POINTS HAVING THE SAME RESIDUE FIELD AS THEIR IMAGE UNDER A MORPHISM

BJORN POONEN

1. Main result

Our result, loosely speaking, is that in a nontrivial family of varieties $f : X \to Y$ over a perfect field k, some fiber $X_t = f^{-1}(t)$ has a point rational over the field of definition of t. The precise statement, which is slightly more general, is given in Theorem 1 below. Denote by $\overline{f(X)}$ the scheme-theoretic image of a morphism $f : X \to Y$ between noetherian schemes, and by $\kappa(x)$ the residue field of a point x of a scheme.

Theorem 1. *Let X and Y be schemes of finite type over a field k. Let $f : X \to Y$ be a k-morphism such that $\dim \overline{f(X)} \geq 1$. Then there exists a closed point $x \in X$ such that the extension $\kappa(x)$ of $\kappa(f(x))$ is purely inseparable.*

Proof. We begin with several straightforward reductions. If we cover Y with finitely many open affine subsets V, one of them must satisfy $\dim \left(V \cap \overline{f(X)}\right) \geq 1$. Similarly, some open affine subset U of $f^{-1}(V)$ satisfies $\dim \left(V \cap \overline{f(U)}\right) \geq 1$. By considering $f|_U : U \to V$ instead of f, we reduce to the case $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$. Let $\phi : B \to A$ correspond to f.

If f' is a composition $X' \xrightarrow{\alpha} X \xrightarrow{f} Y \xrightarrow{\beta} Y'$ of morphisms of schemes of finite type over k with $\dim \overline{f'(X')} \geq 1$, and if we find a closed point $x' \in X'$ with $\kappa(x')$ purely inseparable over $\kappa(f'(x'))$, then $x = \alpha(x') \in X$ will do for f. For instance, composing $X_{\mathrm{red}} \to X$ with f does not affect the dimension of the image in Y, so we may assume X is reduced. Some irreducible component of X will have positive-dimensional image in Y; hence we may assume X is integral.

Replacing Y by $\overline{f(X)}$, or equivalently B by $\phi(B)$, we may assume that ϕ is injective and $\dim Y \geq 1$. Since $\dim B = \dim Y \geq 1$, the polynomial ring $k[t]$ injects into B. Composing f with the associated morphism $Y \to \mathbf{A}^1$, we reduce to the case $Y = \mathbf{A}^1$, $B = k[t]$.

Let $S = k[t] \setminus \{0\}$, and let $\mathfrak{m}$ be a maximal ideal of $S^{-1}A$. Let A' be the image of A in $L := (S^{-1}A)/\mathfrak{m}$. The composition $B = k[t] \to A \to A'$ is still injective, so we may reduce to the case $A = A'$.

Now $S^{-1}A = \operatorname{Frac}(A) = L$ is both a field and a finitely generated $k(t)$-algebra, so $[L : k(t)] < \infty$ by the Nullstellensatz. Write $k(t) \subseteq L_0 \subset L_1 \subset \cdots \subset L_r = L$ with L_0 separable over $k(t)$ and $L_{i+1} = L_i(u_i)$ purely inseparable of degree p over L_i, where p is the characteristic of k. By the Primitive Element Theorem, we may write $L_0 = k(t)(z)$.

Date: February 15, 2000.

1991 *Mathematics Subject Classification.* Primary 14A15; Secondary 14D99.

Key words and phrases. residue field.

This research was supported by NSF grant DMS-9801104, a Sloan Fellowship, and a Packard Fellowship. This article has appeared in *J. Algebra* **243** (2001), 224–227.

Multiplying z by a nonzero element of $k[t]$, we may assume that the characteristic polynomial $P(T)$ of z in L_0 over $k(t)$ has coefficients in $B = k[t]$. Let $A_i = B[z, u_1, \dots, u_i]$, so $S^{-1}A_i = L_i$. Pick $q \in B$ nonzero such that $u_{i+1}^p \in A_i[q^{-1}]$ for each i and $A_r[q^{-1}] = A[q^{-1}]$.

We claim that for some $b \in B$, $b - z \notin A_0[q^{-1}]^*$. It suffices to find $b \in B$ such that $P(b) = \operatorname{Norm}_{L_0/k(t)}(b - z)$ is not a unit in $B[q^{-1}]$. Let T_n be the set of polynomials in t of exact degree n with coefficients in $\{0, 1\}$, so $\#T_n = 2^n$. Let $d = \deg P$. Then $\{\, P(b) : b \in T_n \,\}$ consists of at least $2^n/d$ distinct polynomials, each monic of degree nd if n is larger than the t-degree of the coefficients of P. On the other hand, factoring q over $\overline{k}$ shows that the number of monic polynomials of degree nd in $B[q^{-1}]^*$ is less than $O\left((nd)^{\deg q}\right)$ as $n \to \infty$. By taking n large, we find $b \in T_n$ such that $P(b) \notin B[q^{-1}]^*$, and hence $b - z \notin A_0[q^{-1}]^*$.

Choose a maximal ideal $\mathfrak{n}_0$ of $A_0[q^{-1}]$ containing $b - z$. Since $A_{i+1}[q^{-1}]$ has the form $A_i[q^{-1}][U]/(U^p - \alpha_i)$ for some $\alpha_i \in A_i[q^{-1}]$, there is a unique maximal ideal $\mathfrak{n}$ of $A_r[q^{-1}] = A[q^{-1}]$ above $\mathfrak{n}_0$. Let $x_0 \in \operatorname{Spec} A_0[q^{-1}]$ and $x \in \operatorname{Spec} A[q^{-1}] \subseteq \operatorname{Spec} A = X$ be the corresponding closed points, so $\kappa(x)$ is purely inseparable over $\kappa(x_0)$. It remains to show that the extension $\kappa(x_0)$ of $\kappa(f(x))$ is trivial. Let $\bar{t}$ and $\bar{b} = \bar{z}$ denote the images of t, b, and z in $\kappa(x_0)$. Then $\kappa(x_0) = k(\bar{t}, \bar{z}) = k(\bar{t}, \bar{b}) = k(\bar{t}) = \kappa(f(x))$. □

Remark. In Theorem 1, if in addition some dense open subset of X is smooth over its image in Y, then we can find a closed point $x \in X$ with $\kappa(x) = \kappa(f(x))$: by (IV, 17.16.3(ii)) of [2] one can reduce to the case where X is étale over its image, and then by (IV, 17.6.1(a,c′)) of [2] all residue field extensions are separable. (When we write $\kappa(x) = \kappa(f(x))$, we mean that the field homomorphism $\kappa(f(x)) \to \kappa(x)$ induced by f is an isomorphism.)

Corollary 2. *Let X and Y be schemes of finite type over a perfect field k. Let $f : X \to Y$ be a k-morphism such that $\dim \overline{f(X)} \geq 1$. Then there exists a closed point $x \in X$ such that $\kappa(x) = \kappa(f(x))$.*

Proof. Theorem 1 provides x. The extension $\kappa(x)$ of $\kappa(f(x))$ is automatically separable, since both fields are finite extensions of the perfect field k. □

Remark. Corollary 2 can fail for nonperfect k. Here is a counterexample. Let k_0 be a perfect field of characteristic p, let $k = k_0(s, t)$ where s, t are indeterminates, and let $L = k_0(s^{1/p}, t^{1/p})$. Let $f : X \to Y$ be the morphism of affine k-schemes associated to the inclusion $k[z] \hookrightarrow L[z]$. Suppose that there exists a closed point $x \in X$ with $[\kappa(x) : \kappa(f(x))] = 1$. Let $\alpha \in \overline{L}$ be a root of the polynomial in $L[z]$ generating the prime x. Then $[L(\alpha) : k(\alpha)] = 1$, so $L \subseteq k(\alpha)$. We obtain the contradiction

$$p^2 = [L : kL^p] \leq [k(\alpha) : k \cdot k(\alpha)^p] = [k(\alpha) : k(\alpha^p)] \leq p.$$

(The first inequality is the case $F = k(\alpha)$ of the inequality $[L : kL^p] \leq [F : kF^p]$ for finite extensions of fields $k \subseteq L \subseteq F$ of characteristic p: this follows from $[F : L] = [F^p : L^p] \geq [kF^p : kL^p]$ and $[F : L][L : kL^p] = [F : kF^p][kF^p : kL^p]$.)

2. Arithmetic analogues

Theorem 4 below is an arithmetic analogue of Corollary 2. Lemma 3 is a special case of Theorem 4, and will be used to prove it.

Lemma 3. *Let $f : X \to \operatorname{Spec} \mathbf{Z}$ be a dominant morphism of finite type. Then there exists $x \in X$ such that $\kappa(x) = \kappa(f(x))$ (or equivalently, such that $\kappa(x)$ has prime order).*

Proof. Mimic the proof of Theorem 1 with $\mathbf{Z}$ playing the role of $k[t]$. Eventually we reduce to the statement that if q is a nonzero integer, and $P \in \mathbf{Z}[T]$ is a nonconstant polynomial, then there exists $b \in \mathbf{Z}$ such that $P(b) \notin \mathbf{Z}[q^{-1}]^*$. This holds, by a counting argument again: if $\deg P = d$, then $\{P(1), \dots, P(n)\}$ is a set of at least n/d distinct integers of absolute value $O(n^d)$, but the number of integers in $\mathbf{Z}[q^{-1}]$ up to this bound grows like a power of $\log n$ only. □

Remark. Alternatively, after reducing to the case $\dim X = 1$, one could invoke the Chebotarev Density Theorem. Of course, this would make the proof less elementary.

Theorem 4. *Let X and Y be schemes of finite type over* $\operatorname{Spec} \mathbf{Z}$*, and let $f : X \to Y$ be a morphism such that* $\dim \overline{f(X)} \geq 1$. *Then there exists a closed point $x \in X$ such that $\kappa(x) = \kappa(f(x))$.*

Proof. If X dominates $\operatorname{Spec} \mathbf{Z}$, use the x given by Lemma 3. Otherwise there are finitely many nonzero primes p of $\mathbf{Z}$ for which the fiber X_p of $X \to \operatorname{Spec} \mathbf{Z}$ is nonempty, so $\dim \overline{f(X_p)} \geq 1$ for some p. Apply Corollary 2 to the morphism of fibers $f_p : X_p \to Y_p$ over $\mathbf{F}_p$ to find x. □

3. Application to Shafarevich-Tate groups in a family

The paper [1] constructs a nonisotrivial smooth proper family $\mathcal{X} \to U$ of genus 1 curves over an open subset U of $\mathbf{P}^1_{\mathbf{Q}}$, such that for each $t \in U(\mathbf{Q})$, the fiber $\mathcal{X}_t$ violates the Hasse principle. It also constructs a nonisotrivial smooth proper family $\mathcal{Y} \to U$ of torsors of abelian surfaces over an open subset U of $\mathbf{P}^1_{\mathbf{Q}}$ such that for every $t \in U$ of *odd degree* over $\mathbf{Q}$, $\mathcal{Y}_t$ violates the Hasse principle over the number field $\kappa(t)$. In other words, these fibers represent nonzero elements of the Shafarevich-Tate groups of the associated abelian varieties. Corollary 2 shows that such results cannot be extended to *all* closed fibers of a family: there will always be a closed point $t \in U$ above which the fiber has a point rational over $\kappa(t)$.

Acknowledgement

I thank Laurent Moret-Bailly for many comments. In particular, the suggestion to prove Theorem 1 for not necessarily perfect fields and the suggestion to prove arithmetic analogues are due to him.

References

[1] J.-L. Colliot-Thélène and B. Poonen, Algebraic families of nonzero elements of Shafarevich-Tate groups, *J. Amer. Math. Soc.* **13** (2000), 83–99.

[2] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.* No. 32, 1967.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: poonen@math.berkeley.edu