Rend. Sem. Mat. Univ. Pol. Torino
Vol. 67, 1 (2009), 1 – 14

U. Zannier

ON THE HILBERT IRREDUCIBILITY THEOREM

Abstract. We discuss the Hilbert Irreducibility Theorem, presenting briefly a new approach which leads to novel conclusions, especially in the context of algebraic groups. After a short survey of the issues and of the known theory, we shall illustrate the main principles and mention some new results; in particular, we shall state a toric analogue of Bertini's Theorem and a lifting theorem for rational points on a cover of a power of an elliptic curve.

1. Introduction

This paper is an expanded version of a 'Lezione Lagrangiana', delivered on 12 March, 2009, at the Dipartimento di Matematica dell'Università di Torino. I am grateful to the Organizers for the kind invitation.

I shall discuss some aspects of the Hilbert Irreducibility Theorem and, in accordance with the general spirit of this series of lectures, I shall not insist on technical details. I shall present some new results from the recent paper [30] (where complete proofs may be found). In a way, this prevents me from giving a detailed survey of the topic from its origin, as I would have desired. Nevertheless I shall start with the basics of the context and I shall recall many Examples.

Basics of Hilbert Irreducibility Context. The Hilbert Irreducibility Theorem (HIT from now on) was first stated and proved by Hilbert in 1982 [13]. It roughly asserts that for polynomials in several variables irreducible over the rational field, there always exist rational specializations of some of the variables which preserve irreducibility. Hilbert himself proved the theorem for arbitrary number fields k in place of $\mathbb{Q}$, and later this was extended to other classes of fields. Here we shall always work over a number field k. Let us state in precise terms one of the basic forms of HIT:

Given polynomials $f_1,\dots,f_m \in k[t_1,\dots,t_r,y]$ irreducible over k, where r is a positive integer, there exist specializations $t_i \mapsto \xi_i \in k$ such that all the specialized polynomials $f_i(\xi_1,\dots,\xi_r,y)$, $i=1,\dots,m$, remain irreducible in $k[y]$.

An amusing and illustrative Example occurs for a single polynomial of the form $y^2-g(t)$; the theorem now states that *if $g(\xi)$ is a perfect square in $\mathbb{Q}$ for all $\xi\in\mathbb{Q}$ then g is the square of a polynomial*. We encourage the possible readers who may expect this to be too easy, to convince themselves that this is not quite so.

The above one is a natural statement, which may be seen as an arithmetical analogue of the Bertini Irreducibility Theorem in Algebraic Geometry.[1] It has close connections with the theory of diophantine equations, and admits several important applications, for instance to the *Inverse Galois Problem* of the realization of extensions $L/\mathbb{Q}$ with a given finite Galois group.

[1] In fact, Bertini's Theorem leads very quickly to a function field version of HIT.

For given $f_1,\dots,f_m$, let us call *good* a point $(\xi_1,\dots,\xi_r)\in k^r$ with the stated property, so the HIT asserts the existence of good points, no matter the set of irreducible polynomials f_i. This in a sense concludes the matter; however the main issue becomes now to obtain properties more precise than existence, concerning the distribution of good points. Actually, a first result in this sense appears in most statements of HIT, namely that good specializations are Zariski-dense in k^r (which is essentially implicit also in the above statement).

Many other properties of good points have been proved since the original statement of Hilbert; for instance, they can be taken in $\mathbb{Z}^r$ and they are distributed 'densely' in various meanings: 'almost all' points (asymptotically) in $\mathbb{Z}^r$ are good (Dörge, Siegel, S.D. Cohen, Bombieri–Pila, Heath-Brown,...), good points contain whole arithmetic progressions (Schinzel) and they are dense in p-adic spaces (Eichler, Fried,...). (For these and other properties and for references to original papers we refer to the books [11, 16, 20, 21]; see also the papers [19, 26].)

In some cases one can even prove the much stronger property of finiteness or 'degeneracy' (i.e. not to be Zariski-dense) of the points of k^r which are *not* good. This always amounts to some finiteness statement for diophantine equations; when it can be done it lies usually very deep, and in fact very often it is nowadays unaccessible (except for the case of subvarieties of semi-abelian varieties – e.g. curves – and a few other situations).

Nevertheless, one does not always expect such degeneracy, and anyway, as in the above mentioned results, there are other relevant structural properties for good points which may be proved (which moreover can be amply sufficient in applications of the HIT). Our results go in this direction, i.e. of proving the existence of good points in restricted relevant sets. Before presenting them we shall see several explicit instances.

We note that HIT can be formulated in terms of *covers*, by which we mean a *dominant rational map of finite degree between irreducible varieties*. An irreducible hypersurface $f(t_1,\dots,t_r,y)=0$ defines a cover $\pi: Y\to\mathbb{A}^r$, where π is the projection to the first r coordinates. Then our basic questions can be formulated in terms of the lifting of rational points $t\in\mathbb{A}^r(k)$ to Y: when does it happen that $\pi^{-1}(t)$ contains a point in $Y(k)$, or is k-irreducible?

Now, we may change $\mathbb{A}^r$ with another variety X. Situations which are obviously relevant occur when X is an algebraic group, because these are the fundamental varieties where we are able to generate systematically rational points.[2] Here we shall obtain new results for the *lifting of points in a dense cyclic subgroup* $\Omega\subset X(k)$, for X either a multiplicative torus or a power of an elliptic curve: *under a necessary geometrical condition on* Y (see Definition 1) *we prove that* $\pi^{-1}(x)$ *is* k*-irreducible for each* x *in a suitable coset of finite index in* Ω.

Note that lifting to Y a point on X may be seen as lifting to Y a map to X; an important issue in doing this is whether $\pi: Y\to X$ is ramified or not. In fact, this feature will be the main source of geometrical restrictions alluded to.

Before presenting new results, we insist with some Examples, illustrating many

[2] The original case of HIT is no exception: $\mathbb{A}^n=\mathbb{G}_{\mathrm{a}}^n$ as a variety.

results on HIT obtained in the past. For use throughout the paper, we immediately introduce the following:

Notation

- k is a number field, with algebraic closure $\bar{k} = \overline{\mathbb{Q}}$.

- k^c is the maximal cyclotomic extension of k, i.e. generated over k by all roots of unity.

- A variety X/k shall be called 'K-irreducible' if it is irreducible over the field K, omitting the reference to K if $K = \bar{k}$. We note that usually for our purposes to assume k-irreducibility makes no substantial difference: in fact, if X is $\bar{k}$-irreducible but reducible over $\bar{k}$, the set $X(k)$ lies in the intersection of the $\bar{k}$-components, and thus we are reduced to study a variety of lower dimension.

- We shall often work with $\mathbb{G}_{\mathrm{m}}^n$, i.e. the n-th power of the multiplicative algebraic group: it is $(\mathbb{A}^1 \setminus \{0\})^n$ as a variety, endowed with coordinatewise multiplication. The torsion points in $\mathbb{G}_{\mathrm{m}}^n$ are those whose coordinates are roots of unity; their set shall be denoted $\mathcal{T}_n$. We also call a *torsion coset* in $\mathbb{G}_{\mathrm{m}}^n$ a translate of an algebraic subgroup by a torsion point. It is defined by finitely many equations $x_1^{a_1} \cdots x_n^{a_n} = \theta$, where x_i are coordinates on $\mathbb{G}_{\mathrm{m}}^n$, $a_i \in \mathbb{Z}$ and θ is a root of unity. (See e.g. [1] for simple proofs of this.) Finally, the multiplication map $x \mapsto x^d$ is denoted $[d]$.

Eight Examples

EXAMPLE 1. In the above setting, let us take $X = \mathbb{G}_a$, the additive algebraic group, and Y some algebraic curve. Also, let $\Omega = \mathbb{Z}\xi$ be the cyclic subgroup of $X(k)$ generated by $\xi \in k^*$. Standard versions of HIT say that $\Omega \cap \pi(Y(k))$ contains at most $O(T^c)$ elements of absolute value $\leq T$, where $c = c_Y < 1$, which yields many 'good' points in Ω.[3]

EXAMPLE 2. In the same situation, Schinzel [17] proved that there exists an integer $q > 0$ such that a coset Ω of the subgroup $q\mathbb{Z} \subset \mathbb{Z}$ (i.e. an arithmetic progression Ω) is disjoint from $\pi(Y(k))$.

EXAMPLE 3. The higher-dimensional case $X = \mathbb{G}_a^n$, with corresponding data Y, π, is not essentially different because often we may reduce to curves: if for instance the closure U of $\Omega = \mathbb{Z}\xi$ in X – a line – is such that $V := \pi^{-1}(U) \subset Y$ is an irreducible curve, then we may replace X by U and Y by V, and obtain as in Example 1 (many) points of Ω outside $\pi(Y(k))$. The irreducibility of V cannot be ignored, because the

[3] Siegel pointed out, through his finiteness theorem on integral points on curves ([16, 20]), the best-possible value $c = 1/2$, nowadays obtained also with different means ([12, 26]).

degree of π on some component could be 1. (We note that a Zariski-dense subset of lines in X lift to irreducible curves.)[4]

EXAMPLE 4. Now let $X = \mathbb{G}_{\mathrm{m}}$. As in Example 1, let $\Omega = \{\xi^r : r \in \mathbb{Z}\}$ be a cyclic subgroup of $X(k) = k^*$, supposed Zariski-dense (i.e. ξ not a root of unity). Then one proves (e.g. by Siegel's theorem on S-integral points) that $\Omega \setminus \pi(Y(k))$ is infinite unless Y is birationally equivalent to an unramified cover of X; namely, $\pi : Y \to X$ is a factor of $[d] : X \to Y \to X$, where the left map is birational. This amounts to $k(Y) = k(x^{1/d})$ where $k[x^{\pm 1}] = k[\mathbb{G}_{\mathrm{m}}]$. (This has been observed by Dèbes [7] in another language; for different proofs see [5].)

Note that the restriction on Y here is genuinely geometric and independent of k. By extending possibly k, this becomes necessary, since if $k(Y) = k(x^{1/d})$ we have $\Omega \subset \pi(Y(k))$ if $\xi \in (k^*)^d$. We see here a first instance of the relevance of ramification in this context.

Another remark is that, under the said assumption, here Siegel's theorem yields the expected *finiteness* of $\Omega \cap \pi(Y(k))$. In higher dimensions in general the question of finiteness remains at the moment very far (but see [5], Thm. 2, for results on the so-called *dominant root* assumption).

EXAMPLE 5. Let now $X = \mathbb{G}_{\mathrm{m}}^n$. Contrary to the case of $\mathbb{G}_a$, to work in arbitrary dimension n presents substantial new difficulties. This is because already a cyclic group $\Omega = \xi^{\mathbb{Z}}$ may well be Zariski-dense in X: this happens when the coordinates $\xi_1, \dots, \xi_n$ of ξ are multiplicatively independent, as we now assume. In this case we cannot reduce to the case of curves (if $n > 1$).

The alluded obstacles appear already when Y is a cyclic cover defined by $y^d = f(x_1, \dots, x_n)$, with $\pi(y, x_1, \dots, x_n) = (x_1, \dots, x_n)$. To illustrate this, let us suppose that $\Omega \subset \pi(Y(k))$, i.e. that $f(\xi^r)$ is a d-th power in k for all $r \in \mathbb{Z}$. Note that the $f(\xi^r)$ are the values of a linear recurrence, so we fall in the so-called *Pisot d-th root conjecture*; in the present language it predicted that f is then a d-th power times a monomial. As in Example 4, this amounts to $Y \to X$ being unramified. Now, this conjecture was established in [27], with a method at the basis of what we are going to discuss.

Contrary to the case $n = 1$, no general finiteness conclusions are available to date. For some results we refer to [5] or [29], which however use methods unrelated to the present paper.

EXAMPLE 6. Let again $X = \mathbb{G}_{\mathrm{m}}^n$, but this time let us work not over a number field k but over the cyclotomic closure k^c of k, generated over k by all roots of unity. We take $\Omega \subset \mathbb{G}_{\mathrm{m}}^n(k^c)$ to be the group of all torsion points. In the paper [8] it is proved in particular that either the cover $Y \to X$ is unramified, as in Example 4, or $\Omega \cap \pi(Y(k^c))$ is contained in a proper subvariety of X (which turns out to be a finite union of proper torsion cosets of X). See Theorem 5 below.
We shall emphasise how this has strong implications also in the case of number fields.

[4] This case $n > 1$ becomes more difficult if we seek good quantitative bounds. See [20, 21] for an account of bounds by S.D. Cohen, and [15, 12] for other methods originated by [2].

EXAMPLE 7. The methods can be applied also to products like $\mathbb{G}_{\mathrm{m}}^n \times \mathbb{G}_{\mathrm{a}}$, as in [9] in the context of linear recurrences. The paper [4] by Corvaja, relying for the arithmetic on [9], obtains an elegant generalization of this to arbitrary linear algebraic groups.[5] It is proved in particular that if X is such a group, if Y is smooth and π is finite, then either $Y \to X$ is unramified or any Zariski-dense semigroup $\Omega \subset X(k)$ contains good points.

EXAMPLE 8. Given these results, the problem arises of what happens for X an abelian variety, taking again $\Omega \subset X(k)$ to be a dense subgroup. This is stated at p. 53, §5.4 of [21]. If X is an elliptic curve, then Faltings' finiteness theorem settles the question: either Y has genus > 1 and then $Y(k)$ is finite, or $Y \to X$ is an isogeny; so we have a result analogue and stronger than the above ones. However, already the case $X = E^2$ for an elliptic curve E seems to escape from known results. In the final section of this paper we shall see that this context can be sometimes dealt with by the present methods, by stating as Thm. 2 a HIT for covers of E^n.

Here we shall very briefly describe a new systematic approach to such questions, including and going beyond the Examples. This method consists of two main stages and may be very roughly described as follows:

(A) *To prove a suitable (explicit) HIT over a big cyclotomic field, of infinite degree over* $\mathbb{Q}$.

(B) *To transfer the irreducibility to points over a number field.*

A relevant issue here is that, somewhat surprisingly, HIT may be proved directly over the big field, actually for *explicit* specializations at torsion points (as in [8] – Theorem 5 below)[6]; hence (A) applies. Then the *transfer* (B) leads to sharp new versions of HIT over number fields. This step involves Chebotarev Theorem, which may be seen as a 0-dimensional version of HIT.

It turns out that all of this, especially the group structure of torsion points, leads to the sought additional conclusions on the location of 'good' specializations, in the context of algebraic groups.

We now introduce a natural and most relevant geometrical condition on the covers, which shall turn out to be necessary and sufficient for our purposes.

For X a commutative connected algebraic group, we let $[m] : X \to X$ denote the multiplication map. By 'irreducible' we mean throughout 'k-irreducible' (supposed for all X, Y in a cover).

DEFINITION 1. *We say that the cover $\pi : Y \to X$ satisfies the condition (PB) ('pull-back') if for any integer $m > 0$ the pull-back $[m]^*Y := X \times_{[m],\pi} Y$ is irreducible.*

[5] To reduce to $\mathbb{G}_{\mathrm{m}}$ and $\mathbb{G}_{\mathrm{a}}$ the arguments consider subgroups generated by a single matrix; the component of the identity in the closure of such a subgroup is isomorphic to $\mathbb{G}_{\mathrm{m}}^n \times \mathbb{G}_{\mathrm{a}}^e$, $e = 0, 1$.

[6] Kuyk proved (see [25]) the hilbertianity of cyclotomic fields, and much more, but such – interesting – methods and results play no role here.

For instance: if $X = \mathbb{G}_{\mathrm{m}}^r$ and $Y : f(x_1,\dots,x_r,y) = 0$, the condition (PB) means that $f(x_1^m,\dots,x_r^m,y)$ is irreducible for all $m > 0$. For $X = \mathbb{G}_{\mathrm{a}}^s$, one similarly finds that (PB) is always trivially verified.

REMARKS 1. (i) Note that this condition is unavoidable for our lifting issues. In fact, suppose that $[m]^*Y$ is reducible, equal to the union $U \cup V$ of proper closed subsets. Let Ω be any finitely generated (dense) subgroup of $X(k)$. By enlarging k to a finite extension, assume that U, V are defined over k and that $\Omega \subset [m](X(k))$. Let $x \in \Omega$ and write $x = [m]x'$ for $x' \in X(k)$. If $\pi(y) = x$, the pair (x', y) is in $[m]^*Y(k) = U(k) \cup V(k)$. For 'general' x, this yields a nontrivial splitting of the fiber $\pi^{-1}(x)$ into two subsets defined over k, so $\pi^{-1}(x)$ cannot be k-irreducible.
(ii) It may be proved in a simple way (see [30]) that this condition holds if and only if it holds for $m = \deg\pi$ (so it is a 'computable' condition) and if and only if the map π has no nontrival isogeny factors. Note that when π itself is an isogeny up to birationality, then (if $\deg\pi > 1$) not only we cannot guarantee irreducibility of $\pi^{-1}(x)$, but for large enough k we shall have $\Omega \subset \pi(Y(k))$.
Note finally that these conditions involve ramification: in fact, isogenies yield precisely the unramified covers of algebraic groups. (That this plays a role in lifting points is no surprise, in the same way it plays a role in lifting maps, as in classical monodromy theory.)

Let us now give some statements, starting with the case $X = \mathbb{G}_{\mathrm{m}}^r$.

THEOREM 1. *For $i = 1,\dots,h$, let $\pi_i : Y_i \to X := \mathbb{G}_{\mathrm{m}}^r$ be a cover satisfying (PB). Then, if Ω is a cyclic Zariski-dense subgroup of $X(k)$, there exists a coset C of finite index in Ω such that for all $x \in C$ and for all $i = 1,\dots,h$ the fiber $\pi_i^{-1}(x)$ is irreducible over k.*

This result immediately implies a sharp form of the so-called *Pisot d-th root conjecture*, proved in [27] with a method at the basis of the present one.

In the context of abelian varieties, we have the following analogue for powers of an elliptic curve E without CM:

THEOREM 2. *For $i = 1,\dots,h$, let $\pi_i : Y_i \to E^n$ be a cover satisfying (PB). Then, if Ω is a cyclic Zariski-dense subgroup of $E^n(k)$, there exists a coset C of finite index in Ω such that for all $x \in C$ and for all $i = 1,\dots,h$ the fiber $\pi_i^{-1}(x)$ is irreducible over k.*

Theorem 1 looks similar, but can be obtained more rapidly, due to our results for cyclotomic fields for which we have no counterpart for fields generated by torsion points of abelian varieties (see §4). So, Theorem 2 requires additional and more delicate arguments, and we have stated it separately.

Our next result is a simple application of the method in the function field context: we offer a toric analogue of Bertini Theorem, where algebraic subgroups of $\mathbb{G}_{\mathrm{m}}^n$ replace linear subspaces. We denote by θG the translate of the algebraic subgroup G by the torsion point θ.

THEOREM 3. *Let $\pi : Y \to \mathbb{G}_{\mathrm{m}}^n$ be a cover satisfying (PB). Then there is a finite union $\mathcal{E}$ of proper connected subgroups of $\mathbb{G}_{\mathrm{m}}^n$ such that if a connected subgroup G is not contained in $\mathcal{E}$, then $\pi^{-1}(\theta G)$ is irreducible (over $\overline{\mathbb{Q}}$) for every torsion point θ.*

We note that also here condition (PB) cannot be omitted. The Bertini Theorem may be seen as a version of a similar statement for $\mathbb{G}_{\mathrm{a}}^n$; a main difference is that in the present case the algebraic subgroups form a 'discrete', rather than algebraic, family, with degrees tending to infinity.

Here is a **polynomial version** of the theorem: *Let $f \in \overline{\mathbb{Q}}[x_1,\dots,x_n,y]$ be of degree $d > 0$ in y and such that $f(x_1^d,\dots,x_n^d,y)$ is irreducible. Then there is a finite union $\mathcal{H}_f$ of proper subgroups of $\mathbb{Z}^n$ such that if $(a_1,\dots,a_n) \in \mathbb{Z}^n \setminus \mathcal{H}_f$, then $f(\theta_1 t^{a_1},\dots,\theta_n t^{a_n},y) \in \overline{\mathbb{Q}}[t,t^{-1},y]$ is irreducible for all roots of unity $\theta_1,\dots,\theta_n$.*
In particular, the *Kronecker's substitution* $(x_1,\dots,x_n) \mapsto (t,t^m,\dots,t^{m^{n-1}})$ preserves the irreducibility over $\overline{\mathbb{Q}}$ of a polynomial f as above, for all integers m large enough in terms of f. (We wonder whether it suffices that $m > M_0(\deg f)$.) For results in the same direction, but only over $\mathbb{Q}$, not $\overline{\mathbb{Q}}$, and with an additional assumption on f (not to be self-inversive in the x_i), see [18].

2. A lifting theorem and applications to HIT for covers of algebraic tori

In this section we state, in particular, a lifting theorem and an application to a HIT for covers of algebraic tori. The proof, which we only sketch, uses the combination of parts (A), (B) of the method, just mentioned. To emphasise the essentials we have sticked to simplicity. We denote by $|\cdot|_v$ the sup-norm with respect to a place v:

THEOREM 4. *Let Y be a k^c-irreducible variety and $\pi : Y \to \mathbb{G}_{\mathrm{m}}^n$ be a cover satisfying (PB). Then there is a finite union $\mathcal{E} \subset \mathbb{G}_{\mathrm{m}}^n$ of proper torsion cosets with the following property: if $\zeta \in \mathcal{T}_n \setminus \mathcal{E}$ there exist infinitely many places w of $k(\zeta)$, of residual degree 1 above $l = w|_{\mathbb{Q}}$, such that $\pi(Y(k(\zeta)))$ does not intersect the set $\{x \in k(\zeta)^n : |x-\zeta|_w < 1\}$.*

REMARKS 2. (i) Note that $l = w|_{\mathbb{Q}}$ splits completely in $\mathbb{Q}(\zeta)$, because its residual degree there is 1. Note also that the set $\{x \in \mathbb{Q}^n : |x-\zeta|_w < 1\}$ is not empty, again because the residual degree of $w|l$ is 1. In particular, this set contains a whole residue class in $\mathbb{Z}^n/l\mathbb{Z}^n$. For instance, if $n = 1$, if ζ has order m and if $\xi \in \mathbb{Q}$ has order h modulo l, for some a coprime to h the set contains the powers ξ^{a+hm}, all $m \in \mathbb{Z}$. Many other similar Examples may be given.
(ii) Inspection shows that the result is effective, in the sense that, given Y, π, one may calculate: equations for the set $\mathcal{E}$, roots of unity ζ and places $w|l$ with the relevant properties.

Before sketching a proof of this theorem, let us state a crucial result from [8], representing part (A); more precisely, we need a consequence of [8, Thm. 1], which can be deduced by a purely algebraic argument (see [30]). It is an *explicit* HIT for

torsion points over cyclotomic fields.

THEOREM 5. *Let Y be a k^c-irreducible variety and $\pi : Y \to \mathbb{G}_{\mathrm{m}}^n$ be cover satisfying (PB). Then there exists a finite union $\mathcal{E}$ of proper torsion cosets such that if $\zeta \in \mathcal{T}_n \setminus \mathcal{E}$ then $\zeta \in \pi(Y)$ and if $\pi(u) = \zeta$, then $[k^c(u) : k^c] = \deg \pi$.*

We note that also here the condition (PB) is necessary for the conclusion.

• On comparing Theorem 5 and Theorem 1, we may say, so to speak, that the property of 'being good' spreads out and transfers from torsion points ζ to whole w-adic neighborhoods of them; this is the *transfer* principle (B) alluded to above.

Proof of Theorem 4. We may apply Theorem 5 to Y, π, so let $\mathcal{E}$ be the finite union of proper torsion cosets mentioned there. There is a proper subvariety $\mathcal{E}'$ of $\mathbb{G}_{\mathrm{m}}^n$ such that the fiber of π outside $\mathcal{E}'$ has exactly d-elements (even in a projective closure of Y). The Zariski-closure of the torsion points in $\mathcal{E}'$ is another finite union of torsion cosets; by enlarging $\mathcal{E}$ we may suppose this union is contained in $\mathcal{E}$. Now, for a torsion point $\zeta \notin \mathcal{E}$ let $u \in Y(\bar{k})$ be such that $\pi(u) = \zeta$. By the corollary, u exists and we have $[k^c(u) : k^c] = d$.

In the sequel, we shall tacitly assume that this is the case for the ζ in question. Let $H = H_\zeta$ be the Galois group of the normal closure $K = K_\zeta$ of $k(\zeta, u)/k(\zeta)$. (Note that K depends in fact only on ζ, not on u because $[k^c(u) : k^c] = d$, and we have $K = k(\zeta, u_1, \dots, u_d)$ where u_i are the elements of $\pi^{-1}(\zeta)$.)

It is a well-known simple fact (attributed to Jordan – see [22]) that H cannot be the union of conjugates of a proper subgroup.[7] A subgroup B of a finite group H has at most $[H : B]$ conjugates, all of which contain the origin. Hence if $B \neq H$ their union contains $< [H : B] \cdot |B| = |H|$ elements. Therefore, since $k(\zeta, u) \neq k(\zeta)$, there exists an element $g = g_{\zeta,u} \in H$ such that $u^{g\tau} \neq u^\tau$ for all $\tau \in H$.

We now apply the theorem of Chebotarev to the normal closure K' of $K/\mathbb{Q}$. There exists an element $\sigma \in \Gamma := \mathrm{Gal}(K'/\mathbb{Q})$ which restricts to g on K. In particular, σ fixes $k(\zeta)$ pointwise. We obtain the existence of infinitely many places l of $\mathbb{Q}$ (in fact a set of positive density), unramified in K' and such that the Frobenius class of l in Γ is the class of σ. Let then v be a place of K' above l with $\mathrm{Frob}(v|l) = \sigma$, and denote by w the place of $k(\zeta)$ below v. We let $\{u_1, \dots, u_d\}$ be the fiber of π above ζ and we choose l large enough so that $u_1, \dots, u_d$ are defined and remain distinct modulo v (recall that they are distinct) and so that Y, π have good reduction at v.[8]

Since σ fixes $k(\zeta)$, the residual degree of $w|l$ is 1. Let $a \in \mathbb{G}_{\mathrm{m}}^n(k(\zeta))$ be such that $|\zeta - a|_w < 1$ and consider the fiber of π above a. Suppose that there is an element $b \in Y(k(\zeta))$ so that $\pi(b) = a$. Then $\pi(b) \equiv \zeta \pmod{v}$; hence the reduction of b at v is defined and $b \equiv u_i \pmod{v}$ for some i. In fact, otherwise the fiber above the reduction of ζ, in a projective closure of Y, would contain more than d elements and the same would be true for the fiber above ζ (e.g. by Hensel lifting, or simply by good reduction,

[8] We need just a simple concept of 'good reduction', i.e. we suppose that the reduction of Y, π is defined and has still the same degree. Usually good reduction includes that the reduction of Y is irreducible, which however is not needed for the argument here.

on taking l large enough so that ζ does not lie modulo v in the 'exceptional' variety $\mathcal{E}'$ mentioned in the opening argument).

Now, $b^\sigma = b$, whence $u_i^\sigma \equiv u_i \pmod{v}$, because σ fixes v. However any u_i is a conjugate over $k(\zeta)$ of u, so of the shape u^τ for a $\tau \in H$. Hence σ does not fix any of the u_i and permutes them, so we would have $u_i \equiv u_j$ for some $i \neq j$, a contradiction which proves that no b_i can be defined over $k(\zeta)$, proving the sought conclusion. □

There are several possible variations on Theorem 4 and its proof, which we have not pushed to greater generality for the sake of simplicity. For instance, we also state the following sharpening, whose proofs need only a few modifications in addition to the previous arguments:

Refinement. *Under the same assumptions, let F be a number field, Galois over $k(\zeta)$ and such that $[F : k(\zeta)]$ is not divisible by any prime smaller than $d = \deg \pi$. Then in the conclusion we may further prescribe arbitrarily the Frobenius class in* $\mathrm{Gal}(F/k(\zeta))$ *of the relevant place $w|l$.*

Let us derive Theorem 1, in the weak form $h = 1$ for simplicity. We have a Zariski-dense cyclic subgroup $\Omega = \{\xi^r : r \in \mathbb{Z}\}$ of $\mathbb{G}_{\mathrm{m}}^n(k)$. We write $\xi := (\xi_1, \ldots, \xi_n)$; since Ω is Zariski dense, the ξ_i are multiplicatively independent elements of k.

Let us assume that $Y \to \mathbb{G}_{\mathrm{m}}^n$ satisfies (PB). For a large prime p, let us choose a torsion point ζ of exact order p, satisfying the conclusion of Theorem 4: note that for large p we may choose it out of the proper algebraic subset $\mathcal{E}$. By the hypothesis on ξ, we have that for all large enough p the coordinates ξ_i have multiplicatively independent classes in $k(\zeta)^*/(k(\zeta)^*)^p$. This independence is not difficult to check: if a product $\xi_1^{a_1} \cdots \xi_n^{a_n}$ is nontrivially a p-th power in $k(\zeta)^*$ then it is a p-th power in k^* (for $[k(\zeta) : k]$ divides $p-1$). Find now with a well-known Dirichlet Lemma an integer $q \neq 0$ so that the qa_i have 'small' residues b_i mod p, say $|b_i| < \varepsilon p$; then $\xi_1^{b_1} \cdots \xi_n^{b_n}$ is also a p-th power, say η^p, $\eta \in k^*$, but has height $< n\varepsilon p \max h(\xi_i)$, so $h(\eta) < n\varepsilon \max h(\xi_i)$. For large enough p one can take an arbitrarily small ε, which eventually forces η and $\xi_1^{b_1} \cdots \xi_n^{b_n}$ to be roots of 1, contrary to the independence assumption. (See also [27, Lemma 2]).

Now, the Refinement applies to $F = k(\zeta, \xi^{1/p})$. Note that, by multiplicative independence modulo p-th powers, Kummer Theory shows that $F/k(\zeta)$ is Galois, abelian of degree p^n. We thus may find infinitely many primes l and extensions w of l to $k(\zeta)$ such that:

1. The prime l splits completely in $k(\zeta)$.
2. The image $\pi(Y(k(\zeta)))$ does not intersect the set $\{x \in k(\zeta)^n : |x - \zeta|_w < 1\}$.
3. The Frobenius of w in $F/k(\zeta)$ equals a prescribed element of $\mathrm{Gal}(F/k(\zeta))$.

Now, this Frobenius is an automorphism g fixing $k(\zeta)$ and such that $g(\xi_i^{1/p}) = \theta^{h_i} \xi_i^{1/p}$, for some integers h_i, where θ is a primitive p-th root of unity; by multiplicative independence modulo p-th powers, Kummer Theory again shows that all choices of h_i are possible; if $\zeta = (\theta^{c_1}, \ldots, \theta^{c_n})$ and if a_i are integers coprime to p, we choose $h_i = a_i c_i$.

Now, by (i) we have $\xi^{l/p} \equiv g(\xi^{1/p}) \pmod{v}$, where v is a place of F above w with Frobenius g, so by our choice we have $\xi_i^{b_i \frac{(l-1)}{p}} \equiv \theta^{c_i} \pmod{v}$, where b_i is any inverse to a_i modulo p. Hence, this congruence holds for the place w of $k(\zeta)$ below v. Hence $(\xi_1^{b_1},\dots,\xi_n^{b_n})^{\frac{(l-1)}{p}} \equiv \zeta \pmod{w}$ so by (ii) we conclude that $(\xi_1^{b_1},\dots,\xi_n^{b_n})^{\frac{(l-1)}{p}}$ does not lie in $\pi(Y(k(\zeta)))$. Also, on choosing $b_i = b$ for all i, we get $(\xi_1^{b_1},\dots,\xi_n^{b_n})^{\frac{(l-1)}{p}} = \xi^{\frac{(l-1)}{p}}$. Hence we may state:

COROLLARY 1. *Let Y,π be as in Theorem 1 and let $\xi^{\mathbb{Z}}$ be Zariski-dense in $\mathbb{G}_{\mathrm{m}}^n$, where $\xi = (\xi_1,\dots,\xi_n)$. Then for all large primes p there exist infinitely many primes $l \equiv 1 \pmod{p}$ such that, for any integers $b_1,\dots,b_n$ coprime to p, $(\xi_1^{b_1},\dots,\xi_n^{b_n})^{\frac{(l-1)}{p}}$ does not lie in $\pi(Y(k))$.*

In particular, for b_0 prime to p, the coset of $\xi^{\mathbb{Z}}/\xi^{(l-1)\mathbb{Z}}$ given by $\{\xi^{b\frac{(l-1)}{p}} : b \equiv b_0 \pmod{p}\}$, is disjoint from $\pi(Y(k))$.

The case $h = 1$ of Theorem 1 follows (and the general one may be easily derived from it).

We remark that no other known diophantine method yields such conclusions except in the special case $n = 1$ of curves (e.g. with Siegel's theorem) or under a certain technical condition (with methods as in [5]). Here is an amusing **Example-problem**: Take $Y : \{y^2 = x_1 + x_2 + 1\}$, $\pi(x_1,x_2,y) = (x_1,x_2)$. Take also $\Omega = (1+i,1-i)^{\mathbb{Z}}$ where $i^2 = -1$. I do not know of any method to prove finiteness of solutions $(n,y) \in \mathbb{Z} \times k$ of $y^2 = (1+i)^n + (1-i)^n + 1$. Theorem 1 yields a whole arithmetical progression of integers n such that $(1+i)^n + (1-i)^n + 1$ is not a square in k.

REMARK 1. We observe that a similar use of Chebotarev Theorem in the context of HIT implicitly appears in [17] and, in the function field context, in [10]. However the present applications differs by much, in that we work with points of arbitrarily large degree (i.e. the torsion points), using Chebotarev to descend to a fixed number field.

3. Proof of the toric Bertini Theorem

We now sketch a proof of Theorem 3, postponing to the next section a discussion of the more delicate Theorem 3. The principle of the proof is now simpler. However, some care is needed if we want to preserve irreducibility over $\overline{k}$.

Proof of Theorem 3. Let k be a number field of definition for Y and π, and let us apply, as we may, Theorem 4 to our cover $Y \to \mathbb{G}_{\mathrm{m}}^n$, obtaining a finite union $\mathcal{E}_1$ of torsion cosets as therein. By applying that conclusion to torsion points $\zeta \in \theta G \setminus \mathcal{E}_1$ and recalling that torsion points are Zariski-dense in G, we obtain that if $\theta G \not\subset \mathcal{E}_1$, then $\pi^{-1}(\theta G)$ is irreducible over k^c (for otherwise $\pi^{-1}(\zeta)$ would be *a fortiori* reducible over k^c for the Zariski-dense set of torsion points $\zeta \in \theta G \setminus \mathcal{E}_1$).

The point is now to go from k^c to $\bar{k}$, and for this we consider the cover $W := Y \times Y \to \mathbb{G}_{\mathrm{m}}^{2n} \cong \mathbb{G}_{\mathrm{m}}^n \times \mathbb{G}_{\mathrm{m}}^n$, by the map $\pi_2 := \pi \times \pi$ of degree d^2 where $d := \deg \pi$. Since Y satisfies (PB), the same is true of W, as a cover of $\mathbb{G}_{\mathrm{m}}^{2n}$. Hence by Theorem 4 applied this time to W, π_2 we deduce that there is a finite union $\mathcal{E}_2$ of proper torsion cosets of $\mathbb{G}_{\mathrm{m}}^{2n}$ such that for $\zeta_1 \times \zeta_2$ a torsion point in $\mathbb{G}_{\mathrm{m}}^{2n} \setminus \mathcal{E}_2$ the fiber $\pi_2^{-1}(\zeta_1 \times \zeta_2)$ is k^c-irreducible.

Denote $Z := \pi^{-1}(\theta G)$ and suppose that Z is reducible over $\bar{k}$. If $\theta G \not\subset \mathcal{E}_1$, we have observed that Z is irreducible over k^c and then the function field extension $k^c(Z)/k^c(G)$ contains a nontrivial finite 'constant' extension L/k^c. But then $Z \times Z$ is reducible over k^c, and in fact each k^c-component Z_2 satisfies $[k^c(Z_2) : k^c(G \times G)] \leq [k^c(Z) : k^c(G)]^2/[L : k^c] = d^2/[L : k^c]$.[9] Hence the fiber in $Z \times Z$ above a torsion point $\zeta_1 \times \zeta_2 \in \theta G \times \theta G$ has at least $[L : k^c]$ components irreducible over k^c. We conclude that $\theta G \times \theta G$ is contained in $\mathcal{E}_2$.

Thus if $\pi^{-1}(\theta G)$ is reducible, we obtain that either $\theta G \subset \mathcal{E}_1$ or $\theta G \times \theta G \subset \mathcal{E}_2$. From this we easily deduce that G is anyway contained in a certain finite union $\mathcal{E}$ of proper connected algebraic subgroups of $\mathbb{G}_{\mathrm{m}}^n$, concluding the argument. □

REMARKS 3. (i) The argument is effective, as the Theorem in [8]. (ii) The cover of $\mathbb{G}_{\mathrm{m}}^2$ given by $y^2 = 1 + 2x_1 + x_2$ shows that $\mathcal{E}$ cannot generally be taken $\{(1,1)\}$. (iii) The irreducibility of $\pi^{-1}(cG)$ for arbitrary c is more delicate and to our knowledge not yet completely clarified (see [6], §5, for the case $n = 2$). One may also consider the intersections $Z \cap cG$ of a fixed $Z \subset \mathbb{G}_{\mathrm{m}}^n$ with a family of algebraic cosets cG (possibly only torsion), which is even nearer to Bertini's context; see the Appendix.

See [30] for a result similar but weaker, in the context of elliptic curves. (See also the Appendix of [30] for another kind of multiplicative Bertini Theorem, obtained however with completely different methods).

4. Comments on Theorem 2

A proof of Theorem 2 could be carried out similarly to Theorem 1 (leaving aside the suitable Kummer theory) if an analogue of Theorem 5 would be available in the abelian context. This is however not the case at the moment, and in this respect in [30] we explicitly raised the following:

CONJECTURE 1. *Let A/k be an abelian variety, T be its set of torsion points. Let Y be an irreducible variety and $\pi : Y \to A$ be a dominant rational map of finite degree. Suppose that $\pi(Y(k(T))) \cap T$ is Zariski-dense in A. Then there exist an abelian variety B, an isogeny $\rho : B \to A$ and a birational map $\psi : Y \to B$ such that $\pi = \rho \circ \psi$.*

To prove Theorem 2 without this tool leads to several additional obstacles. In a related context (when [8] was not yet available) some difficulties appeared in the paper

[9] Note that we cannot directly work over L, which *a priori* might depend on G. See the next theorem for an alternative argument, showing that L may be in fact supposed to be fixed.

[27], concerned with the so-called *Pisot d-th root conjecture* for recurrences, which boils down to a consequence of Theorem 1 (see also Example 5 above). In practice, that paper used an alternative approach to step (A) in the case of $\mathbb{G}_{\mathrm{m}}^n$.

Now, it happens that this principle can be carried out in general, also to the present context of abelian varieties rather than multiplicative tori, in spite of the alluded substantial difficulties.[10] Here we only give a very brief sketch of some of the main points, and again refer to [30] for details.

To simplify as far as possible the situation, let us limit ourselves to the case $h = n = 1$. We stress that this restriction is not a mild one, but on the contrary is highly relevant: in fact, the extension both to $h > 1$ and to $n > 1$ contains several other delicate points, which require new devices. But such special case illustrates in a much clearer way at least one of the main principles and so seems appropriate here.

In this manner of carrying out step (A), the crux lies in constructing torsion points ζ on E which do not lift to $Y(k(\zeta))$, and to achieve this by means of congruences, more precisely using the Lang-Weil estimates for points on curves over finite fields. We recall this result in the following form (see also [20, p. 184], or [21, p. 30]): *Let Z/k be an absolutely irreducible variety of dimension n. For a prime p, let $v|p$ be a place of k with residue field contained in the finite field $\mathbb{F}_q$. Then, as $p \to \infty$, the number $|Z_v(\mathbb{F}_q)|$ of points of the reduction Z_v of Z satisfies $|Z_v(\mathbb{F}_q)| = q^n + O(q^{n-\frac{1}{2}})$.*

Let us now go back to our setting of a map $\pi : Y \to E$, and let $\widehat{Y}$ be a component of the Galois closure over k, assuming it to be irreducible over $\overline{k}$. As in a method introduced by Eichler, Fried and by S.D. Cohen (who applied it to HIT), the Lang-Weil statement, applied first to $Z = Y$ and then to $Z = \widehat{Y}$, allows to show that the image $\pi(Y(\mathbb{F}_q))$ has $< cq^n + o(q^n)$ elements, for a $c < 1$, actually $c \leq 1 - (1/d!)$. See [20, pp. 184/185], or [21, Thm. 3.6.2], for details of this deduction.[11]

With this in hand, let us choose p as a large prime splitting completely in k, and $\mathbb{F}_q = \mathbb{F}_p$. By what has just been said, there are points in $E(\mathbb{F}_p)$ (actually $\gg p$ points) which do not lift to points in $Y(\mathbb{F}_p)$. Pick one such point ξ and let ζ be a torsion point on $E(\overline{\mathbb{Q}})$ with reduction ξ modulo some place v above p. (This can be done provided ξ has order prime to p; in turn, this can be easily ensured, for instance choosing p splitting in the field of 2-torsion points of E.) Now, if ζ would lift to a point $y \in Y(k(\zeta))$, ξ would lift to the reduction of y modulo the place v, which (as expected) would lie in $Y(\mathbb{F}_p)$, as is easy to see; so we have a contradiction.

At this point the method continues with part (B), using the theorem of Chebotarev in a manner similar to the proof of the Corollary to Theorem 1. Here some elliptic Kummer Theory has to be invoked to replace the easier multiplicative case (which goes back essentially to Gauss). The tools come from Serre's difficult theorems [23], as explained e.g. in [14]. Suitable analogues of these results on the Galois action

[10] This method independently of [8], leads to obstacles already for the case of tori, and also to further ones special of the abelian context.

[11] This method does not alone work simultaneously for several covers $\pi_i : Y_i \to E$, because the sum $\sum_i |\pi_i(Y_i(\mathbb{F}_q))|$ may well exceed $|E(\mathbb{F}_q)|$, even if this does not happen individually. A way to overcome this may be to choose several primes, one for each cover; in our context however this does not work for the rest of the proof. A suitable method can be found in [30].

of torsion points are at the moment unknown in full generality, and this is the main obstacle for a complete extension of the method.

Actually, in the present simplification we have not mentioned other issues. For instance, for the Chebotarev Theorem to be applied as before, we would need not merely a torsion point ζ which does not lift to $Y(k(\zeta))$; what we would need is the stronger property that any point in the fiber $\pi^{-1}(\zeta)$ has the 'correct' degree $\deg\pi$ over $k(\zeta)$, i.e., that the fiber consists of a single set of conjugate points over $k(\zeta)$. Such a stronger property may be reduced to the weaker 'non-lifting' property with a purely algebraic (standard) method; however this involves simultaneously several varieties, so we fall anyway back to the case $h > 1$, which needs additional delicate considerations. (See especially the last footnote.) We refer to [30] for the details, as any discussion here would take us too far.

Also, another point which may puzzle the reader is that in the above sketch we have not used the irreducibility assumption on the pull-backs of Y. Actually, this appears in the use of Kummer Theory; at that stage, we need that all the primes dividing the order of the torsion point ζ are sufficiently large. To achieve this, the trick is to multiply the points by a large integer $B > 0$, so to kill a 'part' of ζ of small order. Well, this multiplication replaces the cover with a pull-back of it, and now we really need the said assumption.

Still further points concern dimension: on pulling-back the covers, the Lang-Weil Theorem is not sufficiently explicit and the corresponding Weil result works only for curves. To overcome this, we can either use the Bombieri's quantification of Deligne's Riemann-Hypothesis over finite fields (as mentioned in [30]), or reduce to curves by 'cutting' with appropriate algebraic subgroups. (This is the method used in [30], which on the one hand requires proving irreducibility of the said intersections and on the other hand adapts only to products of elliptic curves.) However we do not insist here anymore on these technical points, hoping that the overview we have given has succeeded to describe the methods at least to some small amount.

As to arbitrary finitely generated groups, this seems not to be completely straightforward, but can be dealt with by these methods. Anyway this does introduce any new arithmetical principle, hence we completely disregard this matter here.

References

[1] BOMBIERI E. AND GUBLER W., Heights in Diophantine Geometry, Cambridge Univ. Press, Cambridge 2006.

[2] BOMBIERI E. AND PILA J., *The number of integral points on arcs and ovals*, Duke Math. J. **59** (1989), 337–357.

[3] BROWNAWELL W.D. AND MASSER D., *Vanishing sums in function fields*, Math. Proc. Camb. Phil. Soc. **100** (1986), 427–434.

[4] CORVAJA P., *Rational fixed points for linear group actions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci., Ser. V, **6** (2007), 561–597.

[5] CORVAJA P. AND ZANNIER U., *Some new applications of the subspace theorem*, Compositio Math. **131** (3) (2002), 319–340.

[6] CORVAJA P. AND ZANNIER U., *On the integral points on certain surfaces*, Intern. Math. Res. Notices (2006), 1–20.

[7] DÈBES P., *On the irreducibility of the polynomials $P(t^m, Y)$*, J. Number Theory **42** (2) (1992), 141–157.

[8] DVORNICICH R. AND ZANNIER U., *Cyclotomic diophantine problems (Hilbert Irreducibility and invariant sets for polynomial maps)*, Duke Math. J. **139** (2007).

[9] FERRETTI A. AND ZANNIER U., *Equations in the Hadamard ring of rational functions*, Ann. Scuola Norm. Sup. Pisa, Cl. Sci., Ser. V, **6** (2007), 457–475.

[10] FRIED M., *On Hilbert's Irreducibility Theorem*, J. Number Theory, **6** (1974), 211–231.

[11] FRIED M. AND JARDEN M., *Field arithmetic, Springer-Verlag*.

[12] HEATH-BROWN D.R., *Counting rational points on algebraic varieties*, in: "Analytic Number Theory", LNM **1891**, Springer-Verlag 2002.

[13] HILBERT D., *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzähligen Koeffizienten*, J. reine angew. Math. **110** (1892), 104–129.

[14] LANG S., *Elliptic curves, Diophantine Analysis*, Springer Verlag 1978.

[15] PILA J. AND WILKIE A., *The rational points of a definable set*, Duke Math. J., **33** (2006), 591–616.

[16] SCHINZEL A., Polynomials with special regard to reducibility, Cambridge Univ. Press, Cambridge 2000.

[17] SCHINZEL A., *On Hilbert's Irreducibility Theorem*, Ann. Polonici Math. **XVI** (1965), 333–340.

[18] SCHINZEL A., *An analogue of Hilbert's irreducibility theorem*, Number Theory, W. de Gruyter, Berlin 1990, 509–514.

[19] SCHINZEL A. AND ZANNIER U., *The least admissible value of the parameter in Hilbert's irreducibility theorem*, Acta Arith. **69** (3) (1995), 293–302.

[20] SERRE J-P., Lectures on the Mordell-Weil Theorem, 2-nd ed., Vieweg, 1990.

[21] SERRE J-P., Topics in Galois Theory, Jones and Bartlett, Boston 1992.

[22] SERRE J-P., *On a theorem of Jordan*, Bull. A.M.S. **40** (2003), 429–440.

[23] SERRE J-P., *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (4) (1972), 259–331.

[24] SILVERMAN V., The Arithmetic of Elliptic Curves, *Springer Verlag*, GTM **106**, 1986.

[25] VOLKLEIN H., Groups as Galois Groups, *Cambridge Univ. Press*, Cambridge 1996.

[26] WALKOWIAK Y., *Théorème d'irreductibilité de Hilbert effectif*, Acta Arith. **116** (2005), 343–362.

[27] ZANNIER U., *A proof of Pisot d-th root conjecture*, Annals Math. **2** (2000), 375–383.

[28] ZANNIER U., *On the linear independence of roots of unity over finite extensions of $\mathbb{Q}$*, Acta Arith. **52** (2) (1989), 171–182.

[29] ZANNIER U., *Some applications of Diophantine Approximation to Diophantine Equations*, Forum, Udine 2003.

[30] ZANNIER U., *Hilbert Irreducibility above algebraic groups*, preprint 2009.

AMS Subject Classification: 11C08, 11D72, 11G35

Umberto ZANNIER,
Scuola Normale Superiore,
Piazza dei Cavalieri 7, 56126 Pisa, ITALIA
e-mail: u.zannier@sns.it

Lavoro pervenuto in redazione il 01.04.2009.