ISRAEL JOURNAL OF MATHEMATICS 86 (1994), 25–59

PSEUDO ALGEBRAICALLY CLOSED FIELDS OVER RINGS

BY

MOSHE JARDEN AND AHARON RAZON

School of Mathematical Sciences
Raymond and Beverly Sackler Faculty of Exact Sciences Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel
e-mail: jarden@math.tau.ac.il and razon@math.tau.ac.il

ABSTRACT

We prove that for almost all $\sigma \in G(\mathbb{Q})^e$ the field $\tilde{\mathbb{Q}}(\sigma)$ has the following property: For each absolutely irreducible affine variety V of dimension r and each dominating separable rational map $\varphi\colon V \to \mathbb{A}^r$ there exists a point $\mathbf{a} \in V(\tilde{\mathbb{Q}}(\sigma))$ such that $\varphi(\mathbf{a}) \in \mathbb{Z}^r$. We then say that $\tilde{\mathbb{Q}}(\sigma)$ is **PAC over $\mathbb{Z}$**. This is a stronger property then being PAC. Indeed we show that beside the fields $\tilde{\mathbb{Q}}(\sigma)$ other fields which are algebraic over $\mathbb{Q}$ and are known in the literature to be PAC are not PAC over $\mathbb{Z}$.

Introduction

J. Ax observed in [Ax] that every nonprincipal ultraproduct K of finite fields has the following property, which later on Frey [Fre] called **PAC**: Every absolutely irreducible variety defined over K has a K-rational point. Ax asked in [Ax] whether there exists a PAC field which is algebraic over $\mathbb{Q}$ besides the algebraic closure $\tilde{\mathbb{Q}}$ of $\mathbb{Q}$. The first author [Ja1] gave a host of examples for such fields. Indeed, he proved that if e is a positive integer, then $\tilde{\mathbb{Q}}(\sigma)$ is PAC for almost all $\sigma \in G(\mathbb{Q})^e$. Here $G(\mathbb{Q})$ is the absolute Galois group of $\mathbb{Q}$, 'almost all' is used in the sense of the Haar measure of $G(\mathbb{Q})^e$, and $\tilde{\mathbb{Q}}(\sigma)$ is the fixed field in $\tilde{\mathbb{Q}}$ of $\sigma = (\sigma_1, \ldots, \sigma_e)$. Later on more examples of algebraic extensions of $\mathbb{Q}$ which are PAC were given. Thus, [FJ1] constructs a Galois extension N of $\mathbb{Q}$ which is PAC such that $\mathcal{G}(N/\mathbb{Q})$ is a direct product of symmetric groups. Recently Pop proved for the maximal totally real extension $\mathbb{Q}_{\mathrm{tr}}$ of $\mathbb{Q}$ that $\mathbb{Q}_{\mathrm{tr}}(\sqrt{-1})$ is PAC [Pop].

Received August 22, 1993

Almost all fields $\tilde{\mathbb{Q}}(\sigma)$ mentioned above have a 'density property' which has not yet been proven for any other PAC field: For each valuation w of $\tilde{\mathbb{Q}}$ and each absolutely irreducible variety V defined over $\tilde{\mathbb{Q}}(\sigma)$ the set $V(\tilde{\mathbb{Q}}(\sigma))$ is w-dense in $V(\tilde{\mathbb{Q}})$.

The present work adjusts the proof of the first author to prove that almost all fields $\tilde{\mathbb{Q}}(\sigma)$ have a stronger property than being PAC: For each absolutely irreducible affine variety V of dimension r and each dominating separable rational map $\varphi\colon V \to \mathbb{A}^r$ there exists a point $\mathbf{a} \in V(\tilde{\mathbb{Q}}(\sigma))$ such that $\varphi(\mathbf{a}) \in \mathbb{Z}^r$. We then say that $\tilde{\mathbb{Q}}(\sigma)$ is **PAC over** $\mathbb{Z}$.

This stronger PAC property of almost all fields $\tilde{\mathbb{Q}}(\sigma)$ is responsible for the density property of the $\tilde{\mathbb{Q}}(\sigma)$ (Theorem 9.2) and for Rumely's local global principle of their rings of integers. We prove the latter result in a subsequent work. Moreover, we prove in that work that this property also implies a weak and a strong approximation theorems for absolutely irreducible varieties over $\tilde{\mathbb{Q}}(\sigma)$.

In this work we use Faltings' theorem to prove that the PAC Galois extension N of $\mathbb{Q}$ mentioned above is PAC over no number field. We prove further that the field $\mathbb{Q}_{\mathrm{tr}}(\sqrt{-1})$ is PAC over no totally real number field. It is an open question if $\mathbb{Q}_{\mathrm{sol}}$ is a PAC field. Nevertheless, the same method shows that it is certainly PAC over no number field. Thus, the fields $\tilde{\mathbb{Q}}(\sigma)$ appear to be 'more pseudo algebraically closed than other PAC fields'. We don't know of any other example of an algebraic extension of $\mathbb{Q}$ which is PAC field over $\mathbb{Z}$ or over $\mathbb{Q}$.

Fried and Völklein [FrV] prove that if K is a PAC field of characteristic 0 and G is a finite group, then there are infinitely many positive integers r such that G can be realized over $K(t)$, regularly over K, with exactly r branch points. This result applies also for almost all fields $\tilde{\mathbb{Q}}(\sigma)$. We observe here that since almost all $\tilde{\mathbb{Q}}(\sigma)$ are PAC over $\mathbb{Z}$, the branch points of the cover that realizes G can be taken to be finite and $\mathbb{Z}$-rational.

ACKNOWLEDGEMENT: We are indebted to Wulf-Dieter Geyer for his valuable contributions to Sections 4 and 8. We also thank Dan Haran, for suggestions that have improved the presentation of Section 4.

1. Definitions and basic properties

Recall that a field M is **pseudo algebraically closed (PAC)** if every absolutely irreducible variety V defined over M has an M-rational point. If O is a subring of M, then M may have a stronger property:

Definition 1.1: Let O be a subset of a field M. We say that M is **PAC over** O if for every affine absolutely irreducible variety V of dimension $r \geq 0$ and for each dominating separable rational map $\varphi\colon V \to \mathbb{A}^r$ over M there exists $\mathbf{a} \in V(M)$ such that $\varphi(\mathbf{a}) \in O^r$.

If $\mathbf{x} = (x_1, \ldots, x_n)$ is a generic point of V over M, then the assumption that φ is dominating means that $\text{trans.deg}_M M(\varphi(\mathbf{x})) = r$, and being separable then means that $M(\mathbf{x})/M(\varphi(\mathbf{x}))$ is a finite separable extension. ∎

Remark 1.2: By definition, each PAC field is PAC over itself. Conversely, the following statements hold for a PAC field M over a subset O:

(a) M is PAC. Indeed, if V and $\mathbf{x}$ are as above, then $M(\mathbf{x})$ is a separable extension of M of transcendence degree r. Let $t_1, \ldots, t_r$ be a separating transcendence basis for $M(\mathbf{x})/M$. Then $M(\mathbf{x})/M(\mathbf{t})$ is a finite separable extension and $t_1, \ldots, t_r$ are rational functions in $x_1, \ldots, x_n$ with coefficients in M. So, the map $\mathbf{x} \mapsto \mathbf{t}$ defines a dominating separable rational map $\varphi\colon V \to \mathbb{A}^r$ over M. By definition, $V(M)$ is nonempty. So, M is PAC.

(b) O is infinite. Apply the definition on the absolutely irreducible polynomial $X^2 + T^2 + 1$ to conclude that O is nonempty. If O were finite consider the curve defined by $1 + \prod_{a \in O}(T - a)X = 0$ and let φ be the projection on the T-coordinate. Any solution (t, x) of this equation with $t \in O$ will lead to a contradiction $1 = 0$.

(c) Suppose that V_0 is in definition 1.1 an M-open nonempty subset of V. Then we may use Rabinovich trick [FJ2, Proof of Prop. 10.1] and choose $\mathbf{a}$ to be in $V_0(M)$.

(d) More generally, let $\varphi\colon V \to W$ be a dominating separable rational map of absolutely irreducible quasi projective varieties of dimension r over M. Suppose that W has an M-open subset W_0 which is M-isomorphic to an open subset of $\mathbb{A}^r$. Take affine nonempty M-open subset V_0 of V which is contained in $\varphi^{-1}(W_0)$. Then, there exists $\mathbf{a} \in V_0(M)$ such that $\varphi(\mathbf{a}) \in W_0(O)$.

(e) If S is a subset of M that contains O, then M is also PAC over S. ∎

As in the case of PAC fields, it suffices to check the condition of Definition 1.1 only for plane curves:

LEMMA 1.3: *Let O be a subring of a field M. A necessary and sufficient condition for M to be PAC over O is*

(1) *For each absolutely irreducible polynomial $f \in M[T, X]$ such that $\frac{\partial f}{\partial X} \neq 0$*

and for each $0 \neq g \in M[T]$ *there exists* $(a, b) \in O \times M$ *such that* $f(a, b) = 0$ *and* $g(a) \neq 0$.

Proof: Condition (1) is obviously necessary for M to be PAC over O. So assume (1). Then the following statement is true for $r = 1$.

(2) For each absolutely irreducible polynomial $f \in M[T_1, \ldots, T_r, X]$ such that $\frac{\partial f}{\partial X} \neq 0$ and each $0 \neq g \in M[T_1, \ldots, T_r]$ there exist $a_1, \ldots, a_r \in O$ and $b \in M$ such that $f(\mathbf{a}, b) = 0$ and $g(\mathbf{a}) \neq 0$.

Assume inductively that $r \geq 2$ and that (2) is true for $r-1$. Let u_0, u_1 be algebraically independent elements over M. By [FJ2, Prop. 9.33], $f(T_1, \ldots, T_{r-1}, u_0 + u_1 T_1, X)$ is an absolutely irreducible polynomial with coefficients in $M(u_0, u_1)$. Use the Bertini-Noether theorem [FJ2, Prop. 9.29] to find $c_0, c_1 \in O$ such that the polynomial $f(T_1, \ldots, T_{r-1}, c_0 + c_1 T_1, X)$ is absolutely irreducible, $g(T_1, \ldots, T_{r-1}, c_0 + c_1 T_1) \neq 0$ and $\frac{\partial f}{\partial X}(T_1, \ldots, T_{r-1}, c_0 + c_1 T_1, X) \neq 0$. By the induction hypothesis there exist $a_1, \ldots, a_{r-1} \in O$ and $b \in M$ such that $f(a_1, \ldots, a_{r-1}, c_0 + c_1 a_1, b) = 0$ and $g(a_1, \ldots, a_{r-1}, c_0 + c_1 a_1) \neq 0$. So (2) holds also for r.

Now let V, φ, and $\mathbf{x}$ be as in Definition 1.1. Then $\mathbf{t} = \varphi(\mathbf{x})$ is a separating transcendence basis for $M(\mathbf{x})/M$. Choose a primitive element y for $M(\mathbf{x})/M(\mathbf{t})$ which is integral over $M[\mathbf{t}]$ and let $f \in M[\mathbf{T}, Y]$ be a monic polynomial in Y such that $f(\mathbf{t}, Y) = \mathrm{irr}(M(\mathbf{t}), y)$. Then f is absolutely irreducible and $\partial f / \partial Y \neq 0$. Denote the hypersurface in $\mathbb{A}^{r+1}$ defined by $f(\mathbf{T}, Y) = 0$ over M by W. Let $\pi\colon W \to \mathbb{A}^r$ be the projection on the first r coordinates. The map $(\mathbf{t}, y) \mapsto \mathbf{x}$ defines a birational map $\theta\colon W \to V$ over M such that $\varphi \circ \theta = \pi$. Find $0 \neq g \in M[\mathbf{T}]$, an M-open subset V_0 of V and an M-open subset W_0 of W such that $\varphi|_{V_0}\colon V_0 \to \mathbb{A}^r$ is a morphism, $\theta|_{W_0}\colon W_0 \to V_0$ is an isomorphism and $W_0 = \pi^{-1}(\mathbb{A}^r - V(g))$. By (2) there exist $a_1, \ldots, a_r \in O$ and $b \in M$ such that $f(\mathbf{a}, b) = 0$ and $g(\mathbf{a}) \neq 0$. Then $(\mathbf{a}, b) \in W_0$. Let $\mathbf{c} = \theta(\mathbf{a}, b)$. Then $\mathbf{c} \in V(M)$ and $\varphi(\mathbf{c}) = \mathbf{a} \in O^r$. Conclude that M is PAC over O. ∎

Lemma 1.3 supplies the first example of a PAC field over a subring.

Example 1.4: If M is a separably closed field and O is an infinite subring, then M is PAC over O. ∎

COROLLARY 1.5: *Let M be a PAC field over a subring O with a quotient field K. Then $K_s \cap M$ is PAC over O.*

Proof: Let $f \in (K_s \cap M)[T, X]$ be an absolutely irreducible polynomial and let

$0 \neq g \in (K_s \cap M)[T]$. Then there exist $h_0, h_1 \in (K_s \cap M)[T]$ and $0 \neq h_2 \in (K_s \cap M)[T]$ such that

$$h_0(T,X)f(T,X) + h_1(T,X)\frac{\partial f}{\partial X}(T,X) = h_2(T). \tag{3}$$

Since M is PAC over O, there exists $(a,b) \in O \times M$ such that $f(a,b) = 0$ and $g(a)h_2(a) \neq 0$. By (3), $\frac{\partial f}{\partial X}(a,b) \neq 0$. Hence $b \in K_s$. Thus, $K_s \cap M$ is PAC over O. ∎

Example 1.6: Suppose that M is a PAC field over a subring O. Let $f_1, \ldots, f_d \in M[X]$ with $d \geq 2$ be polynomials which have no root in common and such that $df_1/dX \neq 0$. Let $a_1, \ldots, a_d \in M$ with $a_2 \neq 0$ and let $m \in M$, $m \neq 0$. Then $h^*(T,X) = (mT+a_1)f_1(X)+a_2f_2(X)+\cdots+a_df_d(X)$ is an absolutely irreducible polynomial with $\frac{\partial h^*}{\partial X} \neq 0$. Hence, by Lemma 1.3, there exists $(a,b) \in O \times M$ such that $(ma + a_1)f_1(b) + a_2f_2(b) + \cdots + a_df_d(b) = 0$. ∎

If M is perfect, then the condition on φ to be separable is redundant.

LEMMA 1.7: *Let M be a perfect field which is PAC over a subring O.*

(a) *For each absolutely irreducible variety V of dimension $r \geq 0$, for each nonempty Zariski open subset V_0 of V and for each dominating rational map $\varphi\colon V \to \mathbb{A}^r$ over M there exists $\mathbf{a} \in V_0(M)$ such that $\varphi(\mathbf{a}) \in O^r$.*

(b) *Let F/M be a regular extension of transcendence degree 1, let $t \in F \setminus M$, and let A be a finite subset of M. Then F has an M-rational place π such that $\pi(t) \in O \setminus A$.*

Proof of (a): Let $\mathbf{x}$ be a generic point of V over M, let $F = M(\mathbf{x})$, and let $\mathbf{t} = \varphi(\mathbf{x})$. Then $F/M(\mathbf{t})$ is a finite algebraic extension. Let $E = M(\mathbf{x}')$ be the maximal separable extension of $M(\mathbf{t})$ in F. Then $\mathbf{x}'$ generates an absolutely irreducible variety V' over M of dimension r and the map $\mathbf{x}' \mapsto \mathbf{t}$ extends to a separable rational map $\varphi'\colon V' \to \mathbb{A}^r$.

Each of the coordinates x_i of $\mathbf{x}$ satisfies an equation $x_i^q = f_i(\mathbf{x}')$ for some power q of $\mathrm{char}(M)$ and a rational function f_i of V'. Since M is PAC over O, there exists $\mathbf{a}' \in V'(M)$ such that $\varphi'(\mathbf{a}') \in O^r$, each of the functions f_i is well defined at $\mathbf{a}'$ and the unique point $\mathbf{a}$ of $V(\tilde{M})$ which lies over $\mathbf{a}'$ belongs to $V_0(\tilde{M})$. The coordinates of $\mathbf{a}$ satisfy $a_i^q = f_i(\mathbf{a}')$. Since M is perfect, $\mathbf{a} \in V_0(M)$, as desired.

Proof of (b): Let $x_1, \ldots, x_n$ be generators of the integral closure of $M[t]$ in F [La1, p. 120, Thm. 2]. The curve C which $\mathbf{x}$ defines over M is normal, hence

smooth [Sha, p. 112]. Let $\varphi\colon C \to \mathbb{A}^1$ be the epimorphism which is defined by $\varphi(\mathbf{x}) = t$. By (a), there exists $\mathbf{a} \in C(M)$ which does not belong to $\varphi^{-1}(A)$ such that $\varphi(\mathbf{a}) \in O$. Since $\mathbf{a}$ is simple on C, the specialization $\mathbf{x} \to \mathbf{a}$ extends to an M-rational place π of F [JaR, Cor. A2]. It satisfies $\pi(t) = \varphi(\mathbf{a}) \in O \setminus A$. ∎

2. Algebraic extensions

Each algebraic extension of a PAC field is also PAC [FJ2, Cor. 10.7]. The proof of this result is done first for separable extensions, using Weil's descent, and then for purely inseparable extensions, using Roquette's descent. The application of Weil's descent to PAC over subrings forces extensions of the subrings:

LEMMA 2.1: *Let N/M be a finite separable extension. Suppose that M is a PAC field over a subring O. Let $w_1, \dots, w_d$ be a basis for N/M and let $S = O[w_1, \dots, w_d]$. Then N is PAC over S.*

Proof: Let V be an absolutely irreducible variety in $\mathbb{A}^n$ of dimension r and let $\varphi\colon V \to \mathbb{A}^r$ be a dominating separable rational map defined over N. Replace V by the graph V' of φ in $V \times \mathbb{A}^r$ and φ by the projection of V' on the last r coordinates, if necessary, to assume that φ is the projection on the first r coordinates.

Let $\sigma_1, \dots, \sigma_d$, with $\sigma_1 = 1$, be the d distinct M-isomorphisms of N into M_s. Denote the coordinates of $\mathbb{A}^n$ by x_k, $k = 1, \dots, n$ and those of $\mathbb{A}^{nd}$ by y_{ik}, $i = 1, \dots, d$, and $k = 1, \dots, n$. Let $\lambda\colon \mathbb{A}^{nd} \to \mathbb{A}^n$ be the linear map over N given by

$$\lambda(\mathbf{y}) = \mathbf{x} \quad \text{and} \quad x_k = \sum_{i=1}^{d} w_i y_{ik}, \qquad k = 1, \dots, n, \tag{1}$$

and let

$$\Phi = \sigma_1(\varphi) \times \cdots \times \sigma_d(\varphi)\colon \sigma_1(V) \times \cdots \times \sigma_d(V) \to (\mathbb{A}^r)^d.$$

Then Φ is a dominating separable morphism over N.

By [FJ2, Prop. 9.34] there exists an absolutely irreducible variety $W \subseteq \mathbb{A}^{nd}$ defined over M such that the restriction of $\sigma_1(\lambda) \times \cdots \times \sigma_d(\lambda)$ to W is an isomorphism $\Lambda\colon W \to \sigma_1(V) \times \cdots \times \sigma_d(V)$ (which is defined over the Galois closure of N/M). Consider the projection $\psi\colon W \to \mathbb{A}^{rd}$ given by

$$\psi(\mathbf{y}) = \mathbf{y}_0, \text{ where } \mathbf{y}_0 = (y_{ik})_{1 \le i \le d;\ 1 \le k \le r}. \tag{2}$$

Finally, let λ_0: $\mathbb{A}^{rd} \to \mathbb{A}^r$ be the linear map over N given as in (1), where now $k = 1, \ldots, r$ and let $\Lambda_0 = \sigma_1(\lambda_0) \times \cdots \times \sigma_d(\lambda_0)$. Then the following diagram is commutative:

$$\begin{array}{ccccc} W & \xrightarrow{\Lambda} & \sigma_1(V) \times \cdots \times \sigma_d(V) & \xrightarrow{\pi} & V \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \varphi} \\ \mathbb{A}^{rd} & \xrightarrow{\Lambda_0} & \mathbb{A}^r \times \cdots \times \mathbb{A}^r & \xrightarrow{\pi_0} & \mathbb{A}^r \end{array}$$

where π and π_0 are the projections on the first components. Also, $\pi \circ \Lambda = \lambda|_W$ and $\pi_0 \circ \Lambda_0 = \lambda_0$.

Since both Λ and Λ_0 are isomorphisms, and Φ is a dominating separable morphism over N, so is ψ. Thus $N(W)/N(\psi(W))$ is a finite separable extension. Since the extension $N(\psi(W))/M(\psi(W))$ is also finite and separable, so is $M(W)/M(\psi(W))$.

Thus, ψ is a separable dominating morphism over M. Since M is PAC over O, there exists $\mathbf{b} \in W(M)$ such that $\psi(\mathbf{b}) \in O^{rd}$. Let $\mathbf{a} = \lambda(\mathbf{b})$. By (1) and (2), and by the commutativity of the diagram, $\mathbf{a} \in V(N)$ and $\varphi(\mathbf{a}) \in S^r$. Conclude that N is PAC over S. ∎

Contrary to separable extensions, a variant of Roquette's descent which we establish here proves that purely inseparable extensions of a PAC over a subring O are again PAC over O.

LEMMA 2.2: *Let M'/M be a purely inseparable extension. Let V be an absolutely irreducible affine variety of dimension r over M'. Let φ: $V \to \mathbb{A}^r$ be a dominating separable rational map over M'. Then there exists an absolutely irreducible affine variety W of dimension r, a dominating separable rational map ψ: $W \to \mathbb{A}^r$ over M, and a birational morphism λ: $W \to V$ over M' such that $\psi = \varphi \circ \lambda$.*

Proof: Let $p = \mathrm{char}(M)$. The variety V and the map φ are defined over a subextension M_0' of M'/M of degree p^k. Use induction on k to assume that $k = 1$ and therefore that $(M')^p \subseteq M$.

Choose a generic point $\mathbf{x} = (x_1, \ldots, x_n)$ for V over M' and let $F = M'(\mathbf{x})$ be the function field of V. Then F/M' is a regular extension of transcendence degree r and $\mathbf{t} = (t_1, \ldots, t_r) = \varphi(\mathbf{x})$ is a separating transcendence basis for F/M'. By [FJ2, second part of the proof of Lemma 9.16], $t_1, \ldots, t_r$ form a p-basis for $F/M'F^p$. In particular $F = M'F^p(\mathbf{t})$. Also, $N = F(\mathbf{t}^{1/p})$ is a purely inseparable

extension of F of degree p^r and $M'N^p = M'F^p(\mathbf{t}) = F$. This implies that N/M' is a separable extension [FJ2, Lemma 9.16].

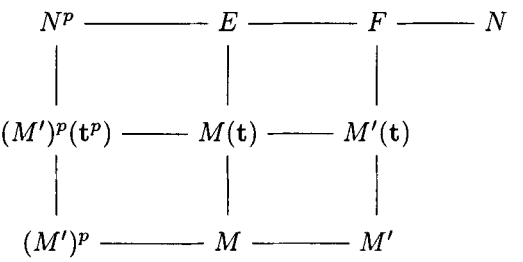
We claim that M' is algebraically closed in N. Indeed, if $a \in \tilde{M} \cap N$, then $a^p \in \tilde{M} \cap F = M'$. Since N/M' is separable, $a \in M'$. Combined with the former paragraph, we get that N/M' is a regular extension. Hence $N^p/(M')^p$ is also a regular extension.

Since $(M')^p \subseteq M$, the field $E = MN^p = MF^p(\mathbf{t})$ is a regular extension of M. As E is contained in F, it is finitely generated over M [FJ2, Lemma 9.30]. Thus there exist $y_1, \ldots, y_m$ such that $E = M(\mathbf{y})$. Note that $M'E = M'F^p(\mathbf{t}) = F$. Hence there exist $f_1, \ldots, f_m, g \in M'[Y_1, \ldots, Y_m]$ such that $g(\mathbf{y}) \neq 0$ and $x_i = f_i(\mathbf{y})/g(\mathbf{y})$, $i = 1, \ldots, n$. Let $y_{m+1} = g(\mathbf{y})^{-1}$ and let W be the variety generated over M by $(\mathbf{y}, y_{m+1})$. Its function field is E and therefore it is absolutely irreducible.

The map $\lambda\colon W \to V$ defined by

$$\lambda(\mathbf{y}, y_{m+1}) = (f_1(\mathbf{y})y_{m+1}, \ldots, f_n(\mathbf{y})y_{m+1}) = \mathbf{x}$$

is a birational morphism over M'.



Observe that E is linearly disjoint from $M'(\mathbf{t})$ over $M(\mathbf{t})$ and $E \cdot M'(\mathbf{t}) = F$. Hence F/E is a purely inseparable extension of degree $[M'(\mathbf{t}) : M(\mathbf{t})]$. Since $F/M'(\mathbf{t})$ is a separable algebraic extension, so is $E/M(\mathbf{t})$. Thus $t_1, \ldots, t_r$ form a separating transcendence basis for E/M.

Choose $h_1, \ldots, h_r \in M(Y_1, \ldots, Y_m)$ such that $t_i = h_i(\mathbf{y})$ and define a rational map $\psi\colon W \to \mathbb{A}^r$ over M by $\psi(\mathbf{y}, y_{m+1}) = (h_1(\mathbf{y}), \ldots, h_r(\mathbf{y})) = \mathbf{t}$. It is separable and dominating and $\varphi \circ \lambda = \psi$, as desired. ∎

COROLLARY 2.3: *Let M be a field with a subring O and let M' be a purely inseparable extension of M. Then M is PAC over O if and only if M' is PAC over O.*

Proof: Suppose first that M is PAC over O. Let $\varphi\colon V \to \mathbb{A}^r$ be a dominating separable rational map from an absolutely irreducible affine variety V over M'. Let $\psi\colon W \to \mathbb{A}^r$ and λ be as in Lemma 2.2. By assumption, there exists $\mathbf{b} \in W(M)$ such that $\psi(\mathbf{b}) \in O^r$ and φ is defined at $\mathbf{a} = \lambda(\mathbf{b})$. Thus $\mathbf{a}$ belongs to $V(M')$ and satisfies $\varphi(\mathbf{a}) = \psi(\mathbf{b}) \in O^r$. So M' is PAC over O.

Now suppose that M' is PAC over O. Consider an absolutely irreducible polynomial $f \in M[T, X]$ which is separable in X. Then there exist $a \in O$ and $b \in M'$ such that $f(a, b) = 0$ and $f(a, X)$ is separable. In particular b is separable over M. Hence, $b \in M$. Conclude from Lemma 1.3 that M is PAC over O. ∎

Remark 2.4: Note that the analog of Corollary 2.3 for PAC fields is not true. Indeed, Hrushovski [Hru, Cor. 5] constructs an example of a non-PAC field whose maximal purely inseparable extension is PAC. ∎

COROLLARY 2.5: *Let M be a PAC field over a subring O with a quotient field M_0. Let N_0 be an algebraic extension of M_0 and let S be the integral closure of O in N_0. Then $N = N_0M$ is PAC over S.*

Proof: By Corollary 2.3, it suffices to consider only the case where N is separable over M. Also, it suffices to consider the case where N/M is finite. In this case there exists a basis $w_1, \ldots, w_d$ for N_0/M_0 such that w_i is integral over O. Then $B = \{w_1, \ldots, w_d\}$ generates N over M. Choose a basis $B_0 \subseteq B$ for N over M. By Lemma 2.1, N is PAC over $O[B_0]$. Hence, N is PAC over S. ∎

Let $g(X)$ be a polynomial with coefficients in a field M. We say that $g(X)$ is **Galois over** M if $g(X)$ is separable and irreducible over M and the splitting field of g over M is generated by each of the roots of g.

PROPOSITION 2.6: *Let M be a perfect field which is PAC over a subfield K. Then, the maximal normal extension M_0 of K in M is PAC.*

Proof: Replace K by its maximal purely inseparable extension, if necessary, to assume that K is perfect. By Remark 1.2(b), K is infinite. By [FJ2, Thm. 10.4] it suffices to prove that every plane curve C which is defined over K has an M_0-rational point.

Let therefore $\mathbf{x} = (x_1, x_2)$ be a generic point of C over K and let $F = K(\mathbf{x})$. Then F is a regular extension of K. Since K is infinite and perfect, Theorem F of [GaJ] gives a separating transcendence element t for F/K such that the Galois closure $\hat{F}$ of $F/K(t)$ is regular over $K(t)$. Choose a primitive element y

for $\hat{F}/K(t)$ which is integral over $K[t]$ and let $h(t,Y) = \mathrm{irr}(y, K(t)) \in K[t,Y]$. Then $h(T,Y)$ is absolutely irreducible polynomial which is monic and separable in Y.

Let $y_1, \ldots, y_n$ be the distinct roots of $h(t,Y)$ in $K(t)_s$. One of them is y. Thus $y_1, \ldots, y_n \in \hat{F}$ and there exist polynomials $g_i, h_j \in K[T,Y]$ and $0 \neq g_0 \in K[T]$ such that $x_i = g_i(t,y)/g_0(t)$, $i = 1,2$, and $y_j = h_j(t,y)/g_0(t)$, $j = 1, \ldots, n$.

Since M is PAC over K, there exist $a \in K$ and $c \in M$ such that $h(a,c) = 0$, $\frac{\partial h}{\partial Y}(a,c) \neq 0$, and $g_0(a) \neq 0$. The specialization $(t,y) \to (a,c)$ extends to a place $\pi\colon \hat{F} \to M \cup \{\infty\}$ which maps each element of M onto itself. In particular $h(a,Y) = \prod_{j=1}^{n}(Y - c_j)$ with $c_j = \pi(y_j) = h_j(a,c)/g_0(a) \in K(c)$, $j = 1, \ldots, n$. Hence $K(c)$ is a Galois extension of K which is contained in M and therefore also in M_0. Also, $b_i = \pi(x_i) = g_i(a,c)/g_0(a) \in K(c)$. So, (b_1, b_2) is the point of $C(M_0)$ we were looking for. ∎

3. Examples of PAC field over subrings

Recall that an integral domain O with a quotient field K is **Hilbertian** if every Hilbert set of K contains points whose coordinates are in O. The remark on page 156 of [FJ2] states that the ring of integers of each global field is Hilbertian. In particular, so is $\mathbb{Z}$. If K_0 is an arbitrary field, n is a positive integer, and $t_1, \ldots, t_n$ are algebraically independent elements over K_0, then $K_0[t_1, \ldots, t_n]$ is a Hilbertian ring. Finally, the holomorphy ring of finitely many valuations of a Hilbertian field is Hilbertian.

If we only demand that every separable Hilbert set of K [FJ2, p. 147] contains points whose coordinates are in O, then we say that O is **separably Hilbertian.** If $\mathrm{char}(K) = p$, we let $K_{\mathrm{ins}} = \bigcup_{m=1}^{\infty} K^{1/p^m}$ be the maximal purely inseparable extension of K and let $O_{\mathrm{ins}} = \bigcup_{m=1}^{\infty} O^{1/p^m}$. If O is Hilbertian, then, since the map $x \mapsto x^{p^m}$ isomorphically maps K^{1/p^m} onto K and O^{1/p^m} onto O, it follows that O_{ins} is separably Hilbertian.

Recall that if $\sigma_1, \ldots, \sigma_e \in G(K)$, then $K_s(\boldsymbol{\sigma})$ is the fixed field in K_s of $\sigma_1, \ldots, \sigma_e$. We denote its maximal purely inseparable extension by $\tilde{K}(\boldsymbol{\sigma})$. The following result strengthen [FJ2, Thm. 16.18].

PROPOSITION 3.1: *Let O be a countable separably Hilbertian integral domain with a quotient field K. Let e be a positive integer. Then, for almost all $\boldsymbol{\sigma} \in G(K)^e$ the fields $K_s(\boldsymbol{\sigma})$ and $\tilde{K}(\boldsymbol{\sigma})$ are PAC over O.*

Proof: By Corollary 2.3 it suffices to prove the statement for the fields $K_s(\boldsymbol{\sigma})$.

For each finite separable extension L of K, for each absolutely irreducible polynomial $f \in L[T, X]$ with $\frac{\partial f}{\partial X} \neq 0$ and for each $0 \neq g \in L[T]$ let

$$S(L, f, g) = \{\boldsymbol{\sigma} \in G(L)^e | \text{ there exists } (a, b) \in O \times K_s(\boldsymbol{\sigma}) \text{ such that } f(a, b) = 0 \text{ and } g(a) \neq 0\}.$$

Denote the normalized Haar measure of $G(L)^e$ by μ_L. We will prove that $\mu_L(S(L, f, g)) = 1$. Since K is countable, Lemma 1.3 will then imply that $K_s(\boldsymbol{\sigma})$ is PAC over O for almost all $\boldsymbol{\sigma} \in G(K)^e$.

To prove the assertion we construct by induction a linearly disjoint sequence of separable extensions L_i of L of degree $d = \deg_X(f)$ for which there exists a point $(a, b) \in O \times L_i$ such that $f(a, b) = 0$ and $g(a) \neq 0$. Indeed, having constructed $L_1, \ldots, L_n$, we use [FJ2, Cor. 11.7] to find $a \in O$ such that $f(a, X)$ is an irreducible polynomial over $L_1 \cdots L_n$ and separable in X and $g(a) \neq 0$. Then we take $b \in K_s$ such that $f(a, b) = 0$ and define $L_{n+1} = L(b)$. Then $L_1, \ldots, L_{n+1}$ are linearly disjoint over L.

By [FJ2, Lemmas 16.7 and 16.11], almost all $L_s(\boldsymbol{\sigma})$ contain one of the fields L_i. Hence $\mu_L(S(L, f, m)) = 1$ as asserted. ∎

Valuations and orderings $v_1, \ldots, v_m, <_1, \ldots, <_n$ of a field K are said to be **independent** if the topologies of K induced by them are distinct.

PROPOSITION 3.2: *Let $v_1, \ldots, v_m, <_1, \ldots, <_n$ be independent valuations and orderings of a countable separably Hilbertian field K. Denote the topology that they induce on K by τ. Then, for almost all $\boldsymbol{\sigma} \in G(K)^e$, the field $K_s(\sigma)$ is PAC over each τ-open subset of K.*

Proof: Each set of the basis of τ has the form

$$A = \{x \in K | \ v_i(x - a_i) > v_i(b_i), \ i = 1, \ldots, m \text{ and } c_j <_j x <_j d_j, \ j = 1, \ldots, n\}$$

where a_i, b_i, c_j, d_j are elements of K. The intersection of A^r with each separable Hilbert subset of K^r is nonempty [Ja2, Lemma 19.5]. So, we may repeat the proof of Proposition 3.1, with a vector $(T_1, \ldots, T_r)$ of variables instead of T and with $\mathbf{a} \in A^r$ instead of $a \in O$ in the third paragraph of the proof. ∎

Example 3.3: Non algebraic PAC extension of a ring. For a field K to be PAC over a subring O is an elementary statement about the pair (K, O). Hence, this

property is preserved by ultraproducts. Let for example, $K = \tilde{\mathbb{Q}}(\sigma)$ be one of the fields as in Proposition 3.1 which is PAC over $\mathbb{Z}$ and $K \neq \tilde{\mathbb{Q}}$. Let (K^*, Z^*) be a nonprincipal ultrapower of (K, Z). Then, since $(K : \mathbb{Q}) = \infty$, the field K^* is not algebraic over $\mathbb{Q}^*$ (=the quotient field of $\mathbb{Z}^*$). Indeed, it has an infinite transcendence degree. On the other hand, K^* is not algebraically closed. So, this example does not fall under the scope of Example 1.4. ∎

Remark 3.4: The proof of Proposition 3.1 can be adjusted to yield a stronger property than "PAC over O":

Let O be a countable separably Hilbertian integral domain with quotient field K. Let e be a positive integer. Then, for almost all $\sigma \in G(K)^e$ the fields $K_s(\sigma)$ and $\tilde{K}(\sigma)$ have the following property: Let V be an absolutely irreducible variety of dimension $r \geq 0$. Let $\varphi: V \to \mathbb{A}^r$ be a dominating separable rational map over $K_s(\sigma)$ (resp., $\tilde{K}(\sigma)$). Let H be a separable Hilbert subset of $K_s(\sigma)^r$ (resp., $\tilde{K}(\sigma)^r$). Then there exists $\mathbf{a} \in V(K_s(\sigma))$ (resp., $\tilde{K}(\sigma)$) such that $\varphi(\mathbf{a}) \in H \cap O^r$.

Proposition 5.2 essentially derives a somewhat weaker form of this property from the Mordell conjecture for infinite finitely generated fields. ∎

4. Covers of curves

Each curve Γ can be covered by another curve Δ of arbitrarily large genus. We construct Δ such that it is not birationally equivalent to a curve which is already defined over a finite field. The latter condition is necessary in positive characteristic in order to apply the theorem of Manin-Grauert-Samuel.

Throughout this section we will be working over a field K that satisfies the following assumption:

Assumption 4.1: K is a perfect field of characteristic $p \geq 0$ which is not an algebraic extension of a finite field. ∎

LEMMA 4.2: *Consider elements $c_1, \ldots, c_r \in \tilde{K}$, which are pairwise nonconjugate over K. Let L be a finite Galois extension of K which contains $c_1, \ldots, c_r$. For each j let $d_j = [K(c_j) : K]$, and let $c_{j1}, \ldots, c_{j,d_j}$ be the conjugates of c_j over K. Let also $m \geq 4$ be an integer.*

Then, for each $1 \leq j \leq r$ and $1 \leq k \leq d_j$ there exist m distinct elements $x_{jk1}, \ldots, x_{jkm} \in L$ and there exists a monic polynomial $q \in K[X]$ of degree $e = 2 + m \sum_{j=1}^{r} d_j$ such that

(a) $q(x_{jkl}) = c_{jk}$, $l = 1, \ldots, m$,

(b) *the equation* $q(X) = c_{jk}$ *has no multiple roots; in particular* $q(X)$ *is a separable polynomial, and*

(c) *if* $p > 0$, *then* $x_{jk4} \notin \tilde{\mathbb{F}}_p(x_{jk1}, x_{jk2}, x_{jk3})$.

Proof: We break the proof into four parts.

PART A: *Construction of* x_{jkl}. By assumption, the elements c_{jk}, $j = 1, \dots, r$, $k = 1, \dots, d_j$ are distinct. Consider first the case where $p = 0$ and choose $b_{j1}, \dots, b_{jm} \in K$ such that

$$b_{jl} + c_{jk} \neq 0 \tag{1a}$$

$$b_{jl} + c_{jk} \neq b_{j'l'} + c_{j'k'} \text{ if } (j,k,l) \neq (j',k',l') \tag{1b}$$

for all j, k, l. Then let $x_{jkl} = b_{jl} + c_{jk}$ and observe that

$$x_{jkl} \neq 0 \tag{2a}$$

$$(j,k,l) \neq (j',k',l') \text{ implies } x_{jkl} \neq x_{j'k'l'}, \text{ and} \tag{2b}$$

$$\sigma c_{jk} = c_{jk'} \text{ implies } \sigma x_{jkl} = x_{jk'l} \tag{2c}$$

for all $1 \leq j \leq r$, $1 \leq k \leq d_j$, $1 \leq l \leq m$, and $\sigma \in \mathcal{G}(L/K)$.

Next suppose that $p > 0$ and let T be a transcendental basis of $K/\mathbb{F}_p$. By Assumption 4.1, T is nonempty and therefore $L_1 = \mathbb{F}_p(T, c_{jk} | \ j = 1, \dots, r \text{ and } k = 1, \dots, d_j)$ is an imperfect field which has a finite degree over $\mathbb{F}_p(T)$. In particular, $[L_1 : L_1^{p^n}] \geq p^n$ for each positive integer n. Hence, we may choose n such that $\mathbb{F}_p(T) \not\subseteq L_1^{p^n}$. Since $\mathbb{F}_p(T)$ is infinite, we may choose $b_{j1}, \dots, b_{jm} \in \mathbb{F}_p(T)$ such that

$$b_{jl} + c_{jk}^{p^n} \neq 0 \tag{3a}$$

$$b_{jl} + c_{jk}^{p^n} \neq b_{j'l'} + c_{j'k'}^{p^n} \text{ if } (j,k,l) \neq (j',k',l') \tag{3b}$$

$$b_{j1}, b_{j2}, b_{j3} \in \mathbb{F}_p(T^{p^n}) \text{ and } b_{j4} \in \mathbb{F}_p(T) \smallsetminus L_1^{p^n} \tag{3c}$$

Now let $x_{jkl} = b_{jl} + c_{jk}^{p^n}$ and observe that again (2) holds.

PART B: *Proof of (c).* If $p > 0$, let L_0 be the algebraic closure of $\mathbb{F}_p$ in L_1. It satisfies $L_0 = L_0^{p^n} \subseteq L_1^{p^n}$ and therefore L_1 is linearly disjoint from $\tilde{\mathbb{F}}_p L_1^{p^n}$ over $L_1^{p^n}$. Since by (3c), $b_{j4} \in L_1 \smallsetminus L_1^{p^n}$, this implies that $x_{jk4} \notin \tilde{\mathbb{F}}_p L_1^{p^n}$. On the other hand $x_{jk1}, x_{jk2}, x_{jk3} \in \tilde{\mathbb{F}}_p L_1^{p^n}$. Hence $x_{jk4} \notin \tilde{\mathbb{F}}_p(x_{jk1}, x_{jk2}, x_{jk3})$. So, (c) holds.

PART C: *Construction of* $q(X)$. Let $e = 2 + m\sum_{j=1}^{r} d_j$. Consider the matrix $A = (x_{jkl}^i)$ of order $(e-2)\times(e-2)$ in which to each triple (j,k,l) with $1 \le j \le r$, $1 \le k \le d_j$, and $1 \le l \le m$ there corresponds a row

$$(x_{jkl}^2\ x_{jkl}^3\ \cdots\ x_{jkl}^{e-1}).$$

If we factor out x_{jkl}^2 from the (j,k,l)th row we get a Van-der-Monde matrix. Conditions (2a) and (2b) imply that $\det(A) \neq 0$. Hence, for each $a \in K$ there are unique $a_2, \ldots, a_{e-1} \in L$ such that

$$a + x_{jkl} + \sum_{i=2}^{e-1} a_i x_{jkl}^i + x_{jkl}^e = c_{jk}, \tag{4}$$
$$j = 1, \ldots, r;\ k = 1, \ldots, d_j;\ l = 1, \ldots, m.$$

Consider $\sigma \in \mathcal{G}(L/K)$, $1 \le j \le r$, and $1 \le l \le m$. For each k between 1 and d_j there exists a unique k' between 1 and d_j such that $\sigma c_{jk} = c_{jk'}$, and therefore, by (2c), $\sigma x_{jkl} = x_{jk'l}$. Hence, σ permutes the system of linear equations (4):

$$a + x_{jk'l} + \sum_{i=2}^{e-1} (\sigma a_i) x_{jk'l}^i + x_{jk'l}^e = c_{jk'}, \tag{5}$$
$$j = 1, \ldots, r;\ k' = 1, \ldots, d_j;\ l = 1, \ldots, m.$$

Since the solution to (4) is unique, $\sigma a_i = a_i$. As $a_i \in L$, this implies that $a_i \in K$, $i = 2, \ldots, e-1$. Thus

$$q_a(X) = a + X + \sum_{i=2}^{e-1} a_i X^i + X^e$$

is a monic polynomial with coefficients in K which satisfies $q_a(x_{jkl}) = c_{jk}$ for all j, k, l.

In order to complete the proof, we have now only to choose a such that the polynomial $q(X) = q_a(X)$ will satisfy (b). To this end choose a transcendental element t over K. Then $q_0(X) - t$ is a monic, irreducible, and separable polynomial in X over $K(t)$. Hence, $q_0(X) - t$ has no multiple roots. So, its discriminant $R(t) = \text{Resultant}(q_0(X) - t,\ q_0'(X))$ is a nonzero polynomial in t. Choose $a \in K$ such that $R(c_{jk} - a) \neq 0$, $j = 1, \ldots, r$, $k = 1, \ldots, d_j$. The identity

$$\begin{aligned}\text{Resultant}(q_a(X) - c_{jk},\ (q_a(X) - c_{jk})') &= \text{Resultant}(q_0(X) - (c_{jk} - a),\ q_0') \\ &= R(c_{jk} - a)\end{aligned}$$

implies that $q_a(X) - c_{jk}$ has no multiple roots, $j = 1, \ldots, r$, $k = 1, \ldots, d_j$, as desired. ∎

LEMMA 4.3: *Let E_0, F_0, E, F be function fields of one variable over an algebraically closed field $\tilde{K}$. Suppose that* $\text{genus}(E_0) = 0$, *no prime divisor of E_0 ramifies both in E and in F_0, E is linearly disjoint from F_0 over E_0, and $F = EF_0$. Let $e = [F_0 : E_0]$ and $n = [E : E_0]$. Then*

$$\text{genus}(F) = e(n + \text{genus}(E) - 1) + n(\text{genus}(F_0) - 1) + 1 \tag{6}$$

Proof: As E and F_0 are linearly disjoint over E_0, we have $[F : E_0] = en$. Hence, by the Riemann genus formula $2 \cdot \text{genus}(F) - 2 = -2en + \deg(\mathfrak{d}')$, where $\mathfrak{d}' = \text{different}(F/E_0)$ [FJ2, p. 24]. Similarly $2 \cdot \text{genus}(E) - 2 = -2n + \deg(\mathfrak{d})$, where $\mathfrak{d} = \text{different}(E/E_0)$ and $2 \cdot \text{genus}(F_0) - 2 = -2e + \deg(\mathfrak{d}_0)$, where $\mathfrak{d}_0 = \text{different}(F_0/E_0)$.

By assumption, none of the prime divisors of $\mathfrak{d}$ ramifies in F. Hence, the contribution of $\mathfrak{d}$ to the degree of $\mathfrak{d}'$ is $e\deg(\mathfrak{d})$. Similarly, the contribution of $\mathfrak{d}_0$ to the degree of $\mathfrak{d}'$ is $n\deg(\mathfrak{d}_0)$. As each prime divisor of $\mathfrak{d}'$ divides either $\mathfrak{d}$ or $\mathfrak{d}_0$, we have $\deg(\mathfrak{d}') = e\deg(\mathfrak{d}) + n\deg(\mathfrak{d}_0)$. Substitute this value in the formula for $\text{genus}(F)$ of the preceding paragraph to get (6). ∎

LEMMA 4.4: *Let F_0 be a function field of one variable over an algebraically closed field $\tilde{K}_0$, and let F be a function field of one variable over an algebraically closed field $\tilde{K}$ that contains $\tilde{K}_0$ such that $\tilde{K}F_0 = F$. Let $x \in F$ be a separating transcendence element for $F/\tilde{K}$. Then there exists $\bar{x} \in F_0$ which is a separating transcendence element for $F/\tilde{K}$ such that $[F_0 : \tilde{K}_0(\bar{x})] = [F : \tilde{K}(\bar{x})] = [F : \tilde{K}(x)]$.*

Proof: Since $F/\tilde{K}(x)$ is a finite separable extension, there exists $y \in F$ which is integral over $\tilde{K}[x]$ such that $F = \tilde{K}(x, y)$. Let $f \in \tilde{K}[X, Y]$ be an irreducible polynomial, monic in Y such that $f(x, y) = 0$.

Write $F_0 = \tilde{K}_0(u, v)$ where u is a separating transcendence element for $F_0/\tilde{K}_0$ and v is a primitive element for $F_0/\tilde{K}_0(u)$. Let $h \in \tilde{K}_0[U, V]$ be an irreducible polynomial such that $h(u, v) = 0$. By assumption $F = \tilde{K}(u, v)$. Hence, there exist polynomials $0 \neq k_0 \in \tilde{K}[U]$, $k_1 \in \tilde{K}[U, V]$, $0 \neq g_0 \in \tilde{K}[X]$, $g_1, g_2 \in \tilde{K}[X, Y]$ such that $\deg_V k_1 < \deg_V h$ and

$$x = \frac{k_1(u, v)}{k_0(u)}, \quad u = \frac{g_1(x, y)}{g_0(x)}, \quad v = \frac{g_2(x, y)}{g_0(x)}. \tag{7}$$

Since $\tilde{K}_0$ is algebraically closed, there exists a place φ: $\tilde{K} \to \tilde{K}_0 \cup \{\infty\}$ which is the identity on $\tilde{K}_0$ such that the images of the coefficients of all the above

polynomials are finite, $\bar{f}(X,Y)$ is irreducible over $\tilde{K}_0$, $\bar{k}_1(u,V) \neq c\bar{k}_0(u)$ for all $c \in \tilde{K}_0$ (Bertini-Noether), and $\bar{k}_0\bar{g}_0 \neq 0$. Here we have put a bar over an element of $\tilde{K}$ or over a polynomial with coefficients in $\tilde{K}$ in order to denote the image under φ.

Since the transcendence degree of F_0 over $\tilde{K}_0$ is equal to the transcendence degree of F over $\tilde{K}$, the fields F_0 and $\tilde{K}$ are algebraically independent (=free) over $\tilde{K}_0$. Hence, as $F_0/\tilde{K}_0$ is regular, it is linearly disjoint from $\tilde{K}/\tilde{K}_0$ [FJ2, Lemma 9.9]. Since $F = \tilde{K}F_0$, φ extends to an F_0-place $\varphi\colon F \to F_0 \cup \{\infty\}$. Apply φ to (7)

$$\bar{x} = \frac{\bar{k}_1(u,v)}{\bar{k}_0(u)}, \quad u = \frac{\bar{g}_1(\bar{x},\bar{y})}{\bar{g}_0(\bar{x})}, \quad v = \frac{\bar{g}_2(\bar{x},\bar{y})}{\bar{g}_0(\bar{x})}. \tag{8}$$

Since $\bar{k}_1(u,V) \neq c\bar{k}_0(u)$ for all $c \in \tilde{K}_0$, $\deg_V \bar{k}_1 < \deg_V h$ and h is irreducible over $\tilde{K}_0$, relation (8) implies that $\bar{x} \notin \tilde{K}_0$. Hence $\bar{x}$ is transcendental over $\tilde{K}_0$ and therefore $\bar{g}_0(\bar{x}) \neq 0$. Hence, (8) implies that $F_0 = \tilde{K}_0(\bar{x},\bar{y})$.

Since $\bar{f}(\bar{x},Y)$ is irreducible and separable over $\tilde{K}_0(\bar{x})$, it follows that $F_0/\tilde{K}_0(\bar{x})$ is a separable extension of degree $\deg_Y f = [F : \tilde{K}(x)]$.

Finally, observe that F_0 is linearly disjoint from $\tilde{K}(\bar{x})$ over $\tilde{K}_0(\bar{x})$. Hence, $[F : \tilde{K}(\bar{x})] = [F_0 : \tilde{K}_0(\bar{x})] = [F : \tilde{K}(x)]$, as desired. ∎

Remark 4.5: Branch points and Möbius transformations. Let F/K be a regular extension of transcendence degree 1. Consider a separating transcendence element t for F/K. The **branch points** of $F/K(t)$ are the images of t in $\tilde{K} \cup \{\infty\}$ of those places of $K(t)$ which are trivial on K and ramify in F (note that the branch points depend on t). The set of all branch points of $F/K(t)$ is finite and invariant under the action of $G(K)$. If x is a primitive element for $F/K(t)$ which is integral over $K[t]$ and $f(t,X) = \mathrm{irr}(x,K(t))$, then for each finite branch point c of $F/K(t)$, the polynomials $f(c,X)$ and $\frac{\partial f}{\partial X}(c,X)$ have common roots [La3, p. 62]; that is $f(c,X)$ has multiple roots.

If t' is another element of F such that $K(t') = K(t)$, then there exists a Möbius transformation $\tau(X) = (aX+b)/(cX+d)$ with coefficients in K (which must satisfy $ad - bc \neq 0$) such that $\tau(t) = t'$. It maps the branch points of $F/K(t)$ (with respect to t) to the branch points of $F/K(t')$ (with respect to t'). Also, if $q(x) = t'$ for some nonconstant $q \in K[X]$, and $\tau^{-1}(X) = (a'X+b')/(c'X+d')$, then $u(X) = (a'q(X)+b')/(c'q(X)+d')$ belongs to $K(X)$ and satisfies $u(x) = t$.

We will use the following basic fact about Möbius transformations: Given two triples (x_1,x_2,x_3) and (x_1',x_2',x_3') of elements of K there exists a unique Möbius

transformation τ such that $\tau(x_i) = x_i'$, $i = 1, 2, 3$. If K_0 is a subfield of K, then τ is already defined over $K_0(\mathbf{x}, \mathbf{x}')$. ∎

LEMMA 4.6: *Let t be a transcendental element over K, let E_0 be a finite Galois extension of $K(t)$, and let $g_0 > 0$. Let $E = \tilde{K}E_0$, and set $d = [E : \tilde{K}(t)]$. Then there exist a rational function $q \in K(X)$, and an element $x \in K(t)_s$ which satisfies $q(x) = t$, E is linearly disjoint from $\tilde{K}(x)$ over $\tilde{K}(t)$, and such that the following holds:*

(a) *If D_0 is a regular extension of K such that $K(t) \subseteq D_0 \subseteq E_0$, then $K(x)D_0$ is a regular extension of K.*

(b) *Let F_1 be a proper extension of $\tilde{K}(x)$ which is contained in $F = E(x)$. Then $\text{genus}(F_1) > \max\{(d-1)(2d-1), g_0\}$.*

(c) *If $\text{char}(K) = p > 0$, then there exists no function field of one variable F_0 over $\tilde{\mathbb{F}}_p$ such that $\tilde{K}(x) \subset \tilde{K}F_0 \subseteq F$.*

Proof: Assume without loss that $d > 1$. We break the proof into four parts.

PART A: *Construction of q and x.* Replace t by a suitable Möbius transformation of t over K, if necessary, to assume that $(t)_\infty$ does not ramify in E. Choose representatives $c_1, \ldots, c_r \in \tilde{K}$ for the conjugacy classes over K of the branch points of $E/\tilde{K}(t)$. Let L be the Galois closure of $K(c_1, \ldots, c_r)/K$. For each j let $d_j = [K(c_j) : K]$. Since $d > 1$, $E/\tilde{K}(t)$ is a ramified extension [FJ2, Prop. 2.15]. Hence $r \geq 1$ and we may choose an integer $m \geq 4$ such that

$$e = 2 + m\sum_{j=1}^{r} d_j > \max\{(d-1)(2d-1), g_0\} + 1. \tag{9}$$

Finally, let $c_{jk}, x_{jkl} \in L$ and $q \in K[X]$ be as in Lemma 4.2.

Now choose $x \in K(t)_s$ such that $q(x) = t$. Then $q(X) - t = \text{irr}(x, \tilde{K}(t))$, $e = [\tilde{K}(x) : \tilde{K}(t)]$ and $(t)_\infty$ totally ramifies in $\tilde{K}(x)$. Indeed, $x^e + a_{e-1}x^{e-1} + \cdots + a_0 = t$ with $a_i \in K$. Let v be a valuation of $\tilde{K}(x)$ over K such that $v(t) < 0$. Then $v(x) < 0$ and therefore $ev(x) = v(t)$. So, the ramification index of $\tilde{K}(x)$ over $\tilde{K}(t)$ is e. By the choice of t, $(t)_\infty$ is unramified in E. Hence $\tilde{K}(x) \cap E = \tilde{K}(t)$. Since E is a Galois extension of $\tilde{K}(t)$, it is linearly disjoint from $\tilde{K}(x)$.

PART B: *Proof of (a).* Let D_0 be a regular extension of K such that $K(t) \subseteq D_0 \subseteq E_0$. Then $D = \tilde{K}D_0$ satisfies $[D : \tilde{K}(t)] = [D_0 : K(t)]$. By the preceding

paragraph, $[D(x) : \tilde{K}(x)] = [D : \tilde{K}(t)]$. As $[K(x)D_0 : K(x)] \leq [D_0 : K(t)]$, we conclude that $[D_0(x) : K(x)] = [D(x) : \tilde{K}(x)]$. Hence, $K(x)D_0$ is linearly disjoint from $\tilde{K}$ over K, which means that $K(x)D_0$ is a regular extension of K. This proves (a).

PART C: *Proof of (b).* For each finite branch point c of $\tilde{K}(x)/\tilde{K}(t)$ the equation $q(X) = c$ has multiple roots (Remark 4.5). Hence, by Lemma 4.2(b), none of the branch points c_j of $E/\tilde{K}(t)$ is a branch point of $\tilde{K}(x)/\tilde{K}(t)$. Let F_1 be as in (b). As $E/\tilde{K}(t)$ is a Galois extension and $\tilde{K}(x) \cap E = \tilde{K}(t)$, there exists a field E_1 between $\tilde{K}(t)$ and E such that $\tilde{K}(x)E_1 = F_1$. In particular $n = [E_1 : \tilde{K}(t)] = [F_1 : \tilde{K}(x)] > 1$. So, we may apply Lemma 4.3 to $\tilde{K}(t), \tilde{K}(x), E_1, F_1$ instead of to E_0, F_0, E, F, substitute $\text{genus}(F_0) = 0$, and compute from (6) and (9) that $\text{genus}(F_1) \geq (e-1)(n-1) > \max\{(d-1)(2d-1), g_0\}$. This proves (b).

PART D: *Proof of (c).* Finally assume that $p > 0$ and that there exists a function field F_0 of one variable over $\tilde{\mathbb{F}}_p$ such that $F_1 = \tilde{K}F_0$ satisfies $\tilde{K}(x) \subset F_1 \subseteq F$. By Lemma 4.4, there exists $\bar{x} \in F_0$ such that

$$n = [F_0 : \tilde{\mathbb{F}}_p(\bar{x})] = [F_1 : \tilde{K}(\bar{x})] = [F_1 : \tilde{K}(x)]. \tag{10}$$

Let $h \in \tilde{K}[X, Y]$ be an irreducible polynomial such that $h(x, \bar{x}) = 0$. Then $\deg_X h = [\tilde{K}(x, \bar{x}) : \tilde{K}(\bar{x})] \leq [F_1 : \tilde{K}(\bar{x})] = n$. Similarly, $\deg_Y h = [\tilde{K}(x, \bar{x}) : \tilde{K}(x)] \leq n$. Hence, $\deg(h) \leq 2n$. It follows that $\text{genus}(\tilde{K}(x, \bar{x})) \leq (2n-1)(n-1) \leq (2d-1)(d-1)$ [FJ2, Cor. 4.8]. (Actually, a theorem of Segre gives a better estimate, $\text{genus}(\tilde{K}(x, \bar{x})) \leq (n-1)^2$.) By (b), $\tilde{K}(x, \bar{x}) = \tilde{K}(x)$. Conclude from (10) that $\tilde{K}(x) = \tilde{K}(\bar{x})$.

It follows that there exists a Möbius transformation τ over $\tilde{K}$ such that $\tau(\bar{x}) = x$. It transforms branch points of $F_0/\tilde{\mathbb{F}}_p(\bar{x})$ into branch points of $F_1/\tilde{K}(x)$. The latter belong to $\tilde{K} \cup \{\infty\}$.

On the other hand, the elements c_{jk} are all branch points of $E/\tilde{K}(t)$. Let E_1 be a field as in Part C. Since $E_1/\tilde{K}(t)$ is a ramified extension [FJ2, Prop. 2.15] there exist j and k such that c_{jk} is a branch point of $E_1/\tilde{K}(t)$.

Since $q(X) - t$ is irreducible over $\tilde{K}(t)$, and since $q(x_{jkl}) = c_{jk}$, the specialization $t \to c_{jk}$ extends to a place of $\tilde{K}(x)$ over $\tilde{K}$ that maps x into x_{jkl}, $l = 1, \ldots, m$. By Lemma 4.2(b), c_{jk} is not a branch point of $\tilde{K}(x)/\tilde{K}(t)$. Hence, x_{jkl} is a branch point of $F_1/\tilde{K}(x)$, $l = 1, \ldots, m$.

Since $F_1 = F_0\tilde{K}(\bar{x})$, each prime of $\tilde{K}(x) = \tilde{K}(\bar{x})$ that ramifies in F_1 must be an extension of a prime of $\tilde{\mathbb{F}}_p(\bar{x})$ that ramifies in F_0. Hence, the branch

points of $F_1/\tilde{K}(x)$ are the images under τ of the branch points of $F_0/\tilde{\mathbb{F}}_p(\bar{x})$. In particular there exist $\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4 \in \tilde{\mathbb{F}}_p \cup \{\infty\}$ such that $\tau(\bar{x}_l) = x_{jkl}$ for $l = 1, 2, 3, 4$. Hence, τ is already defined over $\tilde{\mathbb{F}}_p(x_{jk1}, x_{jk2}, x_{jk3})$. Consequently, $x_{jk4} = \tau(\bar{x}_4) \in \tilde{\mathbb{F}}_p(x_{jk1}, x_{jk2}, x_{jk3})$. This contradiction to Lemma 4.2(c) proves that F_0 as above does not exist. This proves (c) and concludes the proof of the lemma. ∎

PROPOSITION 4.7: *Let $\mathcal{F}$ be a finite set of absolutely irreducible polynomials $f \in K[T, Y]$ such that f is separable in Y and $\deg_T f \geq 1$. Let $g_0 > 0$. Then there exists a nonconstant rational function $q \in K(X)$ such that each $f \in \mathcal{F}$ satisfies:*

(a) *the plane curve Δ which is defined over K by $f(q(X), Y) = 0$ is absolutely irreducible, and*

if $\deg_Y f \geq 2$, then

(b) *the genus of Δ is at least g_0, and*

(c) *Δ is birationally equivalent over $\tilde{K}$ to no curve which is defined over a finite field.*

Proof: Let t be a transcendental element over K. Take a finite Galois extension E_0 of $K(t)$ which contains the roots of all $f(t, Y) = 0$ with $f \in \mathcal{F}$. Let q and x be as in Lemma 4.6.

To prove the Proposition consider $f \in \mathcal{F}$ and let $y \in E_0$ solve the equation $f(t, y) = 0$. As f is absolutely irreducible, $D_0 = K(t, y)$ is a regular extension of K, and $[D_0 : K(t)] = \deg_Y f$. Let Δ be the plane curve defined over K by $f(q(X), Y) = 0$. Then $K(x)D_0$ is the function field of Δ over K. Since, by Lemma 4.6(a), $K(x)D_0$ is a regular extension of K, the curve Δ is absolutely irreducible. Also, $D = \tilde{K}(x)D_0$ is the function field of Δ over $\tilde{K}$.

Assume now that $\deg_Y f \geq 2$. Since $\tilde{K}E_0$ is linearly disjoint from $\tilde{K}(x)$ over $\tilde{K}(t)$ (Lemma 4.6), $\tilde{K}(x) \subset D \subseteq \tilde{K}(x)E_0$. Hence, by Lemma 4.6(b), the genus of Δ is at least g_0. Also, by Lemma 4.6(c), Δ is birationally equivalent over $\tilde{K}$ to no curve which is defined over a finite field. This concludes the proof of the lemma. ∎

5. Hilbert sets over finitely generated fields

We say that a field K is **finitely generated** if it is finitely generated over its prime field. If K is in addition infinite, then K is Hilbertian [FJ2, Cor. 12.8 and

Thm. 12.10].

Our aim in this section is to generalize [Ser, p. 36, Exer. 2] from $\mathbb{Q}$ to an arbitrary finitely generated field K and to prove that each separable Hilbert set of K contains the image of a rational function. The main tools in the proof are the theorems of Manin-Grauert-Samuel and of Faltings, that is, Mordell's Conjecture over functions fields and over number fields.

Definition 5.1: Absolute genus. If an absolutely irreducible curve Γ is defined over a perfect field K, then its genus is preserved under extensions of the field of constants. If K is imperfect, then its genus may drop. The **absolute genus** of Γ is its genus over $\tilde{K}$. ∎

The following generalization of Mordell's Conjecture is well known.

PROPOSITION 5.2 (Mordell's Conjecture): *Let K be a finitely generated field. Suppose that Γ is an absolutely irreducible curve defined over K such that*

(a) *the absolute genus g of Γ is at least 2, and*

(b) *Γ is birationally equivalent over $\tilde{K}$ to no curve which is defined over a finite field.*

Then $\Gamma(K)$ is a finite set.

Proof: Let K_0 be the algebraic closure in K of the prime field of K. Then K_0 is a finite field, if $\mathrm{char}(K) > 0$, and a number field if $\mathrm{char}(K) = 0$. Also, K is a regular extension of K_0 of finite transcendence degree. Let $L = \tilde{K}_0 K$. Then L is a function field over $\tilde{K}_0$ of several variables.

Assume that $\Gamma(K)$ is an infinite set. Then, so is $\Gamma(L)$. By a theorem of Manin-Grauert-Samuel [Sam, p. 107] there exists a curve Δ which is defined over $\tilde{K}_0$ and there exists a birational equivalence $\varphi\colon \Gamma \to \Delta$ which is defined over L. Take a finite extension K_1 of K_0 such that Δ is defined over K_1 and φ is defined over $K_1' = K_1 K$.

If $\mathrm{char}(K) > 0$, then K_1 is a finite field, which is a contradiction to (b). Hence, $\mathrm{char}(K) = 0$ and K_1 is a number field. It follows that $\mathrm{genus}(\Delta) = \mathrm{genus}(\Gamma) \geq 2$. Also, as $\Gamma(K_1')$ is infinite, so is $\Delta(K_1')$. On the other hand, $\Delta(L) \setminus \Delta(\tilde{K}_0)$ is a finite set [Sam, p. 105]. As $\Delta(K_1') \cap \Delta(\tilde{K}_0) = \Delta(K_1)$, this implies that $\Delta(K_1)$ is an infinite set. But this contradicts the famous theorem of Faltings [Fal]. ∎

Consider an arbitrary field K. Let $h_i \in K(T)[X]$ be irreducible with $\deg_X(h_i) > 1$, $i = 1, \ldots, m$, and let $0 \neq g \in K[T]$. We work with two types of Hilbert

sets:

$$H_K(h_1,\dots,h_m;g) = \{a \in K |\ g(a) \neq 0 \text{ and } h_i(a,X) \text{ is irreducible, } i = 1,\dots,n\}$$
$$H'_K(h_1,\dots,h_m;g) = \{a \in K |\ g(a) \neq 0 \text{ and } \textstyle\prod_{i=1}^m h_i(a,b) \neq 0 \text{ for each } b \in K\}$$

If $g = 1$ we omit g.

The following result strengthens [FJ2, Lemma 12.1].

LEMMA 5.3: *Let $f \in K(T)[X]$ be an irreducible polynomial, separable in X, with $\deg_X(f) > 1$. Then there exists a finite Galois extension L of K and there exist absolutely irreducible polynomials $h_1,\dots,h_m \in K[T,X]$, separable in X, with $\deg_X(h_i) > 1$, $i = 1,\dots,m$, and a polynomial $0 \neq r \in K[T]$ such that for every algebraic extension K' of K which is linearly disjoint from L over K we have:*

f is irreducible over K' and $H'_{K'}(h_1,\dots,h_m;r) \subseteq H_{K'}(f)$.

Proof: Write $f(T,X) = r_1(T)^{-1} f_1(T,X)$ with $0 \neq r_1 \in K[T]$ and $f_1 \in K[T,X]$. If $H'_{K'}(h_1,\dots,h_m;r) \subseteq H_{K'}(f_1)$, then $H'_{K'}(h_1,\dots,h_m;rr_1) \subseteq H_{K'}(f)$. So, we may assume that $f \in K[T,X]$. Let $r_0(T)$ be the leading coefficient of f, viewed as a polynomial in X. Replace X by $r_0(T)X$, if necessary, to assume that f is monic in X. We break the rest of the proof into three parts.

PART A: *Construction of L.* Let $f(T,X) = \prod_{i=1}^n (X - x_i)$ be the factorization of $f(T,X)$ in $K(T)_s[X]$. Since f is irreducible, if I is a nonempty proper subset of $\{1,\dots,n\}$, then $f_I(X) = \prod_{i\in I}(X - x_i) \notin K[T,X]$. So $f_I(X)$ has a coefficient $y_I \notin K(T)$, and $g_I = \operatorname{irr}(y_I, K(T)) \in K[T,X]$ is monic and separable in X with $\deg_X(g_I) > 1$.

Let F be a finite Galois extension of $K(T)$ that contains $x_1,\dots,x_n$ and therefore each y_I. Then the algebraic closure L of K in F is a finite Galois extension of K. Let K' be an algebraic extension of K which is linearly disjoint from L. If f factors over K', then the coefficients of the factors belong to $F \cap K'$ and therefore to $L \cap K' = K$. So, the factorization is trivial and therefore $f(T,X)$ is also irreducible over K'.

PART B: *Construction of r and $h_1,\dots,h_m$.* Let I be a nonempty proper subset of $\{1,\dots,n\}$ such that g_I is not absolutely irreducible. Since $y_I \in F$, all roots of $g_I(T,X)$ belong to F. Hence, $g_I = g_{I,1}\cdots g_{I,k}$, where each $g_{I,j} \in L[T,X]$ is absolutely irreducible and $k \geq 2$. Since g_I is monic and separable in X the factors $g_{I,j}$ are relatively prime. By the dimension theorem, $W_I = V(g_{I,1},\dots,g_{I,k})$ is

a finite set [FJ2, Lemma 9.19]. Also, each two of the $g_{I,j}$'s are conjugate by an element of $\mathcal{G}(L/K)$. Hence, if K' is an extension of K as above, each two of the $g_{I,j}$ are conjugate by an element of $\mathcal{G}(LK'/K')$. If $a, b \in K'$ and $g_I(a,b) = 0$, then there exists j, $1 \leq j \leq k$, such that $g_{I,j}(a,b) = 0$. It follows that $g_{I,j}(a,b) = 0$ for $j = 1, \ldots, k$. Hence $(a,b) \in W_I$. Denote the projection of W_I on the first coordinate by A_I.

Let A be the union of all sets A_I and their conjugates over K. It is a finite set. Then $r(T) = \prod_{a \in A}(T-a)^l$, where l is an appropriate power of the characteristic of K, is a polynomial with coefficients in K. List those g_I's which are absolutely irreducible as $h_1, \ldots, h_m$.

PART C: *Conclusion of the proof.* Consider an extension K' of K which is linearly disjoint from L over K. Our construction shows that

(1)

$$H'_{K'}(h_1, \ldots, h_m; r) \subseteq H'_{K'}(g_I |\ I \text{ is a proper nonempty subset of } \{1, \ldots, n\}; r).$$

We prove that the right hand side of (1) is contained in $H_{K'}(f)$.

Assume for $a \in K'$ that $f(a,X) = p(X)q(X)$ factors nontrivially in $K'[X]$. Extend the K'-specialization $T \to a$ to a K'-specialization $(T, x_1, \ldots, x_n) \to (a, c_1, \ldots, c_n)$ [FJ2, Propositions 2.3 and 2.5] so that $f(a,X) = \prod_{i=1}^n (X - c_i)$. For some nonempty proper subset I of $\{1, \ldots, n\}$, $p(X) = \prod_{i \in I}(X - c_i)$, the polynomial $f_I(X)$ maps to $p(X)$, and y_I maps onto a coefficient b of $p(X)$. Then b lies in K' and satisfies $g_I(a,b) = 0$. Thus a does not belong to the right hand side of (1). ∎

PROPOSITION 5.4: *Let K be an infinite finitely generated field. Let $f \in K[T,Y]$ be an absolutely irreducible polynomial which is separable in Y. Let $g \in K[T,Y]$ be an irreducible polynomial which is separable in Y and let $0 \neq r \in K[T]$. Then, there exist a finite purely inseparable extension K' of K, a nonconstant rational function $q \in K'(X)$, and a finite subset S of K' such that $f(q(X), Y)$ is absolutely irreducible and $q(a) \in H_{K'}(g; r)$ for each $a \in K' \setminus S$.*

Proof: Lemma 5.3 gives a finite Galois extension L of K and polynomials $h_1, \ldots, h_m \in K[T,Y]$, which are absolutely irreducible, monic and separable in Y, with $\deg_Y(h_i) > 1$, $i = 1, \ldots, m$, and a polynomial $0 \neq r_1 \in K[T]$ such that for every algebraic extension K' of K which is linearly disjoint from L over K we have:

g is irreducible over K' and $H'_{K'}(h_1,\dots,h_m;r_1) \subseteq H_{K'}(g;r)$.

Apply Proposition 4.7 to the maximal purely inseparable extension $K_{\rm ins}$ of K instead of to K to find a nonconstant rational function $q \in K_{\rm ins}(X)$ such that $f(q(X),Y)$ and $h_i(q(X),Y)$ are absolutely irreducible, and the curve Γ_i defined over $K_{\rm ins}$ by $h_i(q(X),Y)=0$ has genus at least 2, $i=1,\dots,m$, and is birationally equivalent over $\tilde{K}$ to no curve which is defined over a finite field. Let K' be a finite extension of K which is contained in $K_{\rm ins}$, contains the coefficients of q, the curve Γ_i is defined over K', and its genus over K' equals its genus over $K_{\rm ins}$, and therefore to its absolute genus. In particular, K' is linearly disjoint from L over K. By Proposition 5.2, applied to K' instead of to K, K' has a finite subset S such that for each $a \in K' \setminus S$ the function q is defined at a, $r_1(q(a)) \neq 0$, and none of the polynomials $h_i(q(a),Y)$ has a root in K'. Thus $q(a)$ belongs to $H'_{K'}(h_1,\dots,h_m;r_1)$ and therefore to $H_{K'}(g;r)$. ∎

PROBLEM 5.5: *Is it possible in Proposition 5.4 to choose q in $K(X)$ rather than in $K'(X)$?*

The following lemma is a variant of [FJ2, Lemma 12.12].

LEMMA 5.6: *Let $f(T_1,\dots,T_r,X)$ be an absolutely irreducible polynomial over a field K which is Galois in X. Then, there is an absolutely irreducible polynomial $h \in K[\mathbf{T},X]$ which is separable in X and a nonzero polynomial $g \in K[\mathbf{T}]$ such that for each algebraic extension K' of K*

$$H_{K'}(h;g) \subseteq \{\mathbf{a} \in (K')^r \mid f(\mathbf{a},X) \text{ is Galois over } K' \text{ and } \mathcal{G}(f(\mathbf{a},X),K') \text{ is isomorphic to } \mathcal{G}(f(\mathbf{T},X),K(\mathbf{T})) \text{ as permutation groups of the respective roots}\}$$

Proof: Let $E = K(\mathbf{T})$ and denote the distinct roots of $f(\mathbf{T},X)$ in E_s by $x_1,\dots,x_n$. Then $\prod_{i\neq j}(x_i-x_j) = g_1(\mathbf{T})^{-1}g_2(\mathbf{T})$, where $g_1,g_2 \in K[\mathbf{T}]$ are nonzero polynomials; g_1 is a power of the leading coefficient of f to a positive degree. Let $F = E(\mathbf{x})$ be the splitting field of f over E and choose a primitive element z for F/E which is integral over $K[\mathbf{T}]$. Then $h(\mathbf{T},X) = \mathrm{irr}(z,E) \in K[\mathbf{T},X]$ is absolutely irreducible and Galois in X, and the discriminant $g_3(\mathbf{T})$ of z over E belongs to $K[\mathbf{T}]$. Finally put $g = g_1g_2g_3$.

Let K' be an algebraic extension of K, $E' = K'(\mathbf{T})$, and $F' = E'(\mathbf{x})$. Then the isomorphism $\mathcal{G}(F'/E') \cong \mathcal{G}(F/E)$ is also an isomorphism $\mathcal{G}(f(\mathbf{T},X),E') \cong \mathcal{G}(f(\mathbf{T},X),E)$ as permutation groups.

Let $R = K'[\mathbf{T}, g(\mathbf{T})^{-1}]$ and $S = R[z]$. Then S/R is a ring cover for F'/E' ([FJ2, Lemma 5.3]; note that $K[\mathbf{T}]$ is integrally closed).

If $\mathbf{a} \in H_{K'}(h; g)$, then the specialization $\mathbf{T} \to \mathbf{a}$ extends to a K'-homomorphism φ of S onto a Galois extension $L = K'(\varphi(z))$ of K' such that $[L : K'] = [F' : E']$. By [FJ2, Lemma 5.5], φ induces an isomorphism $\sigma \mapsto \bar{\sigma}$ of its decomposition group $D(\varphi)$ onto $\mathcal{G}(L/K')$. It follows that $D(\varphi) = \mathcal{G}(F'/E')$. Moreover, for each $x \in S$ and $\sigma \in \mathcal{G}(F'/E')$ we have $\bar{\sigma}(\varphi(x)) = \varphi(\sigma(x))$. In particular, since all roots of $f(\mathbf{T}, X)$ belong to S and since $f(\mathbf{a}, X)$ has n distinct roots, φ maps the roots of $f(\mathbf{T}, X)$ bijectively on the roots of $f(\mathbf{a}, X)$ and the isomorphism $\mathcal{G}(F'/E') \cong \mathcal{G}(L/K')$ is also an isomorphism $\mathcal{G}(f(\mathbf{T}, X), E') \cong \mathcal{G}(f(\mathbf{a}, X), K')$ of permutation groups. ∎

6. Examples of Non-PAC fields over subrings — symmetric extensions

We show in this section and in the next one that the major examples of algebraic extensions of $\mathbb{Q}$ which are PAC (except for almost all fields $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$) are not PAC over $\mathbb{Q}$. The same holds for $\mathbb{F}_p(t)$. Actually, we work over each finitely generated field.

Definition 6.1: Let t be a transcendental element over a field K. We say that a finite group G is **regular** over a field K if $K(t)$ has a Galois extension E with $\mathcal{G}(E/K(t)) \cong G$ such that E/K is a regular extension.

Alternatively, there exists an absolutely irreducible polynomial $f \in K[T, X]$ such that $f(t, X)$ is Galois over $K(t)$ and $\mathcal{G}(f(t, X), K(t)) \cong G$. It follows that if t is transcendental over an extension L of K, then $\mathcal{G}(f(t, X), L(t)) \cong G$. ∎

PROPOSITION 6.2: *Let K be a finitely generated field, let M be a PAC field over K, and let G be a finite group which is regular over K. Then M/K has a Galois subextension L/K with $\mathcal{G}(L/K) \cong G$.*

Proof: Since M is PAC over K, the field K is infinite (Remark 1.2(b)). By assumption, there exists an absolutely irreducible polynomial $f \in K[T, Y]$ such that $f(T, Y)$ is Galois over $K(T)$ and $\mathcal{G}(f(T, Y), K(T)) \cong G$. By Lemma 5.6, there is an absolutely irreducible polynomial $h \in K[T, Y]$ which is separable in Y and a nonzero polynomial $r \in K[T]$ such that for each algebraic extension K' of K and for each $c \in H_{K'}(h; r)$ the polynomial $f(c, Y)$ is Galois over K' and $\mathcal{G}(f(c, Y), K') \cong G$.

By Proposition 5.4, there exist a finite purely inseparable extension K' of K, a nonconstant rational function $q \in K'(X)$ and a finite subset S of K' such that $f(q(X), Y)$ is absolutely irreducible and $K' \smallsetminus S \subseteq \{a \in K' |\ q(a) \in H_{K'}(h; r)\}$.

By Corollary 1.5, $M_0 = K_s \cap M$ is PAC over K. Hence, by Corollary 2.3, $M_0' = K'M_0$ is PAC over K. Hence, there exists $a \in K \smallsetminus S$ and there exits $b \in M_0'$ such that $f(q(a), b) = 0$. Then $K'(b)/K'$ is Galois and $\mathcal{G}(K'(b)/K') \cong G$. Since $\mathcal{G}(M_0/K) \cong \mathcal{G}(M_0'/K')$, there is a Galois extension L of K which is contained in M_0, and therefore also in M, such that $\mathcal{G}(L/K) \cong G$. ∎

Remark 6.3: Regular groups over fields. Let K be a field. Then every abelian group [FJ2, Lemma 24.46] and each of the groups S_n are regular over K.

Many more finite groups are known to be regular over $\mathbb{Q}$ and hence over every field of characteristic 0. Among them are A_n (Hilbert), all sporadic simple groups (with the possible exception of M_{23}) [Mat, Satz 8.2], and $\mathrm{PGL}_n(\mathbb{F}_q)$, $\mathrm{PU}_n(\mathbb{F}_{q^2})$ for q an odd prime power, $n \geq 4$ an even integer and $n \geq q$ [Voe].

Less groups are known to be regular over $\mathbb{F}_p$. If $\mathrm{char}(K) = p$ and l is a prime number that does not divide $p - 1$ or $l = p$, then each group G of order l^m is regular over $\mathbb{F}_p$ [RCVS, Thm. 6] and hence over every field of characteristic p. Probably, Shafarevich's proof goes through also for $l | p - 1$, but this has yet to be checked. Incidentally, note that it is not known if each group of order l^m is regular over $\mathbb{Q}$.

In particular, if a finite group G is regular over an infinite finitely generated field K, then Propositions 3.1 and 6.2 imply that for almost all $\boldsymbol{\sigma} \in G(K)^e$ there exists a Galois extension L/K such that $L \subseteq K_s(\boldsymbol{\sigma})$ and $\mathcal{G}(L/K) \cong G$. This result however can be proved directly, without appealing to Faltings' theorem or to the Theorem of Manin-Grauert-Samuel. Indeed, there exists a linearly disjoint sequence $L_1, L_2, L_3, \ldots$ of Galois extensions of K with $\mathcal{G}(L_i/K) \cong G$, $i = 1, 2, 3, \ldots$ [FJ2, Lemma 15.8]. Then, for almost all $\boldsymbol{\sigma} \in G(K)^e$ there exists i such that $L_i \subseteq K_s(\boldsymbol{\sigma})$, as follows from [FJ2, Lemma 16.11]. ∎

We call a finite extension L/K **symmetric** if it is Galois and $\mathcal{G}(L/K) \cong S_n$ for some positive integer n. We denote the compositum of all symmetric extensions of K by K_{symm}.

LEMMA 6.4: *Let K be a finitely generated field and let N be a Galois extension of K which is contained in K_{symm}. Then N is PAC over no finite extension K' of K.*

Proof: Let $\hat{K}$ be the Galois closure of K'/K. Then $\hat{K} \subseteq N$ and each composition factor of $\mathcal{G}(N/\hat{K})$ is either A_n, for some positive integer n, or $\mathbb{Z}/2\mathbb{Z}$.

Assume that N is PAC over K'. Then N is also PAC over $\hat{K}$. By Proposition 6.2 and Remark 6.3, $\hat{K}$ has cyclic extension L of degree 5 which is contained in N. This contradiction to the first paragraph implies that N is not PAC over K'. ∎

Example 6.5: An algebraic extension of a finitely generated field K which is PAC but not PAC over K. If K is a finite field, then each infinite algebraic extension N of K is PAC [FJ2, Cor. 10.5] but N is not PAC over K (Remark 1.2). So suppose K is infinite. Then K is Hilbertian.

If $\mathrm{char}(K) = 0$, Theorem 16.46 of [FJ2] gives an example of a Galois extension N of K which is PAC and $\mathcal{G}(N/K)$ is isomorphic to the direct product of symmetric groups. By Lemma 6.4, N is PAC over no finite extension of K. The same is true for K_{symm}.

If $\mathrm{char}(K) > 0$, then K_{ins} is separably Hilbetian [FJ2, p. 149, Exer. 2]. The proof of [FJ2, Thm. 16.46] goes through for K_{ins} using [GJ2, Thm. 10.5]. As a result, K_{ins} has a Galois extension N which is PAC and $\mathcal{G}(N/K_{\mathrm{ins}})$ is isomorphic to the direct product of symmetric groups. As in the preceding paragraph, N is PAC over no finite extension of K. ∎

Example 6.6: The maximal solvable extension $\mathbb{Q}_{\mathrm{sol}}$ of $\mathbb{Q}$. It is not known if $\mathbb{Q}_{\mathrm{sol}}$ is PAC. But since for $n \geq 5$, S_n is not a quotient of $\mathcal{G}(\mathbb{Q}_{\mathrm{sol}}/\mathbb{Q})$, Proposition 6.2 implies that certainly $\mathbb{Q}_{\mathrm{sol}}$ is PAC over no number field. ∎

We don't know of any field N which is PAC and Galois over a finitely generated field, except when N is separably closed. But if such a field exists, the Galois group $\mathcal{G}(N/K)$ must be rich.

PROPOSITION 6.7: *Suppose that a field N is Galois and PAC over a finitely generated field K. Then for each finite group G there exists a finite Galois extension K' of K and a Galois extension L of K' which is contained in N such that $\mathcal{G}(L/K') \cong G$.*

Proof: A theorem of Fried, Völklein, Harbater, and Pop asserts that each finite group G is regular over N [Ja3, Prop. 2.6]. It follows that G is already regular over a finite Galois extension K' of K which is contained in N. By Proposition 6.2, K' has a Galois extension L which is contained in N such that $\mathcal{G}(L/K') \cong G$. ∎

7. Examples of non-PAC fields over rings — finite extensions of $\mathbb{Q}_{\mathrm{tr}}$

Denote the maximal totally real extension of $\mathbb{Q}$ by $\mathbb{Q}_{\mathrm{tr}}$. It is the fixed field in $\tilde{\mathbb{Q}}$ of all involutions of $G(\mathbb{Q})$. It is a Galois extension of $\mathbb{Q}$. Florian Pop [Pop, Main Theorem] proves that $\mathbb{Q}_{\mathrm{tr}}$ is a PRC field. Hence, each algebraic extension M of $\mathbb{Q}_{\mathrm{tr}}$ is PRC [Pre, Thm. 3.1]. If, in addition, M is not formally real, then M is PAC. For example, $\mathbb{Q}_{\mathrm{tr}}(\sqrt{-1})$ is a PAC field. We prove in this section that no finite extension of $\mathbb{Q}_{\mathrm{tr}}$ is PAC over $\mathbb{Q}$.

LEMMA 7.1: *Let K be a field of characteristic $\neq 2$, let $b \in K$, and let k be a positive integer. Set $L = K(\sqrt[2^k]{b})$ and $E = K(\zeta_{2^k})$ (ζ_{2^k} is a primitive root of 1 of order 2^k). Suppose that $[L : K] = 2^k$ and that $L \cap E = K$. Then, for each i between 1 and k, $L_i = K(\sqrt[2^i]{b})$ is the unique subfield of L of degree 2^i over K.*

Proof: The assumption $[L : K] = 2^k$ and the inequalities $[L_i : K] \leq 2^i$ and $[L : L_i] \leq 2^{k-i}$ imply that $[L_i : K] = 2^i$.

On the other hand, suppose that $K \subseteq K_1, K_2 \subseteq L$ and $[K_1 : K] = [K_2 : K]$. By assumption, L is linearly disjoint from E over K. Hence $[K_1E : E] = [K_2E : E]$. As LE/E is a cyclic extension, $K_1E = K_2E$. Thus, $K_1K_2E = K_iE$, $i = 1, 2$ and therefore $[K_1K_2 : K] = [K_1K_2E : E] = [K_iE : E] = [K_i : K]$. Conclude that $K_1 = K_2$. ∎

THEOREM 7.2: *Let K be a totally real number field. Then no finite extension of $\mathbb{Q}_{\mathrm{tr}}$ is PAC over K.*

Proof: Let M be a finite extension of $\mathbb{Q}_{\mathrm{tr}}$. Assume that M is PAC over K. In order to draw a contradiction we choose a positive integer k such that $2^k > [M : \mathbb{Q}_{\mathrm{tr}}]$. Consider the absolutely irreducible polynomial $f(T_1, T_2, T_3, Y) = Y^{2^k} + T_1^2 + T_2^2 + T_3^2$ (Apply [FJ2, Lemma 16.22] on $Y^{2^k} + Z$). As in the proof of Lemma 1.3, find nonzero $c_i, c_i' \in K$, $i = 1, 2, 3$ such that $g(T, Y) = Y^{2^k} + (c_1 + c_1'T)^2 + (c_2 + c_2'T)^2 + (c_3 + c_3'T)^2$ is absolutely irreducible. By [FJ2, Lemma 11.6], K has a Hilbert set $H = H_K(p)$ with $p \in K[T, Y]$ an irreducible polynomial such that $g(b, X)$ is irreducible over $K(\zeta_{2^k})$ for each $b \in H$. By Proposition 5.4, there exist $q \in K(X)$ and a finite subset S of K such that $g(q(X), Y)$ is absolutely irreducible and $g(q(a), Y)$ is irreducible over $K(\zeta_{2^k})$ for each $a \in K \smallsetminus S$.

By assumption there exist $a \in K \smallsetminus S$ and $b \in M$ such that $g(q(a), b) = 0$. Let $c = (c_1 + c_1'q(a))^2 + (c_2 + c_2'q(a))^2 + (c_3 + c_3'q(a))^2$. Then $b^{2^k} = -c$, $[K(b) : K] = 2^k$ and $K(b) \cap K(\zeta_{2^k}) = K$. By Lemma 7.1, $K(\sqrt[2^j]{-c})$ is the unique extension of K of degree 2^j which is contained in $K(b)$, $j = 1, \ldots, k$. Since $K(\sqrt[2^j]{-c})$ is not formally

real, $K(b) \cap \mathbb{Q}_{\mathrm{tr}} = K$. As $\mathbb{Q}_{\mathrm{tr}}/K$ is Galois, $2^k = [\mathbb{Q}_{\mathrm{tr}}(b) : \mathbb{Q}_{\mathrm{tr}}] \leq [M : \mathbb{Q}_{\mathrm{tr}}]$. This contradiction to the choice of k implies that M is not PAC over K. ∎

Remark 7.3: The case $K = \mathbb{Q}$. It is possible to prove that no finite extension of $\mathbb{Q}_{\mathrm{tr}}$ is PAC over $\mathbb{Q}$ without applying Faltings' theorem. One may use in this case the absolutely irreducible polynomial $X^{2^k} + 7T_1^2 + 7T_2^2 + 7T_3^2$ and choose $(a_1, a_2, a_3) \neq (0, 0, 0)$ in $\mathbb{Q}^3$ and $b \in M$ such that $b^{2^k} = -7a_1^2 - 7a_2^2 - 7a_3^2$. Since the equation $t_1^2 + t_2^2 + t_3^2 = 7t_0^2$ has no solutions in $\mathbb{Q}$ [CaF, p. 359, Exer. 4.10, or Se2, p. 45, Lemma A], $c = -b^{2^k}$ is not a square in $\mathbb{Q}$. Using ramification arguments and the identity $(1 - \sqrt{-1})^2 = -2\sqrt{-1}$ in the case $c = 2$, one proves that b satisfies the conditions of Lemma 7.1 over $\mathbb{Q}$. Then one proceeds as in the proof of Theorem 7.2. ∎

The necessary condition on a Galois extension N of $\mathbb{Q}$ to be PAC over $\mathbb{Q}$ which Proposition 6.7 gives is not a sufficient condition. We show that $\mathbb{Q}_{\mathrm{tr}}(\sqrt{-1})$, which is PAC but not PAC over $\mathbb{Q}$ (Theorem 7.2) satisfies this condition. Indeed, already $\mathbb{Q}_{\mathrm{tr}}$ does.

To this end recall that a field M is **PRC (pseudo real closed)** if every absolutely irreducible variety V which is defined over M has an M-rational point provided it has a simple $\bar{M}$-rational point for each real closure $\bar{M}$ of M. The latter condition is equivalent to "the unique ordering of $\bar{M}$ extends to an ordering of the function field of V over $\bar{M}$" [La2, p. 282].

PROPOSITION 7.4: *Let M be a PRC field. Then every finite group G is regular over M.*

Proof: By a theorem of Harbater, G is regular over $E = M((t))$ [Har, Thm. 2.3]. Thus, there exists an absolutely irreducible polynomial $f \in E[Y, Z]$ which is Galois in Z over $E(Y)$ and $\mathcal{G}(f(Y, Z), E(Y)) \cong G$. Choose $x_1, \ldots, x_n \in E$ such that f is Galois over $M(\mathbf{x}, Y)$ and $\mathcal{G}(f(Y, Z), M(\mathbf{x})) \cong G$. Write $f(Y, Z) = g(\mathbf{x}, Y, Z)$ with $g \in M(\mathbf{x})[Y, Z]$.

By Bertini-Noether, there exists a Zariski-open subset U of $\mathbb{A}^n(\widetilde{M(\mathbf{x})})$ which contains $\mathbf{x}$ such that for all $\mathbf{a} \in U$ the polynomial $g(\mathbf{a}, Y, Z)$ is well defined, absolutely irreducible, Galois in Z over $M(\mathbf{a}, Y)$, and $\mathcal{G}(g(\mathbf{a}, Y, Z), M(\mathbf{a}, Y)) \cong G$.

As $M((t))$ is a regular extension of M, so is $M(\mathbf{x})$. Thus, $\mathbf{x}$ generates an absolutely irreducible variety V over M, and $U \cap V \neq \emptyset$. Let $\bar{M}$ be a real closure of M. Then, the unique ordering of $\bar{M}$ extends to $\bar{M}((t))$ [Ja2, Example 18.9] and

therefore to $\bar{M}(\mathbf{x})$. Since M is PRC, there exists an M-rational point $\mathbf{a} \in U \cap V$. Conclude from the preceding paragraph that G is regular over M. ∎

LEMMA 7.5: *For every finite group G there exists a finite group H and an epimorphism $\varphi\colon H \to G$ which maps all involutions of H onto 1.*

Proof: Use [HJ2, Cor. 6.2] with $I = \emptyset$. ∎

THEOREM 7.6: *For every finite group G there exist totally real fields $K \subseteq L$ such that K is Galois over $\mathbb{Q}$, L is Galois over K and $\mathcal{G}(L/K) \cong G$.*

Proof:* Let $\varphi\colon H \to G$ be an epimorphism as in Lemma 7.5. By [Pop], $\mathbb{Q}_{\mathrm{tr}}$ is PRC. Hence, by Proposition 7.4, H is regular over $\mathbb{Q}_{\mathrm{tr}}$. Since $\mathbb{Q}_{\mathrm{tr}}$ is Galois over $\mathbb{Q}$, H is already regular over a finite Galois extension K of $\mathbb{Q}$ which is contained in $\mathbb{Q}_{\mathrm{tr}}$. As K is Hilbertian, there exists a finite Galois extension N of K such that $\mathcal{G}(N/K) \cong H$. Let L be the fixed field in N of $\mathrm{Ker}(\varphi)$. Thus $\mathcal{G}(L/K) \cong G$ and $\mathrm{res}_L \tau = 1$ for each involution τ of $\mathcal{G}(N/K)$.

If $L \not\subseteq \mathbb{Q}_{\mathrm{tr}}$, then there would exist an involution $\tau \in G(\mathbb{Q}) \setminus G(L)$. In particular $\mathrm{res}_N \tau$ would be an involution of $\mathcal{G}(N/K)$ whose restriction to L is not 1. This contradiction to the preceding paragraph proves that L is totally real, as desired. ∎

If in the definition that precedes Proposition 7.4, we let $\bar{M}$ range over the p-adic closures of M, then M becomes **PpC (pseudo p-adically closed)** [HJ1, Def. 12.2]. We denote the maximal totally p-adic extension of $\mathbb{Q}$ by $\mathbb{Q}_{\mathrm{tp}}$. As in the case of $\mathbb{Q}_{\mathrm{tr}}$, [Pop] proves that $\mathbb{Q}_{\mathrm{tp}}$ is a PpC field.

PROBLEM 7.7: *Let G be a finite group. Do there exist totally p-adic number fields $K \subseteq L$ such that K is Galois over $\mathbb{Q}$, L is Galois over K, and $\mathcal{G}(L/K) \cong G$?*

8. Regular realization of finite groups with rational branch points

Let K be a PAC field and let t be a transcendental element over K. We say that a finite group G is **regular over K with branch points $a_1, \ldots, a_r$**, if there exists a finite Galois extension F of $K(t)$ which is regular over K such that $\mathcal{G}(F/K(t)) \cong G$ and $a_1, \ldots, a_r$ are all the branch points of $F/K(t)$. In geometric terms $F/K(t)$ corresponds to a (ramified) Galois cover $\varphi\colon X \to \mathbb{P}^1$ over K which remains a cover with the same Galois group after extending K to $\tilde{K}$. Then $a_1, \ldots, a_r$ are the branch points of φ in $\tilde{K} \cup \{\infty\}$.

* Together with Wulf-Dieter Geyer

THEOREM 8.1: *Let M be a field of characteristic 0 which is PAC over a subring R and let G be a finite group. Then, for infinitely many r, the group G is regular over M with exactly r branch points, all of them in R.*

Proof: Lemma 2 of [FrV] constructs a finite group H with a trivial center such that the Schur multiplier of H is generated by commutators, and an epimorphism $\pi\colon H \to G$. Let h be the number of nontrivial conjugacy classes of H. For each multiple $s \geq 3$ of h such that H is generated by $s-1$ elements consider an s-tuple $\mathbf{C} = (C_1, \ldots, C_s)$ of nontrivial conjugacy classes of H such that each nontrivial conjugacy class appears the same number of times among the C_i's. Fried and Völklein define a covering $\Psi'\colon \mathcal{H}_s^{\mathrm{inn}}(\mathbf{C}) \to \mathcal{U}_s$, where $\mathcal{U}_s$ is a Zariski open subset of $(\mathbb{P}^1)^s$, $\mathcal{H}_s^{\mathrm{inn}}(\mathbf{C})$ is an algebraic set of dimension s, and all of these objects are defined over $\mathbb{Q}$. To each field K of characteristic 0 and to each K-rational point $\mathbf{q} \in \mathcal{H}_s^{\mathrm{inn}}(\mathbf{C})$ they associate a Galois covering $\varphi\colon Y \to \mathbb{P}^1(\mathbb{C})$ which is defined over K with Galois group G whose branch points are the coordinates of $\Psi'(\mathbf{q}) = (b_1, \ldots, b_s)$ such that the elements of C_i generate the conjugacy class of inertia groups of the branch point b_i, $i = 1, \ldots, s$ [FrV, Thm. 1]. If in addition s is large enough, then $\mathcal{H}_s^{\mathrm{inn}}(\mathbf{C})$ is absolutely irreducible [FrV, Prop. 1]. In this case $\mathcal{H}_s^{\mathrm{inn}}(\mathbf{C})$ has an M-rational point $\mathbf{q}$ such that $(b_1, \ldots, b_s) \in (\mathcal{U}_s \cap \mathbb{A}^s)(R)$. This point gives then a regular realization of H over M whose branch points are $b_1, \ldots, b_s$. If we consider the fixed field of $\mathrm{Ker}(\pi)$ in the field that realizes H, we get a regular realization of G over M whose branch points are those b_i such that $C_i \cap \mathrm{Ker}(\pi) = \emptyset$. List these b_i's as $a_1, \ldots, a_r$. Their number is a positive multiple of s/h. So, as s is large, so is r. ∎

Combine Theorem 8.1 with Proposition 3.1:

COROLLARY 8.2: *Let R be a countable Hilbertian integral domain with a quotient field K of characteristic 0 (e.g., $R = \mathbb{Z}$ and $K = \mathbb{Q}$). Then for almost all $\boldsymbol{\sigma} \in G(K)^e$, for each finite group G and for infinitely many positive integers r, the group G is regular over $\tilde{K}(\boldsymbol{\sigma})$ with branch points $a_1, \ldots, a_r \in R$.*

9. The density property

We fix for this section a valued field (M, v) and an extension of v to $\tilde{M}$ which we also denote by v. We say that (M, v) has the **density property** if for each absolutely irreducible variety V defined over M the set $V(M)$ is v-dense in $V(\tilde{M})$.

Since all extensions of v to $\tilde{M}$ are conjugate over M, the density property of (M, v) does not depend on the particular extension. Note that the definition of [GeJ] asks for $V(M)$ to be dense in $V(\tilde{M}_v)$, where $\tilde{M}_v$ is the completion of $\tilde{M}$ with respect to v. But, by a theorem of Abraham Robinson [Pre, p. 241], the valued field $(\tilde{M}_v, v)$ is an elementary extension of $(\tilde{M}, v)$. In particular, $V(\tilde{M})$ is v-dense in $V(\tilde{M}_v)$. So, the two definitions are equivalent.

Note also that $\Gamma_v = v(M^\times)$ is cofinal in $v(\tilde{M}^\times)$ [Ja2, Cor. 7.2]. So, while speaking about v-density in $\tilde{M}$ it suffices to consider approximations with respect to elements of Γ_v only.

LEMMA 9.1 (Prestel): *Let M be a PAC field and let w be a valuation of $\tilde{M}$. Then M is w-dense in $\tilde{M}$.*

Proof: The proof is a slight variation of the proof of [FrJ, Thm. 10.14] (which is also due to Prestel). By [FrJ, Cor. 10.7] the w-closure of M in $\tilde{M}$ is a PAC field. Thus, we may assume that M is w-closed in $\tilde{M}$ and prove that $M = \tilde{M}$.

To this end, let $f \in M[X]$ be an irreducible separable polynomial of degree $n \geq 1$ and let $f(X) = \prod_{i=1}^{n}(X - x_i)$ be its factorization in $\tilde{M}[X]$. Consider $\gamma \in \Gamma = v(\tilde{M}^\times)$ and choose $c \in M^\times$ such that $w(c) \geq n\gamma$. By Eisentein's criteria, the polynomial $f(X)f(Y) - c^2$ is absolutely irreducible. Hence, there exist $x, y \in M$ such that $f(x)f(y) = c^2$. It follows from $w(f(x)) + w(f(y)) = 2w(c)$ that $w(f(x)) \geq n\gamma$ or $w(f(y)) \geq n\gamma$. Suppose for example that the first possibility occurs. Then $\sum_{i=1}^{n} w(x - x_i) \geq n\gamma$. It follows that there exists i such that $w(x - x_i) \geq \gamma$.

Since $\{x_1, \ldots, x_n\}$ is a finite set, it follows that there exists i such that for each $\gamma_0 \in \Gamma$ there exists $\gamma > \gamma_0$ and an $x \in M$ with $w(x - x_i) \geq \gamma$. This implies that $x_i \in M$ and that therefore $n = 1$. Conclude that $M = \tilde{M}$. ∎

We use vector notation. For $\mathbf{a} = (a_1, \ldots, a_n) \in \tilde{M}^n$ we replace $\min_{1 \leq i \leq n} v(a_i)$ by $v(\mathbf{a})$. We denote the valuation ring of v in M by $O_{M,v}$.

THEOREM 9.2: *Suppose that (M, v) is a valued field and M is PAC over $O_{M,v}$. Then (M, v) has the density property.*

Proof: Choose an extension of v to $\tilde{M}$ and denote it again by v. Let V be an absolutely irreducible variety of dimension r in $\mathbb{A}^n$ which is defined over M. Consider a point $\mathbf{b}_0 \in V(\tilde{M})$ and let $\varepsilon \in \Gamma_v$. We have to find $\mathbf{b} \in V(M)$ such that $v(\mathbf{b} - \mathbf{b}_0) > \varepsilon$.

To this end take a generic point $\mathbf{x}$ for V over M. Then $F = M(\mathbf{x})$ is a regular extension of M of transcendence degree r. Let $\varphi_0 \colon F \to \tilde{M} \cup \{\infty\}$ be a place of F over M such that $\varphi_0(\mathbf{x}) = \mathbf{b}_0$.

By Remark 1.2(a), M is PAC. Hence, by [FJ1, Thm. 3.4], F/M is a stable extension. That is, F/M has a separating transcendence base $\mathbf{t} = (t_1, \ldots, t_r)$, such that the Galois closure $\hat{F}$ of $F/M(\mathbf{t})$ is a regular extension of M. If $\varphi_0(t_i) = \infty$ replace t_i by t_i^{-1}. Thus, without loss, assume that $\mathbf{a}_0 = \varphi_0(\mathbf{t}) \neq \infty$.

Choose a primitive element z for $\hat{F}/M(\mathbf{t})$ which is integral over $M[\mathbf{t}]$. Thus $\hat{F} = M(\mathbf{t})[z]$. In particular

$$\mathbf{x} = \kappa_0(\mathbf{t})^{-1}\boldsymbol{\kappa}(\mathbf{t}, z), \text{ with } \boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_n) \in M[\mathbf{T}, Z]^n \text{ and } 0 \neq \kappa_0 \in M[\mathbf{T}].$$

Let $h \in M[\mathbf{T}, Z]$ be an absolutely irreducible polynomial which is monic and separable in Z such that $h(\mathbf{t}, z) = 0$, and let $d = \deg_Z h$. Then $h(\mathbf{t}, Z)$ has d distinct roots $z_1, \ldots, z_d$, all of them belong to $\hat{F}$ (because $\hat{F}/M(\mathbf{t})$ is Galois), and $0 \neq \text{discirminant}(h(\mathbf{t}, Z)) = \prod_{i \neq j}(z_i - z_j) = q \in M[\mathbf{t}]$. Also,

$$\mathbf{z} = \lambda_0(\mathbf{t})^{-1}\boldsymbol{\lambda}(\mathbf{t}, z) \text{ with } \boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_d) \in M[\mathbf{T}, Z]^d \text{ and } 0 \neq \lambda_0 \in M[\mathbf{T}].$$

Extend φ_0 to a place ψ_0 of $\hat{F}$. Since z is integral over $M[\mathbf{t}]$, we have $c_0 = \psi_0(z) \in \tilde{M}$.

Let Γ (resp., W) be the absolutely irreducible variety in $\mathbb{A}^{n+r+1}$ (resp., $\mathbb{A}^{r+1}$) which is generated over M by the point $(\mathbf{x}, \mathbf{t}, z)$ (resp., $(\mathbf{t}, z)$). We may change $(\mathbf{b}_0, \mathbf{a}_0, c_0)$, if necessary, in a small v-adic neighborhood of $\Gamma(\tilde{M})$ to assume that $q(\mathbf{a}_0)\kappa_0(\mathbf{a}_0)\lambda_0(\mathbf{a}_0) \neq 0$ [Mum, p. 82]. In particular $\mathbf{b}_0 = \kappa_0(\mathbf{a}_0)^{-1}\boldsymbol{\kappa}(\mathbf{a}, c)$.

Consider the following open neighborhood of $(\mathbf{a}_0, c_0)$ in $W(\tilde{M})$:

$$W_0 = \{(\mathbf{a}, c) \in W(\tilde{M}) |\ q(\mathbf{a})\kappa_0(\mathbf{a})\lambda_0(\mathbf{a}) \neq 0\}.$$

Then $x_i \colon W_0(\tilde{M}) \to \tilde{M}$ is a continuous function in the v-adic topology, $i = 1, \ldots, n$. Hence, there exists $\delta \in \Gamma_v$ such that for each $(\mathbf{a}, c) \in W_0(\tilde{M})$

(1a) $v(\mathbf{a} - \mathbf{a}_0) > \delta$ implies $q(\mathbf{a})\kappa_0(\mathbf{a})\lambda_0(\mathbf{a}) \neq 0$, and

(1b) $v((\mathbf{a}, c) - (\mathbf{a}_0, c_0)) > \delta$ implies $v(\kappa_0(\mathbf{a})^{-1}\boldsymbol{\kappa}(\mathbf{a}, c) - \mathbf{b}_0) > \varepsilon$.

Choose $\gamma > \delta$ such that for each $\mathbf{a} \in \tilde{M}^r$ with $v(\mathbf{a} - \mathbf{a}_0) > \gamma$ there exists $c \in \tilde{M}$ such that $h(\mathbf{a}, c) = 0$ and $v(c - c_0) > \delta$ [GeJ, Lemma 1.1]. Since M is v-dense in $\tilde{M}$ (Lemma 9.1), we may choose $\mathbf{a}_1 \in M^r$ such that

(2) $v(\mathbf{a}_1 - \mathbf{a}_0) > \gamma$.

Now choose $0 \neq m \in O_M$ such that $v(m) > \gamma$. The polynomial $h(\mathbf{a}_1+m\mathbf{T}, Z) \in M[\mathbf{T}, X]$ is absolutely irreducible and, since discriminant$(h(\mathbf{a}_1, Z)) = q(\mathbf{a}_1) \neq 0$ we have $\frac{\partial h}{\partial Z}(\mathbf{a}_1 + m\mathbf{T}, Z) \neq 0$. Let $\alpha_1, \alpha_2 \in M[\mathbf{T}, Z]$ and $0 \neq \beta \in M[\mathbf{T}]$ such that

$$\alpha_1(\mathbf{T}, Z)h(\mathbf{a}_1 + m\mathbf{T}, Z) + \alpha_2(\mathbf{T}, Z)\frac{\partial h}{\partial Z}(\mathbf{a}_1 + m\mathbf{T}, Z) = \beta(\mathbf{T}).$$

Since M is PAC over $O_{M,v}$, there exists $\mathbf{t}_1 \in O_{M,v}^r$ and $c \in M$ such that $h(\mathbf{a}_1 + m\mathbf{t}_1, c) = 0$ and $\beta(\mathbf{t}_1) \neq 0$, and therefore $\frac{\partial h}{\partial Z}(\mathbf{a}_1+m\mathbf{t}_1, c) \neq 0$. So, $\mathbf{a} = \mathbf{a}_1+m\mathbf{t}_1 \in M^r$ satisfies $h(\mathbf{a}, c) = 0$ and $\frac{\partial h}{\partial Z}(\mathbf{a}, c) \neq 0$.

Let ψ be a place of $\hat{F}$ over M such that $\psi(\mathbf{t}, z) = (\mathbf{a}, c)$ (It is possible to choose ψ such that its residue field will be M.) Note that $v(\mathbf{a} - \mathbf{a}_1) > \gamma > \delta$. Hence, by (2), $v(\mathbf{a} - \mathbf{a}_0) > \delta$. Therefore, $c_j = \psi(z_j) = \lambda_0(\mathbf{a})^{-1}\lambda_j(\mathbf{a}, c) \in M$ and $h(\mathbf{a}, c_j) = 0$, $j = 1, \ldots, d$. Since discriminant$(h(\mathbf{a}, z)) = q(\mathbf{a}) \neq 0$, the elements $c_1, \ldots, c_d$ are distinct. Hence they are all the roots of $h(\mathbf{a}, Z)$. Also, by the choice of γ, there exists k between 1 and d such that $v(c_k - c_0) > \delta$. Assume without loss that $c_k = c$. Then $v(c - c_0) > \delta$. Let $\mathbf{b} = \psi(\mathbf{x}) = \kappa_0(\mathbf{a})^{-1}\boldsymbol{\kappa}(\mathbf{a}, c) \in V(M)$. By the choice of δ, $v(\mathbf{b} - \mathbf{b}_0) > \varepsilon$. This completes the proof of the theorem. ∎

References

[Ax] J. Ax, *The elementary theory of finite fields*, Annals of Mathematics **88** (1968), 239–271.

[CaF] J.W.S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, 1967.

[Fal] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inventiones Mathematicae **73** (1983), 349–366.

[Fre] G. Frey, *Pseudo algebraically closed fields with non-archimedian real valuations*, Journal of Algebra **26** (1973), 202–207.

[FJ1] M. Fried and M. Jarden, *Diophantine properties of subfields of* $\tilde{\mathbb{Q}}$, American Journal of Mathematics **100** (1978), 653–666.

[FJ2] M. D. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 1986.

[FrV] M. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces*, Mathematische Annalen **290** (1991), 771–800.

[GaJ] W.-D. Geyer and M. Jarden, *On stable fields in positive characteristic*, Geometria Dedicata **29** (1989), 335–375.

[HJ1] D. Haran and M. Jarden, *The absolute Galois group of a pseudo p-adically closed field,* Journal für die reine und angewandte Mathematik **383** (1988), 147–206.

[HJ2] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed field,* Annali della Scuola Normale Superiore — Pisa, Serie IV, **12** (1985), 449–489.

[Har] D. Harbater, *Galois coverings of the arithmetic line,* Lecture Notes in Mathematics **1240**, Springer, Berlin, 1987, pp. 165–195.

[Ja1] M. Jarden, *Elementary statements over large algebraic fields,* Transactions of AMS **164** (1972), 67–91.

[Ja2] M. Jarden, *Intersection of local algebraic extensions of a Hilbertian field* (edited by A. Barlotti et al.), NATO ASI Series C **333**, Kluwer, Dordrecht, 1991, pp. 343–405.

[Ja3] M. Jarden, *The inverse Galois problem over formal power series fields,* Israel Journal of Mathematics **85** (1994), 263–275.

[JaR] M. Jarden and Peter Roquette, *The Nullstellensatz over p-adically closed fields,* Journal of the Mathematical Society of Japan **32** (1980), 425–460.

[La1] S. Lang, *Introduction to Algebraic Geometry,* Interscience Publishers, New York, 1958.

[La2] S. Lang, *Algebra,* Addison-Wesley, Reading, 1970.

[La3] S. Lang, *Algebraic Number Theory,* Addison-Wesley, Reading, 1970.

[Mat] B. H. Matzat, *Der Kenntnisstand in der Konstruktiven Galoischen Theorie,* manuscript, Heidelberg, 1990.

[Mum] D. Mumford, *The Red Book of Varieties and Schemes,* Lecture Notes in Mathematics **1358**, Springer, Berlin, 1988.

[Pop] F. Pop, *Fields of totally Σ-adic numbers,* manuscript, Heidelberg, 1992.

[Pre] A. Prestel, *Pseudo real closed fields,* in *Set Theory and Model Theory,* Lecture Notes in Math. **872**, Springer, Berlin, 1981, pp. 127–156.

[RCVS] M. Rzedowski-Calderón and G. Villa-Salvador, *Automorphisms of congruence function fields,* Pacific Journal of Mathematics **150** (1991), 167–178.

[Sam] P. Samuel, *Lectures on Old and New Results on Algebraic Curves,* Tata Institute of Fundamental Research, Bombay, 1966.

[Se1] J.-P. Serre, *Topics in Galois Theory,* Jones and Barlett, Boston, 1992.

[Se2] J.-P. Serre, *A Course in Arithmetic,* Graduate Texts in Mathematics **7**, Springer, New York, 1973.

[Sha] I.R. Shafarevich, *Basic algebraic Geometry*, Grundlehren der mathematischen Wissenschaften **213**, Springer, Berlin, 1977.

[Voe] H. Völklein, *Braid groups, Galois groups and cyclic covers of* $\mathbb{P}^1$, manuscript, 1992.