22 October, 2009

Function Fields of One Variable over PAC Fields

by

Moshe Jarden, Tel Aviv University

and

Florian Pop, University of Pennsylvania

In this note we give evidence for a conjecture of Serre and a conjecture of Bogomolov.

Conjecture II of Serre considers a field F of characteristic p with $\mathrm{cd}(\mathrm{Gal}(F)) \leq 2$ such that either $p = 0$ or $p > 0$ and $[F : F^p] \leq p$ and predicts that $H^1(\mathrm{Gal}(F), G) = 1$ (i.e. each principal homogeneous G-spaces has an F-rational point) for each simply connected semi-simple linear algebraic group G [Ser97, p. 139].

As Serre notes, the hypothesis of the conjecture holds in the case where F is a field of transcendence degree 1 over a perfect field K with $\mathrm{cd}(\mathrm{Gal}(K)) \leq 1$. Indeed, in this case $\mathrm{cd}(\mathrm{Gal}(F)) \leq 2$ [Ser97, p. 83, Prop. 11] and $[F : F^p] \leq p$ if $p > 0$ (by the theory of p-bases [FrJ08, Lemma 2.7.2]). We prove the conjecture for F in the special case, where K is PAC of characteristic 0 that contains all roots of unity.

One of the main ingredients of the proof is the projectivity of $\mathrm{Gal}(K(x)_{\mathrm{ab}})$ (where x is transcendental over K and $K(x)_{\mathrm{ab}}$ is the maximal Abelian extension of $K(x)$). We also use the same ingredient to establish an analog to the wellknown open problem of Shafarevich that $\mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}})$ is free. Under the assumption that K is PAC and contains all roots of unity we prove that $\mathrm{Gal}(K(x)_{\mathrm{ab}})$ is not only projective but even free. This proves a stronger version of a conjecture of Bogomolov for a function field of one variable F over a PAC field that contains all roots of unity [Pos05, Conjecture 1.1].

1. The Projectivity of $\mathrm{Gal}(K(x)_{\mathrm{ab}})$

We denote the separable (resp. algebraic) closure of a field K by K_s (resp. $\tilde{K}$) and its absolute Galois group by $\mathrm{Gal}(K)$. The field K is said to be **PAC** if every absolutely irreducible variety defined over K has a K-rational point. The proof of the projectivity result applies a local-global principle for Brauer groups to reduce the statement to Henselian fields.

For a prime number p and an Abelian group A, we say that A is **p'-divisible**, if for each $a \in A$ and every positive integer n with $p \nmid n$ there exists $b \in A$ such that $a = nb$. Note that if $p = 0$, then "p'-divisible" is the same as "divisible".

Lemma 1.1: *Let p be 0 or a prime number, B a torsion free Abelian group, and A is a p'-divisible subgroup of B of finite index. Then B is also p'-divisible.*

Proof: First suppose $p = 0$ and let $m = (B : A)$. Then, for each $b \in B$ and a positive integer n there exists $a \in A$ such that $mb = mna$. Since B is torsion free, $m = na$. Thus, B is divisible.

Now suppose p is a prime number, let $mp^k = (B : A)$, with $p \nmid m$ and $k \geq 0$, and consider $b \in B$. Then $mp^k b \in A$. Hence, for each positive integer n with $p \nmid n$ there exists $a \in A$ with $mp^k b = mna$. Thus, $p^k b = na$. Since $p \nmid n$, there exist $x, y \in \mathbb{Z}$ such that $xp^k + yn = 1$. It follows from $xp^k b = xna$ that $b = n(xa + yb)$, as claimed. ∎

Corollary 1.2: *Let L/K be an algebraic field extension, v a valuation of L, and $p = 0$ or p is a prime number. Suppose that $v(K^\times)$ is p'-divisible. Then $v(L^\times)$ is p'-divisible.*

Proof: Let $x \in L^\times$ and n a positive integer with $p \nmid n$. Then $v(K(x)^\times)$ is a torsion free Abelian group and $v(K^\times)$ is a subgroup of index at most $[K(x) : K]$. Since $v(K^\times)$ is p'-divisible, Lemma 1.1 gives $y \in K(x)^\times$ such that $v(x) = nv(y)$. It follows that $v(L^\times)$ is p'-divisible. ∎

Given a Henselian valued field (M, v) we use v also for its unique extension to M_s. We use a bar to denote the residue with respect to v of objects associated with M, let O_M be the valuation ring of M, and let $\Gamma_M = v(M^\times)$ be the value group of M.

We write $\mathrm{cd}_l(K)$ and $\mathrm{cd}(K)$ for the lth cohomological dimension and the cohomological dimension of $\mathrm{Gal}(K)$ and note that $\mathrm{cd}(K) \leq 1$ if and only if $\mathrm{Gal}(K)$ is projective [Ser97, p. 58, Cor. 2].

Lemma 1.3: *Let (M, v) be a Henselian valued field. Suppose $p = \mathrm{char}(M) = \mathrm{char}(\bar{M})$, $\mathrm{Gal}(\bar{M})$ is projective, and Γ_M is p'-divisible. Then $\mathrm{Gal}(M)$ is projective.*

Proof: We denote the **inertia field** of M by M_u. It is determined by its absolute Galois group: $\mathrm{Gal}(M_u) = \{\sigma \in \mathrm{Gal}(M) \mid v(\sigma x - x) > 0 \text{ for all } x \in M_s \text{ with } v(x) \geq 0\}$.

The map $\sigma \mapsto \bar{\sigma}$ of $\mathrm{Gal}(M)$ into $\mathrm{Gal}(\bar{M})$ such that $\bar{\sigma}\bar{x} = \overline{\sigma x}$ for each $x \in O_M$ is a well defined epimorphism [Efr06, Thm. 16.1.1] whose kernel is $\mathrm{Gal}(M_u)$. It therefore defines an isomorphism

$$(1) \qquad \mathrm{Gal}(M_u/M) \cong \mathrm{Gal}(\bar{M}).$$

Claim A: *$\bar{M}_u$ is separably closed.* Let $g \in \bar{M}[X]$ be a monic irreducible separable polynomial of degree $n \geq 1$. Then there exists a monic polynomial $f \in O_{M_u}[X]$ of degree n such that $\bar{f} = g$. We observe that f is also irreducible and separable. Moreover, if $f(X) = \prod_{i=1}^n (X - x_i)$ with $x_1, \ldots, x_n \in M_s$, then $g(X) = \prod_{i=1}^n (X - \bar{x}_i)$. Given $1 \leq i, j \leq n$ there exists $\sigma \in \mathrm{Gal}(M_u)$ such that $\sigma x_i = x_j$. By definition, $\bar{x}_j = \overline{\sigma x_i} = \bar{\sigma}\bar{x}_i = \bar{x}_i$. Since g is separable, $i = j$, so $n = 1$. We conclude that $\bar{M}_u$ is separably closed.

Claim B: *Each l-Sylow group of $\mathrm{Gal}(M_u)$ with $l \neq p$ is trivial.* Indeed, let L be the fixed field of an l-Sylow group of $\mathrm{Gal}(M_u)$ in M_s. If $l = 2$, then $\zeta_l = -1 \in L$. If $l \neq 2$, then $[L(\zeta_l) : L] | l - 1$ and $[L(\zeta_l) : L]$ is a power of l, so $\zeta_l \in L$.

Assume that $\mathrm{Gal}(L) \neq 1$. By the the theory of finite l-groups, L has a cyclic extension L' of degree l. By the preceding paragraph and Kummer theory, there exists $a \in L^\times$ such that $L' = L(\sqrt[l]{a})$. By Corollary 1.2, there exists $b \in L^\times$ such that $lv(b) = v(a)$. Then $c = \frac{a}{b^l}$ satisfies $v(c) = 0$. By Claim A, $\bar{L}$ is separably closed. Therefore, $\bar{c}$ has an lth root in $\bar{L}$. By Hensel's lemma, c has an lth root in L. It follows that a has an l-root in L. This contradiction implies that $L = M_s$, as claimed.

Having proved Claim B, we consider again a prime number $l \neq p$ and let G_l be an l-Sylow subgroup of $\mathrm{Gal}(M)$. By the Claim, $G_l \cap \mathrm{Gal}(M_u) = 1$, hence the map res: $\mathrm{Gal}(M) \to \mathrm{Gal}(M_u/M)$ maps G_l isomorphically onto an l-Sylow subgroup of $\mathrm{Gal}(M_u/M)$. By (1), G_l is isomorphic to an l-Sylow subgroup of $\mathrm{Gal}(\bar{M})$. Since the latter group is projective, so is G_l, i.e. $\mathrm{cd}_l(G) \leq 1$ [Ser97, p. 58, Cor. 2].

Finally, if $p \neq 0$, then $\mathrm{cd}_p(M) \leq 1$ [Ser97, p. 75, Prop. 3], because then $\mathrm{char}(M) = p$. It follows that $\mathrm{cd}(M) \leq 1$ [Ser97, p. 58, Cor. 2]. ∎

Lemma 1.4: *Let F be an extension of a PAC field K of transcendence degree 1 and* *characteristic p. Suppose $v(F^\times)$ is p'-divisible for each valuation v of F/K. Then* $\mathrm{Gal}(F)$ *is projective.*

Proof: Let K_{ins} be the maximal purely inseparable algebraic extension of K and set $F' = FK_{\mathrm{ins}}$. Then K_{ins} is PAC [FrJ08, Cor. 11.2.5], trans.deg$(F'/K_{\mathrm{ins}}) = 1$, and $v((F')^\times)$ is p'-divisible for every valuation v of F' (by Corollary 1.2). Moreover, $\mathrm{Gal}(F') = \mathrm{Gal}(F)$. Thus, we may replace K by K_{ins} and F by F', if necessary, to assume that K is perfect.

Let $V(F/K)$ be a system of representatives of the equivalence classes of valuations of F that are trivial on K. For each $v \in V(F/K)$ we choose a Henselian closure F_v of F at v. By [Efr01, Thm. 3.4], there is an injection of Brauer groups,

$$\mathrm{Br}(F) \to \prod_{v\in V(F/K)} \mathrm{Br}(F_v). \tag{2}$$

For each $v \in V(F/K)$ we have, $v(F_v^\times) = v(F^\times)$ is p'-divisible. Also, the residue field $\bar{F}_v$ is an algebraic extension of K. Since K is PAC, a theorem of Ax says that $\mathrm{Gal}(K)$ is projective [FrJ08, Thm. 11.6.2], hence $\mathrm{Gal}(\bar{F}_v)$ is projective [FrJ08, Prop. 22.4.7]. Finally, $\mathrm{char}(F_v) = \mathrm{char}(\bar{F}_v)$. Therefore, by Lemma 1.3, $\mathrm{Gal}(F_v)$ is projective, hence $\mathrm{Br}(F_v) = 0$ [Ser97, p. 78, Prop. 5]. It follows from the injectivity of (2) that $\mathrm{Br}(F) = 0$.

If F_1 is a finite separable extension of F, $v_1 \in V(F_1/K)$, and $v = v_1|_F$, then $v(F^\times)$ is p'-divisible. Hence, by Corollary 1.2, $v_1((F_1)^\times)$ is p'-divisible. It follows from the preceding paragraph that $\mathrm{Br}(F_1) = 0$. Consequently, by [Ser97, p. 78, Prop. 5], $\mathrm{cd}(\mathrm{Gal}(F)) \le 1$. ∎

LEMMA 1.5: *Let p be either 0 or a prime number and let Γ be an additive subgroup of $\mathbb{Q}$. Suppose $\frac{1}{n} \in \Gamma$ for each positive integer n with $p \nmid n$. Then Γ is p'-divisible.*

Proof: We consider $\gamma \in \Gamma$. If $p = 0$, we write $\gamma = \frac{a}{b}$, with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Given $n \in \mathbb{N}$, we have $\frac{\gamma}{n} = a \cdot \frac{1}{nb} \in \Gamma$.

If $p > 0$, we write $\gamma = \frac{a}{bp^k}$, where $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $k \in \mathbb{Z}$, and $p \nmid a, b$. Let $n \in \mathbb{N}$ with $p \nmid n$. If $k \le 0$, then $\frac{\gamma}{n} = ap^{-k} \cdot \frac{1}{nb} \in \Gamma$. If $k > 0$, we may choose $x, y \in \mathbb{Z}$ such that $xp^k + ynb = 1$. Then $\frac{\gamma}{n} = \frac{a}{nbp^k} = \frac{axp^k + aynb}{nbp^k} = ax \cdot \frac{1}{nb} + by \cdot \frac{a}{bp^k} \in \Gamma$, as claimed. ∎

Proposition 1.6: *Let K be a PAC field that contains all roots of unity and let E be an extension of K of transcendence degree* 1. *Then* $\mathrm{Gal}(E_{\mathrm{ab}})$ *is projective.*

Proof: First we consider the case where $E = K(x)$, where x is transcendental over K, and set $F = E_{\mathrm{ab}}$. In the notation of Lemma 1.4 we consider a valuation $v \in V(F/K)$ normalized in such a way that $v(E^\times) = \mathbb{Z}$. Then $v(F^\times) \le \mathbb{Q}$. On the other hand, let $p = \mathrm{char}(K)$ and consider a positive integer n with $p \nmid n$. Let $e \in E$ with $v(e) = 1$. Then $e^{1/n} \in F$ (because K contains a root of 1 of order n). Therefore, $\frac{1}{n} = v(e^{1/n}) \in v(F^\times)$. By Lemma 1.5, $v(F^\times)$ is p'-divisible. We conclude from Lemma 1.4 that $\mathrm{Gal}(F)$ is projective.

In the general case we choose $x \in E$ transcendental over K. By the preceding paragraph, $\mathrm{Gal}(K(x)_{\mathrm{ab}})$ is projective. Since taking purely inseparable extensions of a field does not change its absolute Galois group, $\mathrm{Gal}(K(x)_{\mathrm{ab,ins}}$ is projective. Now note that $\mathrm{Gal}(E_{\mathrm{ab,ins}})$ as a subgroup of $\mathrm{Gal}(K(x)_{\mathrm{ab,ins}})$ is also projective. Hence, $\mathrm{Gal}(E_{\mathrm{ab}})$ is projective. ∎

Remark 1.7: Proposition 1.6 is false if K does not contain all roots of unity. Indeed, the authors will elsewhere provide an example of a prime number l and a PAC field K of characteristic 0 that contains all roots of unity of order n with $l \nmid n$ but not ζ_l such that $\mathrm{Gal}(K(x)_{\mathrm{ab}})$ is not projective. ∎

2. Serre and Shafarevich

We refer to a simply connected semi-simple linear algebraic group G as a **simply connected group**. In this case $H^1(\mathrm{Gal}(K), G)$ will be also denoted by $H^1(K, G)$. Since each element of $H^1(K, G)$ is represented by a principal homogeneous space V of G and V is an absolutely irreducible variety defined over K, V has a K-rational point if K is PAC. Hence, V is equivalent to G [LaT58, Prop. 4]. Thus, $H^1(K, G) = 1$.

The proof of Serre's Conjecture II in our case is based on the following consequence of a theorem of Colliot-Thélène, Gille, and Parimala:

Proposition 2.1: *Let F be a field and G a simply connected group defined over F. Suppose F is a C_2-field of characteristic* 0, $\mathrm{cd}(F) \le 2$, *and* $\mathrm{cd}(F_{\mathrm{ab}}) \le 1$. *Then*

$H^1(F,G) = 1$.

Proof: Let F' be a finite extension of F. Since F is C_2, [CGP04, Thm. 1.1(vi)] implies that if the exponent e of a central simple algebra A over F' is a power of 2 or a power of 3, then e is equal to the index of A.

Since $\mathrm{cd}(F) \leq 2$ and $\mathrm{cd}(F_{\mathrm{ab}}) \leq 1$, [CGP04, Thm. 1.2(v)] implies that $H^1(F,G) = 1$. ∎

Remark 2.2: By Merkuriev-Suslin, the assumption that F is a C_2-field implies that $\mathrm{cd}(F) \leq 2$ [Ser97, end of page 88]. However, we will be able to prove both properties of F directly in the application we have in mind. ∎

The following result establishes the first condition on F.

LEMMA 2.3: *Let F be an extension of transcendence degree 1 over a perfect PAC field K. Suppose either $\mathrm{char}(K) > 0$ and K contains all roots of unity or $\mathrm{char}(K) = 0$. Then $\mathrm{cd}(F) \leq 2$ and F is a C_2-field.*

Proof: By Ax, $\mathrm{cd}(K) \leq 1$ [FrJ08, Thm. 11.6.2]. Hence, by [Ser97, p. 83, Prop. 11], $\mathrm{cd}(F) \leq 2$.

A conjecture of Ax from 1968 says that every perfect PAC field K is C_1 [FrJ08, Problem 21.2.5]. The conjecture holds if K contains an algebraically closed field [FrJ08, Lemma 21.3.6(a)]. In particular, if $p = \mathrm{char}(K) > 0$ and K contains all roots of unity, then $\tilde{\mathbb{F}}_p \subseteq K$, so K is C_1. If $\mathrm{char}(K) = 0$, K is C_1, by [Kol07, Thm. 1]. It follows that in each case, F is C_2 [FrJ08, Prop. 21.2.12]. ∎

THEOREM 2.4: *Let F be an extension of transcendence degree 1 of a PAC field K of characteristic 0. Suppose K contains all roots of unity. Then F satisfies Serre's conjecture II. That is, $H^1(F,G) = 1$ for each simply connected group G defined over F.*

Proof: By Lemma 2.3, $\mathrm{cd}(F) \leq 2$ and F is a C_2-field. By Proposition 1.6, $\mathrm{cd}(F_{\mathrm{ab}}) \leq 1$. It follows from Proposition 2.1 that $H^1(F,G) = 1$ for each simply connected group G. ∎

Remark 2.5: All of the ingredients of the proof of Theorem 2.4 except possibly Proposition 2.1 work also when $\mathrm{char}(K) > 0$. ∎

The proof of the freeness of $\mathrm{Gal}(K(x)_{\mathrm{ab}})$ applies the notion of "quasi-freeness" due to Harbater and Stevenson. To this end recall that a **finite split embedding problem** $\mathcal{E}$ for a profinite group G is a pair $(\varphi\colon G \to A,\ \alpha\colon B \to A)$, where A, B are finite groups, φ, α are epimorphisms, and α has a group theoretic section. A **solution** of $\mathcal{E}$ is an epimorphism $\gamma\colon G \to B$ such that $\alpha \circ \gamma = \varphi$. We say that G is **quasi-free** if its rank m is infinite and every finite split embedding problem for G has m distinct solutions.

THEOREM 2.6: *Let F be a function field of one variable over a PAC field K of cardinality m containing all roots of unity and let x be a variable. Then* $\mathrm{Gal}(F_{\mathrm{ab}})$ *is isomorphic to the free profinite group of rank m.*

Proof: Since K is PAC, K is **ample**, that is every absolutely irreducible curve defined over K with a K-rational simple point has infinitely many K-rational points. By [HaS05, Cor. 4.4], $\mathrm{Gal}(F)$ is quasi-free of rank $m = \mathrm{card}(K)$. Hence, by [Har09, Thm. 2.4], $\mathrm{Gal}(F_{\mathrm{ab}})$ is also quasi-free of rank m. Since by Proposition 1.6, $\mathrm{Gal}(F_{\mathrm{ab}})$ is projective, it follows from a result of Chatzidakis and Melnikov [FrJ08, Lemma 25.1.8] that $\mathrm{Gal}(F_{\mathrm{ab}})$ is free of rank m. ∎

Acknowledgment: The authors thank Jean-Louis Colliot-Thélène for stimulating discussions, in particular for pointing out Proposition 2.1 to them. ∎

References

[CGP04] J.-L. Colliot-Thélńe, P. Gille, and R. Parimala, *Arithmetic of linear algebraic groups over two-dimensional geometric fields*, Duke Mathematical Journal **121** (2004), 285–341.

[Efr01] I. Efrat, *A Hasse principle for function fields over PAC fields*, Israel Journal of Mathematics **122** (2001), 43–60.

[Efr06] I. Efrat, *Valuations, Orderings, and Milnor K-Theory*, Mathematical surveys and monographs **124**, American Mathematical Society, Providence, 2006.

[FrJ08] M. D. Fried and M. Jarden, *Field Arithmetic, Third Edition, revised by Moshe Jarden*, Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2008.

[Har09] D. Harbater, *On function fields with free absolute Galois groups*, Journal für die reine und andgewandte Mathematik **632** (2009), 85–103.

[HaS05] D. Harbater and K. Stevenson, *Local Galois theory in dimension two*, Advances in Mathematics **198** (2005), 623–653.

[Kol07] J. Kollár, *A conjecture of Ax and degenerations of Fano varieties*, Israel Journal of Mathematics **162** (2007), 235–251.

[LaT58] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, American Journal of Mathematics **80** (1958), 659–684.

[Pos05] L. Positselski, *Koszul property and Bogomolov's conjecture*, International Mathematics Research Notices **31** (2005), 1901–1936.

[Ser97] J.-P. Serre, *Galois Cohomology*, Springer, Berlin, 1997.