Thus, R' is an elementary abelian r-group. Clearly, also $R/R' \cong V \oplus W$ is also an

elementary abelian r-group. Since V and W intersect R' trivially, we will identify V and W with their images in R/R'.

Let Γ be the subgroup of the automorphism group of R preserving V and W setwise. Note that any automorphism of V can be lifted to an automorphism of R (which is trivial on W – just lift elementary automorphisms and diagonal automorphisms). Thus, Γ maps onto $\mathrm{GL}(V) \times \mathrm{GL}(W)$. If γ is in the kernel of this map, then γ fixes each $[v, w]$ with $v \in V$ and $w \in W$. Thus, γ is the identity restricted to R'. Also for $v \in V$ or W, $\gamma(v) = vy$ for some $y \in R'$ (depending upon v) and so $\gamma^r(v) = vy^r = v$. Similarly, we see that the kernel is abelian, whence is an elementary abelian r-group.

Note also that the map $v \otimes w \to [v, w]$ extends to a surjection $V \otimes W \to R'$. This surjection is $\mathrm{GL}(V) \times \mathrm{GL}(W)$-equivariant. Since $V \otimes W$ is an irreducible $\mathrm{GL}(V) \times \mathrm{GL}(W)$-module, this implies that $R' \cong V \otimes W$.

Suppose that S is an r'-subgroup of $\mathrm{GL}(V) \times \mathrm{GL}(W)$. Then S embeds in Γ (this uses the fact that the kernel is an r-group). Let us identify $W = V^*$, the dual of V. Then $GL(V)$ embeds diagonally in $GL(V) \times GL(W)$ by acting on the second copy via the dual representation. Assume further that S is actually contained in the diagonal copy of $\mathrm{GL}(V)$. Then, as a $\mathrm{GL}(V)$-module, we can identify $R' = \mathrm{End}(V)$ with $\mathrm{GL}(V)$ acting via conjugation. In particular, $\mathrm{GL}(V)$ leaves invariant a cyclic subgroup Z of R'. If $1 \neq z \in Z$, then since z is invertible in $\mathrm{End}(V)$, it is the sum of d simple tensors and no fewer (simple tensors correspond to rank one elements in $\mathrm{End}(V)$). Indeed, we need the following:

Lemma 6.11 *Let R_0 be a subgroup of R generated by fewer than d elements. Then z is not in the Frattini subgroup of R_0.*

Proof Consider the image of R_0 in $V \oplus W$. Since it is generated by fewer than d elements, this implies that $R_0 \leq \langle V_0, W_0, R' \rangle$ for some proper subspaces $V_0 \subset V$ and $W_0 \subset W$.

Thus, any $x_i \in R_0$ is of the form $v_i w_i z_i$ with $v_i \in V_0$, $w_i \in W_0$ and $z_i \in R'$. Since V, W and R' all have exponent r, applying Lemma 6.10, we see that $x_i^r = [v_i, w_i]^{r(r-1)/2} z_i^r$ and $[x_1, x_2] = [v_1, w_1][w_2, v_1]$. Thus, $\Phi(R_0) \leq [W_0, V_0]$. This can be identified with $V_0 \otimes W_0 \subset V \otimes W$ and so does not contain z. □

We now prove Theorem 6.3.

Theorem 6.12 *Let $\mathcal{C}$ be a class of p'-groups closed under quotients and normal subgroups but which is not closed under central Frattini extensions. Then there exists a finite group G with $G/p(G)$ in $\mathcal{C}$ such that $\mathcal{S}(G)$ is empty.*

Proof Let H be a group not in $\mathcal{C}$ but with H/N in $\mathcal{C}$ for $N \leq \Phi(H)$ with N central in H. By Lemma 6.6, we may take N to be a minimal central subgroup of H contained in $\Phi(N)$.

Since N is central, it follows that N has prime order r for some prime r dividing $|G/N|$ and in particular $r \neq p$.

Fix a set of generators $h_i, 1 \leq i \leq s$ for H. Let J be a cyclic group of order p and V a J-module in characteristic r such that J has no fixed points on V and $\dim V = d > s$. Let $W = V^*$ and define the group $R = R(d, r)$ as above. Since J has order prime to r, J has no fixed points on V^* either. As noted above, J embeds in Γ and acts on R. As above, let Z denote the group of scalars in $R' = V \otimes V^* = \mathrm{End}(V)$.

Let Q be the semidirect product of R and J. Let $Q_0 = p(Q)$. Since J is a p-group, it follows that $Q = Q_0R$. Set $R_0 = R \cap Q_0$. Now consider $Q/R_0 = (R/R_0)J$. Then $p(Q/R_0) = J$ is normal, whence J centralizes R/R_0. Since J has no fixed points on V or V^*, this implies that both V and V^* are contained in R_0. Since R is generated by V and V^*, this implies $R = R_0$, i.e. $Q = p(Q)$.

We now take G to the central product of Q and H where we identify Z with N – more precisely, $G = (Q \times H)/D$. Here $D = \langle (y, z) \rangle$ with z a generator for Z and y a generator for N. We may identify Q and H with their images in G (since in $Q \times H$, they do not intersect D).

We show that there is no supplement A to Q in $\mathcal{C}$. Suppose to the contrary, A is such a supplement. Since $\mathcal{C}$ is closed under normal subgroups, we may assume that no proper normal subgroup of A is a supplement to Q. Since A is in $\mathcal{C}$, A is a p'-group. In particular, $A \cap Q$ has order relatively prime to $|J|$ and so $A \cap Q \leq R$.

Thus, RA/R is a complement to Q/R in G. Since G/Q and Q/R have relatively prime orders, the Schur-Zassenhaus theorem implies that any two complements to Q/R are conjugate. Thus, RA and RH are conjugate in G and so we may assume that $RA = RH$.

Since $RA = RH$, for each $h \in H$, there exists $x \in R$ with $hx \in A$. Now choose $r_1, \ldots, r_s \in R$ with $h_i r_i \in A$.

Let M be the normal closure in A of $\langle h_i r_i, 1 \leq i \leq s \rangle$. Then $HM = HR$, whence $QM = G$. By the choice, this implies that $A = M$.

Since $d > s$, there are proper subspaces, V_0 and W_0, of V and W, respectively such that $\langle r_1, \ldots, r_s \rangle \leq \langle V_0, W_0, R' \rangle$. Let R_0 denote this last subgroup. Since $RA = RH$ and R and H commute, HR_0 is normal in HR. Since A is generated by conjugates of the $h_i r_i$, it follows that $A \leq \langle h_i r_i, R' \rangle \leq R_0 H$.

Let B denote the inverse image of A in $R \times H$. Then $B \leq R_0 \times H$ (because the image of A is contained in $R_0 H$ and $D \leq R_0 \times H$). Thus, by Lemma 6.9, $\Phi(B) \leq \Phi(R_0) \times H$; and so the projection of $\Phi(B)$ into R is contained in $\Phi(R_0)$ and in particular does not contain z (by Lemma 6.11). Thus D is not contained in $\Phi(B)$ and so $B = D \times A_0$ for some subgroup A_0. Note that $A_0 \cong B/D \cong A$. Consider the projection map τ from B onto H. Since $\tau(D) \leq \Phi(H)$, $H = \tau(B) = \langle \tau(D), \tau(A_0) \rangle = \tau(A_0)$. Since $\mathcal{C}$ is closed under quotients and H is not in $\mathcal{C}$ this implies that A_0 is not in $\mathcal{C}$. This contradicts the fact that $A \cong A_0$ is in $\mathcal{C}$. □

6.4 Examples for abelian and metacyclic groups. Continue to keep p a fixed prime. Now we produce examples for $\mathcal{C}$ the class of abelian rank 2 groups or metacyclic groups – even more, we work with 2-generated r-groups for any prime $r \neq p$. Indeed, the quotients we deal with are elementary abelian rank 2 groups of order r^2 or rank 2 abelian groups of order 16 and exponent 4 (to get examples in the metacyclic category when $r = 2$).

Let S denote a nonabelian group of order r^3. Moreover, if r is odd, then assume that also S has exponent r. So S can be generated by a pair of elements x, y of order r with $u = [x, y]$ central of order r. If $r = 2$, this is the dihedral group of order 8. Note that S is not abelian and for r odd is not metacyclic (because it has exponent r).

If $r = 2$, we will need another group. So let $T = \langle x, y, u | u^2 = x^4 = y^4 = [x, u] = [y, u] = 1, u = [x, y] \rangle$. Note that u is central and generates T' and T/T' is abelian of rank 2 and so metacyclic but T is neither abelian nor metacyclic.

Applying the construction in the previous section with $H = S$ or T respectively yields the following:

Example 1a. Let r be a prime distinct from p. There exists a finite group G with $G/p(G)$ elementary abelian of order r^2 such that there is no abelian supplement to $p(G)$ in G. If r is odd, then there is no metacyclic supplement to $p(G)$.

Example 1b. Assume $p \neq 2$. There exists a finite group G with $G/p(G) \cong \mathbf{Z}/4 \times \mathbf{Z}/4$ such that there is no abelian or metacyclic supplement to $p(G)$ in G.

So we see that the families (F1) and (F2) are distinct for $\mathcal{C}$ the class of abelian or metacyclic groups (and other such classes).

We now give three more examples to show that the classes (F2)-(F6) are distinct for metacyclic groups and for abelian p'-groups (and more particularly, when $G/p(G)$ is elementary abelian of order r^2 or $\mathbf{Z}/4 \times \mathbf{Z}/4$). Example 2 shows that (F2) and (F3) are distinct. The remark after example 2 shows that (F3) and (F4) are distinct. Example 3 shows that (F4) and (F5) are distinct. Example 4 shows that (F5) and (F6) are distinct.

The form of the examples are all quite similar. We will need to use some standard properties of *extraspecial* groups. See [4] or [8]. If r is a prime, then a finite r-group E is called extraspecial if $E' = Z(E) = \Phi(E)$ has order r. Recall that E' is the commutator subgroup of E, $Z(E) = \langle z \rangle$ is the center. Necessarily, $|E| = r^{1+2d}$ for some d and there are two isomorphism classes of such groups for a given r and d. If r is odd, we take E to be the group of exponent r. If $r = 2$, this is not possible and we allow either choice. Note that if a and b are in E and do not commute, then $1 \neq [a, b] \in E'$ is some nontrivial power of z. Thus, $[a, b'] = z$ for some b', a power of b.

Set $V = E/E'$. This is a vector space of dimension d over the field of r elements. The map $(v_1, v_2) \mapsto [v_1, v_2]$ is a nondegenerate alternating form on V. Thus, we can talk about totally singular and nonsingular subspaces of V (always with respect to this alternating form). So in particular, a subspace is totally singular if and only if its preimage in E is abelian.

Let Γ be the group of automorphisms of E which are trivial on E'. Then Γ preserves this alternating form. Thus, we have the sequence $1 \to \Delta \to \Gamma \to \mathrm{Sp}(V)$ by mapping Γ into $\mathrm{GL}(V)$. Note that Δ is an elementary abelian r-group. If r is odd, then in fact, $\Gamma \cong \Delta \mathrm{Sp}(V)$ (semidirect). We can identify the complementary $\mathrm{Sp}(V)$ with the centralizer of an involution which is inversion mod E'. If $r = 2$, Γ (which is the full automorphism group of E) also preserves the quadratic form $q : V \to E'$ given by $q(v) = v^2$. In this case, we have a (nonsplit) short exact sequence

$$1 \to \Delta \to \Gamma \to \mathrm{O}(V, q) \to 1,$$

where $\mathrm{O}(V, q)$ is the orthogonal group of the nondegenerate quadratic form q.

In particular, if r is odd, then any subgroup of $\mathrm{Sp}(V)$ can be viewed as acting on E. If $r = 2$, then any odd subgroup of $\mathrm{O}(V, q)$ embeds in Γ. Depending upon the choice of E, we can obtain either class of nondegenerate quadratic forms. In particular, if we choose E so that $\mathrm{O}(V, q) \cong \mathrm{O}^+(2d, 2)$, then V contains two maximal totally singular complementary subspaces each of dimension d. It follows that $\mathrm{GL}(d, 2)$ embeds in Γ for the appropriate choice of E (where the representations of $\mathrm{GL}(d, 2)$ on the two maximal totally singular subspaces are dual to one another).

Let H be a quasi p-subgroup of Γ such that H has no nontrivial fixed points on V or the dual V^*. By the trivial H-module, we will mean the module of order r with trivial H-action. Set $Q = EH$. The fact that H has no fixed points on V^* implies that there is no H-equivariant map from V onto the trivial H-module. This implies that Q is quasi p (precisely as in the construction of the previous section).

If r is odd, we can take any quasi p-subgroup of $\mathrm{Sp}(V)$ such that H has no nontrivial fixed points on V (since $H \leq \mathrm{Sp}(V)$, $V \cong V^*$ as H-modules). If $r = 2$, we can take H to be any odd quasi p-subgroup of $\mathrm{O}(V)$ such that H has no fixed points on V (note H acts completely reducibly on V). If q is of $+$ type, we can also take H to be a quasi p-subgroup of $\mathrm{GL}(d, 2)$ with no nontrivial fixed points on V (equivalently, no fixed points on W or W^* where W is the module of dimension d corresponding to the embedding of $H \leq \mathrm{GL}(d, 2)$). As noted above this is a subgroup which preserves a pair of complementary totally singular subspaces and embeds in Γ.

Let U denote either of the subgroups S or T described above. We take x, y to be the generators given in the description. In particular, x, y have order r if $U = S$ and order 4 if $U = T$. Also, $[x, y] = u$.

Let $G = Q * U$ be the central product where we identify u and z^{-1}. More precisely, $G = (Q \times U)/\langle (z, u) \rangle$. We identify H, Q and U with subgroups of G. Because of the identification of u and z^{-1}, we see that $Z(E) \leq U$.

Note that $G/Q \cong U/(U \cap Q)$ is elementary abelian of order r^2 (or is isomorphic to $\mathbf{Z}/4 \times \mathbf{Z}/4$ if $U = T$). Since $z = [a, b]$ for some $a, b \in E$, $[xa, yb] = [x, y][a, b] = uz = 1$ in G, it follows that $A := \langle xa, yb \rangle$ is abelian. Since U is a supplement to Q and A covers $U/Z(E)$, it follows that A is an abelian complement to Q in G.

We now take various choices for H. Indeed, it is often convenient to take H to be a p-group. In the following examples, we will only remark on the nonexistence of abelian supplements – for r odd, this is equivalent to the nonexistence of a metacyclic supplement and the same is true for $r = 2$ with $U = T$. We also note that we may always assume that the complement is an r-group (and in particular a p'-group) by passing to the Sylow r-subgroup of the complement.
We first record two useful facts.

Lemma 6.13 *If X is a subgroup of H and has no fixed point on V, then $N_G(X) = N_H(X)U$.*

Proof Clearly, $N_H(X)$ and U each normalize X (the latter since U commutes with H). Since $G = QU = (EH)U$, we may write any $g \in G$ in the form $g = ehw$ with $e \in E$, $h \in H$ and $w \in U$. Suppose that g normalizes X. We claim that $g = hw'$ with $w' \in U$ and $h \in N_H(X)$. Since U centralizes H, we may replace g by gw^{-1} and so assume that $w = 1$. Thus, $X = ehX(eh)^{-1}$ and so $X^h := hXh^{-1} = e^{-1}Xe \leq XE$ (the last containment follows because E is normal). Then $X^h \leq XE \cap H = X$, whence $h \in N_H(X)$ and so $e \in N_E(X)$. Since E is normal in G, $N_E(X) = C_E(X)$. Since X has no fixed points on V, $C_E(X) \leq Z(E) \leq U$. □

Lemma 6.14 *There are no abelian supplements to Q contained in HU.*

Proof Note that $HU \cong H \times U$. If $A \leq HU$ is an abelian supplement to Q, then $HU = (Q \cap HU)A = (HZ(E))A$. Moreover, replacing A by a Sylow r-subgroup, allows us to assume that A is an r-group and so is contained in the (unique) Sylow r-subgroup U of HU. Thus, $U = Z(E)A$. Since $Z(E)$ is generated by u, it is contained in the Frattini subgroup of U. Thus, $A = U$ is nonabelian. □

Example 2. Let H be of order p (for example, take d to be minimal with p dividing $r^d \pm 1$). Then $N_G(P)$ does not contain an abelian supplement to Q for any nontrivial p-subgroup P of G.

Proof The only nontrivial p-subgroup of G is (up to conjugacy) H. By Lemma 6.13, $N_G(H) = HU$. By Lemma 6.14, HU contains no abelian supplements. □

If we take a group which is a direct product of the previous example and a p-group, then we obtain an example where $N_G(P)$ does contain an abelian supplement for some nontrivial p-subgroup P, but the normal closure of all such p-groups does not contain Q.

The next example shows that Q may be generated by the p-subgroups of G which contain abelian supplements but the normalizer of a full Sylow p-subgroup does not contain an abelian supplement. Indeed, $N_G(P)$ contains no abelian supplement for any P whose normal closure is Q. In this example, we view $V = V_1 \oplus V_2$ with each V_i nonsingular with the respect to the alternating form on V.

Example 3. Let $H = P_1 \times P_2$ of order p^2 be a subgroup of of $\mathrm{Sp}(V_1) \times \mathrm{Sp}(V_2)$ (and if $r = 2$, a subgroup of $\mathrm{O}(V_1) \times O(V_2)$), where P_i has no fixed points on V_i but is trivial on the other space. Thus, H acts on E and so we can define G as above. Then there is no p-subgroup P of G such that $Q = \langle P^g \mid g \in G\rangle$ and $N_G(P)$ contains an abelian supplement to Q. However, $Q = \langle P_1^g, P_2^g \mid g \in G\rangle$ and $N_G(P_i)$ contains an abelian supplement for $i = 1, 2$.

Proof If $Q = \langle P^g | g \in G\rangle$, then since Q/E is a p-group, P must be a full Sylow p-subgroup of G and so is conjugate to H. As in the previous example, $N_G(H) = HU$ contains no abelian supplements.

On the other hand, since V_i is a nonsingular subspace of V, we can choose $a_i, b_i \in R_i$ (the preimage of V_i) with $[a_i, b_i] = u$. Thus, $[xa_i, yb_i] = [x, y]u = 1$ and $S_i := \langle xb_i, ya_i\rangle$ is abelian. Since this group surjects onto G/Q, it is a supplement. Since x, y, a_i, b_i all centralize P_i, S_i is an abelian supplement to Q centralizing P_i. □

Example 4. Let H be a quasi p-subgroup of Γ with Sylow p-subgroup P such that P has no fixed points of V but it contains a nontrivial subgroup P_0 which does have fixed points on V. Assume also that H is generated by the H-conjugates of P_0. Then $N_G(P)$ contains no abelian supplement, but $N_G(P_0)$ does contain an abelian supplement and $Q = \langle P_0^g | g \in G\rangle$.

Proof By Lemmas 6.13 and 6.14, $N_G(P) = N_H(P)U \leq HU$ and HU contains no abelian supplements to Q.

Since P_0 acts trivially on some subspace of V and since $p \neq r$, this implies that P_0 is trivial on a nonsingular subspace of V, so we can find $a, b \in E$ centralizing P_0 with $[a, b] = u$. Thus, $\langle xb, ya\rangle$ is an abelian complement that normalizes (indeed centralizes) P_0. Clearly the normal closure of P_0 contains H and so Q (since the normal closure of H in Q is Q). □

If r is odd, then we can take $H = \mathrm{Sp}(V)$ – the only condition we need to satisfy is that P has no fixed points on V (and we can certainly choose such a V) but P contains an abelian noncyclic subgroup P_0. Any abelian noncyclic subgroup r'-group will have fixed points on V (restrict to an irreducible submodule for the

the abelian group – the action must be cyclic). Since $H/Z(H)$ is almost always simple, it follows that H is the normal closure of P_0.

If $r = 2$, we take E to be such that the quadratic form on V has + type. As noted, then $H = \mathrm{GL}(d, 2)$ with $d > 2$ embeds in Γ. We choose d so that P acts without fixed points on V and contains a noncyclic abelian subgroup. Thus, H has the desired properties.

References

[1] S.S. Abhyankar - *Coverings of algebraic curves* - Amer. J. Math. **79** (1957), 825-856.

[2] S.S. Abhyankar - *Tame coverings and fundamental groups of algebraic varieties, Part 1* - Amer. J. Math. **84** (1959), 46-94.

[3] S.S. Abhyankar - *Local fundamental groups of algebraic varieties* - Proc. Amer. Math. Soc. **125** (1997), 1635-1641.

[4] M. Aschbacher - *Finite Group Theory* - Cambridge Studies in Advanced Mathematics 10, Cambridge University Press, Cambridge-New York, 1986.

[5] P. Deligne - *Le groupe fondamental du complément d'une courbe plane n'ayant que des points doubles ordinaires est abélien. [d'après W. Fulton]* - Séminaire Bourbaki, exposé 543, vol. 1979/80, Lect. Notes in Math. **842**, Springer Verlag, Berlin 1981.

[6] W. Fulton - *On the fundamental group of the complement of a node curve* - Annals of Math. **111** (1980), 407-409.

[7] W. Fulton, J. Hansen - *A connectedness theorem for projective varieties, with applications to intersections and singularities of mappings* - Annals of Math. **110** (1979), 159-166.

[8] D. Gorenstein - *Finite Groups* - Chelsea Publishing Co., New York, 1980.

[9] A. Grothendieck - *Revêtements Etales et Groupe Fondamental (SGA1)* - Lect. Notes in Math. **224**, Springer Verlag, 1971.

[10] A. Grothendieck and J.P. Murre - *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme* - Lect. Notes in Math. **208**, Springer Verlag, 1971.

[11] M. Hall - *The theory of groups* - Macmillan Co., New York, 1959.

[12] D. Harbater - *Abhyankar's conjecture on Galois groups over curves* - Invent. Math. **117** (1994), 1-25.

[13] D. Harbater - *Fundamental Groups of Curves in Characteristic p* - Proceedings of the International Congress of Mathematicians, Zürich, Switzerland 1994, Birkhäuser Verlag, Basel Switzerland (1995), 656-666.

[14] I. Kaplansky - *Maximal Fields with Valuations,* I - Duke Math. J., **9** (1942), 303-321.

[15] K. Kedlaya - *The algebraic closure of the power series field in positive characteristic* - xxx preprint math.AG/9810142, to appear in Proc. Amer. Math. Soc.

[16] F.-V. Kuhlmann - *Valuation theoretic and model theoretic aspects of local uniformization* - in "Resolution of singularities", pp. 381-456, Progress in Math., vol. 181, Birkhäuser, Basel, 2000.

[17] H. Matsumura - *Commutative Algebra* - Second edition, Benjamin-Cummings, Reading, 1980.

[18] H. Matzat and M. van der Put - *Iterative differential equations and the Abhyankar conjecture* - preprint February 2001.

[19] O.V. Melnikov and A.A. Sharomet - *The Galois group of a multidimensional local field of positive characteristic* - Math. USSR Sbornik **67** (1990), 595-610.

[20] A.N. Parshin - *Local class field theory*, Proc. Steklov Inst. of Math. **165** (1985), 157-185.

[21] M. van der Put - *Recent work on differential Galois theory* - Séminaire Bourbaki, exposé 849, Juin 1998, Astérisque **252**, 1998.

[22] M. van der Put and M.F. Singer - *Galois Theory of Difference Equations* - Lect. Notes in Math. **1666**, Springer Verlag, 1997.

[23] M. Raynaud - *Revêtements de la droite affine en caractéristique p* - Invent. Math. **116** (1994), 425-462.

[24] P. Ribenboim - *Théorie des valuations* - Séminaire de Mathématiques Supérieures vol **9**, Les Presses de l'Université de Montréal 1965.

[25] J.-P. Serre - *Revêtements ramifiés du plan projective* - Séminaire Bourbaki, exposé 204, vol. 1959/60.