Henselianity in NIP $\mathbb{F}_p$-algebras

Will Johnson
Henselianity in NIP $\mathbb{F}_p$-algebras

Will Johnson

We prove an assortment of results on (commutative and unital) NIP rings, especially $\mathbb{F}_p$-algebras. Let $R$ be a NIP ring. Then every prime ideal or radical ideal of $R$ is externally definable, and every localization $S^{-1}R$ is NIP. Suppose $R$ is additionally an $\mathbb{F}_p$-algebra. Then $R$ is a finite product of henselian local rings. Suppose in addition that $R$ is integral. Then $R$ is a henselian local domain, whose prime ideals are linearly ordered by inclusion. Suppose in addition that the residue field $R/m$ is infinite. Then the Artin–Schreier map $R \to R$ is surjective (generalizing the theorem of Kaplan, Scanlon, and Wagner for fields).

1. Introduction

The class of NIP theories has played a major role in contemporary model theory. See [Simon 2015] for an introduction to NIP. In recent years, much work has been done on the problem of classifying NIP fields and NIP rings. A conjectural classification of NIP fields has emerged through work of Anscombe, Halevi, Hasson, and Jahnke [Halevi et al. 2019; Anscombe and Jahnke 2019], and partial results towards this conjectural classification have been obtained by the author in the setting of finite dp-rank [Johnson 2015; 2020; 2021b].

NIP fields are closely connected to NIP valuation rings. Conjecturally:

- Every NIP valuation ring is henselian.
- Every infinite NIP field is elementarily equivalent to Frac($R$) for some NIP nontrivial valuation ring $R$.

These conjectures form the basis for the proposed classification of NIP fields [Anscombe and Jahnke 2019], and are known to hold assuming finite dp-rank [Johnson 2020]. Additionally, the henselianity conjecture is known in positive characteristic: if $R$ is a NIP valuation ring and Frac($R$) has positive characteristic, then $R$ is henselian [Johnson 2021a, Theorem 2.8].

More generally, one would like to understand (commutative) NIP rings, especially NIP integral domains. A first step in this direction is the recent work of d’Elbée and Halevi [2021] on dp-minimal integral domains. Among other things, they show

MSC2020: 03C60.
Keywords: NIP, henselian rings.
that if $R$ is a dp-minimal integral domain, then $R$ is a local ring, the prime ideals of $R$ are a chain, the localization of $R$ at any nonmaximal prime is a valuation ring, and $R$ is a valuation ring whenever its residue field is infinite.

In the present paper, we consider a NIP integral domain $R$ such that $\text{Frac}(R)$ has positive characteristic. By analogy with [d’Elbée and Halevi 2021], we show that $R$ is a local ring whose primes ideals are linearly ordered by inclusion. Generalizing the earlier henselianity theorem for valuation rings, we show that $R$ is a henselian local ring. These results may help to extend the work of d’Elbée and Halevi to “positive characteristic” NIP integral domains.

**Main results.** All rings are assumed to be commutative and unital. In Section 2 we consider a general NIP ring $R$. Our main results are the following:

- Any localization $S^{-1}R$ is interpretable in the Shelah expansion $R^{\text{Sh}}$, and is therefore NIP (Theorem 2.11).
- Any radical ideal in $R$ is externally definable (Theorem 2.14).

In Section 3, we restrict to the case where $R$ is an $\mathbb{F}_p$-algebra, and obtain significantly stronger results:

- $R$ is a finite product of henselian local rings (Theorem 3.21).
- If $R$ is an integral domain, then $R$ is a henselian local domain (Theorem 3.22), and the prime ideals of $R$ are linearly ordered by inclusion (Theorem 3.15).
- If $R$ is a local integral domain with maximal ideal $m$ and $R/m$ is infinite, then the Artin–Schreier map $R \to R$ is surjective (Theorem 3.4).

The henselianity results generalize [Johnson 2021a, Theorem 2.8], which handled the case where $R$ is a valuation ring. The surjectivity of the Artin–Schreier map generalizes a theorem of Kaplan, Scanlon, and Wagner [Kaplan et al. 2011, Theorem 4.4], which handled the case where $R$ is a field.

2. General NIP rings

2A. **Finite width.** The width of a poset $(P, \leq)$ is the maximum size of an antichain in $P$. We write $\text{Spec} R$ for the poset of prime ideals in $R$, ordered by inclusion. This is an abuse of notation, since we are forgetting the usual scheme and topology structure on $\text{Spec} R$, and then adding the poset structure.

**Fact 2.1.** Let $R$ be a NIP ring. Then $\text{Spec} R$ has finite width. Moreover, there is a uniform finite bound on the width of $\text{Spec} R'$ for $R' \succeq R$.

**Fact 2.1** is proved by d’Elbée and Halevi [2021, Proposition 2.1, Remark 2.2], who attribute it to Pierre Simon.

**Fact 2.1** has a number of useful corollaries, which we shall use in later sections. First of all, Dilworth’s theorem gives the following corollary:
**Corollary 2.2.** If $R$ is a NIP ring, then $\text{Spec } R$ is a finite union of chains.

Another trivial corollary of **Fact 2.1** is the following:

**Corollary 2.3.** If $R$ is a NIP ring, then $R$ has finitely many maximal ideals and finitely many minimal prime ideals.

Also, using Beth’s implicit definability, we see the following:

**Corollary 2.4.** If $R$ is a NIP ring, then the maximal ideals of $R$ are definable.

For completeness, we give the proof. The proof uses the following form of Beth’s theorem:

**Fact 2.5.** Let $M$ be an $L_0$-structure. Let $L$ be a language extending $L_0$ and let $T$ be an $L$-theory. Suppose there is a cardinal $\kappa$ such that for any $M' \succeq M$ there are at most $\kappa$-many expansions of $M'$ to a model of $T$. Then every such expansion is an expansion by definitions.

*Proof of Corollary 2.4.* Let $L_0$ be the language of rings and $L$ be $L_0 \cup \{P\}$, where $P$ is a unary predicate symbol. Let $T$ be the statement saying that $P$ is a maximal ideal, i.e.,

$$\forall x, y : P(x) \land P(y) \rightarrow P(x + y),$$

$$P(0),$$

$$\forall x, y : P(x) \rightarrow P(x \cdot y),$$

$$\neg P(1),$$

$$\forall x : \neg P(x) \rightarrow \exists y : P(xy - 1).$$

If $R' \succeq R$, then an expansion of $R'$ to a model of $T$ is the same thing as a maximal ideal of $R'$. The number of such maximal ideals is uniformly bounded by **Fact 2.1**, and so **Fact 2.5** shows that each such maximal ideal is definable. □

(Of course, there are other, more direct, algebraic proofs of **Corollary 2.4**.)

Recall that the Jacobson radical of a ring is the intersection of its maximal ideals.

**Corollary 2.6.** Let $R$ be a NIP integral domain. Then the Jacobson radical of $R$ is nonzero.

*Proof.* In a domain, the intersection of two nonzero ideals is nonzero. □

**Corollary 2.7.** Let $R$ be a NIP integral domain that is not a field. Let $K = \text{Frac}(R)$. There is a nontrivial, nondiscrete Hausdorff field topology on $K$ characterized by either of the following:

- The family of sets $\{aR : a \in K^\times\}$ is a neighborhood basis of 0.
- The set of nonzero ideals of $R$ is a neighborhood basis of 0.
Proof. Everything follows formally by [Prestel and Ziegler 1978, Example 1.2], except that we only get a ring topology. It remains to see that the map \( x \mapsto 1/x \) is continuous. It suffices to consider continuity around \( x = 1 \). Let \( I \) be a nonzero ideal in \( R \). We claim there is a nonzero ideal \( I' \) such that if \( x \in 1 + I' \), then \( 1/x \in 1 + I \). Indeed, take \( I' = I \cap J \), where \( J \) is the Jacobson radical. Suppose \( x \in 1 + (I \cap J) \). Then \( x - 1 \) is in every maximal ideal, implying that \( x \) is in no maximal ideals, so \( x \in R^\times \). Also, \( x \in 1 + I \) implies that \( 1 - x \in I \), and then \( x^{-1}(1-x) \in I \), because \( x \) is a unit. But \( x^{-1}(1-x) = x^{-1} - 1 \), and so \( x^{-1} \in 1 + I \) as desired. \( \square \)

Lemma 2.8. If \( R \) and \( S \) are NIP rings and \( R \equiv S \), then \( R \) and \( S \) have the same number of maximal ideals.

Proof. It suffices to show that \( S \) has as many maximal ideals as \( R \). By Corollaries 2.3 and 2.4 we can write the maximal ideals of \( R \) as \( \phi_1(R, a_1), \ldots, \phi_n(R, a_n) \) for some formulas \( \phi_i \) and parameters \( a_i \) from \( R \). Let \( \psi(y_1, \ldots, y_n) \) be the formula asserting the sets \( \phi_1(R, y_1), \ldots, \phi_n(R, y_n) \) are pairwise distinct maximal ideals.

The formula \( \psi \) is satisfied by the tuple \( (a_1, \ldots, a_n) \) in \( R \), so it is satisfied by some tuple in \( S \), giving \( n \) distinct maximal ideals in \( S \). \( \square \)

2B. Localizations. If \( M \) is a structure, then \( M^{\text{Sh}} \) denotes the Shelah expansion of \( M \). If \( M \) is NIP, then the definable sets in \( M^{\text{Sh}} \) are exactly the externally definable sets in \( M \), and \( M^{\text{Sh}} \) is NIP [Simon 2015, Proposition 3.23, Corollary 3.24].

Say that a collection of sets \( C \) is “uniformly definable” in a structure \( M \) if \( C \subseteq \{ X_a : a \in Y \} \) for some definable family of sets \( \{ X_a \}_{a \in Y} \).

Remark 2.9. Let \( M \) be a structure. Suppose \( D = \bigcup_{i \in I} D_i \) is a directed union, and the \( D_i \) are uniformly definable in \( M \). Then \( D \) is externally definable.

This is well known in certain circles, but here is the proof for completeness:

Proof. Take some \( L(M) \)-formula \( \phi(x, y) \) such that \( D_i = \phi(M, b_i) \) for some \( b_i \in M^y \). Let \( \Sigma(y) \) be the partial type

\[
\{ \phi(a, y) : a \in D \} \cup \{ \neg \phi(a, y) : a \in M^x \setminus D \}.
\]

Then \( \Sigma(y) \) is finitely satisfiable, because for any \( a_1, \ldots, a_n \in D \) and \( e_1, \ldots, e_m \in M^x \setminus D \) we can find some \( i \) such that \( D_i \supseteq \{ a_1, \ldots, a_n \} \), because the union is directed. Then \( D_i \subseteq D \), so \( D_i \cap \{ e_1, \ldots, e_m \} = \emptyset \). Thus \( b_i \) satisfies the relevant finite fragment of \( \Sigma(y) \). By compactness there is a realization \( b \) of \( \Sigma(y) \) in an elementary extension \( N \supseteq M \). Then \( \phi(M, b) = D \), by definition of \( \Sigma(y) \), so \( D \) is externally definable. \( \square \)

Lemma 2.10. Let \( R \) be a NIP ring. Let \( S \) be a multiplicative subset. Then there is an externally definable multiplicative subset \( \tilde{S} \) such that the localization \( S^{-1}R \) is isomorphic (as an \( R \)-algebra) to \( \tilde{S}^{-1}R \).
Proof. For any \( x \in R \), let \( F_x \) denote the set of \( y \in R \) such that \( y \mid x \). Let \( \overline{S} = \bigcup_{x \in S} F_x \). Note that if \( A \) is a ring and \( f : R \to A \) is a homomorphism, then the following are equivalent:

- \( f(s) \) is invertible for every \( s \in S \).
- \( f(x) \) is invertible for \( x, y, s \) with \( xy = s \) and \( s \in S \).
- \( f(x) \) is invertible for \( x, s \) with \( x \in F_s \) and \( s \in S \).
- \( f(x) \) is invertible for \( x \in \overline{S} \).

Therefore \( S^{-1}R \) and \( \overline{S}^{-1}R \) represent the same functor, and are isomorphic.

It remains to see that \( \overline{S} \) is externally definable. This follows by Remark 2.9 because the sets \( F_x \) are uniformly definable, and the union \( \bigcup_{x \in S} F_x \) is a directed union. Indeed, if \( x, y \in S \), then \( xy \in S \) and \( F_{xy} \supseteq F_x \cup F_y \). □

**Theorem 2.11.** Let \( R \) be a NIP ring. Let \( S \) be a multiplicative subset. Then the localization \( S^{-1}R \) and the homomorphism \( R \to S^{-1}R \) are interpretable in \( R^{Sh} \).

**Proof.** By Lemma 2.10, we may replace \( S \) with an externally definable set \( \overline{S} \), and then the result is clear. □

**Corollary 2.12.** Let \( R \) be a NIP ring. Let \( S \) be a multiplicative subset. Then the localization \( S^{-1}R \) is also NIP.

**Proof.** The localization \( S^{-1}R \) is interpretable in the NIP structure \( R^{Sh} \). □

Corollary 2.12 generalizes part of [d’Elbée and Halevi 2021, Proposition 2.8(2)], dropping the assumptions that \( S \) is externally definable and \( R \) is integral.

**Proposition 2.13.** Let \( R \) be a NIP ring. Let \( \mathfrak{p} \) be a prime ideal in \( R \). Then \( \mathfrak{p} \) is externally definable.

**Proof.** By Theorem 2.11, we can interpret \( R \to R_{\mathfrak{p}} \) in \( R^{Sh} \). The maximal ideal of \( R_{\mathfrak{p}} \) is definable in \( R_{\mathfrak{p}} \), as the set of nonunits. It pulls back to \( \mathfrak{p} \) in \( R \). Therefore \( \mathfrak{p} \) is definable in \( R^{Sh} \), hence externally definable in \( R \). □

Proposition 2.13 generalizes a theorem of d’Elbée and Halevi, who proved that (certain) prime ideals in dp-minimal domains are externally definable [d’Elbée and Halevi 2021, Lemma 3.3].

**Theorem 2.14.** Let \( R \) be a NIP ring. Let \( I \) be a radical ideal in \( R \). Then \( I \) is externally definable.

**Proof.** By Corollary 2.2, we can cover the set Spec \( R \) of prime ideals in \( R \) with finitely many chains \( C_1, \ldots, C_n \). The ideal \( I \) is an intersection of prime ideals. Let \( \mathfrak{p}_i \) be the intersection of the prime ideals \( \mathfrak{p} \in C_i \) with \( \mathfrak{p} \supseteq I \). An intersection of a chain of prime ideals is prime, so \( \mathfrak{p}_i \) is prime. Then \( I \) is a finite intersection \( \bigcap_{i=1}^n \mathfrak{p}_i \). Each \( \mathfrak{p}_i \) is externally definable by Proposition 2.13. □
Corollary 2.15. Let $R$ be a NIP ring. Let $I$ be a radical ideal. The quotient $R/I$ is NIP.

Proof. The quotient $R/I$ is interpretable in the NIP structure $R^{Sh}$. □

2C. Automatic connectedness. If $G$ is a definable or type-definable group, then $G^{00}$ is the smallest type-definable group of bounded index in $G$. In a NIP context, $G^{00}$ always exists, and is type-definable over whatever parameters define $G$ [Hrushovski et al. 2008, Proposition 6.1]

Proposition 2.16. Let $R$ be a NIP ring. Suppose that $R/m$ is infinite for every maximal ideal $m$ of $R$.

(1) If $I$ is a definable ideal of $R$, then $I = I^{00}$.

(2) If $R$ is a domain and $K = \text{Frac}(R)$ and if $I$ is a definable $R$-submodule of $K$, then $I = I^{00}$.

In particular, in either case, $I$ has no definable proper subgroups of finite index.

Proof. We may assume $R$ is a monster model, i.e., $\kappa$-saturated for some big cardinal $\kappa$. “Small” will mean “cardinality less than $\kappa$”, and “large” will mean “not small.”

Let $m_1, \ldots, m_n$ be the maximal ideals of $R$. By Corollary 2.3 there are only finitely many, and by Corollary 2.4 they are all definable. The quotients $R/m_i$ are infinite, hence large. Therefore every simple $R$-module is large. Every nontrivial $R$-module has a simple subquotient, so every nontrivial $R$-module is large.

Now suppose $I$ is a definable ideal. If $a \in R$, then the map $I \to I$ sending $x$ to $ax$ must map $I^{00}$ into $I^{00}$. Indeed, if we let $J = \{x \in I : ax \in I^{00}\}$, then $J$ is a type-definable subgroup of $I$ of bounded index, so $J \supseteq I^{00}$. Thus we see that for any $a \in R$, we have $aI^{00} \subseteq I^{00}$. In other words, $I^{00}$ is an ideal. The quotient $I/I^{00}$ is an $R$-module. By definition of $G^{00}$, the quotient $I/I^{00}$ is small. We saw that nontrivial $R$-modules are large, so $I/I^{00}$ must be trivial, implying $I = I^{00}$. This proves (1), and (2) is similar. □

3. NIP $\mathbb{F}_p$-algebras

3A. A variant of the Kaplan–Scanlon–Wagner theorem. In [Kaplan et al. 2011, Theorem 4.4], Kaplan, Scanlon, and Wagner show that if $K$ is an infinite NIP field of characteristic $p > 0$, then the Artin–Schreier map $x \mapsto x^p - x$ is a surjection from $K$ onto $K$. The same idea can be applied to certain local rings, as we will see in Theorem 3.4 below.

Before proving the theorem, we need some (well-known) lemmas on additive polynomials. Fix a field $K$ of characteristic $p$. If $c \in K$, define

$$g_c(x) = x^p - c^{p-1}x.$$
The polynomial \( g_c(x) \) defines an additive homomorphism from \( K \) to \( K \). If \( V \) is a finite-dimensional \( \mathbb{F}_p \)-linear subspace of \( K \) (i.e., a finite subgroup of \((K, +)\)), define

\[
f_V(x) = \prod_{a \in V} (x - a).
\]

We will see shortly that \( f_V \) is an additive homomorphism.

**Lemma 3.1.** If \( c \in K \) is nonzero, then \( g_c(x) = f_{\mathbb{F}_p \cdot c}(x) \). In particular, \( f_{\mathbb{F}_p \cdot c}(x) \) is an additive homomorphism.

**Proof.** Note that \( g_c(c) = 0 \). Therefore, \( \ker g_c \) contains the subgroup generated by \( c \), which is \( \mathbb{F}_p \cdot c \). Since \( g_c \) is monic of degree \( p \), and \( |\mathbb{F}_p \cdot c| = p \), we must have

\[
g_c(x) = \prod_{a \in \mathbb{F}_p \cdot c} (x - a) = f_{\mathbb{F}_p \cdot c}(x).
\]

**Lemma 3.2.** Suppose \( V_1 \subseteq V_2 \) are finite-dimensional subspaces of \( K \) such that \( \dim V_2 = \dim V_1 + 1 \). Suppose \( f_{V_1} \) is an additive homomorphism on \( K \). Then there is \( c \in f_{V_1}(V_2) \) such that \( f_{V_2} = g_c \circ f_{V_1} \), and in particular \( f_{V_2} \) is an additive homomorphism on \( K \).

**Proof.** Take \( a \in V_2 \setminus V_1 \) and let \( c = f_{V_1}(a) \). Let \( h = g_c \circ f_{V_1} \). Then \( h \) is an additive homomorphism on \( K \), and it suffices to show that \( h = f_{V_2} \). Note that if \( x \in V_1 \), then \( h(x) = g_c(f_{V_1}(x)) = g_c(0) = 0 \), since \( f_{V_1} \) vanishes on \( V_1 \). Additionally, \( h(a) = g_c(f_{V_1}(a)) = g_c(c) = 0 \). Thus the kernel of \( h \) contains \( V_1 \) as well as \( a \). It therefore contains the group they generate, which is \( V_1 + \mathbb{F}_p \cdot a = V_2 \). If \( d = \dim V_1 \), then \( |V_1| = p^d \) and \( |V_2| = p^{d+1} \). The polynomial \( f_{V_1} \) is a monic polynomial of degree \( p^d \), and \( g_c \) is a monic polynomial of degree \( p \). Therefore the composition \( h \) is a monic polynomial of degree \( p^{d+1} \). We have just seen that \( h \) vanishes on the set \( V_2 \) of size \( p^{d+1} \), so \( h(x) \) must be \( \prod_{u \in V_2} (x - u) = f_{V_2}(x) \).

**Lemma 3.3.** If \( V \) is a finite-dimensional subspace of \( K \), then \( f_V \) is an additive homomorphism with kernel \( V \).

**Proof.** The fact that \( f_V \) is an additive homomorphism follows by induction on \( \dim V \) using Lemma 3.2. The fact that \( \ker f_V = V \) is immediate from the definition of \( f_V \).

We now can prove our desired theorem on NIP local domains in positive characteristic:

**Theorem 3.4.** Let \( p > 0 \) be a prime. Let \( R \) be a NIP \( \mathbb{F}_p \)-algebra with the following properties: \( R \) is a local ring, \( R \) is an integral domain with maximal ideal \( \mathfrak{m} \), and the quotient field \( k = R/\mathfrak{m} \) is infinite. Then \( x \mapsto x^p - x \) is a surjection from \( R \) onto \( R \).

**Proof.** Let \( K = \text{Frac}(R) \). Note that if \( V \) is a finite-dimensional \( \mathbb{F}_p \)-subspace of \( R \), then \( f_V(x) \in R[x] \), and if \( c \in R \), then \( g_c(x) \in R[x] \).
Claim 3.5. It suffices to find \( c \in R^\times \) such that \( g_c(x) \) is a surjection from \( R \) to \( R \).

Proof of claim. Note that \( c^{-p} g_c(cx) = c^{-p}(c^p x^p - c^{p-1}cx) = x^p - x \). The maps \( x \mapsto cx \) and \( x \mapsto c^{-p}x \) are bijections on \( R \), so if \( g_c \) is surjective then so is \( g_1(x) = x^p - x \). \( \square \)

For any \( c \in R \), the polynomial \( g_c(x) \) defines an additive map \( R \to R \), whose image \( g_c(R) \) is an additive subgroup of \( R \). Let \( G = \{ g_c(R) : c \in R \} \). By the Baldwin–Saxl theorem for NIP groups, there is some integer \( n \) such that if \( G_1, \ldots, G_n \in G \), then there is some \( i \) such that

\[
G_i \supseteq G_1 \cap \cdots \cap G_{i-1} \cap G_{i+1} \cap \cdots \cap G_n.
\]

Fix such an \( n \geq 2 \).

The residue field \( k \) is infinite, and therefore we can find \( \mathbb{F}_p \)-linearly independent \( \alpha_1, \ldots, \alpha_n \in k \). Take \( a_i \in R \) lifting \( \alpha_i \in k \). Note \( \alpha_i \neq 0 \), so \( a_i \notin m \), and thus \( a_i \in R^\times \). Also note that the elements \( \{a_1, \ldots, a_{n-1}\} \) are \( \mathbb{F}_p \)-linearly independent in \( K \).

Let \( [n] = \{1, \ldots, n\} \). If \( S \subseteq [n] \) and \( i \in [n] \), we write \( S \cup i \) and \( S \setminus i \) as abbreviations for \( S \cup \{i\} \) and \( S \setminus \{i\} \). Even worse, we sometimes abbreviate \( \{i\} \) as \( i \).

For \( S \subseteq [n] \), let \( V_S \) be the \( \mathbb{F}_p \)-linear span of \( \{a_i : i \in S\} \). Then \( V_S \) has dimension \( |S| \).

Let

\[
f_S(x) := f_{V_S}(x) = \prod_{a \in V_S} (x - a).
\]

This is a monic polynomial in \( R[x] \). By Lemma 3.3 \( f_S(x) \) induces an additive homomorphism \( K \to K \), and therefore an additive homomorphism \( R \to R \).

Note that \( f_i(x) = f_{V_i}(x) = f_{\mathbb{F}_p a_i}(x) = g_{a_i}(x) \) by Lemma 3.1. By Claim 3.5, it suffices to show that \( f_i \) is a surjection from \( R \) to \( R \), for at least one \( i \).

If \( S \subseteq [n] \) and \( i \in [n] \setminus S \), then \( V_{S \cup i} \) has dimension one more than \( V_S \). By Lemma 3.2, there is some \( c_{S,i} \in f_S(V_{S \cup i}) \) such that \( g_{c_{S,i}} \circ f_S = f_{S \cup i} \). Let \( g_{S,i} := g_{c_{S,i}} \).

Then

\[
g_{S,i} \circ f_S = f_{S \cup i}.
\]

Now \( c_{S,i} \in f_S(V_{S \cup i}) \), but \( f_S(x) \in R[x] \) and \( V_{S \cup i} \subseteq R \). Therefore \( c_{S,i} \in R \), and \( g_{S,i}(x) \in R[x] \).

Claim 3.6. If \( S \subseteq [n] \) and \( i, j \) are distinct elements of \( [n] \setminus S \), then \( c_{S,i}^{p-1} - c_{S,j}^{p-1} \notin m \).

Proof of claim. Otherwise, the two polynomials \( g_{S,i}(x) \) and \( g_{S,j}(x) \) have the same reduction modulo \( m \). From the identities \( f_{S \cup i} = g_{S,i} \circ f_S \) and \( f_{S \cup j} = g_{S,j} \circ f_S \), it follows that \( f_{S \cup i} \equiv f_{S \cup j} \mod m \). Let \( V'_S \) be the \( \mathbb{F}_p \)-linear span of \( \{a_i : i \in S\} \), or equivalently, the image of \( V_S \) under \( R \to R/m \). By inspection, the reduction of \( f_S \) modulo \( m \) is \( \prod_{u \in V'_S} (x - u) \). Since \( V'_{S \cup i} \neq V'_{S \cup j} \), it follows immediately that \( f_{S \cup i} \) and \( f_{S \cup j} \) cannot have the same reduction modulo \( m \), a contradiction. \( \square \)
Each of the groups \( g_{[n]\setminus i, i}(R) \) is in the family \( \mathcal{G} \). By choice of \( n \), one of the factors in the intersection \( \bigcap_{i=1}^{n} g_{[n]\setminus i, i}(R) \) is irrelevant. Without loss of generality, it is the first factor:

\[
g_{[n]\setminus 1, 1}(R) \supseteq \bigcap_{i=2}^{n} g_{[n]\setminus i, i}(R). \tag{2}
\]

We claim that \( f_1(x) \) defines a surjection from \( R \) to \( R \). As \( f_1(x) = g_{\alpha_1}(x) \), this suffices, by Claim 3.5.

Take some \( b_1 \in R \). It suffices to show that \( b_1 \in f_1(R) \). Take some \( b_{\varnothing} \in K^{\text{alg}} \) such that \( f_1(b_{\varnothing}) = b_1 \). It suffices to show that \( b_{\varnothing} \in R \). For \( S \subseteq [n] \), define \( b_S = f_S(b_{\varnothing}) \in K^{\text{alg}} \). (When \( S = \{1\} \) this recovers \( b_1 \), and when \( S = \varnothing \) this recovers \( b_{\varnothing} \), so the notation is consistent.) Note that

\[
g_{S,i}(b_S) = g_{S,i}(f_S(b_{\varnothing})) = f_{S \cup i}(b_{\varnothing}) = b_{S \cup i}. \tag{3}
\]

**Claim 3.7.** If \( 1 \in S \subseteq [n] \), then \( b_S \in R \).

**Proof of claim.** Take a minimal counterexample \( S \). If \( S = \{1\} \), then \( b_S = b_1 \in R \). Otherwise, take \( i \in S \setminus 1 \) and let \( S_0 = S \setminus i \). By choice of \( S \), we have \( b_{S_0} \in R \). Then \( b_S = g_{S_0,i}(b_{S_0}) \). But \( g_{S_0,i}(x) \in R[x] \), so \( b_S \in R \).

In particular, \( b_S \in R \) for \( S = [n] \), as well as \( S = [n] \setminus i \) for \( i > 1 \). Then

\[
b_{[n]} = g_{[n]\setminus i, i}(b_{[n]\setminus i}) \in g_{[n]\setminus i, i}(R)
\]

for \( 1 < i \leq n \). By (2), \( b_{[n]} \in g_{[n]\setminus 1, 1}(R) \). Take \( v \in R \) such that \( g_{[n]\setminus 1, 1}(v) = b_{[n]} \). Then \( g_{[n]\setminus 1, 1}(v) = b_{[n]} = g_{[n]\setminus 1, 1}(b_{[n]\setminus 1}) \), and so

\[
v - b_{[n]\setminus 1} \in \ker g_{[n]\setminus 1, 1} = \mathbb{F}_p \cdot c_{[n]\setminus 1, 1} \subseteq R.
\]

Therefore \( b_{[n]\setminus 1} \in R \). So we see that

\[
b_{[n]\setminus i} \in R \quad \text{for all} \quad 1 \leq i \leq n. \tag{4}
\]

**Claim 3.8.** \( b_{\varnothing} \in R \).

**Proof of claim.** Suppose otherwise. Take \( S \) maximal such that \( b_S \notin R \). By Claim 3.7 and (4), \( S \) is neither \( [n] \) nor \( [n] \setminus i \) for \( 1 \leq i \leq n \). Therefore \( [n] \setminus S \) contains at least two elements \( i, j \). By choice of \( S \), we have \( b_{S \cup i} \in R \) and \( b_{S \cup j} \in R \). By (3),

\[
b_{S \cup i} = g_{S,i}(b_S) = b_S^p - c_{S,i}^{p-1} b_S \quad \text{and} \quad b_{S \cup j} = g_{S,j}(b_S) = b_S^p - c_{S,j}^{p-1} b_S.
\]

Therefore

\[
(c_{S,i}^{p-1} - c_{S,j}^{p-1}) b_S = b_{S \cup j} - b_{S \cup i} \in R.
\]

By Claim 3.6, \( c_{S,i}^{p-1} - c_{S,j}^{p-1} \in R \setminus m = R^\times \), and so \( b_S \in R \), a contradiction. \( \square \)
This completes the proof. We see that $b_{\emptyset} \in R$, and so $b_1 = f_1(b_{\emptyset}) \in f_1(R)$. As $b_1$ was an arbitrary element of $R$, it follows that $f_1$ gives a surjection from $R$ to $R$. But $f_1(x) = g_{a_1}(x)$, and $a_1 \in R^\times$ (since its residue mod $m$ is the nonzero element $\alpha_1$), and so we are done by Claim 3.5. \qed

3B. Linearly ordering the primes.

**Lemma 3.9.** Let $R$ be an $\mathbb{F}_p$-algebra that is integral and has exactly two maximal ideals $m_1$ and $m_2$. Suppose that $R/m_1$ and $R/m_2$ are infinite. Then $R$ isn’t NIP.

The proof uses an identical strategy to [Johnson 2021a, Lemma 2.6].

**Proof.** Suppose $R$ is NIP. By Corollary 2.4, $m_1$ and $m_2$ are definable. Let $K = \text{Frac}(R)$. Regard the localizations $R_{m_1}$ and $R_{m_2}$ as definable subrings of $K$. Note that $R_{m_1} \cap R_{m_2} = R$, by commutative algebra. (If $x \in K \setminus R$, then let $I = \{a \in R : ax \in R\}$; this is a proper ideal in $R$, so it is contained in some $m_i$, and then $I \subseteq m_i$ means precisely that $x \notin R_{m_i}$.)

**Claim 3.10.** If $x \in R$, then the Artin–Schreier roots of $x$ are in $R$.

**Proof of claim.** The rings $R_{m_1}$ and $R_{m_2}$ satisfy the conditions of Theorem 3.4. (The residue field of $R_{m_i}$ is isomorphic to $R/m_i$, hence infinite.) Therefore, there are $y \in R_{m_1}$ and $z \in R_{m_2}$ such that $y^p - y = z^p - z$. Then $y - z$ is in the kernel of the Artin–Schreier map, which is $\mathbb{F}_p$, so $y \in z + \mathbb{F}_p \subseteq R_{m_2}$. As $y \in R_{m_1}$, this implies $y \in R_{m_1} \cap R_{m_2} = R$. Thus, at least one Artin–Schreier root (y) is in $R$. The other Artin–Schreier roots of $x$ are the elements of $y + \mathbb{F}_p$, which are all in $R$. \[\qed\]

Let $J = m_1 \cap m_2$. This is the Jacobson radical of $R$. By Proposition 2.16, $J = J^{00}$, and there are no definable subgroups of finite index. Consider the sets

$$\Delta = \{(x, i, j) \in R \times \mathbb{F}_p \times \mathbb{F}_p : x - i \in m_1, \ x - j \in m_2\},$$

$$\Gamma = \{(x^p - x, i - j) : (x, i, j) \in \Delta\}.$$  

Then $(\Delta, +)$ and $(\Gamma, +)$ are definable groups.

**Claim 3.11.** $\Gamma$ is the graph of a group homomorphism $\psi$ from $(J, +)$ onto $(\mathbb{F}_p, +)$.

**Proof of claim.** First, we show that $\Gamma \subseteq J \times \mathbb{F}_p$. Suppose that $(x, i, j) \in \Delta$. Then $x \equiv i \pmod{m_1}$, so $x^p - x \equiv i^p - i \equiv 0 \pmod{m_1}$, and $x^p - x \in m_1$. Similarly, $x^p - x \in m_2$, and therefore $x^p - x \in J$. Thus $(x^p - x, i - j) \in J \times \mathbb{F}_p$.

Next we show that $\Gamma$ projects onto $J$. Take $y \in J$. By Claim 3.10 there is $x \in R$ with $x^p - x = y$. Then $x^p - x \equiv y \equiv 0 \pmod{m_1}$, so $x^p - x \equiv i \pmod{m_1}$ for some $i \in \mathbb{F}_p$. Similarly, $x^p - x \equiv j \pmod{m_2}$ for some $j \in \mathbb{F}_p$. Then $(x, i, j) \in \Delta$ and $(x^p - x, i - j) = (y, i - j) \in \Gamma$.

Next we show that the projection $\Gamma \rightarrow J$ is one-to-one. Otherwise, $\Gamma \rightarrow J$ has nontrivial kernel, so there is $(x, i, j) \in \Delta$ with $x^p - x = 0$ but $i - j \neq 0$. The fact
that \( x^p - x = 0 \) implies \( x \in \mathbb{F}_p \), and so \( x \equiv i \pmod{m_1} \) implies \( x = i \). Similarly, \( x = j \). But then \( i - j = 0 \), a contradiction.

So now we see that \( \Gamma \rightarrow J \) is one-to-one and onto, implying that \( \Gamma \) is the graph of some group homomorphism \( \psi \) from \( J \) to \( \mathbb{F}_p \). It remains to show that \( \psi \) is onto. Equivalently, we must show that \( \Gamma \) projects onto \( \mathbb{F}_p \). Let \( i \in \mathbb{F}_p \) be given. By the Chinese remainder theorem, there is \( x \in R \) such that \( x \equiv i \pmod{m_1} \) and \( x \equiv 0 \pmod{m_2} \). Then \( (x, i, 0) \in \Delta \), so \((x^p - x, i - 0) \in \Gamma \). The element \((x^p - x, i)\) projects onto \( i \). Equivalently, \( \psi(x^p - x) = i \).

Therefore there is a definable surjective group homomorphism \( \psi : J \rightarrow \mathbb{F}_p \). The kernel \( \ker \psi \) is a definable subgroup of \( J \) of index \( p \). This contradicts Proposition 2.16. \( \square \)

**Lemma 3.12.** Let \( R \) be a NIP integral \( \mathbb{F}_p \)-algebra. Let \( p_1 \) and \( p_2 \) be prime ideals such that \( R/p_1 \) and \( R/p_2 \) are infinite. Then \( p_1 \) and \( p_2 \) are comparable.

**Proof.** Suppose otherwise. Let \( S = R \setminus (p_1 \cup p_2) \). Then \( S \) is a multiplicative subset of \( R \). Let \( R' = S^{-1}R \). Then \( R' \) is NIP by Corollary 2.12. The ring \( R' \) has exactly two maximal ideals \( m_1 \) and \( m_2 \), where \( m_i = p_i R' \). The map \( R/p_i \rightarrow R'/m_i \) is injective, so \( R'/m_i \) is infinite, for \( i = 1, 2 \). This contradicts Lemma 3.9. \( \square \)

**Lemma 3.13.** Let \( R \) be an \( \mathbb{F}_p \)-algebra that is integral and has exactly two maximal ideals \( m_1 \) and \( m_2 \). Then \( R \) isn’t NIP.

**Proof.** Assume otherwise. Going to an elementary extension, we may assume that \( R \) is very saturated (Lemma 2.8). By the Chinese remainder theorem, there is some \( a \in R \) such that \( a \equiv 0 \pmod{m_1} \) but \( a \equiv 1 \pmod{m_2} \).

Let \( \Sigma(x) \) be the partial type saying that \( x \in m_1 \), \( x \notin m_2 \), and \( x \) does not divide \( a^n \) for any \( n \).

**Claim 3.14.** \( \Sigma(x) \) is finitely satisfiable.

**Proof of claim.** Let \( n \) be given. We claim there is an \( x \) such that \( x \in m_1 \), \( x \notin m_2 \), and \( x \) does not divide \( a^i \) for \( i \leq n \). Take \( x = a^{n+1} \). Then \( x \equiv 0^{n+1} \equiv 0 \pmod{m_1} \), so \( x \in m_1 \). But \( x \equiv 1^{n+1} \equiv 1 \pmod{m_2} \), so \( x \notin m_2 \). Finally, suppose \( x = a^{n+1} \) divides \( a^i \) for some \( i \leq n \). Then there is \( u \in R \) with \( ua^{n+1} = a^i \). Since \( R \) is a domain, we can cancel a factor of \( a^i \) from both sides, and see \( ua^{n+1-i} = 1 \). This implies that \( a \) is a unit, contradicting the fact that \( a \in m_1 \). \( \square \)

By saturation, there is \( a' \in R \) satisfying \( \Sigma(x) \). The principal ideal \((a')\) does not intersect the multiplicative set \( S := a^\mathbb{N} \), by definition of \( \Sigma(x) \). Let \( p_1 \) be maximal among ideals containing \((a')\) and avoiding \( S \). Then \( p_1 \) is a prime ideal. (In general, any ideal that is maximal among ideals avoiding a multiplicative set is prime.)

Now \( p_1 \nsubseteq m_2 \), because \( a' \in p_1 \) but \( a' \notin m_2 \). But \( p_1 \) must be contained in some maximal ideal, and so \( p_1 \nsubseteq m_1 \). The inclusion is strict, because \( a \in m_1 \) but \( a \notin p_1 \). Thus \( p_1 \nsubseteq m_1 \) and \( p_1 \nsubseteq m_2 \). In particular, \( p_1 \) is not a maximal ideal.
Similarly, there is a nonmaximal prime ideal \( p_2 \) with \( p_2 \subseteq m_2 \) and \( p_2 \nsubseteq m_1 \). Then \( p_1 \) and \( p_2 \) are incomparable. Otherwise, say, \( p_1 \subseteq p_2 \subseteq m_2 \), and so \( p_1 \subseteq m_2 \), a contradiction. For \( i = 1, 2 \), the fact that \( p_i \) is a nonmaximal prime ideal implies that \( R/p_i \) is a nonfield integral domain, and therefore infinite. This contradicts Lemma 3.12.

\[ \square \]

**Theorem 3.15.** Let \( R \) be a NIP integral \( \mathbb{F}_p \)-algebra. Then the prime ideals of \( R \) are linearly ordered by inclusion.

**Proof.** The same proof as Lemma 3.12, using Lemma 3.13 instead of Lemma 3.9. \( \square \)

**Corollary 3.16.** Let \( R \) be a NIP \( \mathbb{F}_p \)-algebra. Let \( p_1, p_2, \) and \( q \) be prime ideals. If \( p_i \supseteq q \) for \( i = 1, 2 \), then \( p_1 \) is comparable to \( p_2 \).

**Proof.** Otherwise, \( p_1 \) and \( p_2 \) induce incomparable primes in the NIP domain \( R/q \). \( \square \)

### 3C. Henselianity

**Definition 3.17.** A forest is a poset \((P, \leq)\) with the property that if \( x \in P \), then the set \( \{ y \in P : y \geq x \} \) is linearly ordered.

**Definition 3.18.** A ring \( R \) is good if \( \text{Spec} \, R \) is a forest of finite width.

**Lemma 3.19.**

1. If \( R \) is a NIP \( \mathbb{F}_p \)-algebra, then \( R \) is good.
2. If \( R \) is good, then any quotient \( R/I \) is good.
3. If \( R \) is good, then \( R \) is a finite product of local rings.

**Proof.**

1. **Fact 2.1** and **Corollary 3.16**.
2. This is clear, since \( \text{Spec} \, R/I \) is a subposet of \( \text{Spec} \, R \).
3. We now break our usual convention, and regard \( \text{Spec} \, R \) as a scheme, or at least a topological space. By scheme theory, it suffices to write \( \text{Spec} \, R \) as a finite disjoint union of clopen sets \( U_i \) such that each \( U_i \) contains a unique closed point. Let \( m_1, \ldots, m_n \) be the maximal ideals of \( R \). There are finitely many because \( \text{Spec} \, R \) has finite width. Note that every prime ideal \( p \in R \) satisfies \( p \subseteq m_i \) for a unique \( i \). (There is at least one \( i \) by Zorn’s lemma, and at most one \( i \) because \( \text{Spec} \, R \) is a forest.) Let \( U_i \) be the set of primes below \( m_i \). Then \( \text{Spec} \, R \) is a disjoint union of the \( U_i \). It remains to show that each \( U_i \) is clopen. It suffices to show that each \( U_i \) is closed. Take \( i = 1 \). Let \( p_1, \ldots, p_m \) be the minimal primes contained in \( m_1 \). (There are finitely many, because of finite width.) Let \( V_j \) be the set of primes containing \( p_j \). Then \( V_j \) is a closed subset of \( \text{Spec} \, R \) — it is the closed subset cut out by the ideal \( p_j \). Moreover, \( V_j \subseteq U_1 \), because \( \text{Spec} \, R \) is a forest. The sets \( V_1, \ldots, V_m \) cover \( U_1 \), because every prime contains a minimal prime. Then \( U_1 \) is a finite union of closed sets \( \bigcup_{i=1}^m V_i \), and so \( U_1 \) is closed. \( \square \)

**Proposition 3.20.** Let \( R \) be a NIP local \( \mathbb{F}_p \)-algebra. Then \( R \) is a henselian local ring.
Proof. By [Stacks 2005–, Lemma 04GG, condition (9)], it is sufficient to prove the following: any finite \( R \)-algebra is a product of local rings. Let \( S \) be a finite \( R \)-algebra. Let \( a_1, \ldots, a_n \) be elements of \( S \) which generate \( S \) as an \( R \)-module. Each \( a_i \) is integral over \( R \) [Dummit and Foote 2004, Proposition 15.23], so there is a monic polynomial \( P_i(x) \in R[x] \) such that \( P_i(a) = 0 \) in \( S \). Then there is a surjective homomorphism

\[
R[x_1, \ldots, x_n]/(P_1(x_1), \ldots, P_i(x_i)) \to S.
\]

The ring on the left is interpretable in \( R \) — it is a finite-rank free \( R \)-module with basis the monomials \( \prod_{i=1}^n x_i^{n_i} \) for \( \bar{n} \in \prod_{i=1}^n \{0, 1, \ldots, \deg P_i - 1\} \). Therefore, the left-hand side is a NIP ring. By Lemma 3.19, it is good, \( S \) is good, and \( S \) is a finite product of local rings.

Theorem 3.21. Let \( R \) be a NIP \( \mathbb{F}_p \)-algebra. Then \( R \) is a finite product of henselian local rings.

Proof. By Lemma 3.19, \( R \) is good, and \( R \) is a finite product of local rings. These local rings are easily seen to be interpretable in \( R \), so they are also NIP. By Proposition 3.20, they are henselian local rings.

Theorem 3.22. Let \( R \) be a NIP, integral \( \mathbb{F}_p \)-algebra. Then \( R \) is a henselian local domain.

Proof. \( R \) is a local ring by Theorem 3.15. So it is henselian by Proposition 3.20.

Recall that a field \( K \) is large (also called ample) if every smooth irreducible \( K \)-curve with at least one \( K \)-point contains infinitely many \( K \)-points [Pop 2014]. By [Pop 2010, Theorem 1.1], if \( R \) is a henselian local domain that is not a field, then \( \text{Frac}(R) \) is large. Therefore we get the following corollary:

Corollary 3.23. Let \( R \) be a NIP integral domain, and \( K = \text{Frac}(R) \). Suppose \( R \neq K \) and \( K \) has positive characteristic. Then \( K \) is large.

Large stable fields are classified [Johnson et al. 2020]. If we could extend this classification to large NIP fields, then Corollary 3.23 would tell us something very strong about NIP integral domains of positive characteristic.

Acknowledgement

The author was supported by Fudan University, and by grant no. 12101131 of the National Natural Science Foundation of China.

References


Received 4 Nov 2021. Revised 7 Dec 2021.

WILL JOHNSON:
willjohnson@fudan.edu.cn
School of Philosophy, Fudan University, Shanghai, China
Groups of finite Morley rank with a generically multiply transitive action on an abelian group

Ayşe Berkman and Alexandre Borovik

Worst-case expansions of complete theories

Samuel Braunfeld and Michael C. Laskowski

CM-trivial structures without the canonical base property

Thomas Blossier and Léo Jimenez

Kim-independence in positive logic

Jan Dobrowolski and Mark Kamsma

Henselianity in NIP $\mathbb{F}_p$-algebras

Will Johnson