Galois Theory over Rings of Arithmetic Power Series*

Arno Fehm[†] and Elad Paran[‡]

Abstract

Let R be a domain, complete with respect to a norm which defines a non-discrete topology on R. We prove that the quotient field of R is ample, generalizing a theorem of Pop. We then consider the case where R is a ring of arithmetic power series which are holomorphic on the closed disc of radius $0 < r < 1$ around the origin, and apply the above result to prove that the absolute Galois group of the quotient field of R is semi-free. This strengthens a theorem of Harbater, who solved the inverse Galois problem over these fields.

1 Introduction

Let $K(X)$ be the field of rational functions over a field K. A central conjecture in modern Galois theory, coined by Dèbes and Deschamps [DD99, §2.1.2], asserts that any finite split embedding problem over $K(X)$ is solvable. In particular, the conjecture implies a positive solution to the inverse Galois problem over $K = \mathbb{Q}$, and more generally, over any Hilbertian field K.

In the case where K is an *ample field*, the conjecture was proven by Pop in [Pop96], using methods of rigid analytic geometry, and reproven in [HJ98] in an algebraic fashion. We recall the definition:

Definition 1.1. *A field K is* **ample** *(or* **large** *following [Pop96]) if every smooth K-curve that has a K-rational point has infinitely many such points. Equivalently, K is ample if it is existentially closed in the field of power series $K((t))$.*

*This work appeared in *Advances in Mathematics* 226(5):4183-4197, 2011. The present version (August 9, 2011) contains an updated bibliography and simplifies Section 4, thereby correcting a minor mistake.

[†]Tel Aviv University

[‡]Hebrew University of Jerusalem

The family of ample fields includes, among others, all Henselian valued fields, all real closed fields, all separably closed fields, and more generally all pseudo algebraically closed fields.

So far, the only case where the conjecture of Dèbes and Deschamps was proven, is where K is ample. Thus ample fields now play an important role in Galois theory and Field Arithmetic. Moreover, in recent years ample fields drew attention from several other branches of mathematics – for example in arithmetic geometry [Kol99], [FP10], model theory [PP07], and valuation theory [AKP11].

In light of this, it is desirable to determine those fields which are ample. In [Pop10], Pop shows that the class of ample fields is even larger than previously believed, and includes the quotient field of any integral domain which is complete, or more generally, Henselian with respect to a non-trivial ideal. This allows Pop to give a short proof of previous Galois-theoretic results by Harbater-Stevenson [HS05] and the second author [Par09], by reducing them to the case settled in [Pop96].

The proof in [Pop96] of the solvability of split embedding problems over $K(X)$, where K is ample, works by lifting problems from $K(X)$ to $K((t))(X)$, and by reducing solutions over $K((t))(X)$ to solutions over $K(X)$, using the fact that K is existentially closed in $K((t))$. The critical part of the proof, solution over $K((t))(X)$, is achieved by means of *patching*. The method of patching yielded several important results, in particular the mentioned theorem of Pop, and the solution of the general Abhyankar Conjecture by Harbater [Har94]. Patching originates in a series of works by Harbater [Har84b], [Har84c], [Har84a], studying rings of *convergent arithmetic power series*.

Let $0 < r < 1$, and let $\mathbb{C}_r[[t]]$ be the ring of holomorphic functions on the open disc of radius r around the origin which are continuous on the closed disc of radius r. Also, let $\mathbb{C}_{r^+}[[t]] = \bigcup_{s>r} \mathbb{C}_s[[t]]$ be the ring of holomorphic functions on (a neighborhood of) the closed disc of radius r. If A is a subring of $\mathbb{C}$, let $A_r[[t]] = \mathbb{C}_r[[t]] \cap A[[t]]$ and $A_{r^+}[[t]] = \mathbb{C}_{r^+}[[t]] \cap A[[t]]$ be the corresponding rings of functions whose Taylor expansions have coefficients in A.

The purpose of the present work is two-fold. First, we wish to strengthen Harbater's Galois-theoretic results concerning the arithmetic case. That is, we study Galois theory over $\mathrm{Quot}(A_{r^+}[[t]])$ and $\mathrm{Quot}(A_r[[t]])$, for any proper subring A of $\mathbb{Q}$ (in particular, for $A = \mathbb{Z}$). In [Har84c, §2], Harbater applies patching arguments to prove that the inverse Galois problem has a positive solution over $\mathrm{Quot}(\mathbb{Z}_{r^+}[[t]])$, for any $0 < r < 1$. A positive solution to the inverse Galois problem over a field K means that any finite group G occurs as a quotient of the absolute Galois group $\mathrm{Gal}(K)$ of K. However, this only yields partial information on $\mathrm{Gal}(K)$. Here we prove (see Theorem 4.9 below):

Theorem 1.2. *Let A be a proper subring of $\mathbb{Q}$, let $0 < r < 1$, and let $R = A_{r^+}[[t]]$ or $R = A_r[[t]]$. Then $\mathrm{Gal}(\mathrm{Quot}(R))$ is a* semi-free *profinite group*

Here, a profinite group G of infinite rank m is called **semi-free** if any non-trivial finite split embedding problem for G has m independent solutions. A profinite group G is free if and only if it is semi-free and projective. Moreover, semi-free groups exhibit natural behavior, and intuitively can be thought of as "free groups without projectivity". See [BSHH10] for details on this notion. We note (Remark 4.10), that the fields in Theorem 1.2 have non-projective absolute Galois groups, hence our result is optimal in the above sense. Recently, Harbater's results were generalized in a different direction using patching over analytic Berkovich spaces in [Poi10].

Our second objective, which serves as an ingredient in the proof of Theorem 1.2, is to generalize Pop's theorem of [Pop10] concerning quotient fields of Henselian domains. Any ideal $\mathfrak{a}$ of a domain R induces a non-archimedean *semi-norm* (Definition 2.1) on R, given by $||x||_{\mathfrak{a}} = \inf\{e^{-n} : n \in \mathbb{Z}_{\geq 0}, x \in \mathfrak{a}^n\}$. In this work, we consider arbitrary semi-norms, which need not arise from an ideal, and may be archimedean. We introduce the notion of Henselian semi-normed domains – domains satisfying a form of Newton approximation with respect to the given semi-norm (see Definition 2.4). If a domain is Henselian with respect to an ideal, then it is Henselian with respect to the semi-norm induced by that ideal. We then prove (cf. Proposition 2.9 and Theorem 2.10 below):

Theorem 1.3. *If a domain R is complete, or more generally Henselian with respect to a norm that defines a non-discrete topology on R, then $K = \mathrm{Quot}(R)$ is ample.*

The criterion for ampleness given in Theorem 1.3 allows us to unify proofs of ampleness for different classes of fields, and also to prove the ampleness of new fields. In particular, Theorem 1.3 implies Pop's theorem about quotient fields of Henselian domains, and it implies that the field of real numbers $\mathbb{R}$ is ample (Remark 2.13). Using Theorem 1.3 we prove that for any $0 < r < 1$ and a subring A of $\mathbb{C}$, the quotient field of $A_r[[t]]$ is ample. This result does not follow from [Pop10] (see Remark 3.3). Since $\mathrm{Quot}(A_{r^+}[[t]])$ is a union of the increasing chain of ample fields $\mathrm{Quot}(A_s[[t]])$, $s > r$, we deduce that this field is ample as well.

If $R = A_r[[t]]$ or $R = A_{r^+}[[t]]$ for some $0 < r < 1$ and a proper subring A of $\mathbb{Q}$, then R is a Krull domain of dimension exceeding 1, and a theorem of Weissauer implies that $K = \mathrm{Quot}(R)$ is Hilbertian. Combining this with the fact that K is ample, we deduce that any finite split embedding problem over K is solvable. However, in order to show that these fields have a semi-free absolute Galois group, we must show that any non-trivial finite split embedding problem over K has $|K|$-many independent solutions. In order to do so, we prove that these fields are **fully Hilbertian**, a notion developed in [BSP11] (and also applied in [Pop10], without being given an explicit name). This means that given a non-trivial split embedding problem over K and a regular solution over $K(X)$, one can specialize the solution (via substitutions of the form $X \mapsto a \in K$) into $|K|$-many independent solutions over K. Combining the facts that K is fully Hilbertian and ample, we deduce that $\mathrm{Gal}(K)$ is a semi-free profinite group, proving Theorem 1.2.

Finally, we note that in [Har84b, §3], [Har84a], and [Har88, §3], Harbater also considers the rings $A_{r^+}[[t]]_{\mathrm{alg}}$ of algebraic convergent power series (which in [Har84b, Proposition 3.2/3.3] he proves to coincide with other rings $A_{r^+}[[t]]^h$ and $A_r[[t]]^h$ he defines there). We show that all of our results hold for these rings as well.

2 Henselian normed domains

In this section we develop the notion of a Henselian normed domain. We start by recalling some terminology.

Definition 2.1. *Let R be a ring (commutative with 1). A map*

$$||\cdot|| : R \to \mathbb{R}_{\geq 0}$$

is a **semi-norm** *on R if it satisfies for all $x, y \in R$ that*

$$\|x+y\| \leq \|x\| + \|y\|, \quad (2.1.1)$$
$$\|xy\| \leq \|x\| \cdot \|y\|, \quad (2.1.2)$$
$$\|0\| = 0, \quad (2.1.3)$$
$$\|\pm 1\| = 1, \quad (2.1.4)$$

and a **norm** *if it satisfies in addition*

$$\|x\| = 0 \quad \Rightarrow \quad x = 0. \quad (2.1.5)$$

A semi-normed ring $(R, ||\cdot||)$ is **complete** *if every Cauchy sequence $(x_n)_{n\in\mathbb{N}}$, $x_n \in R$, converges to an element of R. We say that $||\cdot||$ is* **discrete** *if the topology induced on R by $||\cdot||$ is discrete.*

Remark 2.2. *Conditions (2.1.1) and (2.1.2) just express continuity of addition and multiplication. In particular, every polynomial* $f \in R[X]$ *gives rise to a continuous function* $R \to R$*. Note that (2.1.2) and (2.1.4) imply that* $||-x|| = ||x||$ *for all* $x \in R$*. Condition (2.1.5) implies that the induced topology on* R *is Hausdorff, and therefore limits, if they exist, are unique. Since* $\{x \in R : ||x|| = 0\}$ *is an ideal, every semi-norm on a field is a norm. Note that an absolute value is a norm that satisfies equality in (2.1.2).*

Example 2.3. *Semi-norms arise naturally in the following situations:*

1. *An absolute value on a field* K *(archimedean or non-archimedean) is a norm on every subring* R *of* K*. In particular, every subring of* $\mathbb{C}$ *is equipped with an archimedean norm.*
2. *Every ideal* $\mathfrak{a}$ *of a ring* R *defines a semi-norm* $||\cdot||_{\mathfrak{a}}$ *on* R *(the* **$\mathfrak{a}$-adic** *semi-norm) by*
$$||x||_{\mathfrak{a}} = \inf\left\{e^{-n} : n \in \mathbb{Z}_{\geq 0}, x \in \mathfrak{a}^n\right\} \in [0,1].$$
The semi-norm $||\cdot||_{\mathfrak{a}}$ *is a norm if and only if the* $\mathfrak{a}$*-adic topology on* R *is Hausdorff, i.e. if* $\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n = (0)$*.*
3. *A semi-norm* $||\cdot||$ *on a ring* R *extends to a semi-norm* $||\cdot||_X$ *on the polynomial ring* $R[X]$ *by sending* $f(X) = \sum_{i=0}^d a_i X^i \in R[X]$ *to*
$$\|f\|_X = \sum_{i=0}^{d} \|a_i\|.$$
If $||\cdot||$ *is a norm, then so is* $||\cdot||_X$*.*
4. *If* $(R, ||\cdot||)$ *is a semi-normed ring and* D *is a compact topological space, then* $||\cdot||$ *extends to a semi-norm* $||\cdot||_D$ *on the ring* $\mathcal{C}(D,R)$ *of continuous functions* $D \to R$ *(the* **uniform** *semi-norm) by sending* $f \in \mathcal{C}(D,R)$ *to*
$$\|f\|_D = \max\{\|f(x)\| : x \in D\}.$$
If $||\cdot||$ *is a norm, then so is* $||\cdot||_D$*.*
5. *If* $||\cdot||_1$ *and* $||\cdot||_2$ *are two semi-norms on a ring* R*, then their maximum* $||\cdot|| = \max\{||\cdot||_1, ||\cdot||_2\}$ *is also a semi-norm on* R*. If* $||\cdot||_1$ *or* $||\cdot||_2$ *is a norm, then so is* $||\cdot||$*.*

Definition 2.4. *A semi-normed ring* $(R, ||\cdot||)$ *is* **Henselian** *if for every* $c \in \mathbb{R}$ *and* $d \in \mathbb{N}$ *there exists* $\epsilon > 0$ *such that every polynomial* $f(X) \in R[X]$ *of degree at most* d *which satisfies the following* *conditions has a zero in R (cf. Example 2.3(3)).*

$$\|f(0)\| < \epsilon \quad (2.4.1)$$
$$\left\|f'(0) - 1\right\| < \epsilon \quad (2.4.2)$$
$$\|f\|_X < c \quad (2.4.3)$$

Lemma 2.5. *If $(R, ||\cdot||)$ is a complete normed ring and $x \in R$ satisfies $||x - 1|| < 1/2$, then $x \in R^\times$ and $||x^{-1} - 1|| < 1$.*

Proof. If $x = 1 - \alpha$ with $||\alpha|| < 1/2$, then $x^{-1} = (1 - \alpha)^{-1} = \sum_{i=0}^{\infty} \alpha^i$ is a convergent geometric series, and hence lies in R. Moreover,

$$\left\|x^{-1} - 1\right\| = \left\|\sum_{i=1}^{\infty} \alpha^i\right\| \leq \sum_{i=1}^{\infty} \|\alpha\|^i < 1. \qquad \square$$

Definition 2.6. *If $f \in R[X]$ is a polynomial we denote by $f^{(k)}$ the k-th Hasse-Schmidt derivative of f with respect to X. That is, the map $f \mapsto f^{(k)}$ is the R-linear extension of the operation*

$$(X^n)^{(k)} = \begin{cases} \binom{n}{k} X^{n-k} & \text{if } k \leq n \\ 0 & \text{if } k > n \end{cases} \quad (2.6.1)$$

on the monomials. In particular, $f^{(0)} = f$ and $f^{(1)} = f'$.

Lemma 2.7. *If $(R, ||\cdot||)$ is a normed ring and $f \in R[X]$ a polynomial of degree at most d, then the following holds for every $k \in \mathbb{N}$ and $x \in R$ with $||x|| < 1$:*

$$\left\|f^{(k)}(x) - f^{(k)}(0)\right\| \leq \|x\| \cdot d! \, \|f\|_X \, .$$

In particular,

$$\left\|f^{(k)}(x)\right\| \leq 2d! \cdot \|f\|_X \quad (2.7.1)$$

and

$$\left\|f'(x) - 1\right\| \leq \left\|f'(0) - 1\right\| + \|x\| \cdot d! \, \|f\|_X \, . \quad (2.7.2)$$

Proof. By (2.6.1), if $f(X) = \sum_{i=0}^{d} a_i X^i$, then

$$f^{(k)}(X) = \sum_{i=k}^{d} a_i \binom{i}{k} X^{i-k} = f^{(k)}(0) + \sum_{i=k+1}^{d} a_i \binom{i}{k} X^{i-k}.$$

Since $||x|| < 1$ and $\binom{i}{k} \leq i!$,

$$\left\|f^{(k)}(x) - f^{(k)}(0)\right\| \leq \sum_{i=k+1}^{d} \|a_i\| \cdot \left\|\binom{i}{k}\right\| \cdot \|x\|^{i-k} \leq \|x\| \cdot d! \sum_{i=k+1}^{d} \|a_i\| \, ,$$

hence $\left\|f^{(k)}(x) - f^{(k)}(0)\right\| \leq \|x\| \cdot d! \, \|f\|_X$ by the definition of $||\cdot||_X$. Since $f^{(k)}(0) = a_k$, certainly $\left\|f^{(k)}(0)\right\| = \|a_k\| \leq \|f\|_X$, and therefore also (2.7.1) follows.

□

Proposition 2.8. *A complete normed ring is Henselian.*

Proof. Let $(R, ||\cdot||)$ be a complete normed ring, and let c and d be given. Choose $0 < \rho < 1/2$ such that $\rho c d! < 1/4$, and choose $0 < \delta < 1/2$ such that $\delta(1-\delta)^{-1} < \rho$ and $4\delta c d d! < 1$. Let $f(X) \in R[X]$ be a polynomial of degree at most d that satisfies (2.4.1)-(2.4.3) for $\epsilon = \delta^2/2$.

If $||x|| < \rho$, then by (2.4.2), (2.4.3) and (2.7.2),

$$\begin{aligned} \left\|f'(x) - 1\right\| &\leq \left\|f'(0) - 1\right\| + \|x\| \cdot d! \, \|f\|_X \\ &< \epsilon + \rho c d! \leq \frac{\delta^2}{2} + \frac{1}{4} < \frac{1}{2}, \end{aligned}$$

so Lemma 2.5 implies that $f'(x) \in R^\times$ and

$$\left\|f'(x)^{-1} - 1\right\| < 1.$$

In particular,

$$\left\|f'(x)^{-1}\right\| < 2. \tag{2.8.1}$$

Moreover, by (2.7.1) and (2.4.3),

$$2\delta \cdot \sum_{k=1}^{d} \left\|f^{(k)}(x)\right\| \leq 2\delta \cdot d \cdot 2d! \cdot \|f\|_X \leq 4\delta c d d! < 1. \tag{2.8.2}$$

We now construct inductively a sequence $a_0 = 0, a_1, a_2, \ldots$ of elements of R that satisfies for each n the following

Induction hypothesis:

$$\|f(a_n)\| < \frac{1}{2}\delta^{n+2}, \tag{A_n}$$

and if $n > 0$, then

$$\|a_n - a_{n-1}\| < \delta^{n+1}. \tag{B_n}$$

Induction base. Consider the case $n = 0$. Then $a_0 = 0 \in R$ and

$$||f(a_0)|| = ||f(0)|| < \epsilon = \frac{1}{2}\delta^2,$$

by (2.4.1), so (A_0) holds.

Induction step. Let $n \geq 0$ and suppose that we already constructed $a_0, \ldots, a_n$. Then, by $a_0 = 0$ and $(B_1), \ldots, (B_n)$,

$$\|a_n\| \leq \sum_{k=1}^{n} \|a_k - a_{k-1}\| \leq \sum_{k=1}^{n} \delta^{k+1} \leq \sum_{k=1}^{\infty} \delta^k = \frac{\delta}{1-\delta} < \rho.$$

Thus, $f'(a_n) \in R^\times$ and $||f'(a_n)^{-1}|| < 2$ by (2.8.1). Therefore, we can define

$$a_{n+1} = a_n - f'(a_n)^{-1} f(a_n) \in R.$$

We now show that a_{n+1} satisfies (A_{n+1}) and (B_{n+1}). Indeed,

$$\left\|f'(a_n)^{-1}\right\| \cdot \|f(a_n)\| < 2 \cdot \frac{1}{2}\delta^{n+2} = \delta^{n+2}$$

by (A_n), so

$$\|a_{n+1} - a_n\| = \left\|f'(a_n)^{-1} f(a_n)\right\| < \delta^{n+2} \tag{2.8.3}$$

and hence (B_{n+1}) holds. By Taylor expansion,

$$\begin{aligned} f(a_{n+1}) &= f(a_n) + \sum_{k=1}^{d} \left[(-1)^k \left(f'(a_n)^{-1} f(a_n)\right)^k \cdot f^{(k)}(a_n)\right] \\ &= \sum_{k=2}^{d} \left[(-1)^k \left(f'(a_n)^{-1} f(a_n)\right)^k \cdot f^{(k)}(a_n)\right], \end{aligned}$$

hence (2.8.3) implies that

$$\begin{aligned} \|f(a_{n+1})\| &\leq \sum_{k=2}^{d} \left[\left\|f'(a_n)^{-1} f(a_n)\right\|^k \cdot \left\|f^{(k)}(a_n)\right\|\right] \\ &\leq (\delta^{n+2})^2 \cdot \sum_{k=2}^{d} (\delta^{n+2})^{k-2} \left\|f^{(k)}(a_n)\right\| \\ &\leq \delta^{2n+3} \cdot \delta \cdot \sum_{k=2}^{d} \left\|f^{(k)}(a_n)\right\|. \end{aligned}$$

Thus, (2.8.2) gives that

$$\|f(a_{n+1})\| < \delta^{2n+3} \cdot \frac{1}{2} \leq \frac{1}{2}\delta^{n+3},$$

so (A_{n+1}) holds, and this concludes the induction step.

End of the proof. The a_n form a sequence in R, which is Cauchy by (B_n). Therefore, since $(R, ||\cdot||)$ is complete by assumption, this sequence converges to an element $a \in R$. By (A_n), this limit a must satisfy $||f(a)|| = 0$, and so we get that $f(a) = 0$ by (2.1.5). □

The proof of the following proposition is based on the proofs of [Pop10, Theorem 1.1] and [Jar11, Proposition 5.7.3].

Proposition 2.9. *The quotient field of an infinite non-discrete Henselian semi-normed domain is ample.*

Proof. Let $(R, ||\cdot||)$ be an infinite non-discrete Henselian semi-normed domain, and let $K = \mathrm{Quot}(R)$. Let C be a K-curve with a smooth K-rational point. We want to prove that $C(K)$ is infinite. Without loss of generality, one can successively make the following assumptions, cf. [Jar11, Lemma 5.3.1]: C is an affine plane curve, $(0,0) \in C$ is a smooth rational point, and the tangent to C in $(0,0)$ is the line $Y = 0$. That is, C is given by a polynomial

$$g(X,Y) = Y + \sum_{i+j\geq 2} g_{ij} X^i Y^j \in K[X,Y],$$

where $g_{ij} \in K$ for all i,j. Write $g_{ij} = \frac{p_{ij}}{q_{ij}}$, $p_{ij}, q_{ij} \in R$, and let $q = \prod_{i,j} q_{ij}$. Then

$$\frac{1}{q} \cdot g(qX, qY) = Y + \sum_{i+j\geq 2} \frac{p_{ij}}{q_{ij}} q^{i+j-1} X^i Y^j \in R[X,Y].$$

Thus, we can assume without loss of generality that $g \in R[X,Y]$.

For $x \in R$ let $f_x(Y) = g(x,Y) \in R[Y]$. Let $d = \deg_Y(g)$ and $c = ||f_0||_Y + 1$. Then there exists $\delta > 0$ such that if $||x|| < \delta$, then $||f_x||_Y < c$. Since $(R, ||\cdot||)$ is Henselian, there exists $\epsilon > 0$ such that the following holds for all $x \in R$ with $||x|| < \delta$: If $||f_x(0)|| < \epsilon$ and $||f'_x(0) - 1|| < \epsilon$, then f_x has a zero in R. But since $f_0(0) = g(0,0) = 0$, and $f'_0(0) = \frac{\partial f}{\partial Y}(0,0) = 1$, these conditions will be satisfied if $||x||$ is sufficiently small. Since $(R, ||\cdot||)$ is an infinite domain, and non-discrete, we can find infinitely many such $x \in R$. Indeed, if $||\cdot||$ is a norm, then the topology on R is Hausdorff and non-discrete, hence every neighborhood of 0 is infinite. And if $||\cdot||$ is not a norm, then $\mathfrak{n} = \{x \in R : ||x|| = 0\}$ is a non-trivial ideal of R, and hence infinite. This gives infinitely many different zeros of g in R. □

Combining these propositions, we get the following result.

Theorem 2.10. *The quotient field of a non-discrete complete normed domain is ample.*

Proof. This follows from Proposition 2.8 and Proposition 2.9. □

Corollary 2.11. *Let R be a non-discrete complete normed domain. Then any finite split embedding problem over* $\mathrm{Quot}(R[X])$ *is solvable.*

Proof. Since $K = \mathrm{Quot}(R)$ is ample by Theorem 2.10, and $\mathrm{Quot}(R[X])$ is a rational function field over K, the result follows from the main theorem of [Pop96]. $\square$

In fact, every non-discrete and relatively algebraically closed subring of a complete normed (or Henselian normed) domain is again Henselian and therefore has an ample quotient field (by Proposition 2.9) and satsifes the consequence of Corollary 2.11:

Lemma 2.12. *If $(R, ||\cdot||)$ is a Henselian semi-normed domain, and $R_0 \subseteq R$ is a subring which is algebraically closed in R, then $(R_0, ||\cdot||)$ is Henselian.*

Proof. If $f \in R_0[X]$ satisfies conditions (2.4.1)-(2.4.3) in $(R_0, ||\cdot||)$, then it also satisfies these conditions in $(R, ||\cdot||)$. Hence, f has a zero in R, which by the assumption that R_0 is algebraically closed in R must lie in R_0. $\square$

Remark 2.13. *In [Pop10], Pop proves that the quotient field of a domain complete with respect to a non-zero ideal, or more generally, the quotient field of a Henselian domain, is ample. In fact, this theorem of Pop is generalized by the results of this section:*

Indeed, if a domain R is Henselian with respect to an ideal $\mathfrak{a}$, then $(R, ||\cdot||_{\mathfrak{a}})$ is Henselian for $\epsilon = 1$ independent of c and d (cf. Example 2.3(2)). If $\mathfrak{a} \neq (0)$, then $||\cdot||_{\mathfrak{a}}$ is non-discrete. If R is complete with respect to $\mathfrak{a}$, then $(R, ||\cdot||_{\mathfrak{a}})$ is complete. If $(R, \mathfrak{a})$ is Hausdorff, then $(R, ||\cdot||_{\mathfrak{a}})$ is a norm. The following diagram summarizes the properties of these notions (the top row is concerned with domains and ideals, while the bottom row is concerned with semi-norms).

$$\begin{array}{ccccc}
\text{complete} & \xRightarrow[\text{if Hausdorff}]{} & \text{Henselian} & \xRightarrow[\text{if } \mathfrak{a} \neq (0)]{\text{[Pop10, Thm. 1.1]}} & \text{ample quotient field} \\
\Downarrow & & \Downarrow & & \\
\text{complete} & \xRightarrow[\text{if normed}]{\text{Prop. 2.8}} & \text{Henselian} & \xRightarrow[\text{if non-discrete}]{\text{Prop. 2.9}} & \text{ample quotient field}
\end{array}$$

The results of this section are a proper generalization of Pop's result. For example, Theorem 2.10 immediately implies the well known fact that $\mathbb{R}$ is ample. The following section gives more non-trivial examples.

Note that in our general case, one cannot always choose ϵ in Definition 2.4 independently of c and d. If $R = \mathbb{R}$ (with the usual absolute value) and $f(X) = \frac{1}{\epsilon}X^2 + X + \frac{\epsilon}{2}$, then $|f(0)| = \epsilon/2 < \epsilon$ and $|f'(0) - 1| = 0 < \epsilon$, but f has no zero in $\mathbb{R}$, although $(\mathbb{R}, |\cdot|)$ is complete and non-discrete.

Remark 2.14. *One could prove Theorem 2.10 directly using [DH90, Theorem 2.1]. However, our approach has the advantage that it shows how Pop's result on Henselian domains fits into the picture.*

Remark 2.15. *In general, Proposition 2.8 does not hold for complete semi-normed domains. For example, let* $R = \bigcup_{n\in\mathbb{N}} \mathbb{Q}[t^{2^{-n}}]$ *and* $\mathfrak{a} = (t, t^{1/2}, t^{1/4}, \dots)$. *Then* $\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n = \mathfrak{a}$. *This implies that* $(R, \mathfrak{a})$ *is complete, since any Cauchy sequence converges to one of its elements. On the other hand, if* $||\cdot|| = ||\cdot||_{\mathfrak{a}}$ *is the semi-norm induced on* R *by* $\mathfrak{a}$, *then* $(R, ||\cdot||)$ *is not Henselian. Indeed, let* $c = 3$, $d = 2$, *and suppose there exists* $\epsilon > 0$ *as in Definition 2.4. Let*

$$F(X) = X^2 + X + t \in R[X].$$

Then $||F(0)|| = ||t|| = 0 < \epsilon$, $||F'(0) - 1|| = ||0|| = 0 < \epsilon$, *and* $||F||_X = 2 < c$. *However, if* $f \in R$ *with* $F(f) = 0$, *then there exists* n *such that* $f \in \mathbb{Q}[t^{2^{-n}}]$, *so* $\alpha = f(1) \in \mathbb{Q}$ *satisfies*

$$0 = F(\alpha) = \alpha^2 + \alpha + 1,$$

a contradiction. In particular, this shows that [Pop10, (1) on p. 2] can only refer to ring-ideal pairs that are complete and Hausdorff *(note that for some authors, e.g. [AM69], the definition of a complete ring already includes the Hausdorff condition).*

3 Rings of convergent power series

The aim of this section is to show that quotient fields of certain rings of convergent power series are ample.

Let $0 < r < 1$, let $A \subseteq \mathbb{C}$ be a subring of the field of complex numbers, and let

$$A_r[[t]] = \mathbb{C}_r[[t]] \cap A[[t]]$$

be the ring of continuous $\mathbb{C}$-valued functions on the closed disc

$$D_r = \{z \in \mathbb{C} : |z| \leq r\}$$

which are holomorphic on the open disc

$$U_r = \{z \in \mathbb{C} : |z| < r\}$$

and, as power series around the center $0 \in \mathbb{C}$, have coefficients in A. Moreover, let

$$A_{r^+}[[t]] = \bigcup_{s>r} A_s[[t]],$$

and for each of these rings R let R_{alg} denote the algebraic closure of $A[t]$ in R.

Let $||\cdot||_{D_r}$ be the the uniform norm on $\mathbb{C}_r[[t]]$, given by

$$\|f\|_{D_r} = \max\{|f(z)| : |z| \leq r\},$$

cf. Example 2.3(4), and let $||\cdot||_{(t)}$ be the (t)-adic norm on $\mathbb{C}[[t]]$ given by

$$\left\|\sum_{n=0}^{\infty} a_n t^n\right\|_{(t)} = e^{-\inf\{n\in\mathbb{Z}_{\geq 0}:a_n\neq 0\}},$$

cf. Example 2.3(2). Finally, let $||\cdot|| = \max\{||\cdot||_{D_r}, ||\cdot||_{(t)}\}$ be the maximum of $||\cdot||_{D_r}$ and $||\cdot||_{(t)}$ restricted to $A_r[[t]]$, cf. Example 2.3(5).

The following observation occurs in [DH90, p. 167].

Lemma 3.1. *$(A_r[[t]], ||\cdot||)$ is complete.*

Proof. Note that $(\mathbb{C}_r[[t]], ||\cdot||_{D_r})$ and $(A[[t]], ||\cdot||_{(t)})$ are complete. Any $||\cdot||$-Cauchy sequence $(f_n)_{n\in\mathbb{N}}$ in $A_r[[t]]$ is $||\cdot||_{D_r}$-Cauchy, so it converges uniformly to some $f \in \mathbb{C}_r[[t]]$, and it is $||\cdot||_{(t)}$-Cauchy, hence it converges t-adically in $A[[t]]$, i.e. the sequence of k-th coefficients of f_n is eventually constant, for every k. Since by the Cauchy integral formula the sequence of k-th coefficients of f_n converges to the k-th coefficient of f (cf. [Har84b, p. 804]), these two limits conincide and $f \in \mathbb{C}_r[[t]] \cap A[[t]] = A_r[[t]]$. □

Proposition 3.2. *For any subring $A \subseteq \mathbb{C}$ and every $0 < r < 1$, the quotient fields of the following domains are ample:*

1. $A_r[[t]]$
2. $A_{r^+}[[t]]$
3. $A_r[[t]]_{\text{alg}}$
4. $A_{r^+}[[t]]_{\text{alg}}$

Proof. By Lemma 3.1, $(A_r[[t]], ||\cdot||)$ is complete. Since $t^n \in A_r[[t]]$ and $||t^n|| = \max\{r^n, e^{-n}\} \to 0$, $(A_r[[t]], ||\cdot||)$ is not discrete. Hence, $\mathrm{Quot}(A_r[[t]])$ is ample by Theorem 2.10. Since $A_{r^+}[[t]] = \bigcup_{s>r} A_s[[t]]$,

$$\mathrm{Quot}(A_{r^+}[[t]]) = \bigcup_{s>r} \mathrm{Quot}(A_s[[t]])$$

is the union of an increasing family of ample fields, and hence ample.

By Proposition 2.8, $(A_r[[t]], ||\cdot||)$ is Henselian, so Lemma 2.12 implies that also $(A_r[[t]]_{\text{alg}}, ||\cdot||)$ is Henselian. Hence, $\mathrm{Quot}(A_r[[t]]_{\text{alg}})$ is ample by Proposition 2.9. This again implies that $\mathrm{Quot}(A_{r^+}[[t]]_{\text{alg}})$ is a union of ample fields, and hence ample. □

Remark 3.3. *By Proposition 3.2, the quotient field of $R = \mathbb{Z}_r[[t]]$ is ample. Note that this does not follow from Pop's result that the quotient field of a Henselian domain is ample, cf. Remark 2.13. Indeed, suppose that $(R', \mathfrak{a})$ is a Henselian domain-ideal pair with* $\mathrm{Quot}(R') = \mathrm{Quot}(R)$ *and $\mathfrak{a} \neq (0)$. Choose any element $0 \neq fg^{-1} \in \mathfrak{a}$, $f, g \in R$, $g \neq 0$. Then there exists $0 < s_0 < r$ such that both f and g are non-zero at s_0, and without loss of generality we can assume that $f(s_0)g(s_0)^{-1} > 0$ (if not, replace fg^{-1} with $-fg^{-1}$). Then there exists $\epsilon > 0$ and a small neighborhood U of s_0 in $\mathbb{R}$ such that $f(s)g(s)^{-1} > \epsilon$ for all $s \in U$. Let $n \in \mathbb{N}$ with $n > \epsilon^{-1}$ and consider the polynomial*

$$F(X) = nX^2 + X + \frac{f}{g} \in R'[X].$$

Then $F(0) = fg^{-1} \in \mathfrak{a}$ and $F'(0) - 1 = 0 \in \mathfrak{a}$, so F has a zero $x \in R'$ since $(R', \mathfrak{a})$ is Henselian. Let $x = f_0 g_0^{-1}$, $f_0, g_0 \in R$, $g_0 \neq 0$. There exists $s \in U$ such that $g_0(s) \neq 0$. Note that $\alpha = f(s)g(s)^{-1} > \epsilon$ and $\beta = f_0(s)g_0(s)^{-1}$ are real numbers, and

$$n\beta^2 + \beta + \alpha = 0.$$

However, an elementary calculation shows that this equation contradicts the choice of n.

Remark 3.4. *Remark 3.3 implies that $K = \mathrm{Quot}(\mathbb{Z}_r[[t]])$ is not complete with respect to a* non-archimedean *absolute value. It is also not complete with respect to an* archimedean *absolute value, since a field complete with respect to an archimedean absolute value is isomorphic to $\mathbb{R}$ or $\mathbb{C}$, [Lan02, Corollary XII.2.4], which is not the case for K (for example since K is Hilbertian, see Theorem 4.9 below).*

4 Galois Theory

We are almost ready to prove our main result. First, recall the following definitions and properties, [ZS60, §VI.13]:

Definition 4.1. *A domain R is called a* **Krull domain** *if there exists a family $\mathcal{F}$ of non-trivial discrete rank-1 valuations on $K = \mathrm{Quot}(R)$, satisfying the following properties:*

(a) Denoting the valuation ring of v by R_v for each $v \in \mathcal{F}$, we have $\bigcap_{v \in \mathcal{F}} R_v = R$.

(b) For each $a \in K^\times$, $v(a) = 0$ for all but finitely many $v \in \mathcal{F}$.

(c) For each $v \in \mathcal{F}$, R_v is the localization of R with respect to the center $\mathfrak{p}(v) = \{a \in R : v(a) > 0\}$ of v on R.

The family $\mathcal{F}$ is unique (up to equivalence of valuations), and is called the **essential family** *of R. It consists of all valuations on K whose valuation ring is the localization of R by a minimal non-zero prime ideal.*

Example 4.2 ([ZS60, p. 82 Example (b)]). *Any integrally closed Noetherian domain is a Krull domain.*

Remark 4.3. *If R is a domain and $\mathcal{F}$ a family of non-trivial discrete valuations on $K = \mathrm{Quot}(R)$, satisfying conditions (a) and (b) of Definition 4.1, then there exists a subfamily of $\mathcal{F}$ satisfying all three conditions of Definition 4.1, and hence R is a Krull domain (see [Mat86, §12]).*

Definition 4.4. *[Pop10, §1] An infinite field K is called a* **Krull field** *if there exists a family $\mathcal{F}$ of discrete rank-1 valuations on K, satisfying:*

(a) For each $a \in K^\times$, $v(a) = 0$ for all but finitely many $v \in \mathcal{F}$.

(b) For each finite Galois extension L/K, the subfamily

$$\{v \in \mathcal{F} : v \text{ is totally split in } L/K\}$$

has cardinality $|K|$ (in particular, for $L = K$ we get $|\mathcal{F}| = |K|$).

Remark 4.5. *The family $\mathcal{F}$ in Definition 4.4 is not unique. In particular, if $\mathcal{F}$ satisfies the conditions of Definition 4.4, and $\mathcal{F}'$ is a subfamily of $\mathcal{F}$ such that $|\mathcal{F} \setminus \mathcal{F}'| < |\mathcal{F}|$, then clearly $\mathcal{F}'$ also satisfies the conditions of Definition 4.4.*

The following proposition is a special case of [Pop10, Theorem 3.4(i)].

Proposition 4.6. *Let R be a Krull domain and let $\mathcal{F}$ be its essential family. Let $\mathfrak{p}$ be a prime ideal of R of height exceeding 1, let $0 \neq x \in \mathfrak{p}$, and suppose that:*

1. *$|R| \leq 2^{\aleph_0}$.*
2. *For any sequence $(b_i)_{i=0}^{\infty}$ in $\{0,1\}^{\mathbb{N}}$, the sequence $f_n = \sum_{i=0}^{n} b_i x^i$ converges x-adically in R.*

Then $\mathrm{Quot}(R)$ is a Krull field, and a corresponding family of valuations is $\mathcal{F}$.

Proposition 4.7. *Let A be a proper subring of $\mathbb{Q}$, and let $0 < r < 1$. Put $R = A_r[[t]]$ or $R = A_{r^+}[[t]]$. Then R has an overring R' that is a Krull domain of dimension exceeding 1, and $K = \mathrm{Quot}(R) = \mathrm{Quot}(R')$ is a Krull field, where a corresponding family of valuations is the essential family of R'.*

Proof. Let $R' = A[[t]] \cap \mathrm{Quot}(R)$. Since $A[[t]]$ is a Krull domain, [Mat86, Theorem 12.4(iii)], so is R', cf. [Mat86, p. 86]. Evaluating power series at 0 yields an epimorphism $R' \to A$ whose kernel $\mathfrak{a}$ contains t. Since A is strictly contained in $\mathbb{Q}$ and hence has dimension at least 1, $\mathfrak{a}$ is contained in a prime ideal $\mathfrak{p}$ of R' of height exceeding 1. A sequence $(b_i)_{i=0}^{\infty}$ in $\{0,1\}^{\mathbb{N}}$ yields an element $f = \sum_{i=0}^{\infty} b_i t^i \in \mathbb{Z}[[t]]$. Since the coefficients of f are bounded, f is holomorphic on the open unit disc, hence $f \in R \subseteq R'$. Clearly, the cardinality of R is $2^{\aleph_0}$. Thus the claim follows by Proposition 4.6. □

Proposition 4.8. *Let A be a proper subring of $\mathbb{Q}$, and let $0 < r < 1$. Put $R = A_r[[t]]$ or $R = A_{r^+}[[t]]$, let $S = R_{\mathrm{alg}}$, and let $K = \mathrm{Quot}(R)$ or $K = \mathrm{Quot}(S)$. Then K is a fully Hilbertian field.*

Proof. First, consider the case $K = \mathrm{Quot}(R)$. By Proposition 4.7, R has an overring R' that is a Krull domain of dimension exceeding 1. By a theorem of Weissauer [FJ08, Theorem 15.4.6], $K = \mathrm{Quot}(R')$ is Hilbertian. Let $\mathcal{F}$ be the essential family of R', and let $\mathcal{F}'$ be the family of all valuations in $\mathcal{F}$ that are trivial on $\mathbb{Q}$. Since $\mathbb{Q}$ is countable, condition (b) of Definition 4.1 implies that $|\mathcal{F} \smallsetminus \mathcal{F}'| \leq \aleph_0$. By Proposition 4.7, K is a Krull field and $\mathcal{F}$ satisfies conditions (a) and (b) of Definition 4.4. In particular, $|\mathcal{F}| = |K| = 2^{\aleph_0} > \aleph_0 \geq |\mathcal{F} \smallsetminus \mathcal{F}'|$. By Remark 4.5, $\mathcal{F}'$ satisfies conditions (a) and (b) of Definition 4.4. This implies that $\mathcal{F}'$ satisfies conditions (i),(ii),(iii) of [BSP11, Proposition 7.4], hence the maximal purely inseparable extension K_{ins} of K is fully Hilbertian. Since $\mathrm{char}(K) = 0$, $K = K_{\mathrm{ins}}$ is fully Hilbertian.

Now instead take $K = \mathrm{Quot}(S)$. As in the proof of the previous proposition, $S' = A[[t]] \cap K$ is a Krull domain of dimension exceeding one, hence K is Hilbertian, again by [FJ08, Theorem 15.4.6]. Equivalently, since S is countable (being algebraic over $A[t]$), K is fully Hilbertian [BSP11, Corollary 2.24]. □

This leads to our main result:

Theorem 4.9. *Let A be a proper subring of $\mathbb{Q}$, let $0 < r < 1$, put $R = A_r[[t]]$ or $R = A_{r^+}[[t]]$, let $S = R_{\mathrm{alg}}$, and let $K = \mathrm{Quot}(R)$ or $K = \mathrm{Quot}(S)$. Then the following holds.*

1. *K is an ample field.*
2. *K is a fully Hilbertian field.*

3. Gal(K) *is a semi-free profinite group.*

Proof. The field K is ample by Proposition 3.2, and fully Hilbertian by Proposition 4.8. Hence, [BSP11, Corollary 2.28] asserts that Gal(K) is semi-free. □

Remark 4.10. *A profinite group is free if and only if it is semi-free and projective, [BSHH10, Theorem 3.6]. Note that* $G = \mathrm{Gal}(K)$*, where* K *is as in Theorem 4.9, is semi-free but not projective, and hence not free:* K *is a subfield of the real field* $\mathbb{Q}((t))$*, and hence real. Consequently,* G *is not torsion-free, and therefore not projective [RZ00, 7.7.6].*

Remark 4.11. *Every fully Hilbertian ample field has a semi-free absolute Galois group. However, there exist ample fields with a semi-free (or even free) absolute Galois group that are* not *fully Hilbertian (cf. [BSP11, Remark 2.14]). Thus for ample fields, the property of being fully Hilbertian, which is interesting for its own sake, is stronger than the property of having a semi-free absolute Galois group.*

Acknowledgments

The first author was supported by the European Commission under contract MRTN-CT-2006-035495. The second author was supported by an ERC grant.

References

[AKP11] Salih Azgin, Franz-Viktor Kuhlmann, and Florian Pop. To appear in *Proceedings of the American Mathematical Society*, 2011.

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[BSHH10] Lior Bary-Soroker, Dan Haran, and David Harbater. Permanence criteria for semi-free profinite groups. *Mathematische Annalen*, 348(3):539–563, 2010.

[BSP11] Lior Bary-Soroker and Elad Paran. Fully Hilbertian fields. To appear in *Israel Journal of Mathematics*, 2011.

[DD99] Pierre Dèbes and Bruno Deschamps. The inverse Galois problem over large fields. In L. Schneps and P. Lochak, editors, *Geometric Galois Action / 2, London Math. Soc. Lecture Note Series*, volume 243, pages 119–138. Cambridge University Press, 1999.

[DH90] Jan Denef and David Harbater. Global approximation in dimension two. *Journal of Algebra*, 129:159–193, 1990.

[FJ08] M. Fried and M. Jarden. *Field Arithmetic*. Ergebnisse der Mathematik III **11**. Springer, 2008. 3rd edition, revised by M. Jarden.

[FP10] Arno Fehm and Sebastian Petersen. On the rank of abelian varieties over ample fields. *International Journal of Number Theory*, 6(3):579–586, 2010.

[Har84a] David Harbater. Algebraic rings of arithmetic power series. *Journal of Algebra*, 91:294–319, 1984.

[Har84b] David Harbater. Convergent arithmetic power series. *American Journal of Mathematics*, 106(4):801–846, 1984.

[Har84c] David Harbater. Mock covers and Galois extensions. *Journal of Algebra*, 91:281–293, 1984.

[Har88] David Harbater. Galois covers of an arithmetic surface. *American Journal of Mathematics*, 110(5):849–885, 1988.

[Har94] David Harbater. Abhyankar's conjecture on Galois groups over curves. *Inventiones Mathematicae*, 117:1–25, 1994.

[HJ98] Dan Haran and Moshe Jarden. Regular split embedding problems over complete valued fields. *Forum Mathematicum*, 10:329–351, 1998.

[HS05] David Harbater and Katherine F. Stevenson. Local Galois theory in dimension two. *Advances in Mathematics*, 198:623–653, 2005.

[Jar11] Moshe Jarden. *Algebraic Patching*. Springer, 2011.

[Kol99] János Kollár. Rationally connected varieties over local fields. *Annals of Mathematics*, 150:357–367, 1999.

[Lan02] Serge Lang. *Algebra*. Springer, third edition, 2002.

[Mat86] H. Matsumura. *Commutative ring theory*. Cambridge University Press, 1986.

[Par09] Elad Paran. Split embedding problems over complete domains. *Annals of Mathematics*, 170(2):899–914, 2009.

[Poi10] Jérôme Poineau. Raccord sur les espaces de Berkovich. *Algebra & Number Theory*, 4(3):297–334, 2010.

[Pop96] Florian Pop. Embedding problems over large fields. *Annals of Mathematics*, 144(1):1–34, 1996.

[Pop10] Florian Pop. Henselian implies large. *Annals of Mathematics*, 172, 2010.

[PP07] Bjorn Poonen and Florian Pop. First-order definitions in function fields over anti-mordellic fields. In Chatzidakis, Macpherson, Pillay, and Wilkie, editors, *Model Theory with applications to algebra and analysis*. Cambridge University Press, 2007.

[RZ00] Luis Ribes and Pavel Zalesskii. *Profinite Groups*. Springer, 2000.

[ZS60] O. Zariski and P. Samuel. *Commutative Algebra, Vol. II*. van Nostrand, 1960.