ANNALS OF
MATHEMATICS

Henselian implies large

By Florian Pop

SECOND SERIES, VOL. 172, NO. 3

November, 2010

ANMAAH

Annals of Mathematics, **172** (2010), 2183–2195

Henselian implies large

By Florian Pop

Abstract

In this note we show that the quotient field of a domain which is Henselian with respect to a nontrivial ideal is a large field, and give some applications of this fact, using a specialization theorem for ramified covers of the line over (generalized) Krull fields.

1. **Introduction**

For a field K, let $K(t)$ be the rational function field in t over K, and let $\mathrm{pr}_t : G_{K(t)} \to G_K$ be the corresponding canonical surjective projection between the corresponding absolute Galois groups. Every finite split embedding problem $\mathrm{EP} = (\,\gamma : G_K \to A, \alpha : B \to A\,)$ for G_K gives rise to the finite split embedding problem $\mathrm{EP}_t := (\,\gamma \circ \mathrm{pr}_t : G_{K(t)} \to A, \alpha : B \to A\,)$ for $G_{K(t)}$. The following are two main open (and equivalent) problems in Galois Theory, see e.g., [DD97]:

Problem$^{\infty}$. *Let K be an arbitrary Hilbertian field. Then every finite split embedding problem* EP *for G_K has proper solutions.*

Problem^{0}. *Let K be an arbitrary field. Then for every finite split embedding problem* EP *for G_K, the corresponding* EP_t *for $G_{K(t)}$ has proper solutions.*

Positive answers to the above Problems would imply —among other things, the Inverse Galois Problem and the Shafarevich Conjecture on the freeness of the kernel of the cyclotomic character. The above Problems have positive solutions over fields K which are *large fields,* see e.g. [Pop96, Main Theorems A and B]. The large fields were introduced in loc. cit., and proved to be the "right class" of fields over which one can do a lot of interesting mathematics, like (inverse) Galois theory, see e.g. Colliot-Thélène [CT00], Pop [Pop96], and the survey article Harbater [Har03], study torsors of finite groups Moret-Bailly [MB01], study rationally connected varieties Kollár [Kol99], study the elementary theory of function fields Poonen–Pop [PP08], etc.[1] Recall that a field K is called a *large field*, if

Supported by NSF grants DMS-0401056 and DMS-0801144.

[1] Maybe this is the reason why the "large fields" acquired several other names —google it: ample, AMPLE, épais, fertile, weite Körper, anti-Mordellic, etc.

every smooth K-curve C satisfies: If $C(K)$ is nonempty, then $C(K)$ is infinite. Examples of large fields are the PAC fields, the complete fields like $k((x))$, the real /p-adically closed fields, and more generally the Henselian *valued* fields, the p-fields, etc. See Pop [Pop96] for more about large fields.

In recent years, Harbater–Stevenson solved Problem$^\infty$ over $K = k((x, y))$ in a stronger form, see [HS05, Th. 1.1], by showing that every nontrivial finite split embedding problem for G_K has $|K|$ distinct proper solutions. And very recently, Paran [Par09] solved Problem^0 over $K = \mathrm{Quot}(R)$, where R is a complete Noetherian local ring (satisfying some further technical conditions). The methods of proof in both cases are ingenious and quite technical. These results also seemed to give further new evidence for the fact that the Problems above can be solved in general, as it was generally believed that the above fields $K = k((x, y))$, and more general $K = \mathrm{Quot}(R)$ with R complete Noetherian local and $\mathrm{Krull.dim}(R) > 1$, were not large fields. Note that these fields are definitely *not* Henselian valued fields!

The first point of this short note is to prove that actually $K = k((x, y))$, and more generally, $K = \mathrm{Quot}(R)$ with R a complete Noetherian ring, are *large fields*, and that the class of large fields is *much richer than previously believed.* In particular, one can deduce Paran [Par09] from the already known fact that Problem^0 has a positive answer over large base fields K. Second, I give a lower bound for the number of distinct solutions of a nontrivial finite split embedding problem over a Hilbertian large field, a result which represents a wide extension of Harbater–Stevenson [HS05]. Finally, using these results, one can generalize Harbater's result [Har09, Th. 4.6] (see Theorem 1.3 below), thus giving new evidence for (a stronger form of) Bogomolov's Freeness Conjecture as presented in Positselski [Pos05].

In order to announce the results of this note, we first recall that a commutative ring R with identity is said to be *Henselian* with respect to an ideal $\mathfrak{a}$, or that $R, \mathfrak{a}$ is a *Henselian pair*, if we denote $\bar{R} := R/\mathfrak{a}$ and $R[X] \to \bar{R}[X]$, $f(X) \mapsto \bar{f}(X)$ the reduction map $(\mathrm{mod}\,\mathfrak{a})$, for every polynomial $f(X) \in R[X]$ the following holds: If $\bar{a} \in \bar{R}$ is a root of $\bar{f}(X)$ such that $\bar{f}'(\bar{a}) \in \bar{R}^\times$, then there exists a lifting $a \in R$ of $\bar{a}$ such that $f(a) = 0$ and $f'(a) \in R^\times$. Intuitively, this means that "simple roots" of $\bar{f}(X)$ lift to "simple roots" of $f(X)$. See [Lf] for basic facts about Henselian rings. The following remarks are in place here:

1) $\mathfrak{a}$-adically complete rings with $\mathfrak{a} \neq (0)$, in particular the power series rings $R = R_0[[x_1, \dots, x_n]]$ where R_0 is a domain and $\mathfrak{a} = (x_1, \dots, x_n)$, are Henselian with respect to $\mathfrak{a}$.

2) If K is a Henselian field with respect to a valuation v, and $R_v, \mathfrak{m}_v$ are the corresponding valuation ring and valuation ideal, then $R_v, \mathfrak{m}_v$ is a Henselian pair.

3) Nevertheless, if $R, \mathfrak{a}$ is a Henselian pair, then $K = \mathrm{Quot}(R)$ is in general *not* a Henselian valued field. This happens for instance if R is Noetherian and $\mathrm{Krull.dim}(R) > 1$.

The generalization of Paran [Par09] is the following:

THEOREM 1.1. *Let R be a domain which is Henselian with respect to some ideal $\mathfrak{a} \neq (0)$. Then $K = \mathrm{Quot}(R)$ is a large field. In particular,* Problem^0 *has a positive answer over K.*

The generalization of Harbater–Stevenson [HS05, Th. 1.1], is as follows: Denote $R = k[[x, y]]$ and $K = k((x, y)) := \mathrm{Quot}(R)$. First, K is a large field by Theorem 1.1 above, and K is Hilbertian by Weissauer's [Wei82, Th. 7.2], applied to the Krull domain R. Second, $\mathcal{V} := \{v_{\mathfrak{p}} \mid \mathfrak{p} \in \mathrm{Spec}(R),\ \mathfrak{p} \text{ minimal nonzero}\}$ is a set of discrete valuations which satisfies:

i) The set $\mathcal{V}_a := \{v \in \mathcal{V} \mid v(a) \neq 0\}$ is finite for every $a \in K^\times$.

ii) If $L|K$ is finite Galois, then $\mathcal{V}_{L|K} := \{v \in \mathcal{V} \mid v \text{ is totally split in } L|K\}$ has cardinality $|\mathcal{V}_{L|K}| = |K|$; see e.g., Theorem 3.4.

A field K endowed with a set $\mathcal{V}$ of discrete valuations satisfying i), ii), is called a *Krull field*.

The point is that the property of $K = k((x, y))$ being a Hilbertian large Krull field implies an even stronger/more precise result than [HS05, Th. 1.1], as follows (see §4 for definitions and Theorem 4.3, which strengthens and proves Theorem 1.2 below):

THEOREM 1.2. *Let K be a Hilbertian large Krull field. Then every nontrivial finite split embedding problem for G_K has $|K|$* independent *and* totally ramified *proper solutions.*

Finally, the generalization of Harbater [Har09, Th. 4.6], is the following:

THEOREM 1.3. *Let $R, \mathfrak{m}$ be an excellent two dimensional Henselian local ring with separably closed residue field k such that the quotient field $K := \mathrm{Quot}(R)$ has $\mathrm{char}(K) = \mathrm{char}(k)$. If $|k| < |R|$, suppose that there exists $x \in \mathfrak{m}$ such that $k[[x]] \subset R$. Then $G_{K^{\mathrm{ab}}}$ is profinite free on $|K^{\mathrm{ab}}|$ generators.*

2. **Proof of Theorem** 1.1

Let $C \to K$ be an integral curve over K with $x \in C(K)$ a smooth K-rational point. We show that actually $|C(K)| = |K|$; thus in particular, $C(K)$ is infinite. Since any two birationally equivalent curves have isomorphic Zariski open subsets, it is sufficient to prove the above assertion for any particular K-curve which is K-birationally equivalent to C and has a smooth K-rational point. Thus by general algebraic geometry non-sense, without loss of generality, we can suppose the following: $C \subset \mathbb{A}^2_K$, and $x \in C(K)$ is the origin of $\mathbb{A}^2_K$, and $C = V(f)$ is defined by an irreducible polynomial $f(X_1, X_2) \in K[X_1, X_2]$ of the form $f(X_1, X_2) = \delta X_2 + \widetilde{f}$, where $\delta \neq 0$, and $\widetilde{f}$ is a polynomial in X_1, X_2 with vanishing terms in degrees < 2. Moreover, since $K = \mathrm{Quot}(R)$ is the field of fractions of R, after "clearing denominators", we can suppose that $f \in R[X_1, X_2]$; hence $\delta \in R$, $\delta \neq 0$.

Let us consider the “change of variables” $X_1 = \delta Y_1$, $X_2 = \delta Y_2$. Then in the new variables Y_1, Y_2 the curve C is defined by $g(Y_1, Y_2) = 0$, where

$$g(Y_1, Y_2) = f(\delta Y_1, \delta Y_2) = \delta^2 Y_2 + \tilde{f}(\delta Y_1, \delta Y_2) = \delta^2 [\, Y_2 + \tilde{g}(Y_1, Y_2)\,]$$

with $\tilde{g} \in R[Y_1, Y_2]$ having vanishing terms in degrees < 2. Likewise, the K-curve C is defined in the (Y_1, Y_2)-affine plane by $h(Y_1, Y_2) := Y_2 + \tilde{g}(Y_1, Y_2) = 0$. And remark that $h(Y_1, Y_2) = 0$ defines a model, say C_h, of C over R. The projection on the Y_1 affine line

$$C_h = \mathrm{Spec}\, R[Y_1, Y_2]/(h) \to \mathbb{A}^1_R$$

is smooth in a neighborhood of the origin of $\mathbb{A}^2_R$ viewed as an R-rational point of C_h.

Coming back to the proof of Theorem 1.1, suppose that in the above context, R is Henselian with respect to $\mathfrak{a}$. For every $a \in \mathfrak{a}$, let us set $h_a(X) := h(a, X)$. Then by the definition of h and h_a we get: $h_a(0) \in \mathfrak{a}$, and $h'_a(0) \in 1 + \mathfrak{a}$. Thus viewing this mod $\mathfrak{a}$, we get: $\bar{0}$ is a simple root of $\bar{h}_a \in \bar{R}[X]$. Since R is Henselian with respect to $\mathfrak{a} \neq (0)$, there exists a (unique) $b \in \mathfrak{a}$ such that $h_a(b) = 0$. Equivalently, $h(a, b) = 0$, i.e., (a, b) defines a K-rational point of C. Moreover, the set of rational points of this form is in bijection with $\mathfrak{a}$. Thus since $|\mathfrak{a}| = |R|$, and $|R| = |K|$, it follows that $C(K)$ has cardinality $|K|$; in particular $C(K)$ is in infinite, and K is large. This concludes the proof of Theorem 1.1.

Note that in the first part of the argument above we did not use the fact that R is Henselian with respect to $\mathfrak{a}$, and the above argument can be generalized to arbitrary dimensions:

PROPOSITION 2.1. *Let* $K = \mathrm{Quot}(R)$ *be the quotient field of some infinite domain, and* $X \to K$ *be an integral* d*-dimensional* K*-variety with a smooth* K*-rational point* $x \in X(K)$. *Then* X *is birationally equivalent to a* K*-hypersurface* $H \subset \mathbb{A}^{d+1}_K$ *which contains the origin, and such that* H *is defined over* R. *The projection on the first* d*-coordinates* $H \to \mathbb{A}^d_R$ *is smooth in a Zariski neighborhood of the origin viewed as an* R*-rational point of* H.

Moreover, if R *is Henselian with respect to an ideal* $\mathfrak{a} \neq (0)$, *then the image of the canonical projection* $H(R) \to \mathbb{A}^d(R) = R^d$ *contains* $\mathfrak{a}^d$.

3. **Two basic facts**

A) *Totally split primes/valuations.*

Notation 3.1. Let R be a domain, $K := \mathrm{Quot}(R)$, and $L|K$ be a finite Galois extension. Let $S \subset L$ be a finite $\mathrm{Gal}(L|K)$-invariant R-subalgebra having quotient field $\mathrm{Quot}(S) = L$ and satisfying $S \cap K = R$.

1) We denote by $\theta \in S$ a generator of $L|K$ having its minimal polynomial $p_\theta(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R[X]$, and discriminant $\delta_\theta \in R$.

2) By general Hilbert decomposition theory, the following are equivalent:

a) $\mathfrak{p} \in \operatorname{Spec}(R)$ is totally split in $S|R$.

b) There exists θ as above such that $\delta_\theta \notin \mathfrak{p}$ and $p_\theta(X)$ has a root in $R_\mathfrak{p}$.

c) There exists θ as above and $\alpha_1, \dots, \alpha_n \in R_\mathfrak{p}$ with $\alpha_i \not\equiv \alpha_j \pmod{\mathfrak{p}_\mathfrak{p}}$ such that

$$\tilde{p}_\theta(X) := \prod_\mu (X - \alpha_\mu) \equiv p_\theta(X) \qquad (\operatorname{mod} \mathfrak{p}_\mathfrak{p}).$$

3) A way to generate the above context is as follows: Let $\theta \in S$ and $p_\theta \in R[X]$ be as at point 1) above. Set $h(T, U) = T^n + a_{n-1}T^{n-1}U + \cdots + a_1 T U^{n-1} + a_0 U^n$. Then for every $r, s \in R$, $s \neq 0$, one has $s^n p_\theta(r/s) = h(r, s)$. And if $\mathfrak{p} \in \operatorname{Spec}(R)$ satisfies: $s, \delta_\theta \notin \mathfrak{p}$ and $h(r, s) \in \mathfrak{p}$, then $\mathfrak{p}$ is totally split in $L|K$.

We will apply the remarks above to get a lower bound for the cardinality of the set of totally split prime ideals in $L|K$ as follows:

4) Let $\mathfrak{m} \in \operatorname{Spec} R$, $\kappa \subset R$ be a system of representatives for $R/\mathfrak{m}$, and denote $\kappa^\bullet := \kappa \backslash \mathfrak{m}$. For a fixed nonzero $x \in \mathfrak{m}$, we say that a formal series of the form $E(X) := \sum_n \varepsilon_n X^n$ with $\varepsilon_n \in \kappa$ is *x-adically convergent* in R if and only if there exists $r_{E(X)} \in R$ such that for all $n > 0$ one has: $r_{E(X)} - \sum_{\nu<n} \varepsilon_\nu x^\nu \in x^n R$; and if so, we say that $r_{E(X)}$ is an *x-adic limit* of $E(X)$. Note that if $\sum_n \varepsilon_n X^n$ and $\sum_n \eta_n X^n$ are x-adically convergent series, as above, having a common limit $r \in R$, then $\varepsilon_n = \eta_n$ for all n (proof by induction on n). In particular, if $\mathscr{E}_\kappa(X)$ is the set of all the x-adically convergent series $E(X)$ in R, and $\mathscr{E}_\kappa(x) \subseteq R$ contains exactly one x-adic limit $r_{E(X)}$ for each $E(X) \in \mathscr{E}_\kappa(X)$, then $\mathscr{E}_\kappa(X) \to \mathscr{E}_\kappa(x)$, $E(X) \mapsto r_{E(X)}$, is one-to-one. Therefore we have $|\mathscr{E}_\kappa(X)| \leq |R|$.

5) Let $\mathscr{P}$ be a set of prime ideals $\mathfrak{p} \subset \mathfrak{m}$, $\mathfrak{p} \neq \mathfrak{m}$, of R such that the subset $\mathscr{P}(x) := \{\, \mathfrak{p} \in \mathscr{P} \mid x \in \mathfrak{p} \,\}$ is nonempty for every $x \in \mathfrak{m}$. Finally, for the finite Galois extension $L|K$ denote $\mathscr{P}_{L|K} := \{\, \mathfrak{p} \in \mathscr{P} \mid \mathfrak{p} \text{ is totally split in } L|K \,\}$.

LEMMA 3.2. *In the above Notation* 3.1, *let* $r, x \in \mathfrak{m}$ *satisfy* $\mathscr{P}(r) \cap \mathscr{P}(ax) = \varnothing$, *where* $a := a_0\delta_\theta$. *Let* $\Sigma = \Sigma^{\mathfrak{m}}_{a,r,x} \subset R$ *be an infinite subset satisfying the following conditions*:

i) $\mathscr{P}(u) \cap \mathscr{P}(arx) = \varnothing$ *for all* $u \in \Sigma$.

ii) $\mathscr{P}(u - v) \subseteq \mathscr{P}(x)$ *for all distinct* $u, v \in \Sigma$.

Then $\mathscr{P}_{L|K}$ *has cardinality* $|\mathscr{P}_{L|K}| \geq |\Sigma|$.

Proof. Since $h(T, U) = T^n + a_{n-1}T^{n-1}U + \cdots + a_0 U^n \in R[T, U]$, we have $h(ru, ax) \in \mathfrak{m}$ for $u \in \Sigma$, because $r, x \in \mathfrak{m}$. Hence by the hypotheses on $\mathscr{P}$, there exists $\mathfrak{p}_u \in \mathscr{P}$ such that $h(ru, ax) \in \mathfrak{p}_u$. We first claim that $r, u, a, x \notin \mathfrak{p}_u$. Indeed, since $h(T, U) \in R[T, U]$, and $h(ru, ax) \in \mathfrak{p}_u$, we have: If $ax \in \mathfrak{p}_u$, then $(ru)^n \in \mathfrak{p}_u$; hence $ru \in \mathfrak{p}_u$; and if $ru \in \mathfrak{p}_u$, then $a_0(ax)^n \in \mathfrak{p}_u$; hence $ax \in \mathfrak{p}_u$, because $a_0|a$ in R. Thus, finally $ru \in \mathfrak{p}_u$ if and only if $ax \in \mathfrak{p}_u$. Since $\mathscr{P}(r) \cap \mathscr{P}(ax) = \varnothing$ and $\mathscr{P}(u) \cap \mathscr{P}(arx) = \varnothing$ by hypothesis, we finally must have $ru, ax \notin \mathfrak{p}_u$.

We conclude that $h(ru,ax) \in \mathfrak{p}_u$ implies $r,u,a,x \notin \mathfrak{p}_u$, and in particular, $\delta_\theta \notin \mathfrak{p}_u$. Therefore, by point 3) above we get: If $h(ru,ax) \in \mathfrak{p}_u$, then $\mathfrak{p}_u$ is totally split in $L|K$.

Claim. Let $I \subset \Sigma$ be a finite set of cardinality $|I| > n$. Then

$$\cap_{u \in I} \mathcal{P}\big(h(ru,ax)\big) = \varnothing.$$

By contradiction, let $\mathfrak{p} \in \mathcal{P}\big(h(ru,ax)\big)$ for all $u \in I$. By Notation 3.1, 2) and 3), applied to $\mathfrak{p}$, there exist $\alpha_1,\dots,\alpha_n \in R_\mathfrak{p}$ such that

$$\tilde{h}(T,U) := \prod_\mu (T - \alpha_\mu U) \in R_\mathfrak{p}[T,U]$$

satisfies: $h(T,U) - \tilde{h}(T,U) \in \mathfrak{p}_\mathfrak{p}[T,U]$. Since $h(ru,ax) \in \mathfrak{p}$ for all $u \in I$, it follows that $\tilde{h}(ru,ax) \in \mathfrak{p}_\mathfrak{p}$ for all $u \in I$. On the other hand, $\tilde{h}(ru,ax) = \prod_\mu (ru - ax\alpha_\mu)$, hence for every $u \in I$ there exists μ_u such that $ru - ax\alpha_{\mu_u} \in \mathfrak{p}_\mathfrak{p}$. Since $|I| > n$, there exists $u \neq v$ in I such that $\mu_u = \mu_v$, and $ru - ax\alpha_{\mu_u}, rv - ax\alpha_{\mu_v} \in \mathfrak{p}_\mathfrak{p}$. Hence $ru - rv = r(u-v) \in \mathfrak{p}_\mathfrak{p}$, i.e., $r(u-v) \in \mathfrak{p}$. Since $r,u,a,x \notin \mathfrak{p}$ by the discussion above, we get $u - v \in \mathfrak{p}$. But $\mathcal{P}(u-v) \subseteq \mathcal{P}(x)$ by hypothesis, hence $x \in \mathfrak{p}$, contradiction! The claim is proved.

To conclude, let $\mathcal{P}_\Sigma := \cup_{u\in\Sigma} \mathcal{P}\big(h(ru,ax)\big)$, and $\Sigma_\mathfrak{p} := \{u \in \Sigma \mid h(ru,ax) \in \mathfrak{p}\}$ for $\mathfrak{p} \in \mathcal{P}_\Sigma$. Then the map $\varphi : \mathcal{P}_\Sigma \to 2^\Sigma$, $\mathfrak{p} \mapsto \Sigma_\mathfrak{p}$, has the properties: $\cup_{\mathfrak{p}\in\mathcal{P}_\Sigma} \Sigma_\mathfrak{p} = \Sigma$; and $|\Sigma_\mathfrak{p}| \le n$ for all $\mathfrak{p} \in \mathcal{P}_\Sigma$. By cardinal arithmetic, and taking into account that Σ is infinite, we see that the set $\{\Sigma_\mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_\Sigma\}$ has cardinality $|\Sigma|$, thus concluding the proof. □

LEMMA 3.3. *In the above Notation* 3.1, *suppose that for every nonzero* $r_0 \in \mathfrak{m}$, *there exists* $r_1 \in \mathfrak{m}$ *such that* $\mathcal{P}(r_0) \cap \mathcal{P}(r_1) = \varnothing$. *Then for every nonzero* $x \in \mathfrak{m}$, *the following holds*: $|\mathcal{P}_{L|K}| \ge |\mathcal{E}_\kappa(X)| \ge \aleph_0\, |R/\mathfrak{m}|$.

Proof. For $L|K$ and the corresponding $a := a_0\delta_\theta$ as in Lemma 3.2, choose $r \in \mathfrak{m}$ such that $\mathcal{P}(r) \cap \mathcal{P}(ax) = \varnothing$. We claim that the set $\Sigma := \kappa^\bullet + x\mathcal{E}_\kappa(x)$ satisfies the conditions i), ii), from loc. cit.: First, if $u := \varepsilon_0 + xE(x) \in \Sigma$ with $\varepsilon_0 \notin \mathfrak{m}$, $xE(x) \in \mathfrak{m}$, then $u \notin \mathfrak{m}$. Thus $\mathcal{P}(u) = \varnothing$, and Σ satisfies i). Second, for $u \neq v$ in Σ, one has $u - v = \pm x^\mu[(\varepsilon_\mu - \eta_\mu) + xr]$ for some $\mu \ge 0$ with $\varepsilon_\mu \neq \eta_\mu$ in κ, and $r \in R$. Since $\varepsilon_\mu \neq \eta_\mu$, we get $\overline{\varepsilon}_\mu \neq \overline{\eta}_\mu$ in $R/\mathfrak{m}$; hence $\overline{\varepsilon}_\mu - \overline{\eta}_\mu \neq 0$ in $R/\mathfrak{m}$. But then $\varepsilon_\mu - \eta_\mu \notin \mathfrak{m}$, and therefore, $(\varepsilon_\mu - \eta_\mu) + xr \notin \mathfrak{m}$. Therefore, $\mathcal{P}(u-v) = \mathcal{P}(x^\mu) \subseteq \mathcal{P}(x)$; hence Σ satisfies condition ii). Conclude by taking into account that $|\Sigma| \ge |x\mathcal{E}_\kappa(x)| = |\mathcal{E}_\kappa(X)|$, and by applying Lemma 3.2. □

THEOREM 3.4. *Let R be a domain whose interal closure $\widetilde{R}$ in $K :=$* Quot(R) *is a Krull domain*, *e.g. R is Noetherian*, *or itself a Krull domain. Let $\mathcal{V}$ be the set of valuations v on K defined by the localizations of $\widetilde{R}$ at its minimal nonzero prime ideals. Then K endowed with $\mathcal{V}$ is a Krull field*, *provided there exists a prime ideal* $\mathfrak{m} \subset R$ *of height* > 1, *a set of representatives* $\kappa \subset R$ *for* $R/\mathfrak{m}$, *and a nonzero* $x \in \mathfrak{m}$, *such that* $|\mathcal{E}_\kappa(x)| = |R|$. *This holds*, *if one of the following is true*:

i) $|R| = \aleph_0$; *or* $|R| = |R/\mathfrak{m}|$; *or* $R \leq 2^{\aleph_0}$ *and all* $\sum_{n\in N} X^n$, $N \subseteq \mathbb{N}$, *belong to* $\mathcal{E}_\kappa(X)$.

ii) $\mathfrak{m}$ *is countably generated and* $\cap_n \mathfrak{m}^n = (0)$, *and all* $\sum_n \varepsilon_n X^n$, $\varepsilon_n \in \kappa$, *belong to* $\mathcal{E}_\kappa(X)$.

The hypothesis ii) *is satisfied if R is complete with respect to a finitely generated nonzero ideal* $\mathfrak{a} \subseteq \mathfrak{m}$, *and $R/\mathfrak{a}$ is either Noetherian or a Krull domain*; *for example*, $R = R_0[[X_1, \dots, X_n]]$, *where R_0 is a Noetherian or a Krull domain such that* $n + \mathrm{Krull.dim}(R_0) > 1$.

Proof. First we prove that either of the conditions i), ii), implies $|\mathcal{E}_\kappa(x)| = |R|$: Let $\kappa \subset R$ be a system of representatives for $R/\mathfrak{m}$, which in case ii) equals the given one, respectively such that $0, 1 \in \kappa$ in case i). Then in the case i), it follows directly from the hypothesis and (elementary) cardinal arithmetic that $|\mathcal{E}_\kappa(x)| = |R|$. In case ii), let $(x_i)_{i\in I}$ be a system of generators of $\mathfrak{m}$ with $|I| \leq \aleph_0$, and let M be the set of all the (formal) monomials in the x_i's. Then $|M| = \aleph_0$. Further, the $\mathfrak{m}$-adic completion morphism $R \to \widehat{R}$ is injective, because $\cap_n \mathfrak{m}^n = (0)$. Since every $\widehat{\alpha} \in \widehat{R}$ is represented by a series of the form $\sum_u a_u u$ with $u \in M$ and $a_u \in \kappa$, we get: $|R| \leq |\widehat{R}| \leq |\kappa^M| \leq |\kappa|^{\aleph_0}$. On the other hand, $|\mathcal{E}_\kappa(x)| = |\kappa|^{\aleph_0}$, and $|\mathcal{E}_\kappa(x)| \leq |R|$. Finally, $|R| = |\kappa|^{\aleph_0} = |\mathcal{E}_\kappa(x)|$, as claimed.

Next we prove that K endowed with $\mathcal{V}$ is a Krull field. By hypothesis we have: Every $v \in \mathcal{V}$ is a discrete valuation with valuation ring of the form $\mathcal{O}_v := \widetilde{R}_\mathfrak{q}$ with $\mathfrak{q} \subset \widetilde{R}$ a minimal nonzero prime ideal; and every nonzero $r \in \widetilde{R}$ is contained in only finitely many $\mathfrak{q}$ as above. In particular, since $\widetilde{R}$ is infinite, $|\mathcal{V}| \leq |\widetilde{R}|$. Let $\mathfrak{n} \subset \widetilde{R}$ be a prime ideal above $\mathfrak{m}$ having height > 1. Since $R/\mathfrak{m} \subseteq \widetilde{R}/\mathfrak{n}$ canonically, we can choose a set of representatives $\omega \subset \widetilde{R}$ for $\widetilde{R}/\mathfrak{n}$ containing the above set of representatives κ for $R/\mathfrak{m}$. Let $\mathcal{P}$ be the set of all the minimal nonzero prime ideals $\mathfrak{q} \subset \mathfrak{n}$ of $\widetilde{R}$, and $\mathcal{W} \subseteq \mathcal{V}$ be the set of all the valuations in $\mathcal{V}$ defined by the $\mathfrak{q} \in \mathcal{P}$. Since $\widetilde{R}$ is a Krull domain, the hypothesis of Lemma 3.3 is satisfied for $\mathfrak{n}$ and $\mathcal{P}$. Hence by loc. cit. we have: If $L|K$ is a finite Galois extension, then $|\mathcal{P}_{L|K}| \geq |\mathcal{E}_\omega(x)|$, or equivalently, $|\mathcal{W}_{L|K}| \geq |\mathcal{E}_\omega(x)|$. On the other hand, since $\kappa \subseteq \omega$, one obviously has $|\mathcal{E}_\omega(x)| \geq |\mathcal{E}_\kappa(x)|$. Further, since $\mathcal{W} \subseteq \mathcal{V}$, one has $\mathcal{W}_{L|K} \subseteq \mathcal{V}_{L|K}$. Thus taking into account all the above (in)equalities we finally get $|\widetilde{R}| \geq |\mathcal{V}| \geq |\mathcal{V}_{L|K}| \geq |\mathcal{W}_{L|K}| \geq |\mathcal{E}_\omega(x)| \geq |\mathcal{E}_\kappa(x)| = |R|$. Since $|R| = |\widetilde{R}| = |K|$, we conclude that $|\mathcal{V}_{L|K}| = |K|$, as claimed. □

B) *Specializations of Galois covers.*

Notation 3.5. Let K be a base field, and B a finite group. Let $\varphi : X \to \mathbb{P}^1_K$ be a finite ramified B-cover, with branch locus $S \subset \mathbb{P}^1_K$. Suppose that X is smooth, and $\mathbb{P}^1_K$ is the projective t-line, i.e., $\mathbb{P}^1_K = \mathrm{Spec}K[t] \cup \mathrm{Spec}K[\frac{1}{t}]$ such that $S \subset \mathrm{Spec}K[t]$. Let $\kappa(X)$ be the function field of X; hence $\kappa(X)\,|\,K(t)$ is a Galois extension with $\mathrm{Gal}\big(\kappa(X)\,|\,K(t)\big) = B$.

1) Let K_A be the relative algebraic closure of K in $\kappa(X)$. Then $A := \mathrm{Gal}(K_A|K)$ shall be called the *arithmetical quotient* of B, and $C := \mathrm{Aut}_{\mathbb{P}^1_{K_A}}(X)$ the *geometric part* of B. One has:

a) The A-cover $\mathbb{P}^1_{K_A} \to \mathbb{P}^1_K$ is étale.

b) The C-cover $X \to \mathbb{P}^1_{K_A}$ is such that X is geometrically integral over K_A.

Hence, first, the inertia groups of φ are contained in C, and second, they generate C.

2) Let $X_{\mathrm{ram}} \subset X$ be the ramification locus of φ, and $X_s \subset X_{\mathrm{ram}}$ be the fiber of φ at $s \in S$; let $e_s := |I_x| > 1$ be the order of the inertia group I_x at $x \mapsto s$.

- From now on suppose that K is Hilbertian and $\kappa(x)|K$ is separable for all $x \in X_{\mathrm{ram}}$.

3) Let $K_\varphi|K$ be a minimal Galois extension such that $X_{\mathrm{ram}} \subset X(K_\varphi)$. For $s \in S$, consider the set $\mathcal{V}_s$ of all the valuations v of K which are totally split in the field extension $K_\varphi|K$ and have $vK \neq \ell \cdot vK$ for all prime numbers $\ell \,|\, e_s$.

4) Let $H_\varphi \subset K$ be a Hilbertian set such that for all $b \in H_\varphi$, the fiber of φ at $t = b$ is irreducible, and the resulting Galois extension $K_b|K$ is linearly disjoint from K_φ over K_A. Hence $\mathrm{Gal}(K_b|K) = B = \mathrm{Gal}\big(\kappa(X)\,|\,K(t)\big)$ in a canonical way.

5) Finally, for $b \in H_\varphi$, and $v \in \mathcal{V}_s$, let $\mathcal{V}_v := \{w \mid w \text{ prolongs } v \text{ to } K_b\}$, and for every $w \in \mathcal{V}_v$, let I_w be the inertia group at $w|v$.

THEOREM 3.6. *There exists a finite subset* $\Sigma_\varphi \subset K^\times$ *such that for every system of independent rank-one valuations* $(v_s)_{s\in S}$ *with* $v_s \in \mathcal{V}_s$ *and* $v_s(\Sigma_\varphi) = 0$, *there exists* $b \in H_\varphi$ *satisfying*:

1) *For every* $s \in S$, *one has* $\{I_w \mid w \in \mathcal{V}_{v_s}\} = \{I_x \mid x \in X_s\}$ *canonically inside* C.

2) *In particular*, $\mathrm{Gal}(K_b\,|\,K_A)$ *is generated by the* I_w *with* $w \in \mathcal{V}_{v_s}$ *and* $s \in S$.

Proof. We begin by a preparation along the following three main steps:

Step 1. Let $A' := \mathrm{Gal}(K_\varphi|K)$, and $B' := B \times_A A'$. Then when $X' := X \times_{K_A} K_\varphi$, the resulting $\varphi' : X' \to \mathbb{P}^1_K$ is a ramified B'-cover dominating both the étale A'-cover $\mathbb{P}^1_{K_\varphi} \to \mathbb{P}^1_K$, and the ramified B-cover $\varphi : X \to \mathbb{P}^1_K$. The geometric part of φ' is $C' = C \times_A \{1\} = C$, and under this identification, the inertia groups of φ' are identified with those of φ; precisely, if $X' \ni x' \mapsto x \in X$ are above $s \in S$, then $I_{x'} = I_x \times_A \{1\} = I_x$.

In the same way, on the valuation theoretical side, $K'_b := K_\varphi K_b$ is the compositum of K_b and K_φ. Since $K_\varphi|K$ and $K_b|K$ are linearly disjoint over K_A, we have $\mathrm{Gal}(K'|\,K) = B \times_A A'$. Let $v_s \in \mathcal{V}_s$, and $w'|v_s$ a prolongation to K'_b, and $w := w'|_{K_b}$. Then by general decomposition theory, $I_{w'}$ projects onto I_w under $B' \to B$. On the other hand, since $v_s \in \mathcal{V}_s$ is totally split in $K_\varphi|K$ (by the definition of $\mathcal{V}_s$), hence in $K_A = K_b \cap K_\varphi$ too, we have: $I_{w'} \subset C'$, and $I_w \subset C$. Since $C' = C \times_A \{1\} = C$ canonically, we have $I_{w'} = I_w$.

Therefore, *mutatis mutandis,* we can and *will* suppose that $K_\varphi = K_A$; i.e., all ramified points of $X \to \mathbb{P}^1_K$ are K_A-rational. Set $S' := S \times_K K_A$.

Step 2. Let R be the integral closure of $K_A[t]$ in $\kappa(X)$. For $s' \in S'$ above $s \in S$, let $x \in X_s$ be a fixed point above s'. Since R is a Dedekind ring, we can choose $u \in R$ satisfying:

- $v_{\mathfrak{p}_x}(u) = 1$, and $v_{\mathfrak{p}_{x\sigma}}(u-1) = 1$ for $\sigma \in C \backslash I_x$; and $\kappa(X) = K_A(t)[u]$.

Hence for $s \in S$, $s' \in S'$ and $x \in X_s$ as above, one has: $v_{\mathfrak{p}_x}(\sigma u) = 1$ for all $\sigma \in I_x$, and $v_{\mathfrak{p}_x}\big(\sigma(u-1)\big) = 1$ for $\sigma \in C \backslash I_x$. Let $f(U,t) \in K_A(t)[U]$ be the minimal polynomial of u over $K_A(t)$. One has $f(U,t) := U^d + a_{d-1}(t)U^{d-1} + \cdots + a_0(t) \in K_A[U,t]$ by that fact that $u \in R$, and recalling that $e_s = |I_x|$, the following hold:

$(*)$ $v_{\mathfrak{p}_{s'}}\big(a_0(t)\big) = 1$; and $v_{\mathfrak{p}_{s'}}\big(a_m(t)\big) \geq 1$ for $m < e_s$; and $v_{\mathfrak{p}_{s'}}\big(a_{e_s}(t)\big) = 0$.

Let $p_{s'}(t) := t - \theta_{s'} \in K_A[t]$ define s'. Then the $\theta_{s'} \in K_A$, $s' \in S'$, are distinct simple roots of $a_0(t)$ by condition $(*)$ above. In particular, the following hold:

$(**)$ $a_{e_s}(\theta_{s'}) \neq 0$; and $a_0(t) = p_{s'}(t)\, b_{s'}(t)$ in $K_A[t]$ with $b_{s'}(\theta_{s'}) \neq 0$ in K_A.

In particular, setting $R_{s'} := R[1/b_{s'}(t)]$, we have: x is the only zero of u in $\mathrm{Spec} R_{s'}$, and u is a uniformizing parameter at x in $R_{s'}$. Therefore, u is a prime element of $R_{s'}$, and a uniformizing parameter at $x \in \mathrm{Spec} R_{s'}$. Hence there exist integers $\mu, \nu \geq 0$, and $u_{\sigma s'} \in R$ for $\sigma \in C$, such that the following hold:

a) If $\sigma \in I_x$, then $\sigma(u) = u\, u_{\sigma s'}/b_{s'}(t)^{\mu}$ in $R_{s'}$, with $u_{\sigma s'}/b_{s'}(t)^{\mu} \in R_{s'}^{\times}$. In particular, there exists $\tilde{u}_{\sigma s'} \in R$ such that $u_{\sigma s'}\, \tilde{u}_{\sigma s'} = b_{s'}(t)^{\nu}$ (for ν large enough).

b) If $\sigma \in C \backslash I_x$, then $\sigma(u) = 1 + u\, u_{\sigma s'}/b_{s'}(t)^{\mu}$ in $R_{s'}$, with $u_{\sigma s'}/b_{s'}(t)^{\mu} \in R_{s'}$.

And since $u_{\sigma s'}$, $\tilde{u}_{\sigma s'} \in R$, their minimal polynomials $f_{\sigma s'}(U,t)$, $\tilde{f}_{\sigma s'}(U,t)$ actually belong to $K_A[U,t]$.

Let $\mathfrak{o} = \mathbb{Z}[\alpha_1, \dots, \alpha_r] \subset K$ with $\alpha_i \neq 0$ be a $\mathbb{Z}$-algebra of finite type such that denoting by $\mathfrak{o}_{K_A}$ its integral closure in K_A, the following hold: First, the ramified B-cover $\varphi : X \to \mathbb{P}^1_K$ is defined over $\mathfrak{o}$. Second, $f(U,t)$, $p_{s'}(t)$, $f_{\sigma s'}(U,t)$, $\tilde{f}_{\sigma s'}(U,t)$ belong to $\mathfrak{o}_{K_A}[U,t]$ for all $s' \in S'$ and $\sigma \in C$. Third, $\theta_{s'}$, $a_{e_s}(\theta_{s'})$, $b_{s'}(\theta_{s'})$, $1/a_{e_s}(\theta_{s'})$, $1/b_{s'}(\theta_{s'})$ belong to $\mathfrak{o}_{K_A}$ for all $s' \in S'$ and $s \in S$.

Definition of the set Σ_{φ}. We define $\Sigma_{\varphi} \subset K^{\times}$ to be the set of generators $\Sigma_{\varphi} := \{\alpha_1, \dots, \alpha_r\}$.

Notice that $a_{e_s}(\theta_{s'}), b_{s'}(\theta_{s'}) \in \mathfrak{o}_{K_A}^{\times}$ for all $s' \in S'$. Hence if $v \in \mathcal{V}_s$ satisfies $v(\Sigma_{\varphi}) = 0$, then $\mathfrak{o} \subset \mathcal{O}_v$; and if v^{a} prolongs v to an algebraic closure K^{a} of K, then $\mathfrak{o}_{K_A} \subset \mathcal{O}_{v^{\mathrm{a}}}$, and in particular, $a_{e_s}(\theta_{s'})$, $b_{s'}(\theta_{s'})$ are v^{a}-units.

Step 3. Recall that for $v \in \mathcal{V}_s$, one has by definition: First, $vK \neq \ell \cdot vK$ for $\ell | e_s$; hence there exists $\pi_s \in K^{\times}$ such that $v(\pi_s) > 0$ and $v(\pi_s)$ has order e_s in $vK/(e_s \cdot vK)$. Second, v is totally split in $K_A|K$; hence since v has rank one, K is dense in K_A endowed with v^{a}. By Geyer [Gey78], we have: Since $(v_s)_{s \in S}$ are independent by hypothesis, there exists $b \in H_{\varphi}$ such that $v_s^{\mathrm{a}}(b - \theta_{s'}) = v_s(\pi_s) > 0$, $s \in S$. Further, since $a_{e_s}(t)$, $b_{s'}(t)$ have v_s^{a}-integral coefficients, and $v_s^{\mathrm{a}}(b - \theta_{s'}) > 0$, and $a_{e_s}(\theta_{s'})$, $b_{s'}(\theta_{s'})$ are v_s^{a}-units, it follows that $a_{e_s}(b), b_{s'}(b)$ are v_s^{a}-units too. Recalling that $K_b \hookleftarrow K$ with $\mathrm{Gal}(K_b\,|\,K) = B$ is the fiber of $X \to \mathbb{P}^1_K$ at $t = b$, we have:

Claim. Let w be the restriction of v_s^{a} to K_b. Then $I_x = I_w$ inside B.

Indeed, since $a_0(b) = (b-\theta_{s'})\, b_{s'}(b)$, and $w(b-\theta_{s'}) = v_s^{\mathrm{a}}(b-\theta_{s'}) = v_s(\pi_s) > 0$, one has $w\big(a_0(b)\big) = w(\pi_s) > 0$. Hence $f(U,b) = U^n + \cdots + a_0(b)$ has a root $\xi_{s'}$ such that $w(\xi_{s'}) > 0$. Let $\mathcal{R} \subset R$ be the integral closure of $\mathcal{O}_{v_s}[t]$ in R. Since $\mathfrak{o}_{K_A}$ is integral over $\mathfrak{o}$, and u, $u_{\sigma s'}$, $\tilde{u}_{\sigma s'}$ are integral over $\mathfrak{o}_{K_A}[t]$ (by the definition of $\mathfrak{o}$ and $\mathfrak{o}_{K_A}$), it follows that u, $u_{\sigma s'}$, $\tilde{u}_{\sigma s'}$ are integral over $\mathfrak{o}[t] \subset \mathcal{O}_{v_s}[t]$; hence u, $u_{\sigma s'}$, $\tilde{u}_{\sigma s'} \in \mathcal{R}$. Let $\mathcal{O}_b$ be the integral closure of $\mathcal{O}_{v_s}$ in K_b. Then B acts on $\mathcal{O}_b$, and the B-equivariant projection $\Psi : R \to K_b$ defined by $(u,t) \mapsto (\xi_{s'}, b)$, has a B-equivariant restriction $\psi : \mathcal{R} \to \mathcal{O}_b$. Recall that $a_0(t) = (t-\theta_{s'})\, b_{s'}(t)$ in $\mathfrak{o}_{K_A}[t]$, hence in $\mathcal{O}_w[t]$, and $b_{s'}(b) \in \mathcal{O}_w^{\times}$. Therefore, the canonical B-equivariant projections Ψ and ψ, have canonical prolongations to C-equivariant projections $\Psi_{s'} : R_{s'} \to K_b$, and $\psi_{s'} : \mathcal{R}_{s'} \to \mathcal{O}_b$, where $\mathcal{R}_{s'} := \mathcal{R}[1/b_{s'}(t)]$. Hence we have:

a)$'$ If $\sigma \in I_x$, then $\sigma(\xi_{s'}) = \xi_{s'}\, \psi(u_{\sigma s'})/b_{s'}(b)^{\mu}$ in $\mathcal{O}_b$ and $\psi(u_{\sigma s'})/b_{s'}(b)^{\mu} \in \mathcal{O}_b{}^{\times}$.
b)$'$ If $\sigma \in C\backslash I_x$, then $\sigma(\xi_{s'}) = 1 + \xi_{s'}\psi(u_{\sigma s'})/b_{s'}(b)^{\mu}$ in $\mathcal{O}_b$ and $\psi(u_{\sigma s'})/b_{s'}(b)^{\mu} \in \mathcal{O}_b$.

And for $\sigma \in I_x$, we have $\psi(u_{\sigma s'})\, \psi(\tilde{u}_{\sigma s'}) = b_{s'}(b)^{\nu} \in \mathcal{O}_w^{\times}$; hence $\psi(u_{\sigma s'}) \in \mathcal{O}_w^{\times}$. Therefore:

a)$''$ If $\sigma \in I_x$, then $w\big(\sigma(\xi_{s'})\big) = w(\xi_{s'}) > 0$.
b)$''$ If $\sigma \in C\backslash I_x$, then $w\big(\sigma(\xi_{s'})\big) = 0$.

On the other hand, $a_0(b) = N_{K_b|K_A}(\xi_{s'}) = \prod_{\sigma \in C} \sigma(\xi_{s'})$, and $w\big(a_0(b)\big) = w(\pi_s)$. Hence the following hold: First, $w(\pi_s) = w\big(a_0(b)\big) = |I_x|\, w(\xi_{s'})$; hence since $w(\pi_s) = v_s(\pi_s)$ has order $e_s = |I_x|$ in $v_s K/(e_s \cdot v_s K)$ we get $e(w|v_s) \geq |I_x|$; thus $|I_w| \geq |I_x|$. Second, if $\sigma \in C\backslash I_x$, then by b)$''$ we have: $0 = w\big(\sigma(\xi_{s'})\big) = (w \circ \sigma)(\xi_{s'})$; hence $\sigma \notin D_w$ because $w(\xi_s) > 0$; and since v_s is totally split in $K_A|K$, one has $D_w \subseteq C$; thus $D_w \subseteq I_x$. Hence since $|D_w| \geq |I_w| \geq |I_x|$, we conclude that $|D_w| = |I_x|$. Therefore, $D_w = I_w = I_x \subseteq D_x$, thus proving the claim.

To 1): Recall that by Hilbert decomposition theory, one has $\mathcal{V}_{v_s} \cong B/D_w$, and $X_s \cong B/D_x$ as B-sets. Since $D_w = I_w = I_x$, we see that $\mathcal{V}_{v_s}$ projects B-equivariantly onto X_s, the fibers being isomorphic to D_x/I_x. This concludes the proof of assertion 1).

To 2): Since I_x with $x \in X_s$, $s \in S$, generate C, the same is true for I_w with $w \in \mathcal{V}_{v_s}$ and $s \in S$, by assertion 1). Hence by Hilbert decomposition theory, $K_b \,|\, K_A$ has no nontrivial subextension in which all the v_s, $s \in S$, are unramified. □

4. **A generalization of Theorem** 1.2

Definition/Remarks 4.1. Let $\aleph$ be an infinite cardinal.

1) A field K endowed with a set of nonequivalent valuations $\mathcal{V}$ shall be called a *generalized* $\aleph$ *Krull field*, respectively a *generalized Krull field* provided $\aleph = |K|$, if the following hold:

i) If $\Sigma \subset K^\times$ has cardinality $|\Sigma| < \aleph$, then $\mathcal{V}_\Sigma := \{v \in \mathcal{V} \mid v(\Sigma) \neq 0\}$ has $|\mathcal{V}_\Sigma| < \aleph$.

ii) For every finite Galois extension $L|K$, and every integer $n > 1$, the set

$$\mathcal{V}_{L|K,n} := \{v \in \mathcal{V} \mid v \text{ totally split in } L|K,\ vK \neq \ell \cdot vK \text{ for } \ell \,|\, n,\ \ell > 1\}$$

has $|\mathcal{V}_{L|K,n}| \geq \aleph$.

Note that in particular, the Krull fields are exactly the generalized $\aleph_0$ Krull fields with respect to sets $\mathcal{V}$ of discrete valuations.

2) Prominent examples of Krull fields are the following:

a) The global fields (by the Chebotarev Density Theorem).

b) The function fields $K|k$ with $\text{tr.deg}(K|k) > 0$. (Indeed, by point 3 below, it is sufficient to consider the case $K = k(t_1, \dots, t_d)$ is a rational function field, etc.)

c) The quotient fields of domains R as in Theorem 3.4.

3) The class of generalized $\aleph$ Krull fields is closed under finite field extensions.

Definitions/Notation 4.2. For an embedding problem

$$\text{EP} = (\gamma : G_K \to A,\ \alpha : B \to A)$$

over K, let K_A be the fixed field of $\ker(\gamma)$; hence $\text{Gal}(K_A|K) = A$ canonically. And for proper solutions β of EP, let K_β be the fixed field of $\ker(\beta)$; hence $\text{Gal}(K_\beta|K) = B$ canonically.

1) A family of proper solutions $\{\beta_j\}_{j \in J}$ of EP is called *independent*, if for all $j \in J$ one has: K_{β_j} and the compositum $L_j := \cup_{j' \neq j} K_{j'}$ are linearly disjoint over K_A.

2) If K endowed with $\mathcal{V}$ is a generalized $\aleph$ Krull field, a proper solution β of EP is called *totally ramified*, if $K_\beta|K_A$ has no proper subextension in which all the $v \in \mathcal{V}$ are unramified.

THEOREM 4.3. *Let K endowed with a set of rank-one valuations $\mathcal{V}$ be a generalized $\aleph$ Krull field. Suppose that K is large and Hilbertian. Then every nontrivial finite split embedding problem for G_K has at least $\aleph$ independent and totally ramified proper solutions.*

Proof. Let $\text{EP} = (\gamma : G_K \to A,\ \alpha : B \to A)$ be a nontrivial finite split embedding problem over K, and $\text{EP}_t = (\gamma \circ \text{pr}_t : G_{K(t)} \to A,\ \alpha : B \to A)$ be the nontrivial finite split embedding problem for $G_{K(t)}$. By Theorem A of Pop [Pop96], EP_t has proper regular solutions β_t, which means that if $K_A \subseteq K(t)_{\beta_t}$ are the fixed fields of $\ker(\gamma)$ in K^{s}, respectively of $\ker(\beta_t)$ in $K(t)^{\mathrm{s}}$, then $K(t)_{\beta_t} \cap K^{\mathrm{s}} = K_A$. Moreover, if $\varphi : X \to \mathbb{P}^1_K$ is the B-ramified cover defining $\beta_t : G_{K(t)} \to B$, then sorting through the proof of loc. cit., one can see that the ramification points of φ are actually K_φ-rational, where $K_\varphi|K_A$ is some cyclotomic extension. Hence Theorem 3.6 is applicable here.

Using Zorn's Lemma, let $\{\beta_j\}_{j\in J}$ be a maximal set of independent proper solutions of EP, given by specializing φ as in Theorem 3.6. Note that these solutions are totally ramified by assertion 2) of loc. cit. We claim that $|J| \geq \aleph$. Indeed, by contradiction, suppose that $|J| < \aleph$. For every β_j, set $K_{\beta_j} = K[\xi_j]$, and let $p_j(T) = T^n + a_{j,n-1}T^{n-1} + \dots + a_{j,0} \in K[t]$ be the minimal polynomial of ξ_j, and $\delta_j \in K^\times$ its discriminant. If $v \in \mathcal{V}$ satisfies: $p_j(T) \in \mathcal{O}_v[T]$ and $v(\delta_j) = 0$, then v is unramified in $K_\beta|K$. Hence denoting $\Sigma_j := \{\delta_j, a_{j,0}, \dots, a_{j,n-1}\} \cap K^\times$, the following hold: If v is ramified in $K_{\beta_j}|K$, then $v(\Sigma_j) \neq 0$; or equivalently one has $\mathcal{V}_j := \{v \in \mathcal{V} \mid v \text{ is ramified in } K_{\beta_j}|K\} \subseteq \{v \mid v(\Sigma_j) \neq 0\} =: \mathcal{V}_{\Sigma_j}$.

Thus if $\Sigma_J := \cup_{j\in J}\Sigma_j$, we have $\mathcal{V}_{\Sigma_J} := \{v \in \mathcal{V} \mid v(\Sigma_J) \neq 0\} = \cup_{j\in J}\mathcal{V}_{\Sigma_j}$. Therefore we get $\mathcal{V}_J := \cup_{j\in J}\mathcal{V}_j \subseteq \cup_{j\in J}\mathcal{V}_{\Sigma_j} =: \mathcal{V}_{\Sigma_J}$. Since each Σ_j is finite, and we supposed that $|J| < \aleph$, it follows that $\Sigma_J = \cup_{j\in J}\Sigma_j$ has cardinality $|\Sigma_J| < \aleph$. But then by condition i) in the definition of $\mathcal{V}$, we have $|\mathcal{V}_{\Sigma_J}| < \aleph$; hence $|\mathcal{V}_J| < \aleph$ because $\mathcal{V}_J \subseteq \mathcal{V}_{\Sigma_J}$. Hence by condition ii) in the definition of $\mathcal{V}$, and with K_φ and e_s as in Notation 3.5, one has: $|\mathcal{V}_{K_\varphi|K,e_s} \backslash \mathcal{V}_J| \geq \aleph$ for each $s \in S$. Since S is finite, we can choose a system of independent valuations $(v_s)_{s\in S}$ with $v_s \in \mathcal{V}_{K_\varphi|K,e_s} \backslash \mathcal{V}_J$. For this system $(v_s)_{s\in S}$, consider a solution β of EP as given by Theorem 3.6. Let $L_J|K$ be the compositum of all the K_{β_j}, $j \in J$. We claim that $L_J \cap K_\beta = K_A$. Indeed, since $v_s \notin \mathcal{V}_J$, the v_s, $s \in S$, are unramified in $K_{\beta_j}|K$, for all $j \in J$; hence in $L_J|K$. Thus, the v_s are unramified in $L_J \cap K_\beta$ too. But then by assertion 2) of Theorem 3.6, we get $L_J \cap K_\beta = K_A$. Now, the family of distinct totally ramified solutions $\{\beta\} \cup \{\beta_j\}_{j\in J}$ is independent and contradicts the maximality of $\{\beta_j\}_{j\in J}$. □

5. **Proof of Theorem** 1.3

First, K is large, by Theorem 1.1; and Hilbertian by Weissauer [Wei82, Th. 7.2], because the integral closure of R is a Krull domain with Krull.dim > 1. Hence every split nontrivial embedding problem for G_K has $|K|$ proper solutions by Theorems 1.2 and 3.4. Second, the same is true correspondingly for $G_{K^{\text{ab}}}$, by [Har09, Th. 2.4]. Finally, $\text{cd}(K^{\text{ab}}) \leq 1$, by Colliot-Thélène–Ojanguren–Parimala [CTOP02, Th 2.2], and [Har09, Th. 4.4], if $\text{char}(K) > 0$. One concludes by applying [HS05, Th. 2.1].

Thanks. I would like to thank D. Harbater, M. Jarden, and others for inspiration and discussions; and E. Paran for pointing out a gap in the first version of the manuscript, and the referee for his useful comments.

References

[CT00] J.-L. COLLIOT-THÉLÈNE, Rational connectedness and Galois covers of the projective line, *Ann. of Math.* **151** (2000), 359–373. MR 2001b:14046 Zbl 0990.12003

[CTOP02] J.-L. COLLIOT-THÉLÈNE, M. OJANGUREN, and R. PARIMALA, Quadratic forms over fraction fields of two-dimensional Henselian rings and Brauer groups of related schemes, in *Algebra*, *arithmetic and geometry*, *Parts* I, II (Mumbai, 2000), *Tata Inst. Fund. Res. Stud. Math.* **16**, Tata Inst. Fund. Res., Bombay, 2002, pp. 185–217. MR 2004c:14031 Zbl 1055.14019

[DD97] P. DÈBES and B. DESCHAMPS, The regular inverse Galois problem over large fields, in *Geometric Galois Actions* II (L. SCHNEPS and P. LOCHAK, eds.), *London Math. Soc. Lecture Note Ser.* **243**, Cambridge Univ. Press, Cambridge, 1997, pp. 119–138. MR 99j:12002 Zbl 0905.12004

[Gey78] W.-D. GEYER, Galois groups of intersections of local fields, *Israel J. Math.* **30** (1978), 382–396. MR 80a:12017 Zbl 0383.12014

[Har03] D. HARBATER, Patching and Galois theory, in *Galois Groups and Fundamental Groups*, *Math. Sci. Res. Inst. Publ.* **41**, Cambridge Univ. Press, Cambridge, 2003, pp. 313–424. MR 2004j:14030 Zbl 1071.14029

[Har09] ———, On function fields with free absolute Galois groups, *J. Reine Angew. Math.* **632** (2009), 85–103. MR 2010h:12002 Zbl 05598020

[HS05] D. HARBATER and K. F. STEVENSON, Local Galois theory in dimension two, *Adv. Math.* **198** (2005), 623–653. MR 2007e:12002 Zbl 1104.12003

[Kol99] J. KOLLÁR, Rationally connected varieties over local fields, *Ann. of Math.* **150** (1999), 357–367. MR 2000h:14019 Zbl 0976.14016

[MB01] L. MORET-BAILLY, *R*-équivalence simultanée de torseurs: un complément à l'article de P. Gille, *J. Number Theory* **91** (2001), 293–296. MR 2002k:14076 Zbl 1076.14531

[Par09] E. PARAN, Split embedding problems of complete domains, *Ann. of Math.* **170** (2009), 899–914. MR 2552112 Zbl pre05610434

[PP08] B. POONEN and E. POP, First order characterization of function field invariants over large fields, in *Model Theory with Applications to Algebra and Analysis* (CHATZIDAKIS, MACPHERSONS, PILLAYS, and WILKIE, eds.), *London Math. Soc. Lecture Note Ser.* **350**, Cambridge Univ. Press, 2008, pp. 255–272. MR 2010e:03034 Zbl 1174.03015

[Pop96] F. POP, Embedding problems over large fields, *Ann. of Math.* **144** (1996), 1–34. MR 97h:12013 Zbl 0862.12003

[Pos05] L. POSITSELSKI, Koszul property and Bogomolov's conjecture, *Int. Math. Res. Not.* **31** (2005), 1901–1936. MR 2006h:19002 Zbl 1160.19301

[Wei82] R. WEISSAUER, Der Hilbertsche Irreduzibilitätssatz, *J. Reine Angew. Math.* **334** (1982), 203–220. MR 84c:12020 Zbl 0477.12029

(Received December 29, 2007)
(Revised April 19, 2009)

E-mail address: pop@math.upenn.edu
UNIVERSITY OF PENNSYLVANIA, DEPARTMENT OF MATHEMATICS, 209 SOUTH 33RD STREET, PHILADELPHIA 19104, UNITED STATES
http://www.math.upenn.edu/∼pop

ISSN 0003-486X

ANNALS OF MATHEMATICS

This periodical is published bimonthly by the Department of Mathematics at Princeton University with the cooperation of the Institute for Advanced Study. Annals is typeset in TeX by Sarah R. Warren and produced by Mathematical Sciences Publishers. The six numbers each year are divided into two volumes of three numbers each.

Editorial correspondence

Papers submitted for publication and editorial correspondence should be addressed to Maureen Schupsky, Annals of Mathematics, Fine Hall-Washington Road, Princeton University, Princeton, NJ, 08544-1000 U.S.A. The e-mail address is annals@math.princeton.edu.

Preparing and submitting papers

The Annals requests that all papers include an abstract of about 150 words which explains to the nonspecialist mathematician what the paper is about. It should not make any reference to the bibliography. Authors are encouraged to initially submit their papers electronically and in PDF format. Please send the file to: annals@math.princeton.edu or to the Mathematics e-print arXiv: front.math.ucdavis.edu/submissions. If a paper is submitted through the arXiv, then please e-mail us with the arXiv number of the paper.

Proofs

A PDF file of the galley proof will be sent to the corresponding author for correction. If requested, a paper copy will also be sent to the author.

Offprints

Authors of single-authored papers will receive 30 offprints. (Authors of papers with one co-author will receive 15 offprints, and authors of papers with two or more co-authors will receive 10 offprints.) Extra offprints may be purchased through the editorial office.

Subscriptions

The price for a print and online subscription, or an online-only subscription, is $390 per year for institutions. In addition, there is a postage surcharge of $40 for print subscriptions that are mailed to countries outside of the United States. Individuals interested in subscriptions for their own personal use should contact the publisher at the address below. Subscriptions and changes of address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 (e-mail: contact@mathscipub.org; phone: 1-510-643-8638; fax: 1-510-295-2608). (Checks should be made payable to "Mathematical Sciences Publishers".)

Back issues and reprints

Orders for missing issues and back issues should be sent to Mathematical Sciences Publishers at the above address. Claims for missing issues must be made within 12 months of the publication date. Online versions of papers published five or more years ago are available through JSTOR (www.jstor.org).

Microfilm

Beginning with Volume 1, microfilm may be purchased from NA Publishing, Inc., 4750 Venture Drive, Suite 400, PO Box 998, Ann Arbor, MI 48106-0998; phone: 1-800-420-6272 or 734-302-6500; email: info@napubco.com, website: www.napubco.com/contact.html.

Printed in U.S.A. by Sheridan Printing Company, Inc., Alpha, NJ

TABLE OF CONTENTS