GALOIS THEORY OVER INTEGRAL TATE ALGEBRAS*

by

Moshe Jarden

School of Mathematics, Tel Aviv University Ramat Aviv, Tel Aviv 69978, Israel e-mail: jarden@post.tau.ac.il and

Elad Paran

Mathematics Department, The Open University of Israel Raanana 43107, Israel e-mail: paranela@post.tau.ac.il

Abstract

We prove that if F is the quotient field of an integral Tate algebra over a complete nonarchimedean absolute valued field K, then Gal(F) is semi-free.

MR Classification: 12E30

^{*} Research supported by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation, and by an ISF grant.

Introduction

Integral Tate algebras over complete fields with respect to absolute values play a central role in rigid analytic geometry, analogous to the role of finitely generated integral domains over fields in algebraic geometry. Given a finitely generated domain A over a field K, the absolute Galois group $\operatorname{Gal}(F)$ of $F = \operatorname{Quot}(A)$ is in general unknown. We do not know if every group can be realized over F, let alone if every finite split embedding problem over F is solvable. In contrast, we prove that if K is complete under a non-archimedean absolute value $|\cdot|$ and A is a Tate algebra over K, then not only the inverse Galois problem over F has an affirmative solution but $\operatorname{Gal}(F)$ is even "semi-free".

To be more specific, recall that the **free affinoid algebra** $T_n = T_n(K)$ is defined as the ring of all formal power series $\sum a_i X_1^{i_1} \cdots X_n^{i_n}$ with coefficients a_i in K that converge to 0 as $\mathbf{i} \to \infty$. Each finitely generated integral extension domain A of $T_n(K)$ is an **integral Tate algebra**. A **finite split embedding problem** over F = Quot(A) is an epimorphism α : $B \to \text{Gal}(F'/F)$ of finite groups, where F' is a finite Galois extension of F and there exists a homomorphism α' : $\text{Gal}(F'/F) \to B$ such that $\alpha \circ \alpha' = \text{id}_{\text{Gal}(F'/F)}$. A **solution field** of the embedding problem is a Galois extension F'' of F that contains F' for which there exists an isomorphism γ : $\text{Gal}(F'/F) \to B$ such that $\alpha \circ \gamma = \text{res}_{F''/F'}$. One says [BHH11] that the absolute Galois group Gal(F) of F is **semi-free** if every finite split embedding problem α : $B \to \text{Gal}(F'/F)$ over F with a nontrivial kernel has a set $\{F_i \mid i \in I\}$ of solution fields of cardinality card(F) such that the fields F_i are linearly disjoint over F'. In particular, each finite group occurs as a Galois group of a Galois extension of F.

If $\operatorname{Gal}(F)$ is semi-free and projective, then by Chatzidakis-Melnikov, $\operatorname{Gal}(F)$ is a free profinite group [FrJ08, Theorem 25.1.7]. However, most of the absolute Galois groups that one encounters are not projective. This is in particular the case for $\operatorname{Gal}(F)$, at least if K is not real closed and the order of $\operatorname{Gal}(K)$ is is divisible by a prime $l \neq \operatorname{char}(K)$ (Proposition 7.1). Thus, the semi-freeness of $\operatorname{Gal}(F)$ is the best known approximation to freeness.

Semi-freeness of absolute Galois groups of fields has been previously proved for several types of fields, for example for function fields of one variable over an ample field ([Jar11, Theorem 11.7.1] or [BHH11, Theorem 7.2]), for fields of formal power series in at least two variables over an arbitrary field, and for $\text{Quot}(R[[X_1, \ldots, X_n]])$, where R is a Noetherian integral domain that is not a field and $n \geq 1$. The two latter examples are consequences of a theorem of Weissauer that those fields are Hilbertian, and a theorem of Pop asserting that those fields are ample (passage following the proof of Proposition 1.4) and Krull (Definition 1.1) [Jar11, Theorem 12.4.3], and on another result of Pop: If a field F is Hilbertian, ample, and Krull, then Gal(F) is semi-free of rank card(F)

[Jar11, Theorem 12.4.1].

Our proof takes a detour through the maximal purely inseparable extension F_{ins} of F. First we observe that the properties of being Hilbertian, ample, and Krull are preserved under finite algebraic extensions. Thus, it suffices to prove these properties for $F_n = \text{Quot}(T_n(K))$. The proof of Hilbertianity applies a theorem of Weissauer about generalized Krull domains (Corollary 3.4). To prove that F_n is ample, we use a criterion of Pop [Jar11, Proposition 5.7.7] and show that F_n is the quotient field of a domain complete with respect to a nonzero ideal. The main effort is however done in the proof that F_n is Krull (Proposition 4.4).

Using that F is Hilbertian and Krull, we apply [BaP10, Proposition 7.4] to conclude that F_{ins} is fully Hilbertian (Theorem 5.1(b)). This notion is a powerful strengthening of Hilbertianity that, combined with ampleness, implies the semi-freeness of the absolute Galois group of F. Since $\text{Gal}(F_{\text{ins}}) \cong \text{Gal}(F)$, the group Gal(F) is also semi-free.

Interesting examples for integral Tate algebras are the rings R_I of holomorphic functions on certain connected affinoids (Section 6) used by the method of "algebraic patching" in [HaV96] and subsequent works to solve finite split embedding problems over K(x), where K is a complete field with respect to an absolute value, and more generally when K is an ample field.

Acknowledgement: The authors thank Dan Haran for useful discussions.

1. Krull fields and fully Hilbertian fields

We recall the notions of a "Krull field" and of a "fully Hilbertian field" and prove that if K is an ample Hilbertian Krull field, then K_{ins} is fully Hilbertian and Gal(K) is semi-free.

Definition 1.1: [Pop10, §1] and [Jar11, Definition 12.2.2]. Let K be a field and let \mathcal{V} be a set of discrete valuations of K. We say that (K, \mathcal{V}) is a **Krull field** (or that K is a **Krull field with respect to** \mathcal{V}) if

(a) for each $a \in K^{\times}$ the set $\mathcal{V}_a = \{v \in \mathcal{V} \mid v(a) \neq 0\}$ is finite, and

(b) for each finite Galois extension K' of K the set $\operatorname{Spl}_{\mathcal{V}}(K'/K)$ of all $v \in \mathcal{V}$ that totally split in K' has the same cardinality as of K (in particular, taking K' = K, we get that $\operatorname{card}(\mathcal{V}) = \operatorname{card}(K)$).

We say that K is a **Krull field** if K is a Krull field with respect to some set of discrete valuations.

LEMMA 1.2: Let (K, \mathcal{V}) be a Krull field and and let F be a subfield of K with $\operatorname{card}(F) < \operatorname{card}(K)$. Denote the set of all $v \in \mathcal{V}$ that are trivial on F by \mathcal{F} . Then K is also a Krull field with respect to \mathcal{F} .

Proof: If F is finite, then $\mathcal{F} = \mathcal{V}$. Otherwise, F is infinite, hence K is uncountable. Since $\mathcal{F} \subseteq \mathcal{V}$, the family \mathcal{F} satisfies Condition (a) of Definition 1.1. By definition, $\mathcal{V} \setminus \mathcal{F} = \bigcup_{a \in F^{\times}} \mathcal{V}_a$, hence $\operatorname{card}(\mathcal{V} \setminus \mathcal{F}) = \operatorname{card}(\bigcup_{a \in F^{\times}} \mathcal{V}_a) \leq \operatorname{card}(F) \cdot \aleph_0 < \operatorname{card}(K)^2 = \operatorname{card}(K)$. Consequently, \mathcal{F} satisfies Condition (b) of Definition 1.1.

The following notion is introduced in the introduction to [BaP10].

Definition 1.3: A field K is said to be **fully Hilbertian** if every irreducible polynomial $f \in K[X, Y]$ which is separable in Y has the following property: Let (x, y) be a zero of f in some field extension of K such that x is transcendental over K, set F = K(x, y), and let L be the algebraic closure of K in F. Then there exists a subset A of K with card(A) = card(K) such that for each $a \in A$, f(a, Y) is irreducible over K and there exists $b_a \in \tilde{K}$ with $f(a, b_a) = 0$ and $L \subseteq K(b_a)$ such that the fields $K(b_a)$, $a \in A$, are linearly disjoint over L.

We denote the maximal purely inseparable extension of a field K by K_{ins} .

PROPOSITION 1.4: Let K be a Hilbertian Krull field. Then K_{ins} is fully Hilbertian.

Proof: If K is countable, then Hilbertianity and full Hilbertianity are equivalent properties [BaP10, Corollary 2.24]. Thus K is fully Hilbertian, hence by [BaP10, Theorem 1.3], so is K_{ins} .

Now assume K is uncountable, and let \mathcal{V} be a family of valuations on K such that (K, \mathcal{V}) is Krull. Let F be the prime field of K, and let \mathcal{F} be the family of valuations in \mathcal{V} which are trivial on F. Since K is uncountable, $\operatorname{card}(F) < \operatorname{card}(K)$, hence by Lemma 1.2, (K, \mathcal{F}) is also Krull. By [BaP10, Proposition 7.4], K_{ins} is fully Hilbertian.

Recall that a field K is **ample** if K is existentially closed in the field K((t)) of formal power series in the free variable t. Alternatively, if each absolutely irreducible K-curve with a simple K-rational point has infinitely many K-rational points [Jar11, Definition 5.3.2]. Examples of ample fields are PAC fields [Jar11, Example 5.6.1], quotient fields of domains that are complete (or even Henselian) with respect to nonzero ideals [Jar11, Proposition 5.7.3], and fields whose absolute Galois groups are pro-p for a single prime number p [Jar08, Theorem 5.8.3]. The strongest result about ample fields concerning solutions of finite embedding problems is that the absolute Galois groups of function fields of one variable over them are semi-free ([Jar11, Theorem 11.7.1] or [BHH11, Theorem 7.2]).

The next result is due to Pop ([Pop10, Thm. 1.2] or [Jar11, Thm. 12.4.1]):

PROPOSITION 1.5: Let K be an ample Hilbertian Krull field. Then Gal(K) is semi-free of rank card(K).

Proof: By Proposition 1.4, K_{ins} is fully Hilbertian. By [Pop96, Prop. 1.2] or [Jar11, Lemma 5.5.1], K_{ins} is ample. By [BaP10, Corollary 2.28], $\text{Gal}(K_{\text{ins}})$ is semi-free. Hence $\text{Gal}(K) \cong \text{Gal}(K_{\text{ins}})$ is semi-free.

Remark 1.6: Our proof of Proposition 1.5 is essentially the same as that of Pop. However, as an interim result we have proven that K_{ins} is fully Hilbertian (Proposition 1.4). That property for ample fields is stronger than just having a semi-free absolute Galois group [BaP10, Remark 2.14]. Thus, Proposition 1.4 is interesting for its own sake.

When K is also perfect, Proposition 1.4 asserts that K itself is fully Hilbertian. It is unknown whether this holds if K is non-perfect.

2. Generalized Krull Domains

One method to produce Krull fields is to start with Krull domains or rather with "generalized Krull domains" with certain additional properties. The latter notion was introduced by Ribenboim in [Rib56].

Definition 2.1: Let R be an integral domain with quotient field K. Then R is a generalized Krull domain if K has a family \mathcal{V} of rank-1 (i.e. real-valued) valuations satisfying the following properties:

- (a) Denoting the valuation ring of v by R_v , we have $\bigcap_{v \in \mathcal{V}} R_v = R$.
- (b) For each $a \in K^{\times}$ the set $\mathcal{V}_a = \{v \in \mathcal{V} \mid v(a) \neq 0\}$ is finite.
- (c) For each $v \in \mathcal{V}$, R_v is the localization of R by the center $\mathfrak{p}_v = \{a \in R \mid v(a) > 0\}$ of v on R.

An equivalent formulation of this definition appears in [FrJ08, §15.4].

If R is a generalized Krull domain, then the family \mathcal{V} as above is unique up to equivalence of valuations [Par11, Lemma 1.3]. It is called the **essential family** of R. If every $v \in \mathcal{V}$ is discrete, then R is a **Krull domain**. All unique factorization domains and all integrally closed Noetherian domains are Krull domains [ZaS75, §VI.13]. By (a), every generalized Krull domain is integrally closed.

The quotient field K of a generalized Krull domain with an essential family \mathcal{V} satisfies Condition (a) of Definition 1.1. The following result proves that it satisfies a weak form of Condition (b) of that definition.

PROPOSITION 2.2: Let R be a generalized Krull domain of dimension at least 2, with essential family \mathcal{V} . Suppose F' is a finite Galois extension of F = Quot(R). Then there exist infinitely many valuations in \mathcal{V} that totally split in F'.

Proof: Let \mathfrak{m} be a maximal ideal of R, of height at least 2. By [FrJ08, Lemma 15.4.2], $R_{\mathfrak{m}}$ is also a generalized Krull domain of dimension at least 2. Replacing R by $R_{\mathfrak{m}}$, we assume that R is local and \mathfrak{m} is its unique maximal ideal.



We choose a primitive element z for F'/F integral over R, and let

$$f(T) = T^{n} + c_{n-1}T^{n-1} + \dots + c_0 \in R[T]$$

be its minimal polynomial over F. In particular, $c_0 \neq 0$. Then we multiply z with an element of \mathfrak{m} to assume that $d = \operatorname{discr}(f(T)) \in \mathfrak{m}$

We suppose by induction that $v_1, \ldots, v_k \in \mathcal{V}$ are valuations that totally split in F'. If k = 0, we set a = d. If $k \ge 1$ we choose for each $1 \le i \le k$ an element $a_i \in R$ with $v_i(a_i) > 0$, and set $a = da_1 \cdots a_k$. Then $v_i(a) > 0$ for $i = 1, \ldots, k$ and $a \in \mathfrak{m}$.

By [FrJ08, Lemma 15.4.1(a)], $\mathcal{V}_a \neq \emptyset$. there exists $w \in \mathcal{V}$ with w(a) > 0. By (b) the set $\mathcal{V}_a \cup \mathcal{V}_{c_0}$ consists of finitely many elements w_1, w_2, \ldots, w_m .

For each $w \in \mathcal{V}$, let $\mathfrak{p}_w = \{x \in R \mid w(x) > 0\}$ be the center of w on R. Since R is a generalized Krull domain and \mathcal{V} is its essential family of valuations, $R_{\mathfrak{p}_w}$ is the valuation ring of w in F. Since w is of rank 1, \mathfrak{p}_w is a minimal prime ideal of R. We set $\mathfrak{p}_i = \mathfrak{p}_{w_i}$ for $i = 1, \ldots, m$. Since the height of \mathfrak{m} is at least 2, \mathfrak{m} properly contains each \mathfrak{p}_i . Hence, \mathfrak{m} strictly contains $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_m$ [AtM69, Proposition 1.11]. We choose $b \in \mathfrak{m} \setminus (\mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_m)$ and consider $w \in \mathcal{V}_b$. Then w(a) = 0 and $w(c_0) = 0$, otherwise $w = w_i$ for some $1 \leq i \leq m$, so $w_i(b) > 0$, hence $b \in \mathfrak{p}_i$ in contrast to the choice of b. Thus,

(1) If $w \in \mathcal{V}$ satisfies w(a) > 0 or $w(c_0) > 0$, then w(b) = 0. Since $a, b \in \mathfrak{m}$ the element

Since $a, b \in \mathfrak{m}$, the element

(2)
$$c = c_0^{n-1}a^n + c_0^{n-2}c_{n-1}a^{n-1}b + \dots + c_0c_2a^2b^{n-2} + c_1ab^{n-1} + b^n$$

belongs to \mathfrak{m} , hence by [FrJ08, Lemma 15.4.1(a)], there exists $v_{k+1} \in \mathcal{V}$ such that $v_{k+1}(c) > 0$. If $v_{k+1}(b) > 0$, then $v_{k+1}(c_0) > 0$ or $v_{k+1}(a) > 0$, contradicting (1). Hence, $v_{k+1}(b) = 0$. By (2), $v_{k+1}(a) = 0$. Therefore, $v_{k+1} \neq v_1, \ldots, v_k$ and $v_{k+1}(d) = 0$.

Finally we prove that v_{k+1} totally splits in F'. Indeed, $f(\frac{c_0a}{b}) = \frac{c_0c}{b^n}$, so $v_{k+1}(f(\frac{c_0a}{b})) > 0$. Let v'_{k+1} be an extension of v_{k+1} to F', and use a bar to denote reduction modulo v'_{k+1} . Then $\bar{c}_0 \frac{\bar{a}}{b}$ is a root of $\bar{f}(T)$ in \bar{F} . Since $\bar{d} \neq 0$, this implies that v_{k+1} totally splits in F' (see also [Jar11, Remark 12.2.1(b)]).

COROLLARY 2.3: Let R be a countable generalized Krull domain of dimension at least 2 with an essential family \mathcal{V} . Then $(\text{Quot}(R), \mathcal{V})$ is a Krull field.

Proof: Condition (a) of Definition 1.1 follows from Condition (a) of Definition 2.1. Condition (b) of Definition 1.1 is a consequence of Proposition 2.2, because $\operatorname{card}(\operatorname{Quot}(R)) = \aleph_0$.

3. Free Affinoid Algebras

We recall the notion of a free affinoid algebra and prove that its quotient field is Hilbertian and ample. In the next section we prove that such a field is Krull.

Let R be a domain, complete with respect to a non-archimedean absolute value $|\cdot|$. Let R[[X]] be the ring of formal power series in X over R. We consider the following subring of R[[X]]:

$$R\{X\} = \left\{ \sum_{i=0}^{\infty} a_i X^i \in R[[X]] \mid a_i \in R, \lim_{i \to \infty} |a_i| = 0 \right\}.$$

The absolute value of R extends to an absolute value of $R{X}$ by

$$|\sum_{i} f_i X^i| = \max_{i \ge 0} (|f_i|)$$

and $R{X}$ is complete with respect to $|\cdot|$ [Jar11, Lemma 2.2.1(c)]. Thus, for each $f \in R{X}$ there exists $a \in R$ with |f| = |a|.

Setup 3.1: We use the following convention for the rest of this work.

Let K be a complete field with respect to a non-archimedian absolute value $|\cdot|$. The **free affinoid algebra** $T_n = T_n(K)$ is the subring of $K[[X_1, \ldots, X_n]]$ consisting of all power series $f = \sum a_i X_1^{i_1} \cdots X_n^{i_n}$ with coefficients $\mathbf{a_i}$ in K that converge to 0 as $\min(i_1, \ldots, i_n) \to \infty$, where $(i_1, \ldots, i_n) = \mathbf{i}$. The absolute value of K extends to an absolute value of T_n by $|f| = \max(|a_i|)$ [FrP04, p. 46]. For each $n \ge 0$ we consider the subring $O_n = \{f \in T_n \mid |f| \le 1\}$ of T_n and observe that $O_n = O_{n-1}\{X_n\}$ when $n \ge 1$.

One observes that $T_n = T_{n-1}\{X_n\}$ for each $n \ge 1$. A non-zero element $f = \sum f_i X_n^i \in T_n$ is said to be **regular** (over T_{n-1}), if $f_d \in T_{n-1}^{\times}$, where $d = \max(i \mid |f_i| = |f|)$.

We denote the quotient field of T_n by F_n .

LEMMA 3.2: The ring T_n is a unique factorization domain of Krull dimension n. Moreover, if p is a prime element in T_n , then there exists an automorphism σ of T_n such that $\sigma(p)$ is an associate of an irreducible monic polynomial $q \in O_{n-1}[X_n]$ with |q| = 1.

Proof: That T_n is a unique factorization domain of dimension n is stated in [FrP04, Theorem 3.2.1(2)]. Given p as in the lemma, we multiply p with an appropriate element of $K^{\times} \subseteq T_n^{\times}$ to assume that |p| = 1. By the Weierstrass preparation theorem [FrP04, Theorem 3.1.1(1)], there exists an automorphism σ such that $p' = \sigma(p)$ is regular with |p'| = 1 (note that "regular" in [FrP04] includes the condition on the norm to be 1).

PROPOSITION 3.3: The ring O_n is a generalized Krull domain with quotient field F_n and dim $(O_n) = n+1$. Moreover, if w denotes the real valuation on F_n that corresponds to the absolute value $|\cdot|$, and if \mathcal{V} is the family of valuations of F_n that correspond to the prime elements of T_n , then the essential family of O_n is $\mathcal{V}' = \mathcal{V} \cup \{w\}$.

Proof: We set $T = T_n$, $O = O_n$, and $F = F_n$. Let $0 \neq f \in T$. Then there exists $a \in K^{\times}$ with |a| = |f|, so $f = \frac{f}{a} \cdot a \in O \cdot K$. Therefore, $\operatorname{Quot}(O) = \operatorname{Quot}(T) = F$.

Since O_0 is a real valuation ring, its dimension is 1. Inductively, assuming that $\dim(O_{n-1}) = n$, we observe that the map $X_n \mapsto 0$ extends to an epimorphism $O_n \to O_{n-1}$ whose kernel $O_n X_n$ has height 1. Hence, $\dim(O_n) = \dim(O_{n-1}) + 1 = n + 1$.

We denote the valuation ring of F at $v \in \mathcal{V}$ by R_v . Since T is a unique factorization domain, Conditions (a), (b), (c) of Definition 2.1 hold for (T, \mathcal{V}) rather than for the pair (R, \mathcal{V}) of that definition. In particular, each element of F^{\times} satisfies v(a) = 0 for all but finitely many $v \in \mathcal{V}$, hence v(a) = 0 for all but finitely many $v \in \mathcal{V}'$ as well. Thus, \mathcal{V}' satisfies Condition (b) of Definition 2.1.

Suppose $f \in \bigcap_{v \in \mathcal{V}} R_v$. Since $\bigcap_{v \in \mathcal{V}} R_v = T$, we have $f \in T$. In addition, $w(f) \ge 0$. Equivalently, $|f| \le 1$, hence $f \in O$. Thus, (O, \mathcal{V}') satisfies Condition (a) of Definition 2.1.

It remains to prove that if $v \in \mathcal{V}'$, then $R_v = O_{\mathfrak{p}_v}$, where \mathfrak{p}_v is the center of vin O. First suppose that $v \in \mathcal{V}$. Then v is the p-adic valuation of F for some prime element p of T. In particular, v is trivial on K, because $K^{\times} \subseteq T^{\times}$. Since T is a unique factorization domain, $R_v = T_{\mathfrak{q}_v}$, where \mathfrak{q}_v is the center of v in T. Suppose $\frac{f}{g} \in R_v = T_{\mathfrak{q}_v}$, with $f, g \in T$ and $g \notin \mathfrak{q}_v$. We choose $b \in K^{\times}$ with $|b| \leq \min(|f^{-1}|, |g^{-1}|)$. Then g' = bgand f' = bf are in O. Moreover, v(g') = v(b) + v(g) = v(g) = 0. Thus, $g' \notin \mathfrak{p}_v$, hence $\frac{f}{g} = \frac{f'}{g'} = O_{\mathfrak{p}_v}$. This proves that $R_v = O_{\mathfrak{p}_v}$.

Finally, suppose that v = w and let $\frac{f}{g} \in F$ with $f, g \in O, w(f) \ge w(g)$. Dividing f, g by an element of K with value w(g), we may assume that w(g) = 0. Thus, $\frac{f}{g} \in O_{\mathfrak{p}_w}$, as needed.

COROLLARY 3.4: For each $n \ge 1$ the field F_n is Hilbertian.

Proof: By Proposition 3.3, O_n is generalized Krull domain of dimension at least 2 with quotient field F_n . By Weissauer's Theorem [FrJ08, Theorem 15.4.6], F_n is Hilbertian.

Remark 3.5: The case where n = 1 of Corollary 3.4 is [Jar11, Theorem 2.3.3]. For n > 1, Corollary 3.4 may be deduced without the use of Proposition 3.3. Indeed, the ring T_n is a unique factorization domain, and in particular a generalized Krull domain. Since dim $(T_n) = n > 1$, Weissauer's Theorem implies that $F_n = \text{Quot}(T_n)$ is Hilbertian. Nevertheless, Proposition 3.3 will be used in the proof of Proposition 4.4.

4. Proof that F_n is Ample and Krull

In the next section, we prove that the maximal purely inseparable extension of F_n is fully Hilbertian by proving that F_n is a Krull field (We keep the convention of Setup 3.1.) The main difficulty is to prove that the essential family of T_n satisfies Condition (b) of Definition 1.1.

LEMMA 4.1: Let A be an integral domain. Suppose A is complete with respect to a real valuation v and A is contained in the valuation ring R_v of v in Quot(A). Let t be a nonzero element of A with v(t) > 0. If $A[t^{-1}] \cap R_v = A$, then A is complete and Hausdorff with respect to the t-adic topology on A.

Proof: First note that since v(t) > 0 and $v(t) \in \mathbb{R}$, we have $\bigcap_{n=1}^{\infty} (tA)^n = \{0\}$. That is, A is Hausdorff with respect to the t-adic topology. Now we consider a Cauchy sequence $\{a_i\}_{i=1}^{\infty}$ in A with respect to the t-adic topology. Then there exists a sequence of integers $\{n_i\}_{i=1}^{\infty}$ with $t^{n_i}|a_{i+1} - a_i$ and $n_i \to \infty$. Thus, $v(a_{i+1} - a_i) \ge n_i v(t)$ for each i, so $v(a_{i+1} - a_i) \to \infty$. Since A is complete with respect to v, there exists $a \in A$ with $v(a_i - a) \to \infty$. For each $i \ge 1$, let m_i be an integer satisfying $\frac{v(a_i - a)}{v(t)} - 1 \le m_i \le \frac{v(a_i - a)}{v(t)}$. Then, $m_i \to \infty$ and $v(\frac{a_i - a}{t^{m_i}}) \ge 0$, which implies that $\frac{a_i - a}{t^{m_i}} \in A[t^{-1}] \cap R_v = A$ for each i. Thus, $t^{m_i}|a_i - a$ for each $i \ge 1$. Hence a_i converges t-adically to a.

LEMMA 4.2: Let $n \ge 0$ and let $t \in K^{\times}$ with |t| < 1. Then O_n is complete with respect to the t-adic topology.

Proof: Let $R_n = \{x \in F_n \mid |x| \leq 1\}$ be the valuation ring of $|\cdot|$ in F_n . Since $t \in K^{\times}$, we have $O_n[t^{-1}] \leq T_n$. Hence, $O_n \subseteq R_n \cap (O_n)[t^{-1}] \subseteq R_n \cap T_n = O_n$, so $O_n = (O_n)[t^{-1}] \cap R_n$. Hence by Lemma 4.1, O_n is complete with respect to the *t*-adic topology.

COROLLARY 4.3: For each $n \ge 1$, F_n is an ample field.

Proof: By Proposition 3.3, $F_n = \text{Quot}(O_n)$. By Lemma 4.2, O_n is complete with respect to the *t*-adic topology (for each $t \in K^{\times}$ with |t| < 1). Hence, by [Pop10, Theorem 1.1] or [Jar11, Proposition 5.7.7], F_n is ample.

Now we prove that F_n is a Krull field. The proof is an adaptation of [Par10, Proposition 5.5].

PROPOSITION 4.4: For each $n \ge 1$, F_n is a Krull field.

Proof: Set $F = F_n = \text{Quot}(T_n)$. By Lemma 3.2, T_n is a unique factorization domain. We choose a system of representatives S for the associate classes of the prime elements of T_n . Let \mathcal{V} be the family of all s-adic valuations of F with s ranging on S. Then each $v \in \mathcal{V}$ is discrete and \mathcal{V} satisfies Condition (a) of Definition 1.1. Let F' be a finite

Galois extension of F. We prove that there are card(K) valuations in \mathcal{V} that totally split in F'.

By Proposition 3.3, O_n is a generalized Krull domain with quotient field F. Therefore, we may choose a primitive element z for F'/F integral over O_n . Let $f = \operatorname{irr}(z, F)$. Then f is a monic polynomial with coefficients in O_n and f(z) = 0. In particular, $d = \operatorname{discr}(f)$ is a non-zero element of O_n .

Let \mathcal{V}' be the essential family of O_n (Definition 2.1). By Proposition 2.2, infinitely many valuations of \mathcal{V}' totally split in F'. By Proposition 3.3, $\mathcal{V}' \smallsetminus \mathcal{V}$ consists of one element. Hence, we may choose an $s \in S$ that totally splits in F' and $s \nmid d$. By Lemma 3.2, we may apply an automorphism of T_n to assume that s is an irreducible monic polynomial in $O_{n-1}[X_n]$ with |s| = 1.

We divide the rest of the proof into two parts.

PART A: Modification of s. We set $X = X_n$. As a generalized Krull domain, O_n is integrally closed. Set $P = O_n \cap T_n s$. Since s does not divide d, z generates the integral closure $O'_{n,P}$ of the local ring of $O_{n,P}$ [FrJ08, Lemma 6.1.2]. Let P' be a prime ideal of $O'_{n,P}$ lying over $PO'_{n,P}$. Then, the residue of z modulo P' generates the residue field $\overline{F'}$ of F' over $\overline{F} = O_{n,P}/PO_{n,P}$. Since s totally splits in F', we have $\overline{F'} = \overline{F}$. Hence, there exists $a \in O_n$ such that

(1)
$$f(a) \equiv 0 \mod O_n s \text{ and } b = f'(a) \not\equiv 0 \mod O_n s.$$

Since $s \in O_{n-1}[X]$ is monic with |s| = 1, s (viewed as an element of T_n) is regular. By the Weierstrass division theorem [FrP04, Theorem 3.1.1(2)], for each $g \in T_n$, there exist $q \in T_n$ and $r \in T_{n-1}[X]$ such that g = qs + r, $\deg_X(r) < \deg_X(s)$, and $|g| = \max(|q|, |r|)$. If also $g \in O_n$, then $|g| \le 1$, so $|q|, |r| \le 1$, hence $q, r \in O_n$. Therefore, $r \in T_{n-1}[X] \cap O_n = O_{n-1}[X]$.

It follows that $O_n/O_n s = O_{n-1}[x]$, where x (the reduction of X modulo s) satisfies a monic equation over O_{n-1} of degree $k = \deg_X(s)$. We denote the reduction of b modulo s by b_s . Then, $b_s^2 = q_s(x)$, where $q_s \in O_{n-1}[X]$ is a polynomial of degree less than k. Set $c = q_s(X)$. Then, $c \in O_{n-1}[X]$ satisfies

(2)
$$c \equiv b^2 \mod O_n s.$$

We choose $0 \neq t \in O_0$ with |t| < 1. For each $e \in O_0 \subseteq O_n$ with $|e| \leq |t|$ we set

$$(3) s_e = s + ce.$$

Then,

(4) there exists $u \in O_n^{\times}$ such that $cu \equiv b^2 \mod s_e O_n$.

Indeed, by (2) there exists $g \in O_n$ such that $c = b^2 + gs$. Then, u = 1 + ge is invertible in O_n , because $|ge| \leq |e| < 1$ and O_n is complete with respect to $|\cdot|$. By (3), $c = b^2 + gs_e - gce \equiv b^2 - gce \mod s_eO_n$. Hence, $cu = c(1 + ge) \equiv b^2 \mod s_eO_n$, as claimed.

By (1) and (3), $f(a) \in O_n s \subseteq O_n s + O_n ce = O_n s_e + O_n ce$. Hence, by (2) and (1),

(5)
$$\bar{f}(\bar{a}) \in (\bar{c}\bar{e})\bar{O}_n = (\bar{b}^2\bar{e})\bar{O}_n = \bar{f}'(\bar{a})^2(\bar{O}_n\bar{e}),$$

where the bar denotes reduction of elements of O_n modulo s_e .

Since s is monic of degree k in X and $\deg_X(c) < k$, s_e is also monic of degree k (by (3)). Also, $|s_e| = 1$, because $|ce| < |e| \le 1 = |s|$. Applying the Weierstrass division theorem to s_e , we get that the ring $\bar{O}_n = O_{n-1}[\bar{X}]$ is a finite module over O_{n-1} . By Lemma 4.2, O_{n-1} is complete and Hausdorff with respect to tO_{n-1} . Since \bar{O}_n is a finite O_{n-1} -module, it follows from [ZaS75, p. 256, Theorem 5] that \bar{O}_n is complete with respect to the $t\bar{O}_n$ -adic topology.

Since $|e| \leq |t|$, we have $O_n e \subseteq O_n t$. Hence, by (5), $\bar{f}(\bar{a}) \in \bar{f}'(\bar{a})^2(\bar{O}_n \bar{e}) \subseteq \bar{f}'(\bar{a})^2(\bar{O}_n t)$. Therefore, by Hensel's Lemma (for the ring \bar{O}_n and the ideal $\bar{O}_n t$), there exists $a_e \in O_n$ such that $\bar{f}(\bar{a}_e) = 0$ [Eis95, p. 185], i.e. $f(a_e) \in O_n s_e$.

PART B: Many totally split primes. For each $e \in O_0$ satisfying $|e| \leq |t|$ let $s_e = s + ce$, as in (3), and let p_e be a prime factor of s_e in the unique factorization domain T_n . Dividing by a nonzero element of K of the same absolute value as p_e , we may assume that $|p_e| = 1$. It follows that p_e is also a prime element of O_n . Since $f(a_e) \in O_n s_e$, we also have $f(a_e) \in O_n p_e$.

We claim that if e, e' are distinct elements in O with $|e|, |e'| \leq |t|$, then $p_e, p_{e'}$ are non-associate prime elements of O_n . Indeed, suppose p_e is a product of $p_{e'}$ by an invertible element of O_n . Then p_e divides (s + ce) - (s + ce'), so $p_e|c(e - e')$. If $p_e|c$, then $p_e|s$, and since s is prime in O_n , s and p_e are associates, which implies that s|c. By (2) $c \equiv b^2 \mod O_n s$, so $b \equiv 0 \mod O_n s$, in contrast to (1). Thus, p_e does not divide c. If $p_e|e - e'$, then $|p_e| \leq |e - e'| \leq |t| < 1$, in contrast to the choice of p_e in the preceding paragraph. It follows that $p_e, p_{e'}$ are non-associate prime elements of O_n . This implies that $p_e, p_{e'}$ are non-associate prime elements of T_n . Indeed, if p_e and $p_{e'}$ are associates in T_n , then $\frac{p_e}{p_{e'}}, \frac{p_{e'}}{p_e} \in T_n$, and since $|p_e| = |p_{e'}| = 1$ this implies that $\frac{p_e}{p_{e'}}, \frac{p_{e'}}{p_e} \in O_n$, a contradiction.

Thus, each e in O with $|e| \leq 1$ yields a distinct prime p_e of T_n such that f has a root modulo p_e . Only finitely many of these primes divide d (since T_n is a unique factorization domain), all others split completely in F' (same argument as for s in Part A). The corresponding valuations in \mathcal{V} totally split in F'.

Finally we note that since K is complete with respect to a non-trivial nonarchimedean absolute value, we have $\operatorname{card}(K) = \operatorname{card}(K)^{\aleph_0}$ [Vam75, Lemma 2]. Since

 $K \subset T_n \subset K[[X_1, \ldots, X_n]]$, we have $\operatorname{card}(K) \leq \operatorname{card}(T_n) \leq \operatorname{card}(K)^{\aleph_0} = \operatorname{card}(K)$. Hence, $\operatorname{card}(T_n) = \operatorname{card}(K)$. Therefore, $\operatorname{card}(F) = \operatorname{card}(K)$. Consequently, F is a Krull field.

Remark 4.5: In the case where the absolute value $|\cdot|$ is discrete (that is, the corresponding valuation is discrete), Proposition 4.4 follows by applying [Pop10, Theorem 3.4(ii)] to the ring O_n and the ideal $\langle t, X_1 \rangle$, where t is a uniformizer of O. In the case where $|\cdot|$ is non-discrete (in particular, when K is algebraically closed), we cannot rely on [Pop10, Theorem 3.4].

5. Tate Algebras

We prove the main result of this work, namely that the quotient field of a Tate algebra has a semi-free absolute Galois group.

THEOREM 5.1: Let A be an integral Tate algebra over a complete field K with respect to a non-archimedean absolute value and let F = Quot(A). Then:

(a) F is Hilbertian and Krull.

(b) The maximal purely inseparable extension F_{ins} of F is fully Hilbertian.

(c) F is ample and Gal(F) is semi-free of rank card(F).

Proof: By definition, A is a finitely generated integral extension domain of T_n for some $n \ge 1$. Thus, in the notation of Setup 3.1, F is a finite field extension of $F_n = \text{Quot}(T_n)$. By Corollary 3.4, F_n is Hilbertian. By Proposition 4.4, F_n is a Krull field. Since F is a finite extension of F_n , F is Hilbertian [FrJ08, Proposition 12.3.3] and Krull [Jar11, Lemma 12.2.4], This proves (a).

It follows from [BaP10, Proposition 7.4] that F_{ins} is fully Hilbertian, which is (b).

By Corollary 4.3, F_n is ample. Hence, by [Pop96, Proposition 1.2] or [Jar11, Lemma 5.5.1], F is ample. Since F_{ins} is an algebraic extension of F, it is also ample. It follows from [BaP10, Theorem 1.6] that $Gal(F_{ins})$ is semi-free of rank $card(F_{ins})$. Since $Gal(F) = Gal(F_{ins})$ and $card(F) = card(F_{ins})$, we find that Gal(F) is semi-free of rank card(F).

Remark 5.2: The conclusion that Gal(F) is semi-free of rank card(F) follows also from [Pop10, Theorem 1.1] (see also [Jar11, Theorem 12.4.1]). We note that Pop's proof replaces the field F by a finite purely inseparable extension, like the step we take in (b).

6. Rings of Convergent Power Series

We apply Theorem 5.1 to rings of convergent power series that play a central role in "algebraic patching".

Let K be a complete field with respect to an absolute value $|\cdot|$ and let x be a variable. We extend $|\cdot|$ to the field K(x) by the rule $|\sum_{j=1}^{d} a_i x^i| = \max(|a_0|, \ldots, |a_d|)$ for $a_i \in K$ (the Gauss extension). Now we consider a positive integer n, let $I = \{1, \ldots, n\}$ and consider $c_1, \ldots, c_n \in K$ and $r_1, \ldots, r_n \in K^{\times}$ such that $|r_i| \leq |c_i - c_j|$ for all distinct i, j in I. Then we set $w_i = \frac{r_i}{x - c_i}$ and note that $|w_i| = 1$ for all i. Finally we consider the subring $R_0 = K[w_1, \ldots, w_n]$ of K(x) and let $R = R_I$ be the completion of the ring R_0 with respect to $|\cdot|$. This is the ring of holomorphic function on the connected affinoid $\bigcap_{i \in I} D(c_i, r_i)$, where $D(c_i, r_i) = \{z \in \mathbb{P}^1(\tilde{K}) \mid |z - c_i| \geq |r_i|\}$ [FrP04, Example 3.3.5].

In the case where the r_i 's are independent of i, the rings R_J , with J ranging on the subsets of I, satisfy certain rules that make them part of a "patching data" [Jar11, Definition 1.1.1] that eventually lead to the solution of all finite split embedding problems over K(x) [Jar11, Proposition 7.3.1]. Indeed, [Jar11, Proposition 7.4.4] proves even that Gal(K(x)) is semi-free profinite group of rank card(K). We prove here that the absolute Galois groups of the quotient fields of these rings are themselves semi-free.

The following lemma appears in [FrP04, Example 3.3.5] in the case where K is algebraically closed.

LEMMA 6.1: The integral domain R is an integral Tate algebra.

Proof: Let $T_{n0} = K[X_1, \ldots, X_n]$ equipped with the Gauss extension of $|\cdot|$. The map $X_i \mapsto w_i$ for $i \in I$ extends to a K-epimorphism $\varphi_0: T_{n,0} \to R_0$. For each $f = \sum a_j \prod_{i \in I} X_i^{j_i} \in T_{n0}$ with distinct monomials $\prod_{i \in I} X_i^{j_i}$, we have $|f| = \max(|a_j|)$. Since $|w_i| = 1$ for all $i \in I$, we have $|\varphi_0(f)| \leq \max(|a_j|) = |f|$. Since T_n and R are the completions of T_{n0} and R_0 with respect to the absolute value, this implies that φ_0 extends to a continuous K-epimorphism $\varphi: T_n \to R$. Then $R = T_n/\operatorname{Ker}(\varphi)$. By [FrP, Theorem 3.2.1(4)], R is a finitely generated extension of T_d , with $d = \dim(R)$. Thus, R is a Tate algebra.

Taking Lemma 6.1 into account, we get the following example for Theorem 5.1:

THEOREM 6.2: Let $R = R_I$ be as above and set F = Quot(R). Then, F is Hilbertian, Krull, and ample, Gal(F) is semi-free of rank card(F), and the maximal purely inseparable extension F_{ins} of F is fully Hilbertian.

7. Non-projectivity

Let A be an integral Tate algebra over a complete field K with respect to a nonarchimedean absolute value and let F = Quot(A). By Theorem 5.1, Gal(F) is semifree. We prove that in most cases this result can not be improved to "Gal(F) is free" by showing that Gal(F) is not projective.

PROPOSITION 7.1: Let A be an integral Tate algebra over a field K which is complete with respect to a non-archimedean absolute value $|\cdot|$ and let F = Quot(A). Then Gal(F) is not projective in each of the following cases:

- (a) $\dim(A) \ge 2$.
- (b) dim(A) = 1, K is not real closed [Lan93, Section XI.2], and the order of Gal(K) [FrJ08, Section 22.8] is divisible by a prime number $l \neq char(K)$.

Proof: Since K is complete with respect to $|\cdot|$, the field $K' = K(\sqrt{-1})$ is also complete with respect to the unique extension of $|\cdot|$. Moreover, under the assumptions of (b), K'is not formally real and the order of Gal(K) is divisible by a prime number $l \neq \operatorname{char}(K)$. By definition, the domain A is integral and finitely generated over $T_n = T_n(K)$ for some $n \geq 1$. By the going up theorem, dim(A) = dim(T_n) [HuS06, Theorem 2.2.5]. By Lemma 3.2, dim(T_n) = n, hence dim(A) = n. Let $T'_n = T_n[\sqrt{-1}]$, $A' = A[\sqrt{-1}]$, and $F' = F(\sqrt{-1})$. Then $T'_n = T_n(K')$ (because there exists a positive real number γ such that $|a + b\sqrt{-1}| \leq \gamma \max(|a|, |b|)$ for all $a, b \in K$ [CaF67, p. 57, Corollary] and $F' = \operatorname{Quot}(A')$. Moreover, A' is integral over $T_n(K')$, so A' is an integral Tate algebra over K' and dim(A') = dim(A). If Gal(F) is projective, so is Gal(F') [Rib70, Chapter IV, Proposition 2.1(a)]. Thus, replacing K, T_n, A, F , respectively, by K', T'_n, A', F' , if necessary, we may assume that K is not formally real, so K can not be ordered.

Now we set $T_0 = F_0 = K$. By Lemma 3.2, T_n is a unique factorization domain. In particular, T_n is Noetherian. The map $(X_1, \ldots, X_{n-1}, X_n) \mapsto (X_1, \ldots, X_{n-1}, 0)$ extends to a continuous K-epimorphism $T_n \mapsto T_{n-1}$ with $T_n X_n$ as its kernel. In particular, $T_n X_n$ is a prime ideal of T_n and X_n is a prime element of T_n .

We denote the discrete valuation of F_n that corresponds to X_n by v. Then the residue field of F_n with respect to v is F_{n-1} . We consider an extension w of v to F and let F_w be a Henselian closure of F with respect to w. The field F_w is a discrete Henselian valuation ring whose residue field \bar{F}_w is a finite extension of F_{n-1} . Since $K \subseteq F_{n-1}$ and K is not formally real, \bar{F}_w not formally real.

If $l \neq \operatorname{char}(K)$ is a prime number, then $l \in K^{\times}$, so l is invertible in the valuation ring of F_w . By [AGV63, Chap. x, Théorème 2.3], $\operatorname{cd}_l(\operatorname{Gal}(F_w)) = \operatorname{cd}_l(\operatorname{Gal}(F_{n-1})) + 1$. Since $\operatorname{Gal}(F_w)$ is a closed subgroup of $\operatorname{Gal}(F_n)$, we have $\operatorname{cd}_l(N) \leq \operatorname{cd}_l(F_n)$ [Rib70, p. 204, Proposition 2.1(a)]. Hence,

(1)
$$\operatorname{cd}_{l}(\operatorname{Gal}(F_{n})) \ge \operatorname{cd}_{l}(\operatorname{Gal}(F_{n-1})) + 1.$$

End of proof under Assumption (a): As in the second paragraph of the proof, X_n is a prime element of T_{n-1} . Let $l \neq \operatorname{char}(K)$ be a prime number. By Eisenstein's criterion, $F_{n-1}(\sqrt[l]{X_n})$ is a separable extension of F_{n-1} of degree l. Hence, by [Rib70, Chapter IV, Corollary 2.3], $\operatorname{cd}_l(F_{n-1}) \geq 1$. Consequently, by (1), $\operatorname{cd}_l(F_n) \geq 2$, so $\operatorname{Gal}(F)$ is not projective. End of proof under Assumption (b): Let $l \neq \text{char}(K)$ be a prime number that does not divide the order of Gal(K). By [Rib70, Chapter IV, Corollary 2.3], $\text{cd}_l(K) \geq 1$. Therefore, by (1), $\text{cd}(F_1) \geq 2$.

If K is a real closed field, then its unique ordering can be extended to K((x)) (e.g. by defining 0 < x < a for each positive $a \in K$), hence to $F_1 = \text{Quot}(K\{x\})$. Therefore, $\text{Gal}(F_1)$ contains an involution and consequently $\text{cd}_2(\text{Gal}(F_1)) = \infty$ [Rib70, Chapter IV, Proposition 2.1(a) and Corollary 2.5]. In particular, $\text{Gal}(F_1)$ is not projective. From the remaining cases, it seems that the first one to handle should be when K is separably closed.

PROBLEM 7.2: Let K be a separably closed field, x a variable, and $F = \text{Quot}(K\{x\})$. Is it true that Gal(F) is projective?

References

- [AGV73] M. Artin, A. Grothendieck, and J.-L. Verdier, Théorie des topos et cohomologie étale des schémas, Lecture Notes in Mathematics 305, Springer-Verlag, 1973 (SGA 4, vol. 3).
- [AtM69] M.F. Atiyah and I.G. Mackdonald, Introduction to Commutative Algebra, Addison– Wesley, Reading, 1969.
- [BaP10] L. Bary-Soroker and E. Paran, Fully Hilbertian fields, manuscript, Tel Aviv, 2010.
- [BHH11] L. Bary-Soroker, D. Haran and D. Harbater, *Permanence criteria for semi-free profinite groups*, Mathematische Annalen, to appear.
- [CaF67] J. W. S. Cassels and A. Fröhlich, Algebraic Number Theory, Academic Press, London, 1967.
- [Eis95] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Graduate Texts in Mathematics 150, Springer-Verlag, New York, 1995.
- [FrJ08] M. D. Fried and M. Jarden, Field Arithmetic, Third Edition, revised by Moshe Jarden, Ergebnisse der Mathematik (3) 11, Springer, Heidelberg, 2008.
- [FrP04] J. Fresnel and M. v.d. Put, Rigid Analytic Geometry and its Applications, Progress in Mathematics 218, Birkhäuser Boston, 2004.
- [HaV96] D. Haran and H. Völklein, Galois groups over complete valued fields, Israel Journal of Mathematics 93 (1996), 9–27.

- [HuS06] C. Huneke and I. Swanson, Integral closure of ideals, rings, and modules, London Mathematical Society Lecture Note Series 336, Cambridge University Press, New York, 2006.
- [Jar11] M. Jarden, Algebraic Patching, Monographs in Mathematics, Springer, Heidelberg.
- [Lan93] S. Lang, Algebra, Third Edition, Eddison-Wesley, Reading, 1993.
- [Par10] E. Paran, Galois theory over complete local domains, Mathematische Annalen 348 (2011), 395–413.
- [Par11] E. Paran, *Hilbertianity of fields of power series*, Journal of the Institute of Mathematics Jussieu,
- [Pop96] F. Pop, Embedding problems over large fields, Annals of Mathematics 144 (1996), 1–34.
- [Pop10] F. Pop, Henselian implies large, Annals of Mathematics 172 (2010), 101–113.
- [Vam75] P. Vamos, Multiply maximally complete fields, Journal of the London Mathematical Society s2-12(1) (1975), 103–111.
- [Rib56] P. Ribenboim, Anneaux Normaux réels à charctère fini, Summa Brasiliensis Math.
 3 (1956), 213–253.
- [Rib70] L. Ribes, Introduction to Profinite Groups and Galois Cohomology, Queen's papers in Pure and Applied Mathematics 24, Queen's University, Kingston, 1970.
- [ZaS75] O. Zariski and P. Samuel, Commutative Algebra II, Springer, New York, 1975.