ORBITS OF AUTOMORPHISM GROUPS OF FIELDS

KIRAN S. KEDLAYA AND BJORN POONEN

Abstract. We address several specific aspects of the following general question: can a field K have so many automorphisms that the action of the automorphism group on the elements of K has relatively few orbits? We prove that any field which has only finitely many orbits under its automorphism group is finite. We extend the techniques of that proof to approach a broader conjecture, which asks whether the automorphism group of one field over a subfield can have only finitely many orbits on the complement of the subfield. Finally, we apply similar methods to analyze the field of Mal'cev-Neumann "generalized power series" over a base field; these form near-counterexamples to our conjecture when the base field has characteristic zero, but often fall surprisingly far short in positive characteristic.

Can an infinite field K have so many automorphisms that the action of the automorphism group on the elements of K has only finitely many orbits? In Section 1, we prove that the answer is "no" (Theorem 1.1), even though the corresponding answer for division rings is "yes" (see Remark 1.2). Our proof constructs a "trace map" from the given field to a finite field, and exploits the peculiar combination of additive and multiplicative properties of this map.

Section 2 attempts to prove a relative version of Theorem 1.1, by considering, for a nontrivial extension of fields $k \subset K$, the action of $\mathrm{Aut}(K/k)$ on K. In this situation each element of k forms an orbit, so we study only the orbits of $\mathrm{Aut}(K/k)$ on $K - k$. Our Conjecture 2.1 asserts that if $\mathrm{Aut}(K/k)$ acts on $K - k$ with finitely many orbits, then k and K are either both finite or both algebraically closed. This conjecture contains Theorem 1.1 as a special case, as one sees by taking k to be the minimal subfield of K. Using variants of the techniques of Section 1 (including a "norm map" serving as a multiplicative analogue of our earlier "trace map"), we prove some weaker versions of our conjecture. For instance, under the hypothesis of Conjecture 2.1 and the assumption that k and K are not finite, k satisfies Kaplansky's "Hypothesis A" (Proposition 2.11), and both k and K are radically closed (Corollary 2.13).

Whereas the results of Sections 1 and 2 restrict the possibilities for fields with many automorphisms (few orbits), Section 3 investigates some specific candidates for fields that *could* have many automorphisms. Specifically, we study the Mal'cev-Neumann fields of "generalized power series" over a base field k. If k has characteristic zero or satisfies Hypothesis A, then the Mal'cev-Neumann field over k has relatively few orbits under its automorphism group (Theorem 3.4), though not so few as to contradict Conjecture 2.1. In contrast, if k does not satisfy Hypothesis A, then the Mal'cev-Neumann field over k has only automorphisms given by rescaling the series parameter (Theorem 3.6). The techniques used here are similar to those used in the previous sections; indeed, the historical order of things is that we considered the Mal'cev-Neumann fields as a source of potential counterexamples to

Date: August 26, 2005 (small corrections made June 7, 2006 and October 29, 2008).
This article has been published in *Math. Res. Letters* **12** (2005), no. 4, 475–481.

Conjecture 2.1, and the ideas used in the proof of Theorem 3.6 led ultimately to the proof of Theorem 1.1.

1. Fields with finitely many orbits

This section is devoted to the proof of the following theorem.

Theorem 1.1. *Let K be a field on which the number of orbits of $\mathrm{Aut}(K)$ is finite. Then K is finite.*

Remark 1.2. The noncommutative analogue of Theorem 1.1 is false, as explained to us by George Bergman and P.M. Cohn as follows. Let $\overline{\mathbb{F}_2}$ be an algebraic closure of $\mathbb{F}_2$. Let $G = \mathrm{Gal}(\overline{\mathbb{F}_2}/\mathbb{F}_2)$. Given a division ring L_i containing $\overline{\mathbb{F}_2}$ in its center and admitting an extension of the G-action, suppose the fixed subring L_i^G contains elements x, y transcendental over $\mathbb{F}_2$ but not conjugate by an element of L_i^G. Let T be L_i with an element u universally adjoined subject to the relation $xu = uy$; equivalently, T is the tensor L_i-ring $L_i\langle M\rangle$ where M is the L_i-bimodule $M = L_i \otimes_{\mathbb{F}_2(t)} L_i$ in which t acts as right multiplication by x on the left factor and left multiplication by y on the right factor, and $u = 1 \otimes 1 \in M \subseteq T$. The action of G on L_i induces an action on T, and $u \in T^G$. As in [C, Theorem 5.5.1], T admits a universal field of fractions L_{i+1}, which inherits a G-action. In L_{i+1}, x and y are conjugate by the image of u. Repeating this construction transfinitely starting with the rational function field $L_0 = \overline{\mathbb{F}_2}(z)$ with G acting trivially on z, we eventually obtain a division ring L containing $\overline{\mathbb{F}_2}$ in its center admitting an extension of the G-action, such that any two elements of L^G transcendental over $\mathbb{F}_2$ are conjugate by an element of L^G. Let $K = L^G$, which is infinite since it contains $\mathbb{F}_2(z)$. If $a \in K$ is algebraic over $\mathbb{F}_2$, then $\overline{\mathbb{F}_2}(a) \subseteq L$ is a finite field extension of $\overline{\mathbb{F}_2}$, so $a \in \overline{\mathbb{F}_2}$; however, a is also fixed by G, so $a \in \mathbb{F}_2$. In other words, every element of $K - \mathbb{F}_2$ is transcendental over $\mathbb{F}_2$. Consequently, the inner automorphism group of K acts with three orbits: $\{0\}$, $\{1\}$, and everything else.

For the rest of this section, we assume that K is a field such that

The number of orbits of $\mathrm{Aut}(K)$ on K is finite.

The integral closure k of the prime subfield in K must be a finite field $\mathbb{F}_q$, or else k alone would contribute infinitely many orbits. Write $q = p^e$ where p is prime and $e \in \mathbb{Z}_{\geq 1}$. The $\mathbb{F}_p$-vector space K can be made a module over the polynomial ring $\mathbb{F}_p[F]$ by setting $F \cdot \alpha = \alpha^p$ for all $\alpha \in K$.

Lemma 1.3 (Bergman and Kearnes)**.** *There exists a unique map $\mathrm{Tr}\colon K \to \mathbb{F}_q$ such that for any $x \in K$ and any nonzero $P(F) \in \mathbb{F}_p[F]$, there exists $y \in K$ satisfying $P(F)(y) = x - \mathrm{Tr}(x)$. Moreover, $\mathrm{Tr}(F(x)) = F(\mathrm{Tr}(x))$, and $\mathrm{Tr}(\mathrm{Tr}(x)) = \mathrm{Tr}(x)$, and Tr is $\mathbb{F}_q$-linear. If x and y are in the same orbit of $\mathrm{Aut}(K/\mathbb{F}_q)$, then $\mathrm{Tr}(x) = \mathrm{Tr}(y)$.*

In particular (this being the case we will need), if $\mathrm{Tr}(x) = 0$, then for all n, there exists $y_n \in K$ such that $y_n^{p^n} - y_n = x$. (This consequence of Lemma 1.3 could also be proved directly.)

Remark 1.4. A map like Tr exists in some other contexts; for one example, see Section 3.

Remark 1.5. One can make an analogous multiplicative construction: for every $x \in K^*$, there is a unique $c \in \mathbb{F}_q^*$ such that x/c has an n-th root for each positive integer n. We will not need this yet, but it will come up in Section 2.

Using the interpretation of K as an $\mathbb{F}_p[F]$-module, we may deduce Lemma 1.3 from the following lemma suggested by Hendrik Lenstra, which may be of independent interest. Let R be an integral domain. A submodule N of an R-module M is said to be *characteristic* if $\alpha(N) = N$ for every module automorphism α of M. For $a \in R$, define $M_a := \{m \in M : am = 0\}$. The *torsion submodule* M_t of M is $\bigcup_{a \in R-\{0\}} M_a$. The *divisible submodule* M_d of M is the set of $m \in M$ such that for every $a \in R - \{0\}$ there exists $x \in M$ with $ax = m$.

Lemma 1.6 (Lenstra)**.** *Let R be an integral domain, and let M be an R-module with finitely many characteristic submodules. Then $M = M_t \oplus M_d$. Moreover there exists $c \in R - \{0\}$ annihilating M_t, and for any such c we have $cM = M_d$.*

Proof. The submodule M_a is characteristic for any $a \in R$, so there are only finitely many possibilities for it. If $M_{a_1}, \ldots, M_{a_n}$ is an exhaustive list of the M_a for $a \neq 0$, put $c = a_1 \cdots a_n$. Then $M_c = M_t$.

From now on, let c be any nonzero element of R annihilating M_t. Since R is a domain, cM is torsion-free. For any nonzero $a \in R$, the chain

$$cM \supseteq acM \supseteq a^2cM \supseteq \cdots$$

must be eventually constant, since each term is characteristic. Choose r such that $a^r cM = a^{r+1}cM$; then $cM = acM$ since $a^r \neq 0$ and cM is torsion-free. This holds for all nonzero a, so $cM \subseteq M_d$. On the other hand, $M_d \subseteq cM$, so $M_d = cM$. In the exact sequence

$$0 \to M_c \to M \xrightarrow{c} cM \to 0,$$

since M is torsion-free and since we proved $cM = ccM$ above, the submodule cM of the middle term M is mapped isomorphically to $ccM = cM$ on the right. Thus the sequence splits, so $M = M_c \oplus cM = M_t \oplus M_d$. □

Proof of Lemma 1.3. Set $M = K$ and $R = \mathbb{F}_p[F]$. Any field automorphism of K is an R-module automorphism, because Frobenius commutes with all field automorphisms. Characteristic submodules are unions of orbits under $\mathrm{Aut}(K)$, so there are at most finitely many. Moreover, $M_t = \mathbb{F}_q$ because $\mathbb{F}_q$ is integrally closed in K. The condition characterizing Tr in Lemma 1.3 says that $\mathrm{id}_K - \mathrm{Tr}$ maps K into M_d. If $\mathrm{Tr}\colon K \to \mathbb{F}_q$ is any map satisfying this condition, then id_K decomposes as the sum of Tr (which maps K into $\mathbb{F}_q = M_t$) and $\mathrm{id}_K - \mathrm{Tr}$ (which maps K into M_d); thus Tr can only be the projection $M \to M_t$ in the decomposition $M \simeq M_t \oplus M_d$ of Lemma 1.6.

We now observe that the map Tr defined this way has the claimed properties. By construction, Tr satisfies the condition involving $P(F)$. By Lemma 1.6, $M_d = (F^e - 1)M$, which is an $\mathbb{F}_q$-subspace of K. Since Tr is a projection for a decomposition $M_t \oplus M_d$ into $\mathbb{F}_q$-subspaces, it is an $\mathbb{F}_q$-linear map satisfying $\mathrm{Tr}(\mathrm{Tr}(x)) = \mathrm{Tr}(x)$. Since F maps M_t and M_d into themselves, $\mathrm{Tr}(F(x)) = F(\mathrm{Tr}(x))$ holds. By uniqueness, Tr is equivariant for field automorphisms, so Tr is constant on orbits of $\mathrm{Aut}(K/\mathbb{F}_q)$. □

In the notation of the previous proof, F maps $M_t = \mathbb{F}_q$ onto itself, and maps M_d onto itself, so K is perfect. For $x \in K$ and $n \in \mathbb{Z}$, define $s_n(x) = \mathrm{Tr}(x^{1+p^n}) = \mathrm{Tr}(xF^n(x))$.

Lemma 1.7. *There exists $m \in \mathbb{Z}_{\geq 1}$ such that $s_{m+n}(x) = s_n(x)$ for all $x \in K$ and $n \in \mathbb{Z}$.*

Proof. Since $\mathrm{Aut}(K/\mathbb{F}_q)$ has finite index in $\mathrm{Aut}(K)$, the set S of $\mathrm{Aut}(K/\mathbb{F}_q)$-orbits is finite. Let $\sim$ be the equivalence relation on K induced by this partition. For each positive integer

i divisible by e, the map $x \mapsto F^i(x) - x$ induces a map $S \to S$. Since S is finite, there exist $i < j$ for which these maps coincide. (Thanks to Bergman for pointing this out, thus supplanting a more complicated construction.) For $n \in \mathbb{Z}$ and $x \in K$, we have

$$F^n(F^i(x) - x) \cdot (F^i(x) - x) \sim F^n(F^j(x) - x) \cdot (F^j(x) - x),$$

which expands to

$$\begin{aligned} &F^{n+i}(x)F^i(x) - F^n(x)F^i(x) - F^{n+i}(x)x + F^n(x)x \\ &\sim F^{n+j}(x)F^j(x) - F^n(x)F^j(x) - F^{n+j}(x)x + F^n(x)x. \end{aligned}$$

Applying Tr, and using the fact that F^i and F^j act trivially on the image of Tr, we get

$$\begin{aligned} s_n(x) - s_{n-i}(x) - s_{n+i}(x) + s_n(x) &= s_n(x) - s_{n-j}(x) - s_{n+j}(x) + s_n(x) \\ s_{n+j}(x) - s_{n+i}(x) - s_{n-i}(x) + s_{n-j}(x) &= 0. \end{aligned}$$

For fixed x, this linear recurrence implies that the sequence $(s_n(x))_{n\in\mathbb{Z}}$ is periodic (since $s_n(x) \in \mathbb{F}_q$ for all n). The coefficients of the recurrence are independent of x, so only finitely many sequences are possible, so one can find a uniform period that works for all x. □

Lemma 1.8. *Suppose $x \in K$ satisfies $\mathrm{Tr}(x) = 0$. Then $\mathrm{Tr}(x^2) = 0$. If moreover $p = 2$, then $\mathrm{Tr}(x^3) = 0$ also.*

Proof. Choose m as in Lemma 1.7. Replace m by a multiple if necessary, to assume that e divides m. Since $\mathrm{Tr}(x) = 0$, there exists $y \in K$ such that $F^m y - y = x$. Now

$$\begin{aligned} \mathrm{Tr}(x^2) &= \mathrm{Tr}((y^{p^m} - y)^2) = \mathrm{Tr}(y^{2p^m}) - 2\,\mathrm{Tr}(y^{p^m+1}) + \mathrm{Tr}(y^2) \\ &= s_0(y)^{p^m} - 2s_m(y) + s_0(y) = 2s_0(y) - 2s_m(y) = 0. \end{aligned}$$

In case $p = 2$, we also have

$$\begin{aligned} \mathrm{Tr}(x^3) &= \mathrm{Tr}((y^{2^m} + y)^3) = \mathrm{Tr}(y^{3\cdot 2^m}) + \mathrm{Tr}(y^{2^{m+1}+1}) + \mathrm{Tr}(y^{2^m+2}) + \mathrm{Tr}(y^3) \\ &= s_1(y)^{2^m} + s_{m+1}(y) + s_{m-1}(y^2) + s_1(y) \\ &= s_1(y) + s_{-1}(y^2) = \mathrm{Tr}(y^3) + \mathrm{Tr}(y^3) = 0. \end{aligned}$$

□

Proof of Theorem 1.1. We claim that $K = \mathbb{F}_q$. If not, then there exists $x \in K^*$ with $\mathrm{Tr}(x) = 0$. Let $c = \mathrm{Tr}(x^{-1})$. Lemma 1.8 implies

$$\begin{aligned} 0 &= \mathrm{Tr}((x + x^{-1} - c)^2) \\ &= \mathrm{Tr}(x^2) + 2\,\mathrm{Tr}(1) - 2c\,\mathrm{Tr}(x) + \mathrm{Tr}((x^{-1} - c)^2) = 0 + 2 - 0 + 0, \end{aligned}$$

which is a contradiction if $p \neq 2$. If $p = 2$, applying Lemma 1.8 repeatedly yields

$$\begin{aligned} 0 &= \mathrm{Tr}((x^2 + x^{-1} - c)^3) = \mathrm{Tr}((x^4 + (x^{-2} + c^2))(x^2 + (x^{-1} + c))) \\ &= \mathrm{Tr}(x^6) + (\mathrm{Tr}(x^3) + c\,\mathrm{Tr}(x^4)) + (1 + c^2\,\mathrm{Tr}(x^2)) + \mathrm{Tr}((x^{-1} - c)^3) \\ &= 0 + 0 + 0 + 1 + 0 + 0, \end{aligned}$$

again a contradiction. □

Remark 1.9. Lenstra points out an alternate argument for $p \neq 2$: Lemma 1.8 and the identity $xy = \frac{(x+y)^2 - x^2 - y^2}{2}$ imply that $\ker(\mathrm{Tr})$ is closed under multiplication. Then

$$K \cdot \ker(\mathrm{Tr}) = (\mathbb{F}_q + \ker(\mathrm{Tr}))\ker(\mathrm{Tr}) \subseteq \ker(\mathrm{Tr})$$

so $\ker(\mathrm{Tr})$ is an ideal of K. Since $\mathrm{Tr}|_{\mathbb{F}_q}$ is not identically zero, $\ker(\mathrm{Tr})$ can be only the zero ideal, so $K = \mathbb{F}_q$.

Remark 1.10. Here are two model-theoretic statements for a field K that are equivalent to Theorem 1.1:

(1) If the set of definable subsets of K (i.e., $\emptyset$-definable subsets in the language of rings) is finite, then K is finite.
(2) If the set of complete 1-types realized by elements of K is finite, then K is finite.

Statements 1 and 2 are equivalent to each other, because their hypotheses are equivalent: the set of elements of K having a given type is by definition an intersection of definable subsets. Statement 1 implies Theorem 1.1, since each definable subset of K is a union of $\mathrm{Aut}(K)$-orbits.

Finally, let us prove that Theorem 1.1 implies Statement 2. Let K be a field in which only finitely many complete 1-types are realized. By Theorem 9.14 of [Po] (with the comments preceding Theorem 9.13 of [Po]), or by Exercise 10.2.5 of [Ho], there exists an elementary extension L of K that is strongly ω-homogeneous. Since L is an elementary extension, every element of L is of one of the finitely many types realized by elements of K. But L is strongly ω-homogeneous, so any two elements of L of the same type are in the same orbit of $\mathrm{Aut}(L)$. Thus L has finitely many orbits. Applying Theorem 1.1 to L, we find that L is finite. So its subfield K also is finite.

Remark 1.11. One may ask to what extent Theorem 1.1 may be generalized to larger classes of rings; that is, one may ask for which classes of infinite rings R does $\mathrm{Aut}(R)$ always act with infinitely many orbits. For example, we do not know whether there exists an infinite integral domain R such that $\mathrm{Aut}(R)$ has finitely many orbits on R: the proof of Theorem 1.1 seems inadequate to treat this case, since the formal properties of Tr are satisfied, for instance, by the constant coefficient map $\mathbb{F}_q[[t]] \to \mathbb{F}_q$.

Remark 1.12. We can construct infinite commutative rings with finitely many orbits. If V is a nonzero vector space over $\mathbb{F}_p$, then the ring $R = \mathbb{F}_p \oplus V$ in which $vw = 0$ for all $v, w \in V$ carries an action of the group $\mathrm{GL}(V)$, and there are $2p$ orbits, namely $\{a\}$ and $\{a\} + (V - \{0\})$ for all $a \in \mathbb{F}_p$.

Remark 1.13. Here is an example of an infinite *reduced* (but disconnected) commutative ring whose automorphism group acts with finitely many orbits. Let C be the Cantor set, and let R be the ring of continuous functions from C with its usual topology to $\mathbb{F}_p$ with the discrete topology. Since every nonempty open subset of C is homeomorphic to C itself, the group $\mathrm{Aut}(C)$ of homeomorphisms from C to C acts transitively on the set of labeled partitions of C into any fixed finite number of disjoint nonempty open subsets. In particular, two elements of R lie in the same orbit of $\mathrm{Aut}(R)$ if and only if they have the same image (as functions to $\mathbb{F}_p$); hence $\mathrm{Aut}(R)$ acts on R with $2^p - 1$ orbits.

2. Fields with relatively few orbits

The term "relatively" in the section title refers to automorphisms of one field relative to a subfield. The following conjecture includes Theorem 1.1.

Conjecture 2.1. *Let K/k be a nontrivial extension of fields. Then the number of orbits of $\mathrm{Aut}(K/k)$ on $K-k$ is finite if and only if k and K are either both finite or both algebraically closed.*

The "if" part holds: for finite fields it is trivial, and for algebraically closed fields it follows from the theory of transcendence bases.

Remark 2.2. In Remark 1.10, we mentioned a model-theoretic strengthening of Theorem 1.1 in which the hypothesis of finitely many $\mathrm{Aut}(K)$-orbits was replaced by the weaker hypothesis of finitely many definable subsets. Similarly we could ask whether for a model-theoretic strengthening of Conjecture 2.1 in which the hypothesis is weakened to say only that

$$\{S \cap (K-k) : S \text{ is a subset of } K \text{ definable over } k\}$$

is finite, or equivalently that the set of types over k realized by elements of $K-k$ is finite. (The equivalence follows, since the set of elements of $K-k$ of a given type over k is an intersection of sets of the form $S \cap (K-k)$ with S definable over k.) These equivalent statements imply Conjecture 2.1, but it is not clear whether they are implied by Conjecture 2.1.

For the rest of this section, we assume that

$$\boxed{\text{The number of orbits of } \mathrm{Aut}(K/k) \text{ on } K-k \text{ is finite.}}$$

$$\boxed{\text{The field } K \text{ is infinite.}}$$

and hope to prove that k and K are algebraically closed. We do not succeed, but we deduce a number of facts restricting the possibilities for k and K.

Proposition 2.3. *The field k is infinite.*

Proof. If k is finite, then the number of orbits of $\mathrm{Aut}(K/k)$ on $K = (K-k) \cup k$ is finite, so the number of orbits of $\mathrm{Aut}(K)$ on K is finite, contradicting Theorem 1.1. □

Proposition 2.4. *The field k is integrally closed in K.*

Proof. Suppose the integral closure ℓ of k in K were not k. Since k is infinite, $\ell - k$ would be infinite, so $K-k$ would contain infinitely many finite orbits, a contradiction. □

Proposition 2.5. *Both k and K are perfect.*

Proof. Suppose they are of characteristic p. Let F be the Frobenius endomorphism of K, as in Section 1. Let $S_n = F^n(K-k) - F^{n+1}(K-k)$. The S_n are disjoint, and each is a union of orbits of $\mathrm{Aut}(K/k)$, so some S_n is empty. But F defines a bijection $S_m \to S_{m+1}$ for each m, so S_0 is empty. In other words, $K-k \subseteq K^p$. Taking differences of elements, we obtain $K \subseteq K^p$, so K is perfect. By Proposition 2.4, k also is perfect. □

For $x, y \in K-k$, we redefine $x \sim y$ to mean that x and y belong to the same orbit of $\mathrm{Aut}(K/k)$. The following lemma arose out of a discussion with Bergman.

Lemma 2.6. *If $x \in K-k$ and $c \in k$, then $x \sim x+c$.*

Proof. For $a \in k^*$ and $b \in k$, the linear map $L_{a,b}\colon K \to K$ given by $x \mapsto ax + b$ permutes the additive cosets of k in K. Let G be the group formed by these maps; then G acts on the $\mathrm{Aut}(K/k)$-orbits in $K - k$ (since G commutes with the action of $\mathrm{Aut}(K/k)$). There is a normal subgroup H of G of finite index that acts trivially on these orbits. Let $n = (G : H)$. Then $L_{a^n,0} = L_{a,0}^n \in H$ for all $a \in k^*$. Taking a commutator with $L_{1,1}$ shows that $L_{1,a^n-1} \in H$ for any $a \in k^*$. By the following lemma, $L_{1,c} \in H$ for all $c \in k$. By the definition of H, we get $x \sim x + c$ for all $x \in K - k$ and $c \in k$. □

Lemma 2.7. *Let k be an infinite perfect field. Then for any positive integer n, the additive group of k is generated by elements of the form $a^n - 1$ for $a \in k^*$.*

Proof. Since k is perfect, we may assume without loss of generality that n is not divisible by the characteristic of k. Let G be the additive subgroup of k generated by elements of the form $a^n - 1$ for $a \in k^*$. Since

$$(a^n - 1)(b^n - 1) = [(ab)^n - 1] - (a^n - 1) - (b^n - 1),$$

G is closed under multiplication.

Since k is infinite, so is G, and we can fix distinct nonzero $g_1, \ldots, g_n \in G$. Then for all but finitely many $x \in k$, the element $\gamma_i := (g_i x + 1)^n - 1$ is in G for $i = 1, \ldots, n$. If we expand using the binomial theorem, and view the γ_i as the right-hand sides of a system of linear equations in the "variables" $\binom{n}{1}x$, $\binom{n}{2}x^2$, $\ldots$, $\binom{n}{n}x^n$, then Cramer's Rule gives a formula $D\binom{n}{1}x = D'$, where $D = \det(g_i^j)_{1 \le i,j \le n} \neq 0$, and D' is given by some polynomial in the g_i and γ_i with integer coefficients and no constant term. By the previous paragraph, $D' \in G$. Thus $Dnx \in G$ for all but finitely many $x \in k$. Since Dn is nonzero and independent of x, the elements Dnx exhaust all but finitely many elements of k. Thus $k - G$ is finite.

On the other hand, $k - G$ is a union of cosets of the infinite group G, so $k - G = \emptyset$. Hence $G = k$. □

Lemma 2.8. *Let R be a ring, and let M be an R-module. For each $r \in R$, let M_r be the submodule of M annihilated by r. Suppose that $f \in R$ is such that M_f has no nonzero proper submodules. Also suppose that there is a proper submodule N of M such that the sequence $(f^m(M - N))_{m \ge 1}$ has only finitely many distinct sets. Then for some $n \ge 0$, $f^n M = f^{n+1} M$ and M is the direct sum of M_{f^n} and $f^n M$.*

Proof. Since $M - N$ generates M as a module, the sequence $(f^m M)_{m \ge 1}$ also contains only finitely many sets. But this sequence is decreasing, so $f^m M = f^{m+1} M$ for some m.

Let n be the smallest nonnegative integer such that $f^n M = f^{n+1} M$. If $n = 0$, we are done, so assume $n > 0$. Applying f yields $f^{n+1} M = f^{n+2} M$ and so on, so $f^n M = f^{n'} M$ for all $n' \ge n$. Thus, in the exact sequence

$$0 \to M_{f^n} \to M \xrightarrow{f^n} f^n M \to 0,$$

the submodule $f^n M$ of M in the middle surjects onto $f^{2n} M = f^n M$ on the right. In particular, $M_{f^n} + f^n M = M$.

It remains to show that $M_{f^n} \cap f^n M = 0$. If not, let f^e be the smallest power of f annihilating $M_{f^n} \cap f^n M$; then $f^{e-1}(M_{f^n} \cap f^n M)$ is a nonzero submodule of $M_f \cap f^n M$. The hypothesis on M_f implies $M_f \cap f^n M = M_f$, so $M_f \subseteq f^n M$.

Applying f^{n-1} to $M_{f^n} + f^n M = M$ yields

$$f^{n-1} M \subseteq M_f + f^{2n-1} M = M_f + f^n M = f^n M$$

contradicting the minimality of n. $\square$

Remark 2.9. If under the hypotheses of Lemma 2.8 one has also $f^n M = M$, then $M \xrightarrow{f} M$ is surjective. (This is because $M = f^n M = f^{n+1} M = f(f^n M) = f(M)$.)

Proposition 2.10. *For each $l \geq 1$, the l-th power maps on k and K are surjective.*

Proof. Since k is integrally closed in K, it suffices to prove the result for K. We may reduce to the case that l is prime. By Proposition 2.5, we may assume l is not the characteristic of k.

The hypotheses of Lemma 2.8 with $R = \mathbb{Z}$, $M = K^*$, $N = k^*$, and $f = l$ (the l-th power map) hold since each set $f^m(K^* - k^*)$ is a union of $\mathrm{Aut}(K/k)$-orbits in $K - k$. Let $N\colon K^* \to (K^*)_{l^n}$ be the projection $M \to M_{f^n}$ given by the direct sum decomposition in Lemma 2.8. The construction of N is invariant under $\mathrm{Aut}(K/k)$, so $x \sim y$ implies $N(x) \sim N(y)$, which in turn implies $N(x) = N(y)$ because $N(x)$ and $N(y)$ are in $(K^*)_{l^n} = (k^*)_{l^n} \subseteq k$.

By Lemma 2.6, for any $x \in K - k$, we have $x^{-1} \sim x^{-1} + 1$, so $N(x^{-1}) = N(x^{-1} + 1)$. Multiplying by $N(x)$, we get $1 = N(1 + x)$. In other words, $N(y) = 1$ for all $y \in K - k$, and hence for all $y \in K^*$. Thus $M = f^n M$. By Remark 2.9, f is surjective; that is, the l-power map on K^* is surjective. $\square$

Our next proposition is an additive analogue of Proposition 2.10. Call a polynomial $P(x)$ *additive* if $P(x + y) = P(x) + P(y)$ as polynomials.

Proposition 2.11. *Every nonzero additive polynomial over k induces surjective maps on k and K.*

In particular, k satisfies (the field-theoretic component of) Kaplansky's "Hypothesis A"; see the next section.

Proof. We may assume $\mathrm{char}(k) = p > 0$. It suffices to consider additive polynomials P of degree > 1 that cannot be written as the composite of two other additive polynomials of degree > 1. We will apply Lemma 2.8 with $R = \mathbb{F}_p[P]$ (the subring generated by P in the endomorphism ring of the additive group of K), $M = K$, $N = k$, and $f = P$. As in the proof of Proposition 2.10, each set $f^m(M - N)$ is a union of $\mathrm{Aut}(K/k)$-orbits in $K - k$. We need also to check that the kernel of $P\colon K \to K$ has no nonzero proper submodules. This holds, because by Proposition 1.8.2 of [G] such a submodule Z would give rise to a nontrivial factorization $P = Q \circ R$ of additive polynomials over k where $R(x) = \prod_{\alpha \in Z}(x - \alpha)$ is in $k[x]$ (each α is in k, since k is integrally closed in K).

Let $\mathrm{Tr}\colon K \to \ker(P^n)$ be the projection $M \to M_{f^n}$ given by the direct sum decomposition in Lemma 2.8. Again $x \sim y$ implies $\mathrm{Tr}(x) = \mathrm{Tr}(y)$. For $x \in K - k$ and $c \in \ker(P^n) \subseteq k$ we have $x \sim x + c$ by Lemma 2.6. Applying Tr yields $\mathrm{Tr}(x) = \mathrm{Tr}(x) + c$, so $\ker(P^n) = 0$. By Remark 2.9, P is surjective on K. Since k is integrally closed in K, P is surjective on k also. $\square$

Proposition 2.12. *The field K has no nontrivial abelian extensions. The same is true of k.*

Proof. Because k is integrally closed in K, it suffices to prove that K has no abelian extensions of degree $n \geq 2$. We prove this by strong induction on n.

Suppose that $n \geq 2$, and the result is known for every $n' < n$.

Case 1: n is not prime. The result for n follows from the result for the prime factors of n.

Case 2: $n = \mathrm{char}(k)$. By Proposition 2.11, the map $x \mapsto x^n - x$ on K is surjective, so by Artin-Schreier theory, K has no abelian extension of degree n.

Case 3: n is a prime other than $\mathrm{char}(k)$. Adjoining all n-th roots of unity to K gives an abelian extension of degree at most $\phi(n) < n$; by the inductive hypothesis this extension is trivial. Thus the n-th roots of unity are already in K. By Kummer theory, all abelian extensions of K of degree n are contained in the field K_n obtained by adjoining the n-th roots of all elements of K. Proposition 2.10 implies that $K_n = K$, so abelian extensions of K of degree n do not exist. □

Corollary 2.13. *The field K is radically closed (that is, if $x \in \overline{K}$ and $x^n \in K$ for some $n \geq 1$, then $x \in K$). The same is true of k.*

Corollary 2.14. *If $\mathrm{char}(k) = p > 0$, then k contains an algebraic closure of $\mathbb{F}_p$.*

3. Automorphisms of Mal'cev-Neumann fields

For k a field and G an ordered abelian group, the *Mal'cev-Neumann field* $k((t^G))$ is the set of formal sums $\sum_{i \in G} c_i t^i$ whose *support* $\{i : c_i \neq 0\}$ is a well-ordered subset of G; multiplication is given by formal series convolution

$$\left(\sum_{i \in G} c_i t^i\right)\left(\sum_{i \in G} d_i t^i\right) = \sum_{i \in G}\left(\sum_{j \in G} c_j d_{i-j}\right) t^i.$$

This construction actually dates back to Hahn [Ha], but the names of Mal'cev and Neumann are often associated to this field because they generalized the construction to the case of a division ring k and a nonabelian ordered group G, in which case $k((t^G))$ is a division ring. The elements of $k((t^G))$ are sometimes also called "generalized power series".

There is a natural inclusion of fields $k \hookrightarrow k((t^G))$ mapping c to ct^0. Suppose $x = \sum_{i \in G} c_i t^i \in k((t^G))^*$. The smallest j such that $c_j \neq 0$ is called the *valuation* $v(x)$ of x. For that j, we call $c_j t^j$ the *leading term* of x, and call c_j the *leading coefficient* of x. Call x *monic* if its leading coefficient is 1. The map $v \colon k((t^G))^* \to G$ is a valuation in the usual sense. Define $v(0) := \infty$. The disjoint union $G \cup \{\infty\}$ is ordered so that $g < \infty$ for all $g \in G$.

From now on, we take $G = \mathbb{Q}$. Then $k((t^{\mathbb{Q}}))$ has an absolute value defined by $|x| := e^{-v(x)}$ for nonzero x. Let $\mathrm{Aut}_{\mathrm{conts}}(k((t^{\mathbb{Q}}))/k)$ be the group of continuous automorphisms of $k((t^{\mathbb{Q}}))$ whose restriction to k is the identity. A continuous automorphism ϕ need not preserve the valuation, but it is easy to show that for each ϕ there exists $r \in \mathbb{Q}_{>0}$ such that $v(\phi(x)) = rv(x)$.

3.1. Automorphisms in the presence of Hypothesis A.

Theorem 3.1. *Suppose that k is a field of characteristic 0. For any monic $x \in k((t^{\mathbb{Q}}))^*$ of positive valuation there exists $\phi_x \in \mathrm{Aut}_{\mathrm{conts}}(k((t^{\mathbb{Q}}))/k)$ mapping t to x, defined by "substitution".*

Proof. We will define $\phi_x(\sum c_i t^i)$ as $\sum c_i x^i$, but we need to make sense of the latter.

Write $x = t^m(1 + \epsilon)$ where $m \in \mathbb{Q}_{>0}$ and $v(\epsilon) > 0$. Define $x^i = t^{mi} \sum_{n=0}^{\infty} \binom{i}{n} \epsilon^n$; since $v(\epsilon^n) \to \infty$, the series converges to an element of $k((t^{\mathbb{Q}}))$. Next, if one substitutes this definition of x^i into $\sum c_i x^i$, one obtains a double series of monomials in t such that there are only finitely many monomials having a given exponent, and the set of all occurring exponents

is well-ordered; this follows from the following standard lemmas. (Here $S_1 + \cdots + S_n := \{ s_1 + \cdots + s_n : s_i \in S_i \text{ for all } i \}$ and $nS := S + \cdots + S$.)

(i) If $S_1, \ldots, S_n$ are well-ordered subsets of $\mathbb{Q}$, then $S_1 + \cdots + S_n$ is well-ordered ([Pa, Lemma 13.2.9(ii)] in the key case $n = 2$).

(ii) If $S_1, \cdots, S_n$ are well-ordered subsets of $\mathbb{Q}$, then for any $x \in \mathbb{Q}$, the number of n-tuples $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ such that $s_1 + \cdots + s_n = x$ is finite ([Pa, Lemma 13.2.9(i)] in the key case $n = 2$).

(iii) If S is a well-ordered subset of $\mathbb{Q} \cap (0, +\infty)$, then $\tilde{S} = \cup_{n=1}^{\infty} nS$ also is well-ordered; moreover, $\cap_{n=1}^{\infty} n\tilde{S} = \emptyset$ [Pa, Lemma 13.2.10].

Collecting terms with the same exponent, we obtain an element of $k((t^{\mathbb{Q}}))$, and we define $\phi_x(\sum c_i t^i)$ to be this element.

A similar argument shows that ϕ_x respects addition and multiplication. It also acts as the identity on k. Looking at leading terms shows that if $y \in k((t^{\mathbb{Q}}))^*$, then

$$v(\phi_x(y)) = v(x)v(y). \tag{1}$$

In particular, ϕ_x is injective and continuous. Also by (1), $k((t^{\mathbb{Q}}))$ is an immediate extension of $\phi_x(k((t^{\mathbb{Q}})))$, but the latter is abstractly isomorphic to $k((t^{\mathbb{Q}}))$ and hence is maximally complete (see [Ka1] for definitions). Thus this immediate extension is trivial. Hence ϕ_x is an automorphism. □

Remark 3.2. The proof of Theorem 3.1 does not work in characteristic $p > 0$, as we now explain. The binomial theorem does not apply to $(1 + \epsilon)^i$ if p divides the denominator of i. Instead one must write $i = p^b q$ where $b \in \mathbb{Z}$ and $q \in \mathbb{Q}$ has denominator not divisible by p, and define

$$(1 + \epsilon)^i = ((1 + \epsilon)^q)^{p^b}$$

where $(1+\epsilon)^q$ is defined using the binomial theorem, and the map $z \mapsto z^{p^b}$ is defined termwise. But now if $x = t - t^2$ and $y = t^{-1/p} + t^{-1/p^2} + \ldots$, then $\phi_x(y)$ makes no sense, since a short calculation shows that the double series that should represent it has infinitely many terms of valuation 0.

The phenomenon in Remark 3.2 was observed already by Kaplansky in the course of his study of immediate maximal extensions of valued fields [Ka1]; this study hinges on a key definition, which we now recall.

Hypothesis A. If k is a field of characteristic $p > 0$ and G is an ordered abelian group, say that the pair (k, G) *satisfies Hypothesis A* is satisfied if the following two conditions hold:

(1) Every nonzero additive polynomial over k induces a surjective map from k to itself; i.e., for any $a_0, \ldots, a_n \in k$ not all zero and any $b \in k$, the equation

$$a_n x^{p^n} + \cdots + a_1 x^p + a_0 x = b$$

has a solution $x \in k$. (In particular, k is perfect.)

(2) The group G is p-divisible, i.e., $pG = G$.

If G is omitted, we say that k satisfies Hypothesis A if the first condition above holds. As discussed in [Ka2, pp. 20–21], Whaples [W] proved that k satisfies Hypothesis A if and only if k has no finite extension of degree divisible by p. If instead k has characteristic 0, then by convention, k and (k, G) satisfy Hypothesis A.

We now have the following generalization of Theorem 3.1.

Theorem 3.3. *Suppose that k is a field satisfying Hypothesis A. For any monic $x \in k((t^{\mathbb{Q}}))^*$ of positive valuation there exists $\phi_x \in \mathrm{Aut}_{\mathrm{conts}}(k((t^{\mathbb{Q}}))/k)$ mapping t to x.*

Proof. Let $k(t^{\mathbb{Q}})$ be the subfield of $k((t^{\mathbb{Q}}))$ generated by k and t^i for all $i \in \mathbb{Q}$. For $i \in \mathbb{Q}$, define $x^i \in k((t^{\mathbb{Q}}))$ as in the proof of Theorem 3.1, using the modifications outlined in Remark 3.2. Let $k(x^{\mathbb{Q}})$ be the subfield of $k((t^{\mathbb{Q}}))$ generated by k and x^i for all $i \in \mathbb{Q}$. If we forget the embeddings into $k((t^{\mathbb{Q}}))$, then there is a k-isomorphism $k(t) \to k(x)$ mapping t to x; this extends to a k-isomorphism $k(t^{\mathbb{Q}}) \to k(x^{\mathbb{Q}})$ mapping t^i to x^i for each $i \in \mathbb{Q}$. Now $k((t^{\mathbb{Q}}))$ is a maximally complete immediate extension of both $k(t^{\mathbb{Q}})$ and $k(x^{\mathbb{Q}})$ (see [Ka1] for definitions), so by [Ka1, Theorem 5], the k-isomorphism $k(t^{\mathbb{Q}}) \to k(x^{\mathbb{Q}})$ extends to a continuous automorphism $k((t^{\mathbb{Q}})) \to k((t^{\mathbb{Q}}))$ (still mapping t to x). □

Theorem 3.4. *Suppose that k is a radically closed field satisfying Hypothesis A. Define*

$$S_0 = \{\, y \in k((t^{\mathbb{Q}}))^* : v(y) > 0 \,\}$$
$$S_\infty = \{\, y \in k((t^{\mathbb{Q}}))^* : v(y) < 0 \,\}$$
$$S_c = c + S_0 \qquad \text{for } c \in k.$$

Then the S_c for $c \in k$ and S_∞ are all the orbits of $\mathrm{Aut}_{\mathrm{conts}}(k((t^{\mathbb{Q}}))/k)$ on $k((t^{\mathbb{Q}})) - k$.

Proof. For any group homomorphism $\lambda\colon \mathbb{Q} \to k^*$, define $\psi_\lambda \in \mathrm{Aut}_{\mathrm{conts}}(k((t^{\mathbb{Q}}))/k)$ by

$$\psi_\lambda\left(\sum c_i t^i\right) = \sum \lambda(i) c_i t^i.$$

Given $i > 0$ and $a \in k^*$, we can find λ such that $\psi_\lambda(t^i) = at^i$, since k is radically closed. Thus every element of S_0 is in the same orbit as a monic element of S_0. By Theorem 3.3, every monic element of S_0 is in the same orbit as t. Thus S_0 is contained in an orbit.

On the other hand, S_0 is preserved by each continuous automorphism of $k((t^{\mathbb{Q}}))$, since

$$S_0 = \{\, x \in k((t^{\mathbb{Q}}))^* : x^n \to 0 \text{ as } n \to \infty \,\}.$$

Thus S_0 is an orbit.

The maps $x \mapsto x + c$ for $c \in k$ and $x \mapsto x^{-1}$ are $\mathrm{Aut}_{\mathrm{conts}}(k((t^{\mathbb{Q}}))/k)$-equivariant bijections from $k((t^{\mathbb{Q}})) - k$ to itself, so they map orbits to orbits. Thus each S_c is an orbit, and S_∞ is an orbit. Their union is all of $k((t^{\mathbb{Q}})) - k$, so they are all the orbits. □

Remark 3.5. If we used $\mathrm{Aut}(k((t^{\mathbb{Q}}))/k)$ in place of $\mathrm{Aut}_{\mathrm{conts}}(k((t^{\mathbb{Q}}))/k)$, the orbits could be even larger. For example, if k is algebraically closed, then $k((t^{\mathbb{Q}}))$ is algebraically closed, so $k((t^{\mathbb{Q}})) - k$ consists of one orbit under $\mathrm{Aut}(k((t^{\mathbb{Q}}))/k)$.

3.2. **Automorphisms in the absence of Hypothesis A.** Now, in the spirit of [Ka1, Section 5], we consider what happens when Hypothesis A fails in the field aspect; we find that $k((t^{\mathbb{Q}}))$ has very few endomorphisms over k.

Theorem 3.6. *Let k be a perfect field not satisfying Hypothesis A. Then the endomorphisms of $k((t^{\mathbb{Q}}))$ over k are the maps of the form*

$$\sum_i c_i t^i \mapsto \sum_i \lambda(i) c_i t^{ri}$$

where $\lambda\colon \mathbb{Q} \to k^*$ is a group homomorphism and $r \in \mathbb{Q}_{>0}$.

In particular all endomorphisms of $k((t^{\mathbb{Q}}))$ are automorphisms, and they are all continuous.

Corollary 3.7. *If k is finite, then the endomorphisms of $k((t^{\mathbb{Q}}))$ over k are the maps of the form $\sum c_i t^i \mapsto \sum c_i t^{ri}$ where $r \in \mathbb{Q}_{>0}$.*

Proof. If $q = \#k$, then $x^q - x = 1$ has no solution in k, so k does not satisfy Hypothesis A. Apply Theorem 3.6 and observe that every group homomorphism $\lambda\colon \mathbb{Q} \to k^*$ is trivial. □

We will deduce Theorem 3.6 from a slightly more general result, Theorem 3.9 below. Let $\mathrm{Tr}\colon k((t^{\mathbb{Q}})) \to k$ be the "trace" map carrying a series $x = \sum c_i t^i$ to its constant coefficient c_0. For any field K with $k \subseteq K \subseteq k((t^{\mathbb{Q}}))$, let $K^{\mathrm{Tr}} = \{\, x \in K : \mathrm{Tr}(x) = 0 \,\}$; this is a k-subspace of K. Let p be the characteristic of k.

Lemma 3.8. *If k is perfect, then each nonzero additive polynomial P over k maps $k((t^{\mathbb{Q}}))^{\mathrm{Tr}}$ bijectively to itself.*

Proof. The additive polynomials $x \mapsto x^p$ and $x \mapsto ax$ for $a \in k$ map $k((t^{\mathbb{Q}}))^{\mathrm{Tr}}$ into itself. Any additive polynomial can be built from these using composition and addition, so P maps $k((t^{\mathbb{Q}}))^{\mathrm{Tr}}$ into itself. Since k is integrally closed in $k((t^{\mathbb{Q}}))$, each P acts injectively on $k((t^{\mathbb{Q}}))^{\mathrm{Tr}}$.

It remains to show that $P\colon k((t^{\mathbb{Q}}))^{\mathrm{Tr}} \to k((t^{\mathbb{Q}}))^{\mathrm{Tr}}$ is surjective. The result is true for $x \mapsto x^p$ so we may reduce to the case in which P is separable. By additivity, it suffices to solve $P(x) = b$ in the following two cases.

Case 1: b has only positive exponents.

Then $v(b) > 0$. Since the lowest degree monomial in P has degree 1, there exists a formal power series solution

$$c_0 b + c_1 b^p + c_2 b^{p^2} + \cdots$$

with coefficients in k; this converges to an actual solution to $P(x) = b$.

Case 2: b has only negative exponents.

Since k is perfect, one can solve for coefficients $c_i \in k$ making

$$c_n b^{1/p^n} + c_{n+1} b^{1/p^{n+1}} + \cdots \tag{2}$$

a formal solution, where $\deg P = p^n$. Since b has only negative exponents, the same is true for each b^{1/p^m}. Moreover, given $\epsilon > 0$, only finitely many of the b^{1/p^m} contribute monomials with exponents more negative than $-\epsilon$. Thus the series (2) makes sense as an element of $k((t^{\mathbb{Q}}))^{\mathrm{Tr}}$; moreover, it represents a solution to $P(x) = b$. □

Theorem 3.9. *Let k be a perfect field not satisfying Hypothesis A. Suppose K is a field such that $k(t^{\mathbb{Q}}) \subseteq K \subseteq k((t^{\mathbb{Q}}))$ and $P(K^{\mathrm{Tr}}) = K^{\mathrm{Tr}}$ for each nonzero additive polynomial P over k. Then the k-homomorphisms $s\colon K \to k((t^{\mathbb{Q}}))$ are the maps of the form*

$$\sum_i c_i t^i \mapsto \sum_i \lambda(i) c_i t^{ri}$$

where $\lambda\colon \mathbb{Q} \to k^*$ is a group homomorphism and $r \in \mathbb{Q}_{>0}$.

Remark 3.10. In the special case where k is a finite field $\mathbb{F}_q$, a slight modification of our proof (left to the reader) shows that the hypothesis $P(K^{\mathrm{Tr}}) = K^{\mathrm{Tr}}$ need be assumed only for $P(x) = x^q - x$.

Remark 3.11. Theorem 3.9 applies, for instance, when k is a perfect field not satisfying Hypothesis A and K is the integral closure of $k(t)$ or $k((t))$ in $k((t^{\mathbb{Q}}))$. (Both of these integral closures can be described fairly explicitly: see [Ke1, Ke2].)

The rest of this section will be devoted to proving Theorem 3.9. We thus assume for the remainder of this section that

$$\boxed{\text{The field } k \text{ is perfect and does not satisfy Hypothesis A.}}$$

$$\boxed{\text{The field } K \text{ satisfies } k(t^{\mathbb{Q}}) \subseteq K \subseteq k((t^{\mathbb{Q}})).}$$

$$\boxed{\text{For each nonzero additive polynomial } P \text{ over } k, \text{ we have } P(K^{\mathrm{Tr}}) = K^{\mathrm{Tr}}.}$$

$$\boxed{\text{We have a } k\text{-homomorphism } s\colon K \to k((t^{\mathbb{Q}})).}$$

We first need some auxiliary results in the spirit of the proof of Theorem 1.1.

Lemma 3.12. *We have $\bigcap_P P(K) = K^{\mathrm{Tr}}$, where the intersection is taken over all nonzero additive polynomials P over k.*

Proof. Let I be the intersection. Each $P(K)$ is a subgroup of K, and multiplication by an element of k permutes these subgroups, so I is a k-subspace of K. Since $P(K) \supseteq P(K^{\mathrm{Tr}}) = K^{\mathrm{Tr}}$ for each P, we have $I \supseteq K^{\mathrm{Tr}}$. But K^{Tr} has codimension 1 in K, and $I \neq K$ because k does not satisfy Hypothesis A. Thus $I = K^{\mathrm{Tr}}$. □

Lemma 3.13. *We have $\mathrm{Tr}(s(x)) = \mathrm{Tr}(x)$ for all $x \in K$.*

Proof. Since s acts trivially on k, it suffices to consider the case $x \in K^{\mathrm{Tr}}$. Then $x \in \bigcap_P P(K)$ by Lemma 3.12, so $s(x) \in \bigcap P(s(K)) \subseteq \bigcap P(k((t^{\mathbb{Q}})))$, and the latter equals $k((t^{\mathbb{Q}}))^{\mathrm{Tr}}$, by Lemma 3.12 applied to $k((t^{\mathbb{Q}}))$. □

Lemma 3.14. *Suppose $x \in K^*$ and $\mathrm{Tr}(x) = 0$. Then $v(x) > 0$ if and only if $\mathrm{Tr}\left(\frac{x^p}{x^p - x}\right) = 0$.*

Proof. Since $\mathrm{Tr}(x) = 0$, we have $v(x) \neq 0$. If $v(x) > 0$, then $v\left(\frac{x^p}{x^p-x}\right) = (p-1)v(x) > 0$, so $\mathrm{Tr}\left(\frac{x^p}{x^p-x}\right) = 0$. If $v(x) < 0$, then x^p and $x^p - x$ have the same leading term, so $\mathrm{Tr}\left(\frac{x^p}{x^p-x}\right) = 1$. □

Lemmas 3.13 and 3.14 imply the following:

Corollary 3.15. *If $x \in K^*$, then $v(x)$ and $v(s(x))$ have the same sign.*

The map $\mathcal{L}\colon k((t^{\mathbb{Q}}))^* \to k^* t^{\mathbb{Q}}$ that returns the leading term of a series is a group homomorphism, so the map $\mathbb{Q} \mapsto k^* t^{\mathbb{Q}}$ defined by $i \mapsto \mathcal{L}(s(t^i))$ must have the form $i \mapsto \lambda(i) t^{ri}$ for some homomorphism $\lambda\colon \mathbb{Q} \to k^*$ and some $r \in \mathbb{Q}$. Corollary 3.15 shows that $r > 0$. By composing s with an automorphism of $k((t^{\mathbb{Q}}))$ of the type described in Theorem 3.6, we reduce to the following case:

$$\boxed{\text{For all } i \in \mathbb{Q}, \text{ the leading term of } s(t^i) \text{ is } t^i.}$$

We now hope to prove that $s(x) = x$ for all $x \in K$.

Lemma 3.16. *Under the boxed assumptions, we have $s(t) = t$.*

Proof. If not, then for some $b \in \mathbb{Q}_{>0}$ and $c \in k^*$, we have

$$s(t) = t(1 + ct^b + (\text{higher order terms})).$$

Write $b = p^e b'$ where e is the p-adic valuation of b. Choose a large negative integer ℓ not divisible by p, and set $j = b'/\ell$. Thus $j < 0$, the p-adic valuation of j is 0, and $b/j = p^e \ell \in \mathbb{Z}[1/p]$. By choosing $|\ell|$ large enough, we may assume also that $0 < j + b$.

We compute $s(t^j)$ by raising $s(t)$ to an integer power, and then taking an integer root. Since the latter integer is prime to p, and since $s(t^j)$ has leading coefficient 1 by hypothesis, we obtain

$$\begin{aligned} s(t^j) &= t^j(1 + jct^b + (\text{higher order terms})) \\ &= t^j + jct^{j+b} + (\text{higher order terms})). \end{aligned}$$

Let n be a positive integer greater than $-e$. For any $x \in k((t^{\mathbb{Q}}))$, define $h(x)$ to be the $y \in k((t^{\mathbb{Q}}))^{\mathrm{Tr}}$ such that $y^{p^n} + y = x - \mathrm{Tr}(x)$. It is unique by Lemma 3.8, which also describes how to compute it. Moreover, if $x \in K$, then $h(x) \in K$, by hypothesis. Lemma 3.13 implies that $s(h(x)) = h(s(x))$. We compute

$$\begin{aligned} h(t^j) &= t^{j/p^n} + \ (\text{other terms with smaller negative exponent}) \\ s(h(t^j)) &= h(s(t^j)) \\ &= t^{j/p^n} + \ (\text{terms with negative exponent}) \ + jct^{j+b} + (\text{higher order terms}) \\ &= t^{-a} + \ (\text{terms with negative exponent}) \ + jct^{pma} + (\text{higher order terms}), \end{aligned}$$

where $a = -j/p^n \in \mathbb{Q}_{>0}$ and $m := -(j+b)p^{n-1}/j \in \mathbb{Z}_{>0}$. In the multinomial expansion for $s(h(t^j))^{1+pm}$, any product involving at least one of the terms of $s(h(t^j))$ with positive exponent will have exponent at least $pm(-a) + 1(pma) = 0$. Moreover, there is exactly one product in the multinomial expansion with exponent exactly 0, namely

$$\binom{1+pm}{1} \left(t^{-a}\right)^{pm} (jct^{pma})^1 = (1+pm)jc,$$

which is nonzero in k. Thus $\mathrm{Tr}\left(s(h(t^j))^{1+pm}\right) \neq 0$.

On the other hand, $h(t^j)^{1+pm}$ has only terms with negative exponent, so $\mathrm{Tr}\left(h(t^j)^{1+pm}\right) = 0$. This contradicts Lemma 3.13. □

Corollary 3.17. *For every $i \in \mathbb{Q}$, we have $s(t^i) = t^i$.*

Proof. This follows from $s(t) = t$ and the assumption that the leading coefficient of $s(t^i)$ is 1. □

Now, for any $x \in K$ and $l \in \mathbb{Q}$,

$$\begin{aligned} \mathrm{Tr}\left(t^{-l} s(x)\right) &= \mathrm{Tr}\left(s(t^{-l}x)\right) && \text{(by Corollary 3.17)} \\ &= \mathrm{Tr}\left(t^{-l}x\right) && \text{(by Lemma 3.13).} \end{aligned}$$

In other words, the coefficient of t^l in $s(x)$ equals the coefficient of t^l in x. This holds for all l, so $s(x) = x$. This completes the proof of Theorem 3.9.

Acknowledgments. This paper is the result of a discussion with George Bergman, Keith Kearnes, Hendrik Lenstra, and Thomas Scanlon; their contributions are noted throughout the text. We thank also Anand Pillay and Alex Wilkie for discussions concerning Remarks 1.10 and 2.2. Kedlaya was partially supported by a National Science Foundation postdoctoral fellowship (grant DMS-0071597) and NSF grant DMS-0400727. Poonen was partially

supported by NSF grants DMS-9801104 and DMS-0301280 and a Packard Fellowship; he thanks also the Isaac Newton Institute for hosting a visit in the summer of 2005.

References

[C] P. M. Cohn, *Skew Field Constructions*, London Math. Soc. Lecture Note Series **27**, Cambridge Univ. Press, Cambridge, 1977.

[G] D. Goss, *Basic Structures of Function Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete **35**, Springer-Verlag, 1996.

[Ha] H. Hahn, Über die nichtarchimedische Größensysteme (1907), reprinted in *Gesammelte Abhandlungen* I, Springer-Verlag, 1995.

[Ho] W. Hodges, *Model Theory*, Cambridge Univ. Press, Cambridge, 1993.

[Ka1] I. Kaplansky, Maximal fields with valuations, *Duke Math. J.* **9** (1942), 303–321.

[Ka2] I. Kaplansky, *Selected Papers and Other Writings*, Springer-Verlag, 1995.

[Ke1] K.S. Kedlaya, The algebraic closure of the power series field in positive characteristic, *Proc. Amer. Math. Soc.* **129** (2001), 3461–3470.

[Ke2] K.S. Kedlaya, Finite automata and algebraic extensions of function fields, preprint, `arXiv:math.AC/0410375`; to appear in *J. Théor. Nombres Bordeaux*.

[Pa] D.S. Passman, *The Algebraic Structure of Group Rings*, Wiley, 1977.

[Po] B. Poizat, *A Course in Model Theory* (translated by M. Klein), Springer-Verlag, New York, 2000.

[W] G. Whaples, Galois cohomology of additive polynomials and n-th power mappings of fields, *Duke Math. J.* **24** (1957), 143–150.

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

E-mail address: `kedlaya@math.mit.edu`

URL: `http://math.mit.edu/~kedlaya`

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA

E-mail address: `poonen@math.berkeley.edu`

URL: `http://math.berkeley.edu/~poonen`