ISRAEL JOURNAL OF MATHEMATICS, Vol. 69, No. 3, 1990

FØLNER SEQUENCES AND HILBERT'S IRREDUCIBILITY THEOREM OVER Q†

BY

PAUL FEIT

Department of Mathematics, Princeton University, Princeton, NJ 08544, USA

ABSTRACT

Let $f(X; T_1, \ldots, T_n)$ be an irreducible polynomial over $\mathbf{Q}$. Let B be the set of $\boldsymbol{b} \in \mathbf{Z}^n$ such that $f(X; \boldsymbol{b})$ is of lesser degree or reducible over $\mathbf{Q}$. Let $\mathcal{F} = \{F_j\}_{j=1}^{\infty}$ be a Følner sequence in $\mathbf{Z}^n$ — that is, a sequence of finite nonempty subsets $F_j \subseteq \mathbf{Z}^n$ such that for each $v \in \mathbf{Z}^n$,

$$\lim_{j\to\infty} \frac{|F_j \cap (F_j + v)|}{|F_j|} = 1.$$

Suppose $\mathcal{F}$ satisfies the extra condition that for W a proper $\mathbf{Q}$-subvariety of $\mathbf{P}^n - \mathbf{A}^n$ and $\varepsilon > 0$, there is a neighborhood U of $W(\mathbf{R})$ in the real topology such that

$$\limsup_{j\to\infty} \frac{|F_j \cap U|}{|F_j|} < \varepsilon,$$

where $\mathbf{Z}^n$ is identified with $\mathbf{A}^n(\mathbf{Z})$. We prove

$$\lim_{j\to\infty} \frac{|F_j \cap B|}{|F_j|} = 0.$$

Introduction

Let $X; T_1, \ldots, T_n$ be indeterminates for some $n \in \mathbf{N}$. For $f \in \mathbf{Z}[X; T_1, \ldots, T_n]$ irreducible, define

(1) $\quad V(f) = \{\boldsymbol{b} \in \mathbf{Z}^n : \partial_X f(X; \boldsymbol{b}) < \partial_X f(X; \boldsymbol{T}) \text{ or } f(X; \boldsymbol{b}) \text{ is reducible over } \mathbf{Q}\}.$

If $\boldsymbol{f} = f_1, \ldots, f_k$ is a sequence of irreducible polynomials in $\mathbf{Z}[X; \boldsymbol{T}]$, let $V(\boldsymbol{f}) = \bigcup_{j=1}^{k} V(f_j)$.

The classical Hilbert's Irreducibility Theorem states that $\mathbf{Z}^n - V(\boldsymbol{f})$ is

† The work on this paper was supported by NSF Grant DMS 8601130.
Received March 2, 1989 and in revised form November 13, 1989

infinite for every sequence f of irreducible polynomials. This is a very weak statement about $V(f)$. Much stronger constraints are known, both for general f and for those sequences with further restrictions; see, for example, the work of Cohen [1] and Fried [3], [4].

Let $\mathcal{F} = \{F_j\}_{j=1}^{\infty}$ be a sequence of finite non-empty subsets of $\mathbf{Z}^n$. Then $\mathcal{F}$ is a Følner sequence if for each $v \in \mathbf{Z}^n$,

$$\lim_{j\to\infty} \frac{|F_j \cap (F_j + v)|}{|F_j|} = 1. \tag{2}$$

In ergodic theory, one can define a higher dimensional "time average" of a bounded function $f: \mathbf{Z}^n \to \mathbf{R}$ by

$$\limsup_{j\to\infty} \frac{1}{|F_j|} \left\{ \sum_{x\in F_j} f(x) \right\}, \tag{3}$$

which has the translation invariant properties of the classical time average. Furstenberg considers higher dimensional averages in [5]. Define the $\mathcal{F}$-density of a subset $B \subseteq \mathbf{Z}^n$ by

$$\delta(B) = \limsup_{j\to\infty} \frac{|B \cap F_j|}{|F_j|}. \tag{4}$$

When $\mathcal{F}$ is a Følner sequence, the function δ has many of the properties of a Haar measure — e.g., translation invariance, positivity — but vanishes on finite subsets. Our main theorem is

THEOREM A. *Let ∞ be the variety $\mathbf{P}^n - \mathbf{A}^n$, and identify $\mathbf{Z}^n$ with $\mathbf{A}^n(\mathbf{Z})$. Suppose $\mathcal{F}$ is a Følner sequence and δ satisfies the following condition: if W is a proper $\mathbf{Q}$-subvariety of ∞ and $\varepsilon > 0$, then there is a neighborhood U of $W(\mathbf{C})$, with respect to the complex topology of $\mathbf{P}^n(\mathbf{C})$, such that $\delta(\mathbf{Z}^n \cap U) < \varepsilon$. In this case, $\delta(V(f)) = 0$ for every sequence of irreducible polynomials f in $\mathbf{Z}[X; T_1, \ldots, T_n]$.*

For example, setting F_j equal to the set of integer points in $[-j, j]^n$ determines a Følner sequence which satisfies the hypothesis. In this case, Cohen shows that $V(f) \cap F_j$ grows at order at most $j^{n-1/2}\log(j)$, and also characterizes the bounding constant. His argument uses number theory to produce a global estimate based on local analysis at each prime of $\mathbf{Z}$. Our result is not so sharp; we assume the theorem fails and produce a contradiction in a non-constructive manner.

We should mention that other, more constructive, methods can be used to describe a set of the form $V(f)$. A set H is called a universal Hilbert subset (UHS) if $H \cap V(f)$ is finite for any choice of f. Sprindžuk [11], [12] has explicitly given UHSs; in some cases, he has a criteria for an irreducible f under which $H \cap V(f)$ is computable.

The proof of Theorem A is modeled on Hilbert's original argument [7]. The reasoning is combinatorial rather than number theoretic. Our generalization relies heavily on work of Furstenberg which extends a lemma used by Hilbert to higher dimensions:

(5) *the Van der Waerdon condition*: if δ is an $\mathscr{F}$-density for some Følner sequnce $\mathscr{F}$, $v \in \mathbf{Z}^n$ and $B \subseteq \mathbf{Z}^n$ so $\delta(B) > 0$, then there is $k \in \mathbf{N}$ so $\delta(B \cap (B + kv)) > 0$.

We include a short proof, conveyed to the author by Furstenberg in conversation.

The author does not know if the condition on $\mathscr{F}$ in Theorem A is necessary. We will first give an example where it fails, and then outline the proof of Theorem A to illustrate our present need for the restriction. Suppose $n = 2$, and for $j \in \mathbf{N}$ let G_j be the set of integer points in $\mathbf{R}^2$ which are less than distance j from $(2^j, 0)$. Let δ' be the corresponding density. If $M \subseteq \mathbf{Z}^n$, then $\delta(M) = 0$ unless the closure of M in $\mathbf{P}^2$ contains the point with homogeneous coordinates $[1, 0, 0]$; in practice, δ' detects only behavior near this point.

Suppose $f \in \mathbf{Z}[X; T_1, \ldots, T_n]$ is irreducible. Put

$$W = \{(r, t_1, \ldots, t_n) \in \mathbf{C}^{n+1} : f(x; t_1, \ldots, t_n) = 0\}. \tag{6}$$

We may regard W as an algebraic variety defined over $\mathbf{Q}$, and regard $(x; \boldsymbol{t}) \to (\boldsymbol{t})$ as an algebraic projection to $\mathbf{A}^n \subseteq \mathbf{P}^n$. Our sole interest in W is that it admits a rational function $\alpha : (x; \boldsymbol{t}) \to x$ which may naturally be treated as a root of f. Without loss of generality, we may replace W by a normalization; smoothing W is permissible. In particular, we may enlarge W and extend projection to a function $\theta : W \to \mathbf{P}^n$ whose image now overlaps ∞. Let B be a set of $\boldsymbol{b} \in \mathbf{Z}^n$ such that α assumes an integer value on $\theta^{-1}\boldsymbol{b}$. Theorem A reduces to the claim that if $\delta(B) > 0$, then $\partial_X f = 1$ — that is, α is the pullback of a polynomial on $\mathbf{P}^n$. If $x \in W$ is a smooth point at which

(7.a) α is holomorphic,

(7.b) $\theta(x)$ is a limit point of B, and some technical conditions hold, it is not difficult to prove that α must be a constant. Now suppose $x \in W$ such that $\theta(x) \in \bar{B} \cap \infty$ and the only poles of the divisor of α at x lie along ∞. We may reduce this pole by replacing α, regarded as a "multivalued function" on $\mathbf{P}^n$, by $\alpha(\boldsymbol{T}) - \alpha(\boldsymbol{T} + \boldsymbol{b})$ where $\boldsymbol{b} \in \mathbf{Z}^n$. Property (5) enables us to do the replacement without losing essential properties of the original α. After finitely many such replacements, we produce α' with no pole at x, and this α' must be a constant. Then an algebraic argument demonstrates that the initial α must have been polynomial.

In the last paragraph, the crucial requirement on α and x is that the only pole of α at x lies along ∞. This restriction fails for each x on a $\mathbf{Q}$-subvariety of codimension 2. If δ does not satisfy the hypothesis of Theorem A, as our example δ' does not, there might not be a suitable x.

Our thumbnail sketch of the argument is slightly disingenuous. We shall not construct a variety W; instead, roots of polynomials are characterized as complex meromorphic germs rather than algebraic functions. The difficulty is that once a suitable W and α are fixed, the algebraic object $\alpha(\boldsymbol{T} + \boldsymbol{b})$ for some $\boldsymbol{b} \in \mathbf{Z}^n$ need not be defined on W. Essentially, to define $\alpha(\boldsymbol{T} + \boldsymbol{b})$ one must first specify a splitting field L of $f(X; \boldsymbol{T})$ *and* of $f^* = f(X; \boldsymbol{T} + \boldsymbol{b})$, identify α with a root of f in L, and chose a prime of L over ∞. Instead of shifting varieties, we (essentially) fix a smooth open subset U of W, and consider the field K of complex meromorphic germs of $U \cap \theta^{-1}\infty$. For our choice U, K will contain the unramified closure for a completion of the function field of W with respect to a choice of prime over ∞. In addition, K will be closed under $\alpha \mapsto \alpha(\boldsymbol{T} + \boldsymbol{b})$. In the paper, U and K are constructed without reference to varieties.

The main theorem is stated in Section 1; we include elementary reductions to the simpler Proposition 1.4. Section 2 is a review of Følner sequences. Section 3 offers a formal treatment on lifting homomorphisms $\alpha(\boldsymbol{T}) \mapsto \alpha(\boldsymbol{T} + \boldsymbol{b})$ to extension fields of $\mathbf{Q}(\boldsymbol{T})$. In Section 4, we prove a higher dimensional analogue to the fact that a holomorphic germ about $\infty \in \mathbf{P}^1$ which vanishes on an infinite set of integers must be 0. Constructions in Section 5 yield fields of meromorphic germs which are closed under the algebraic homomorphisms of Section 3, and yet are sufficiently geometric that Theorem 4.2 applies. The proof of the main theorem, in Section 6, falls from machinery of the previous three sections.

I would like to thank T. Tamagawa and S. Kakutani for suggesting this problem. I am indebted to H. Furstenberg for his insights into the combinatorics of the higher dimensional case; Section 2 is based on discussions with him. I. N. Bernstein convinced me that Hilbert's classical analysis at the point ∞ of

$\mathbf{P}^1$ applies to the generic point at $\mathbf{P}^n - \mathbf{A}^n$ for $n > 1$. Finally, I am grateful to all of the mathematicians who have permitted me to introduce this question into conversation.

§0. Notation

§0.A. Basics

Let **N**, **Z**, **Q**, **R** and **C** denote the sets of natural, integral, rational, real and complex numbers, respectively. For $n \in \mathbf{N}$, let

$$\mathbf{N}(n) = \{m \in \mathbf{N}\,;\, m \leqq n\}. \tag{0.1}$$

For $b \in \mathbf{C}$ and $r \in (0, \infty)$, put

$$B(b, r) = \{z \in \mathbf{C} : |z - b| < r\}. \tag{0.2}$$

By "ring", we mean commutative ring with non-zero identity. For R a ring and $t_1, \ldots, t_n$ a list of members in a larger ring of indeterminates, let $R[t_1, \ldots, t_n]$ denote the ring generated by R and $t_1, \ldots, t_n$; if R is a field, let $R(t_1, \ldots, t_n)$ be the field generated by $R[t_1, \ldots, t_n]$. In the case where $t_1, \ldots, t_n$ are indeterminates, let ∂_j denote the degree map with respect to t_j for each $j \in \mathbf{N}(n)$.

For S and T sets, let

$$S \triangle T = (S - T) \cup (T - S). \tag{0.3}$$

If S is a finite set, then denote the cardinality of S by $|S|$. The closure of a subset S of a topological space is denoted by $\bar{S}$.

§0.B. Projective spaces

Fix $n \in \mathbf{N}$. Let $\mathbf{P}^n$ denote n-dimensional projective space, which we regard both as a **Z**-scheme and as the corresponding complex manifold. In cases of possible ambiguity, denote by $\mathbf{P}^n(K)$ the set of K-rational points of $\mathbf{P}^n$ for a ring K. In a topological context, $\mathbf{P}^n$ always refers to the corresponding complex manifold.

Fix a choice $t_1, \ldots, t_{n+1}$ of homomogeneous coordinates. For $z = (z_1, \ldots, z_{n+1}) \in \mathbf{C}^{n+1} - \{0\}$, denote the corresponding class in $\mathbf{P}^n$ by $[z]$ or $[z_1, \ldots, z_{n+1}]$. For $j \in \mathbf{N}(n+1)$, we refer to the map

$$(x_1, \ldots, x_n) \in \mathbf{C}^n \mapsto [x_1, \ldots, x_{j-1}, 1, x_j, \ldots, x_n] \in \mathbf{P}^n \tag{0.4}$$

or its image as the j-th chart. Throughout the paper, we regard the n-dimensional affine scheme $\mathbf{A}^n$ as a subscheme of $\mathbf{P}^n$ via the $n+1$-st chart. The subvariety $t_{n+1}=0$ is denoted by ∞. Finally, we identify $\mathbf{C}^n$ with $\mathbf{A}^n(\mathbf{C}) \subseteq \mathbf{P}^n(\mathbf{C})$.

The term "affine transformation" will refer to either of two sorts of map. A function $\mathbf{Z}^n \to \mathbf{Z}^n$ of the form $x \mapsto L(x)+v$ where $v \in \mathbf{Z}^n$ and L is an invertible group homomorphism is called affine. If $L' : \mathbf{Z}^n \times \mathbf{Z} \to \mathbf{Z}^n \times \mathbf{Z}$ is a group isomorphism such that $L'(\{0\}) \times \mathbf{Z}) \subseteq \{0\} \times \mathbf{Z}$, then L' determines an algebraic automorphism of $\mathbf{P}^n$ which preserves the subscheme $\mathbf{A}^n$; such an automorphism is also called affine. There is a bijection from affine transformations of $\mathbf{P}^n$ to affine transformations of $\mathbf{Z}^n$ determined by restriction to $\mathbf{A}^n(\mathbf{Z})$.

§0.C. Germs

Let X and Y be topological spaces, and let $N \subseteq X$. By a Y-valued function element about N, we mean a continuous function f from a neighborhood of N to Y. Two Y-valued function elements f and g are considered equivalent if they agree on a neighborhood of N. An equivalence class of function elements is called a (Y-valued) N-germ.

We adopt the standard conventions concerning germs of functions, and freely identify a germ with any function which represents it. If X is a complex manifold and $N \subseteq X$, denote the ring of holomorphic germs into $\mathbf{C}$ by $\mathcal{O}_N$. If N is connected, then $\mathcal{O}_N$ is a domain, and we define $\mathcal{M}_N$, the field of meromorphic N-germs, to be the field of fractions of θ_N. (This notion of meromorphic may be more restrictive than that with which the reader is familiar, but is sufficient for our needs.)

Suppose X is a complex manifold, $N \subseteq X$ is a connected non-empty subset and $\theta : X \to \mathbf{P}^n$ is an open mapping whose image lies in $\mathbf{P}^n$ minus a hyperplane. Then $f \mapsto f \circ \theta$ determines an injection from the rational functions on $\mathbf{P}^n(\mathbf{C})$ into $\mathcal{M}_N$. When the choice of θ is clear from the context, regard $\mathcal{M}_N$ as an extension field of $\mathbf{C}(T_1, \ldots, T_n)$.

§1. Statements and reductions

Fix $n \in \mathbf{N}$. Let $J(n)$ be the set of all subsets of $\mathbf{Z}^n$.

DEFINITION 1.1. A (n-dimensional) density is a function $\delta : J(n) \to [0, 1]$ such that

(1.1.a) $$\forall S, T \in J(n), \qquad \delta(S \cup T) \leqq \delta(S) + \delta(T),$$

(1.1.b) $\forall S, T \in J(n), \quad (S \subseteq T \Rightarrow \delta(S) \leqq \delta(T),$

(1.1.c) $\forall S \in J(n), \quad \forall v \in \mathbf{Z}^n, \quad \delta(S+v) = \delta(S),$

(1.1.d) $\delta(\{0\}) = 0.$

Note that the density of any finite set is 0.

Let δ be a density. We say that δ satisfies the VW (or Van der Waerdon) condition if

(1.2) for $S \in J(n)$ and $v \in \mathbf{Z}^n$ so $\delta(S) > 0$, there is $k \in \mathbf{N}$ so $\delta(S \cap (S + kv)) > 0$.

Let W be a proper $\mathbf{Q}$-subvariety of $\infty \subseteq \mathbf{P}^n$. We say δ is concentrated on W if

(1.3) there exists $\varepsilon > 0$ such that for every open neighborhood U of $W(\mathbf{C})$, $\delta(U \cap \mathbf{Z}^n) \geqq \varepsilon$.

We say δ is $\mathbf{Q}$-diffuse if it is not concentrated on any proper $\mathbf{Q}$-subvariety.

Existence of $\mathbf{Q}$-diffuse densities satisfying the VW condition is discussed in Section 2.

Fix indeterminates $X; T_1, \ldots, T_n$. We frequently write $\boldsymbol{T}$ for $T_1, \ldots, T_n$. For $g \in \mathbf{Q}[\boldsymbol{T}]$, let

(1.4) $$Z(g) = \{\boldsymbol{b} \in \mathbf{Z}^n : g(\boldsymbol{b}) = 0\}.$$

By the roots of $f \in \mathbf{Q}[X; \boldsymbol{T}]$, we always mean the roots of f regarded as a polynomial in X over ground field $\mathbf{Q}(\boldsymbol{T})$. In particular, $\boldsymbol{b} = (b_1, \ldots, b_n) \in \mathbf{Z}^n$ is said to preserve the Galois group of a separable $f \in \mathbf{Z}[X; \boldsymbol{T}]$ if the substitution homomorphism $T_j \mapsto b_j$ extends to the roots of f in a manner which identifies the Galois permutation groups for $f(X; \boldsymbol{T})$ and $f(X; \boldsymbol{b})$. For $f \in \mathbf{Z}[X; \boldsymbol{T}]$, put

(1.5)
$$G(f) = \{\boldsymbol{b} \in \mathbf{Z}^n : \boldsymbol{b} \text{ does not preserve the Galois group of } f\},$$
$$V(f) = \{\boldsymbol{b} \in \mathbf{Z}^n : \partial_X f(X; \boldsymbol{b}) < \partial_X f(X; \boldsymbol{T}) \text{ or } f(X; \boldsymbol{b}) \text{ is reducible}\},$$

and, if $\partial_X f \geqq 2$, put

(1.6) $$I(f) = \{\boldsymbol{b} \in \mathbf{Z}^n : \partial_X f(X; \boldsymbol{b}) < \partial_X f(X; \boldsymbol{T}) \text{ or } f(X; \boldsymbol{b}) \text{ has an integer root}\}.$$

Our main theorem is

THEOREM 1.1. *Let $n \in \mathbf{N}$, let $X; T_1, \ldots, T_n$ be indeterminates over $\mathbf{Q}$, and let $f(X; T_1, \ldots, T_n)$ be an irreducible polynomial in the ring $\mathbf{Q}[X; T_1, \ldots, T_n]$*

which has positive degree in the variable X. Let δ be an n-dimensional $\mathbf{Q}$-diffuse density which satisfies the VW condition. Then $\delta(G(f))=0$.

A few lemmas reduce Theorem 1.1 to a statement which does not involve Galois groups. Begin with

LEMMA 1.2. *Let $f\in\mathbf{Q}[X;\boldsymbol{T}]$ be irreducible. Then there is a list of polynomials $g_1,\ldots,g_k\in\mathbf{Z}[\boldsymbol{T}]-\{0\}$ and a list of monic irreducible polynomails $h_1,\ldots,h_m\in\mathbf{Z}[X;\boldsymbol{T}]$, each of degree >1 in X, for which*

$$G(f)\subseteq\left\{\bigcup_{j=1}^{k} Z(g_j)\right\}\cup\left\{\bigcup_{i=1}^{m} I(h_i)\right\}. \tag{1.7}$$

PROOF. This reduction is already in [7], and has been extended to other cases — see [3], for example. We outline the proof.

First, suppose $f\in\mathbf{Q}[X;\boldsymbol{T}]$ is an irreducible polynomial of degree $\geqq 2$ in X. Let $\alpha_1,\ldots,\alpha_r$ be the roots of f, let $K=\mathbf{Q}(\boldsymbol{T})[\alpha_1,\ldots,\alpha_r]$, and let π be a generator of K over $\mathbf{Q}(\boldsymbol{T})$ which is integral over $\mathbf{Z}[\boldsymbol{T}]$. Let f^* be the monic irreducible polynomial of π over $\mathbf{Q}(\boldsymbol{T})$. Express π as a $\mathbf{Q}(\boldsymbol{T})$-linear sum of powers of $\alpha_1,\ldots,\alpha_r$, and, for each $j\in\mathbf{N}(r)$, express α_j as a $\mathbf{Q}(\boldsymbol{T})$-linear sum of powers of π; regarding each member of $\mathbf{Q}(\boldsymbol{T})$ as a ratio in $\mathbf{Z}[\boldsymbol{T}]$, let g be a least common multiple for the set of all denominators of coefficients appearing in these expressions. The reader may easily verify that if $\boldsymbol{b}\in\mathbf{Z}^n$ has the property that $f^*(X;\boldsymbol{b})$ is irreducible over $\mathbf{Q}$ and $g(\boldsymbol{b})\neq 0$, then the corresponding substitution homomorphism extends to an identification of roots such that the Galois closures of $f(X;\boldsymbol{T})$ and $f(X;\boldsymbol{b})$ have the same degree over their respective ground fields. It follows that $G(f)\subseteq Z(g)\cup V(f^*)$.

Now fix a monic irreducible polynomial $f\in\mathbf{Z}[X;\boldsymbol{T}]$ of degree $\geqq 2$ in X. Let $\alpha_1,\ldots,\alpha_r$ be the roots of f. For $N\subseteq N(r)$, let $P(N)$ be the set of values of the Newton symmetric polynomials in $|N|$ variables on $\{\alpha_j\}_{j\in N}$. Put

$$P=\bigcup\{P(N):N\subseteq\mathbf{N}(r)\}-\mathbf{Q}[\boldsymbol{T}]. \tag{1.8}$$

For $N\subseteq\mathbf{N}(r)$ so $N\notin\{\phi,\mathbf{N}(r)\}$, there is at least one member of $P(N)$ in P. Let $h_1,\ldots,h_m$ be a list of all monic irreducible polynomials for elements in P.

Suppose $\boldsymbol{b}\in\mathbf{Z}^n$ such that $f(X;\boldsymbol{b})$ is reducible. Reducibility may be interpreted to mean that there is a prime β of the splitting field of f over the ideal generated by $\{T_j-b_j\}_{j=1}^{n}$ in $\mathbf{Q}[\boldsymbol{T}]$ and a proper non-empty subset $N\subseteq\mathbf{N}(r)$ such that

$$(1.9) \qquad \prod_{j\in N}(X-\alpha_j), \quad \prod_{j\notin N}(X-\alpha_j)$$

are, modulo β, polynomials in $\mathbf{Q}[X]$. Moreover, the product of the factors in (1.9) mod(β) has coefficients in $\mathbf{Z}$, so each factor has integral coefficients. For each h_s which admits a symmetric combination of $\{\alpha_j\}_{j\in N}$ as a root, $h_s(X;\boldsymbol{b})$ has an integral root. As $\boldsymbol{b}$ was arbitrary, we deduce that $V(f)\subseteq\bigcup_{s=1}^m I(h_s)$. □

LEMMA 1.3. *Let δ be an n-dimensional density which satisfies the VW condition. Suppose $S\subseteq\mathbf{Z}^n$, $m\in\mathbf{N}$ and $v\in\mathbf{Z}^n-\{0\}$ such that*

$$(1.10) \qquad |\{k\in\mathbf{N}: x+kv\in S\}|\leqq m \qquad \text{for each } x\in S.$$

Then $\delta(S)=0$.

PROOF. Assume $\delta(S)>0$, and then a simple induction based on the VW condition yields a contradiction. □

COROLLARY 1.3.1. *Let δ be an n-dimensional density which satisfies VW condition. Fix $T_1,\dots,T_n$ indeterminates, and let $p(T_1,\dots,T_n)\in\mathbf{Z}[T_1,\dots,T_n]-\{0\}$. Then $\delta(Z(p))=0$.*

PROOF. Proof is by induction on the index $k\in\mathbf{N}(n)\cup\{0\}$ such that $p\in\mathbf{Z}[T_1,\dots,T_k]$. When $k=0$, p is a non-zero constant and the claim is vacuous.

Suppose k is given for which $\delta(Z(q))=0$ for each $q\in\mathbf{Z}[T_1,\dots,T_k]-\{0\}\subseteq\mathbf{Z}[T_1,\dots,T_n]$, and assume $p\in\mathbf{Z}[T_1,\dots,T_{k+1}]-\{0\}$. Let m and $q(T_1,\dots,T_k)$ be respectively the degree and leading coefficient of p, regarded as a polynomial in T_{k+1}. Put

$$(1.11) \qquad \begin{aligned} J&=\{(b_1,\dots,b_n)\in\mathbf{Z}^n: p(b_1,\dots,b_n)=0\},\\ J_1&=\{(b_1,\dots,b_n)\in\mathbf{Z}^n: q(b_1,\dots,b_n)=0\},\\ J_2&=J-J_1. \end{aligned}$$

By assumption, J_1 has density 0. Let v be the $k+1$-standard basis vector of $\mathbf{Z}^n$. For $\boldsymbol{b}\in\mathbf{Z}^n$, there are at most m values in

$$(1.12) \qquad \{\boldsymbol{b}+rv: r\in\mathbf{N}\}\cap J_2$$

because $p(b_1,\dots,b_k,T_{k+1},\dots,T_n)$ has no more than m roots as a polynomial in T_{k+1} over $\mathbf{Q}$. Hence $\delta(J_2)=0$, and $\delta(J)\leqq\delta(J_1\cup J_2)\leqq\delta(J_1)+\delta(J_2)$ must be 0. □

Theorem 1.1 has been reduced to the following proposition, whose proof occupies all sections after §2:

PROPOSITION 1.4. *Let f be a monic irreducible polynomial of $\mathbf{Z}[X; T_1, \ldots, T_n]$ whose degree in X is $\geqq 2$, and let δ be an n-dimensional $\mathbf{Q}$-diffuse density which satisfies the VW condition. Then $\delta(I(f)) = 0$.*

§2. Følner sequences

We give an argument, due to Furstenberg, demonstrating that a density derived from a Følner sequence must satisfy the VW condition. A few comments concerning the "**Q**-diffuse" condition are included.

Throughout this section, $n \in \mathbf{N}$ is fixed. Let $\mathscr{F}$ be the set of functions from $\mathbf{N}$ into the space of non-empty finite subsets of $\mathbf{Z}^n$. For $F \in \mathscr{F}$ and $v \in \mathbf{Z}^n$, let "$F + v$" denote the function $k \mapsto F[k] + v$.

There is an equivalence relation on $\mathscr{F}$, which we denote by "$\sim$", such that for $F, G \in \mathscr{F}$,

$$F \sim G \Leftrightarrow \lim_{k \to \infty} |F[k] \triangle G[k]| / |F[k]| = 0. \tag{2.1}$$

For $F \in \mathscr{F}$ and $S \subseteq \mathbf{Z}^n$, define the F-density of S to be

$$\delta_F(S) = \limsup_{k \to \infty} |S \cap F[k]| / |F[k]|. \tag{2.2}$$

A member $F \in \mathscr{F}$ is called a (n-dimensional) Følner sequence if $F \sim F + v$ for each $v \in \mathbf{Z}^n$.

The following comments are elementary; verification is left to the reader. For F a Følner sequence and $\delta = \delta_F$,

(2.3.a) for $S \subseteq \mathbf{Z}^n$, $\delta(S) \in [0, 1]$,
(2.3.b) for $S \subseteq T \subseteq \mathbf{Z}^n$, $\delta(S) \leqq \delta(T)$,
(2.3.c) for $S, T \subseteq \mathbf{Z}^n$, $\delta(S \cup T) \leqq \delta(S) + \delta(T)$,
(2.3.d) if F is a Følner sequence, them $\lim_{k \to \infty} |F[k]| = \infty$,
(2.3.e) if $G \in \mathscr{F}$ and $G \sim F$, then G is a Følner sequence and $\delta = \delta_G$,
(2.3.f) a subsequence of a Følner sequence is a Følner sequence,
(2.3.g) if F is a Følner sequence, $S \subseteq \mathbf{Z}^n$ and $v \in \mathbf{Z}^n$, then $\delta(S + v) = \delta(S)$,
(2.3.h) if F is a Følner sequence and $\{v_k\}_{k=1}^{\infty}$ is a sequence in $\mathbf{Z}^n$, then $k \mapsto F[k] + v_k$ is a Følner sequence,
(2.3.i) if F is a Følner sequence and $L : \mathbf{Z}^n \to \mathbf{Z}^n$ is an additive automorphism, then $L \circ F$ is a Følner sequence,

(2.3.j) $\delta_F(\mathbf{Z}^n) = 1$ and $\delta(\{0\}) = 0$.

The combinatorics of Følner sequences can be placed in the context of ergodic theory. Regard the set of functions $\mathbf{Z}^n \to [0, 1]$ as a product of a family of copies of $[0, 1]$ indexed by $\mathbf{Z}^n$; let X denote this set with the product topology. For $v \in \mathbf{Z}^n$, let T_v denote the continuous function $X \to X$ such that

$$(2.4) \qquad (T_v f)(x) = f(x + v) \qquad \text{for } f \in X \text{ and } x \in \mathbf{Z}^n.$$

Clearly $T_v \circ T_w = T_{v+w}$ for $v, w \in \mathbf{Z}^n$. For Y another topological space, let $C(X, Y)$ denote the set of continuous functions $X \to Y$.

Let $\mathcal{P}$ denote the set of probability measures on $\mathcal{B}$, the Borel ring of X. Then $\mathcal{P}$ is compact with respect to the topology induced by the family of functions

$$(2.5) \qquad \{(\mu \mapsto \int f d\mu) : f \in C(X, [0, 1])\},$$

which is called the weak topology. For $T : X \to X$ a continuous function and $\mu \in \mathcal{P}$, define $T^*\mu \in \mathcal{P}$ by $(T^*\mu)(A) = \mu(T^{-1}(A))$ for $A \in \mathcal{B}$. Tautologically, $\mu \mapsto T^*\mu$ is continuous on $\mathcal{P}$. For $\theta \in X$, let $\mu_\theta \in \mathcal{P}$ be the unique measure such that $\int f d\mu_\theta = f(\theta)$ for $f \in C(X, \mathbf{R})$. If $f \in C(X, \mathbf{R})$, $\theta \in X$ and $v \in \mathbf{Z}^n$,

$$(2.6) \qquad \int f d(T_v^*\mu_\theta) = f(T_v(\theta)).$$

Let $\pi_0 : X \to [0, 1]$ be the function $\pi_0(\theta) = \theta(0)$.

We are ready to prove

THEOREM 2.1 (Furstenberg). *A Følner density satisfies the VW condition.*

PROOF. Fix F a Følner sequence, $S \subseteq \mathbf{Z}^n$ such that $\delta_F(S) > 0$, and $\boldsymbol{b} \in \mathbf{Z}^n$. Define $\theta : \mathbf{Z}^n \to [0, 1]$ by

$$(2.7) \qquad \theta(x) = \begin{cases} 1 & \text{if } x \in S, \\ 0 & \text{if } x \notin S. \end{cases}$$

Let F_0 be a subsequence of F such that

$$(2.8) \qquad \lim_{k \to \infty} |S \cap F_0[k]| / |F_0[k]| = \delta_{F_0}(S).$$

By the diagonal argument, there is a subsequence F_1 of F_0 such that for $m \in \mathbf{N}$ and $v_1, \ldots, v_m \in \mathbf{Z}^n$, there is a value $c(v_1, \ldots, v_m) \in [0, 1]$ such that

$$(2.9) \qquad \lim_{k \to \infty} |F_1[k]|^{-1} \sum_{x \in F_1[k]} (\theta(x + v_1) \cdots \theta(x + v_m)) = c(v_1, \ldots, v_m).$$

Since $\mathscr{P}$ is compact, there is a subsequence F_2 of F_1 and a measure $\nu \in \mathscr{P}$ such that

$$|F_2[k]|^{-1} \sum_{x \in F_2[k]} T_x^* \mu_\theta \to \nu. \tag{2.10}$$

Let $v \in \mathbf{Z}^n$. Continuity implies

$$\begin{aligned} T_v^* \nu &= \lim_{k\to\infty} T_v^*\left(|F_2[k]|^{-1} \cdot \sum_{x\in F_2[k]} T_x^* \mu_\theta \right) \\ &= \lim_{k\to\infty} |F_2[k]|^{-1} \cdot \sum_{x\in F_2[k]} T_{x+v}^* \mu_\theta \qquad (2.11) \\ &= \lim_{k\to\infty} |F_2[k]+v|^{-1} \cdot \sum_{x\in F_2[k]+v} T_x^* \mu_\theta. \end{aligned}$$

For $f \in C(X, [0,1])$, put

$$D = \left| \int f d\nu - \int f d(T_v^* \nu) \right| \tag{2.12}$$

and then

$$\begin{aligned} D &= \lim_{k\to\infty} \left| |F_2[k]|^{-1} \left\{ \sum_{x\in F_2[k]} f(T_x\theta) - \sum_{x\in F_2[k]+v} f(T_x\theta) \right\} \right|, \qquad (2.13) \\ \Rightarrow D &\leqq \liminf_{k\to\infty} \left\{ |F_2[k]|^{-1} \sum_{x\in F_2[k]\triangle(F_2[k]+v)} |f(T_x\theta)| \right\}, \\ \Rightarrow D &\leqq \liminf_{k\to\infty} \frac{|F_2[k]\triangle(F_2[k]+v)|}{|F_2[k]|} = 0. \end{aligned}$$

Thus, $T_v^* \nu = \nu$.

Unwinding definitions yield that for $m \in \mathbf{N}$ and $v_1, \ldots, v_m \in \mathbf{Z}^n$,

$$\int (\pi_0 \circ T_{v_1}) \cdots (\pi_0 \circ T_{v_m}) d\nu = c(v_1, \ldots, v_m). \tag{2.14}$$

Then $\pi_0 \in C(X, [0,1])$ and $\int \pi_0 d\nu = c(0) = \delta_F(S) > 0$. Let $T = T_{\mathbf{b}}$. By the Poincaré Recurrence Theorem, there is $d \in \mathbf{N}$ such that $\int \pi_0 \cdot (\pi_0 \circ T^d) d\nu > 0$. As $T^d = T_{d\mathbf{b}}$, we conclude

$$\lim_{k\to\infty} |F_2[k]|^{-1} \cdot \sum_{x\in F_2[k]} \theta(x) \cdot \theta(x + d\mathbf{b}) = c(0, d\mathbf{b}) > 0, \tag{2.15}$$

where

$$(2.16)\quad |F_2[k]|^{-1} \cdot \sum_{x \in F_2[k]} \theta(x) \cdot \theta(x + d\mathbf{b}) = |S \cap S - d\mathbf{b}) \cap F_2[k]|/|F_2[k]|,$$

for each $k \in \mathbf{N}$. Consequently $\delta_F(S \cap (S - d\mathbf{b})) > 0$. □

Let W be a subset of $\infty \subseteq \mathbf{P}^n(\mathbf{R})$. Put

$$(2.17)\qquad L(W) = \{(z_1, \ldots, z_n) \in \mathbf{R}^n : [z_1, \ldots, z_n, 0] \in W\}.$$

For $\theta \in (0, 2\pi)$, let $L(W, \theta)$ be the set of non-zero vectors in $\mathbf{R}^n$ which make an angle of $< \theta$ with some member of L. Let δ be an n-dimensional density. The reader should convince himself that δ is $\mathbf{Q}$-diffuse if and only if for every proper $\mathbf{Q}$-subvariety V of ∞ and every $\varepsilon > 0$, there is $\theta \in (0, 2\pi)$ such that $\delta(L(V(\mathbf{R}), \theta)) < \varepsilon$. The latter geometric criterion can often be verified by computational methods.

Let ν be a Haar measure — that is, a volume — on $\mathbf{R}^n$. A simple example of a Følner sequence which produces a $\mathbf{Q}$-diffuse density is given by

Proposition 2.2. *Suppose U is a bounded subset of $\mathbf{R}^n$ whose closure and interior have the same positive volume. Let $\{r_k\}_{k=1}^{\infty}$ be a sequence of positive numbers that converges to ∞. Then (provided that none of its members is empty), the sequence*

$$(2.18)\qquad F : k \mapsto \{v \in \mathbf{Z}^n : v \in r_k \cdot U\}$$

is a Følner sequence whose denisty is $\mathbf{Q}$-diffuse.

Proof. We sketch the argument. The details are exercises in elementary measure theory. Let $I = [0, 1)^n$, and normalize ν so $\nu(I) = 1$. Then for D a measureable subset of $\mathbf{R}^n$,

$$(2.19)\qquad |\{w \in \mathbf{Z}^n : w + I \cap D \neq \varnothing\}| \geqq \nu(D)$$

where the cardinality on the left is the volume of $\bigcup\{w + I : w \in E\}$ where $E = \{w \in \mathbf{Z}^n : w + I \cap D \neq \varnothing\}$.

First, let $\varepsilon \in (0, 1)$. There is a compact subset C of $\mathrm{Int}(U)$ such that $\nu(C) > (1 - \varepsilon)\nu(U)$, and an open neighborhood V of $\overline{U}$ such that $\nu(V) < (1 + \varepsilon)\nu(U)$. Let ρ be the smaller of the distances from C to the complement of $\mathrm{Int}(U)$ and from $\overline{U}$ to the complement of V.

Let $v \in \mathbf{Z}^n$, and suppose $r > (\|v\| + \sqrt{n})/\rho$. For $w \in \mathbf{Z}^n$.

$$w \in rU \Rightarrow w + I \subseteq rV,$$

$$(2.20) \qquad w + I \cap rC \neq \varnothing \Rightarrow w, w + v \in rU,$$

$$w + I \cap rU \neq \varnothing \Rightarrow w \in rV.$$

From (2.19) and (2.20), we conclude that for $k \gg 0$

$$(2.21) \qquad \frac{1-\varepsilon}{1+\varepsilon} < \frac{|\mathbf{Z}^n \cap r_k U \cap (r_k U - v)|}{|\mathbf{Z}^n \cap r_k U|} < \frac{1+\varepsilon}{1-\varepsilon}.$$

It follows tediously that F is a Følner sequence.

Next, suppose that $W_0 \subseteq \infty$ is a proper **Q**-subvariety, and put $W = W_0(\mathbf{R})$. Again, we leave it to the reader to convince him or herself that for $\theta \in (0, 2\pi)$, $\delta_F(L(W, \theta)) = v(U \cap L(W, \theta))/v(U)$. (This can be verified by approximating the intersection within by compact subsets and outside by open subsets, as in the previous paragraph.) Now $L(W)$ has volume 0, and $L(W) \cap U = \bigcap \{L(W, 1/n) \cap U : n \in \mathbf{N}\}$ is a limit of a decreasing sequence of measurable sets of finite measure. Consequently, for every $\varepsilon > 0$ there is $n \in \mathbf{N}$ for which $v(L(W, 1/n) \cap U) < \varepsilon$. □

REMARK 2.1. For a density of the type constructed in Proposition 2.2, Cohen's estimates [1] yield stronger results than those under consideration. However, **Q**-diffuse densities can be more exotic. For $P \in \infty(\mathbf{R})$, the example in the Introduction can be modified to produce a Følner density which vanishes on $S \subseteq \mathbf{Z}^n$ unless $P \in \bar{S}$; if P is not algebraic over **Q**, such a density is **Q**-diffuse.

§3. The algebra of translation

For $f \in \mathbf{Q}(T_1, \ldots, T_n)$ and $\boldsymbol{b} \in \mathbf{Z}^n$, the element $f(\boldsymbol{T} + \boldsymbol{b}) - f(\boldsymbol{T})$ has a pole along ∞ of order less than that of f. Our present work relies on extending $f \mapsto f(\boldsymbol{T} + \boldsymbol{b})$ to the algebraic functions. As the higher dimensional case is messier than the 1-dimensional argument used in [7], a formal treatment is given here.

For P a polynomial over a ring R and $\sigma : R \to S$ a ring homomorphism, let P^σ denote the polynomial over S derived by replacing each coefficient of P by its image under σ. For k a field, let $k^* = k - \{0\}$; also denote the ring of formal power series in a variable T over k, and its field of fractions, by $k[[T]]$ and $k\langle\langle k \rangle\rangle$, respectively.

THEOREM 3.1. *Let K be a field of characteristic* 0 *and let K^a/K be an algebraic closure. Let $\|$ be a non-Archimedean valuation of K^a whose restriction to K is discrete and complete. Let R and $\mathscr{P}$ be respectively the valuation ring of and the prime ideal of $\|$ restricted to K. We require that* $\mathrm{char}(R/\mathscr{P})=0$. *Let π be a generator of $\mathscr{P}$ and let $\sigma: R \to R$ be a ring automorphism such that $|x-\sigma(x)|<|x|$ if $x=\pi$ or x is a unit of R.*

(A) *Suppose L/K is a subextension of K^a. Then there is a unique ring homomorphism $\tau: L \to K^a$ such that*

$$\tau_{|R}=\sigma \quad \text{and} \quad |x-\tau(x)|<|x| \qquad \text{for all } x \in L^*. \tag{3.1}$$

(B) *Let τ be the unique ring homomorphism which satisfies* (3.1) *for $L=K^a$. Define a function*

$$\Delta(x)=x-\tau(x) \qquad \text{for } x \in K^a. \tag{3.2}$$

Then for $x \in K^a$ and $\varepsilon>0$, there is $m \in \mathbf{N}$ such that $|\Delta^m(x)|<\varepsilon$.

PROOF. Let $R, K, \sigma, \mathscr{P}, \|$ and K^a be as hypothesized. Fix K^c a completion of K^a with respect to $\|$, and denote the norm of K^c by $\|$ as well. Let R^c and $\mathscr{P}^c$ be the ring of $\|$ on K^c and its unique maximal ideal, respectively.

Let Sub be the set of subextensions of K^c/K. For $L \in \mathrm{Sub}$, let $\mathrm{Hm}(L)$ be the set of field homomorphisms $\sigma: L \to K^c$ for which $\sigma(R)=R$. We say $\sigma \in \mathrm{Hm}(L)$ has the $*$-property if $|x-\sigma(x)|<|x|$ for each $x \in L$. Let L^u denote the unramified closure of L in K^c, and let L^0 be the closure of L^u in the $\|$ topology. Also let

$$R^L=R^c \cap L \quad \text{and} \quad \mathscr{P}^L=\mathscr{P}^c \cap L. \tag{3.3}$$

We say L is discrete if the restriction of $\|$ to L is discrete.

Put $k=R^c/\mathscr{P}^c$, and fix $\varphi: R^c \to k$ the canonical projection. For $L \in \mathrm{Sub}$, let $k^L=\varphi(R^L)$.

Suppose $L \in \mathrm{Sub}$ and $\sigma \in \mathrm{Hm}(L)$. Then $\| \circ \sigma = \|$ on K; consequently, if L/K is finite or if σ has the $*$-property, then $\| \circ \sigma = \|$ on L. If σ has the $*$-property and L is discrete, it is clear that

(3.4.a) the continuous extension of σ to the topological closure of L must also have the $*$-property,

$$\varphi \circ \sigma = \varphi \text{ on } R^L. \tag{3.4.b}$$

Put

$$(3.5)\qquad M(\sigma)=\{x\in L^*: |x-\sigma(x)|<|x|\}.$$

If $x, y \in M(\sigma)$,

$$\begin{aligned} &|xy-\sigma(xy)| = |xy - x\sigma(y) + x\sigma(y) - \sigma(x)\sigma(y)| \\ (3.6)\qquad &\Rightarrow |xy-\sigma(xy)| \leqq \max\{|x|\,|y-\sigma(y)|, |x-\sigma(x)|\,|y|\}, \\ &\Rightarrow xy \in M(\sigma), \end{aligned}$$

and

$$\begin{aligned} &|x^{-1}-\sigma(x^{-1})| = |x|^{-1}\cdot|\sigma(x)|^{-1}\cdot|\sigma(x)-x| < |x|^{-1}, \\ (3.7)\qquad &\Rightarrow x^{-1}\in M(\sigma). \end{aligned}$$

Clearly $1\in M(\sigma)$. Thus $M(\sigma)$ is a multiplicative subgroup of L^*. When L is discrete, σ has the $*$-property if the units of R^L and a generator $\mathscr{P}^L$ lie in $M(\sigma)$.

Let $L \in \mathrm{Sub}$ so L/K is finite. By a system of ramified roots for L, we mean a function $\omega: \mathbf{N} \to K^c$ such that

$$(3.8.a)\qquad \forall m, n \in \mathbf{N}, \qquad \omega(mn)^m = \omega(n),$$

$$(3.8.b)\qquad \omega(1) \text{ is a generator of } \mathscr{P}^L \text{ in } R^L.$$

In the context of a fixed system of ramified roots, denote $\omega(1)$ by π. Also, for $r\in\mathbf{Q}$, let π^r be the unique value in K^c such that

$$(3.9)\qquad \forall p\in\mathbf{Z},\quad \forall q\in\mathbf{N},\quad (r=p/q \Rightarrow \pi^r = (\omega(q)^p)).$$

Let T be a formal variable. The theory of discrete valuation rings of residue class field characteristic 0 assures existence of a field isomorphism $\theta: k\langle\langle T\rangle\rangle \to L^0$ such that

$$(3.10.a)\qquad \theta(k[\![T]\!]) = R^{L^0},$$

$$(3.10.b)\qquad \theta(T) = \pi.$$

Consequently, the algebraic closure of L^0 is $\bigcup_{n=1}^{\infty} L^0[\pi^{1/n}]$.

Step I. Uniqueness and Claim (B)

Let $\sigma, \tau \in \mathrm{Hm}(K^a)$ so $\sigma_{|R} = \tau_{|R}$ and σ and τ have the $*$-property. We claim $\sigma = \tau$. Now σ and τ extend continuously to endomorphisms of K^c, and we denote the continuations by σ and τ, respectively.

Let α be a unit of R^{K^u} and let $q(T)$ be the monic minimal polynomial for α. Let L be a splitting field of $q(T)$ over K. Then q^φ is irreducible and separable over k^K. Now $(q^\sigma)^\varphi = q^\varphi$ splits in k^L, and so q^σ also splits in L. As $\sigma(\alpha)$ and $\tau(\alpha)$ are roots of $q^\sigma = q^\tau$ in L whose images $\mathrm{mod}(\mathscr{P}^L)$ agree, we deduce $\sigma(\alpha) = \tau(\alpha)$. Consequently σ and τ agree on K^0.

Fix a system of ramified roots for K. Let T be an indeterminate. For $n \in \mathrm{N}$, there is a unique $d_n(T) \in k[\![T]\!]$ such that

$$d_n(T)^n = 1 + T, \tag{3.11.a}$$

$$d_n(0) = 1. \tag{3.11.b}$$

Let $K^\infty = \bigcup_{n=1}^\infty K^0[\pi^{1/n}]$, and then K^∞ is algebraically closed.

Let $n \in \mathrm{N}$. Now $K^a \cap K^0[\pi^{1/n}]$ is dense in $K^0[\pi^{1/n}]$. Thus σ and τ still satisfy the $*$-property on $K^0[\pi^{1/n}]$. We have established that $\sigma_{|K^0} = \tau_{|K^0}$. From (3.10) and uniqueness of the solution to (3.11), we conclude

$$\sigma(\pi^{1/n}) = \pi^{1/n} \cdot d_n(\{\sigma(\pi) - \pi\}/\pi) = \tau(\pi^{1/n}). \tag{3.12}$$

As (3.12) is true for every n, σ and τ agree on K^∞, where $K^a \subseteq K^\infty$.

Define Δ on $x \in K^\infty$ by $\Delta(x) = x - \sigma(x)$. Fix $n \in \mathrm{N}$ and put $K' = K^0[\pi^{1/n}]$ where $x \in K'$. Now (3.12) implies that $\Delta(K') \subseteq K'$. Hence, there is $r \in (0, 1)$, dependent on n, so that $|\Delta(x)| \leqq r \cdot |x|$ for each $x \in K'$. Claim (B) follows.

Step II. Existence

Let $L \in \mathrm{Sub}$ so L/K is finite, and let $\sigma \in \mathrm{Hm}(L)$ have the $*$-property. We claim that σ admits an extension to K^a with the $*$-property. Fix a system of unramified roots for L. Uniqueness of unramified closure implies that there is an extension σ^u of σ to L^u such that $\varphi \circ \sigma^u = \varphi$. Then $M(\sigma^u)$ contains the units of R^{L^u} and a generator of that $\mathscr{P}^{L^u}$, so σ^u satisfies the $*$-property. Let σ_0 denote the continuous extension of σ^u to L^0, and let $d_n(T)$ be the power series described in (3.11.a,b). The defining property of $\{d_n(T)\}_{n=1}^\infty$ insures that

$$\forall\, m, n \in \mathrm{N}, \qquad d_{nm}(T)^m = d_n(T). \tag{3.13}$$

Let $L^\infty = \bigcup_{n=1}^\infty L^0[\pi^{1/n}]$. The characterization of L^∞ given by (3.10.a,b) implies existence of a homomorphism $\sigma' : L^\infty \to L^\infty$ which agrees with σ on R^{L^0} and such that $\sigma'(\pi^{1/n}) = \pi^{1/n} \cdot d_n(\{\sigma(\pi) - \pi\}/\pi)$ for each $n \in \mathrm{N}$. Now σ' factors to a ring endomorphism of k^{L^∞}; as every class in this quotient is represented by an element in L^0, the factored map is the identity. Consequently, $M(\sigma')$ contains the units of R^{L^∞} and $\pi^{1/n}$ for each $n \in \mathrm{N}$. The homomorphism σ' extends σ and satisfies the $*$-property on a domain which includes the algebraic closure of K. □

DEFINITION 3.1. Let K be a field, let L/K be an algebraic extension field, and let $\|$ be a non-Archimedean valuation on L. A field homomorphism $\sigma : K \to L$ is called a shift if the two properties of Theorem 3.1 hold, that is,

$$\forall x \in K, \qquad |x - \sigma(x)| < |x|, \tag{3.14.a}$$

(3.14.b) for Δ the function $x \mapsto x - \sigma(x)$, $x \in K$ and $\varepsilon > 0$, there is $m \in \mathbf{N}$ such that $|\Delta^m(x)| < \varepsilon$.

Observe that the condition that σ be a shift depends only on the prime associated to $\|$.

DEFINITION 3.2. Let k be a field, let $n \in \mathbf{N}$, and let $\boldsymbol{T} = T_1, \ldots, T_n$ be indeterminates. Identify $k(\boldsymbol{T})$ with the field of meromorphic algebraic functions on $\mathbf{P}^n(k)$, and let ∞ denote the prime of this field associated to the ∞-subvariety. We leave it to the reader that for $v \in k^n$, the homomorphism

$$p(\boldsymbol{T}) \mapsto p(\boldsymbol{T} + v) \tag{3.15}$$

is a shift on $k(\boldsymbol{T})$ with respect to ∞. Denote this shift, as well as any shift extending it to a subfield of an algebraic extension of a completion at ∞, by sh_v.

THEOREM 3.2. *Let k be a field of characteristic 0, let $n \in \mathbf{N}$, and let $\boldsymbol{T} = T_1, \ldots, T_n$ be indeterminates. Let L be an extension field of $k(\boldsymbol{T})$ and let $\|$ be a non-Archimedean valuation on L. Assume*

(3.16.a) *the restriction of $\|$ to K corresponds to the prime ∞,*

(3.16.b) *L is an algebraic closure of a completion of $k(\boldsymbol{T})$ in $\|$.*

Let $e_1, \ldots, e_n$ denote the standard k-basis for k^n. For $c \in k$ and $r \in \mathbf{N}(n)$, let $\mathrm{sh}_{c;r}$ denote the shift on L with respect to $c \cdot e_r$, and also define $\Delta_{c;r}(x) = x - \sigma_{c;r}(x)$ on $x \in L$. For $r \in \mathbf{N}(n)$, let K_r denote the algebraic closure of $k(\{T_j\}_{j \neq r})$ in L, and let K denote the algebraic closure of $k(\boldsymbol{T})$ in L. Let k^a denote the algebraic closure of k in L.

(A) *For $c \in k^*$ and $r \in \mathbf{N}(n)$, $\ker(\Delta_{c;r}) \cap K = K_r$.*

(B) *Let $x \in K$. There is $m \in \mathbf{N}$ and a sequence $c_1, \ldots, c_m \in k^*$ such that*

$$\{\Delta_{c_1;r} \circ \cdots \circ \Delta_{c_m;r}\}(x) = 0 \tag{3.17}$$

if and only if $x \in K_r[T_r]$.

(C) $\bigcap_{r=1}^n K_r[T_r] = k^a[\boldsymbol{T}]$.

PROOF. (A) Clearly, for $v \in k^n \subseteq (k^a)^n$, the v-shift on $k^a[\boldsymbol{T}]$ defined with respect to choice of ground field k^a is also a ν-shift as defined with respect to k. Without loss of generality, assume $r = 1$. Fix $c \in k^*$. Put $\sigma = \mathrm{sh}_{c;1}$ and $\Delta = \Delta_{c;1}$. Let

$$N = \ker(\Delta_{|K}) = \{x \in K : \sigma(x) = x\}. \tag{3.18}$$

Clearly N is a field.

The assumptions $c \neq 0$ and $\mathrm{char}(k) = 0$ render many combinatorial steps trivial. It is easily established that $N \cap k[T_1, \ldots, T_n] = k[T_2, \ldots, T_n]$. Also, if p is an irreducible polynomial in $k[T_1, \ldots, T_n]$ such that $\partial_1 p > 0$, then $\{\sigma^j(p)\}_{j=0}^{\infty}$ is an indexed family of pairwise coprime irreducibles. From this observation, it is simple to show

$$N \cap k(T_1, \ldots, T_n) = k(T_2, \ldots, T_n). \tag{3.19}$$

If $P(X)$ is the monic minimal polynomial for $\alpha \in K$ over $k(\boldsymbol{T})$, then $\sigma(\alpha)$ satisfies the irreducible polynomial P^σ. Consequently, $\Delta(\alpha) = 0$ only if $\alpha \in K_1$. We have $N \subseteq K_1$.

To prove that $N = K_1$, it suffices to show Δ vanishes on $\alpha \in K$ which are integral over $k[T_2, \ldots, T_n]$. Proof is by contradiction. Suppose α is integral over $k[T_2, \ldots, T_n]$ and $\Delta(\alpha) \neq 0$. There is $m \in \mathbf{N}$ so $|\Delta^m(\alpha)| \leqq 1$. Since σ preserves $k[T_2, \ldots, T_n]$, Δ maps the integral closure of $k[T_2, \ldots, T_n]$ to itself. Let P be the monic minimal polynomial of $\Delta^m(\alpha)$. Each coefficient of P lies in $k[T_2, \ldots, T_n]$ and in the valuation ring of $\|$. But then P has coefficients in k,

$$\Delta^m(\alpha) \in k^a \Rightarrow \Delta^{m+1}(\alpha) = 0. \tag{3.20}$$

Replacing α by $\Delta^k(\alpha)$ for a suitable k, we may assume that $\Delta(\alpha) \neq 0$ and $\Delta^2(\alpha) = 0$. Let $y = \Delta(\alpha)$. Then $y \in N$ and $\sigma(\alpha) = \alpha - y$. Since $\mathrm{char}(k) = 0$, $\{\sigma^k(\alpha) : k \in \mathbf{N}\}$ is an infinite set. But σ permutes the conjugates of α over N, which is a finite set. We have reached an impossibility.

(B) Let $r \in \mathbf{N}(n)$ and $c \in k^*$, and put $\Delta = \Delta_{c;r}$. From (A), it is simple to show that Δ restricts to a surjection $K_r[T_r] \to K_r[T_r]$. If $x \in K$ so $\Delta(x) \in K_r[T_r]$, then for $y \in K_r[T_r]$ such that $\Delta(x) = \Delta(y)$,

$$x - y \in \ker(\Delta) = K_r \Rightarrow x \in K_r[T_r]. \tag{3.21}$$

This technicality implies (B).

(C) Proof is by a double induction. If $n = 1$, then $K = k^a$ and the claim is tautological. Assume $n \in \mathbf{N}$ is chosen so that the result is true when the number of indeterminates is less than n. For $j \in \mathbf{N}(n)$, let ∂_j be the degree map on $K_j[T_j]$. Let $\alpha \in \bigcap_{j=1}^{n} K_j[T_j]$, and let $m = \partial_n \alpha$. If $m = 0$, we are done by induction.

Without loss of generality, we may assume $m \geqq 1$ and the result is true for $\beta \in \bigcap_{j=1}^{n} K_j[T_j]$ such that $\partial_n \beta < m$. Express

$$\alpha = \sum_{r=0}^{m} a_r T_n^r \tag{3.22}$$

where $a_r \in K_n$ for each r. If $a_n \in k^a[T_1, \ldots, T_{n-1}]$, then applying the inductive hypothesis to $\alpha - a_m T_n^m$ finishes the argument.

There is a unique algebraic derivation D of K such that

$$\begin{aligned} &D(k) = \{0\}, \\ &D(T_j) = 0 \qquad \text{for } j \in \mathbf{N}(n-1), \\ &D(T_n) = 1. \end{aligned} \tag{3.23}$$

General nonsense states that D maps K_j into K_j for $j \in \mathbf{N}(n-1)$ and that $D(K_n) = \{0\}$. Consequently, D maps $K_j[T_j]$ into itself for each $j \in \mathbf{N}(n)$. In particular, $D\alpha \subseteq \bigcap_{j=1}^{n} K_j[T_j]$. But now

$$D\alpha = \sum_{r=1}^{m} r a_r T_n^{r-1}, \tag{3.24}$$

and so $\partial_n(D\alpha) < m$. Thus $D\alpha \in k^a[X_1, \ldots, X_n]$ and $a_n \in k^a[X_1, \ldots, X_{n-1}]$. We are done. □

§4. Points of concentration

If a holomorphic germ f about the point ∞ in $\mathbf{P}^1$ vanishes on an infinite number of integers, then $f = 0$. In this section, the principle is extended to germs on $\mathbf{P}^n$. Fix $n \in \mathbf{N}$ and a choice of homogeneous coordinates $t_1, \ldots, t_{n+1}$ on $\mathbf{P}^n$.

The domain of a function f is denoted by dom(f). Suppose $S \subseteq \mathbf{Z}^n \subseteq \mathbf{P}^n$. Define $l(S) = \bar{S} - S = \bar{S} \cap \infty$. Now $\bar{S} = S \cup l(S)$, S is a discrete subset and $\bar{S}$ is compact. Hence, if U is a neighborhood of $l(S)$, then $S - U$ is finite.

Definition 4.1. Let δ be an n-dimensional density, let $x \in \mathbf{P}^n$ and let $S \subseteq \mathbf{Z}^n$. Obviously, the following conditions on x are equivalent:

(4.1.a) for U is a neighborhood of x, $\delta(S \cap U) > 0$,

(4.1.b) for U is a neighborhood of x, there is $M \subseteq S$ such that $\bar{M} \subseteq U$ and $\delta(M) > 0$.

If (4.1.a,b) hold, we say that x is a point of concentration for S in δ. The points of concentration for S lie in $l(S)$.

LEMMA 4.1. *Let δ be an n-dimensional density and let $S \subseteq \mathbf{Z}^n$. Suppose $\delta(S) > 0$.*

(A) *There is a point of concentration for S.*

(B) *If δ is $\mathbf{Q}$-diffuse and W is a proper subvariety of ∞, then there is a point of concentration for S which is not on $W(\mathbf{C})$.*

PROOF. (A) If no point of concentration for S exists, then there is a cover of $l(S)$ by open sets U such that $\delta(S \cap U) = 0$. But $l(S)$ is compact, and thus there would be a finite subcover, in which case $\delta(S) = 0$.

(B) Simply replace S by $S - U$ where U is a neighborhood of $W(\mathbf{C})$ such that $\delta(\mathbf{Z}^n \cap U) < \delta(S)/2$, and invoke (A). □

The main result of this section is

THEOREM 4.2. *Let U be an open subset of $\mathbf{P}^n(\mathbf{C})$ such that $U \cap \infty$ is connected. Let δ be an n-dimensional density which satisfies the VW condition. Suppose $S \subseteq \mathbf{Z}^n$ such that $\bar{S} - S \subseteq U$ and $\delta(S) > 0$.*

Let α be a holomorphic $(\infty \cap U)$-germ into $\mathbf{C}$. Suppose there is a representative f of α such that $f(s) = 0$ for each $s \in S \cap \mathrm{dom}(f)$. Then $\alpha = 0$.

PROOF. Assume the stated hypothesis. Note that if there is a representative f of α which vanishes on $S \cap \mathrm{dom}(f)$, then for any representative g of α, g vanishes on $S \cap \mathrm{dom}(g)$ minus a finite set; hereafter, we ignore these finite sets.

Affine coordinate changes preserve $\mathbf{Z}^n$ and change densities to densities. Without loss of generality, we may apply affine transformations.

Let $x = [x_1, \ldots, x_{n+1}]$ be a point of concentration for S. After suitable change of coordinates, we may assume that $x_1 \neq 0$. Let f represent α. It suffices to prove that f vanishes on a neighborhood of x. Our proof is by contradiction; assume that the x-germ of f is not 0. Let V be the 1st chart of $\mathbf{P}^n(\mathbf{C})$, and let X_j be the coordinate function t_{j+1}/t_1 on V. Let $u_j = X_j(x)$ for $j \in \mathbf{N}(n)$. Continuity assures that $f(x) = 0$.

There is a neighborhood U_0 of x such that $U_0 \subseteq \mathrm{dom}(f)$ and there is an expansion of f in terms of the 1st chart coordinates

$$f(X_1, \ldots, X_n) = \sum_{k=1}^{\infty} f_k(X_1 - u_1, \ldots, X_n - u_n), \tag{4.2}$$

where $f_k(T_1, \ldots, T_n)$ is a homogeneous polynomial of degree k over $\mathbf{C}$ for each $k \in \mathbf{N}$, and the sum converges absolutely and uniformly on U_0. By assumption, $f_k \neq 0$ for at least one index k. Suppose $d \in \mathbf{N}$ so $(T_n)^d$ divides $f_k(T_1, \ldots, T_n)$ for every index k. In this case, $f/(X_n - u_n)^d$ is a holomorphic function on U whose germ is non-zero but which still satisfies the hypothesis of Theorem 4.1. Without loss of generality, assume there is at least one index k for which $T_n \nmid f_k$.

For $c \in \mathbf{Z}$, let σ_c be the affine transformation

$$(4.3) \qquad [t_1, \ldots, t_{n+1}] \mapsto [t_1, t_2, t_3 + ct_2, \ldots, t_n + ct_2, t_{n+1}].$$

Obviously σ_c preserves the 1st chart and

$$(4.4.a) \qquad \forall c, d \in \mathbf{Z}, \qquad \sigma_c \circ \sigma_d = \sigma_{c+d},$$

$$(4.4.b) \qquad \sigma_0 \text{ is the identity morphism.}$$

Let $c \in \mathbf{Z}$. Put $v_j = X_j(\sigma_{-c}(x))$ for $j \in \mathbf{N}(n)$, and then $f \circ \sigma_c$ is given by a power series

$$(4.5) \qquad \sum_{k=1}^{\infty} g_k(X_1 - v_1, \ldots, X_n - v_n),$$

where

$$(4.6) \qquad g_k(T_1, \ldots, T_n) = f_k(T_1, T_2 + cT_1, \ldots, T_{n-1} + cT_1, T_n) \qquad \text{for } k \in \mathbf{N}.$$

We are free to replace α with the germ of $f \circ \sigma_c$ for any of the infinitely many $c \in \mathbf{Z}$. Hence, there is a suitable change of coordinates which reduces us to the case where there is $k \in \mathbf{N}$ such that the $(T_1)^k$ coefficient in f_k is a non-zero complex number.

Let ι denote the 1st chart map. By the Analytic Weierstrass Preparation Theorem, there exists U_1 open in $\mathbf{C}^{n-1}$ and $r \in (0, \infty)$ so that, for $B = B(u_1, r)$, $U_2 = \iota(B \times U_1) \subseteq U_0$ is a neighborhood of x and, and terms of the coordinates, f restricted to U_2 satisfies

$$(4.7) \qquad \begin{aligned} &f(X_1, \ldots, X_n) \\ &\quad = \beta(X_1, \ldots, X_n) \cdot \left\{ (X_1 - u_1)^k + \sum_{j=0}^{k-1} \beta_j(X_2, \ldots, X_n)(X_1 - u_1)^j \right\}, \end{aligned}$$

where β_j is homomorphic on U_1 for each $j \in \mathbf{N}(k-1) \cup \{0\}$, and β is holomorphic and non-vanishing on U_2. Let $M = S \cap U_2$. If $d \in M$ has coordinates $(d_1, \ldots, d_n)$ with respect to the standard basis of $\mathbf{Z}^n$, then

$$
(4.8)\qquad
\begin{aligned}
0 &= \left(\frac{d_2}{d_1} - u_1\right)^k + \sum_{j=0}^{k-1} \beta_j\left(\frac{d_3}{d_1}, \dots, \frac{d_n}{d_1}, \frac{1}{d_1}\right)\left(\frac{d_2}{d_1} - u_1\right)^j && \text{if } n > 1,\\
0 &= \left(\frac{1}{d_1} - u_1\right)^k + \sum_{j=0}^{k-1} \beta_j\left(\frac{1}{d_1} - u_1\right)^j && \text{if } n = 1.
\end{aligned}
$$

If $n = 1$, there are at most k points for which (4.8) is true. If $n > 1$, then for $d_1; d_3, \dots, d_n \in \mathbf{Z}$, there are at most k values $d_2 \in \mathbf{Z}$ for which $(d_1, \dots, d_n) \in M$. But choice of x implies that M has positive density. A contradiction of Lemma 1.3 has been reached. □

§5. Spaces with ramification constraint

We wish to combine the algebra of §3 with the geometry of §4. To do so, roots of polynomials in several variables must be embedded inside a field which is closed under "shifts" and whose members are functions. Unfortunately, shift operations preserve few finite extensions of the ground field. We shall produce a suitable field of germs, which corresponds to an infinite extension field, in which algebraic shifts have geometric meaning.

The objects of central interest are functions between complex varieties $f: U \to V$ which are locally invertible outside a prescribed set $I \subseteq U$. We refer to such a specified set I as a "ramification constraint". Much of the nuances of non-smooth varieties are avoided by working in the language of covering spaces. Ultimately, we get results for a subset I of a complex manifold U when there is a function $\sigma: U \to \mathbf{C}$ such that $I = \sigma^{-1}\{0\}$ and the Jacobian of σ is non-vanishing on I. The structure theory developed here merely rephrases existing theory to emphasize the shift operations of §3.

For X a topological space and $x \in X$, let $\pi_1(X, x)$ be the fundamental group of X based at x. In most cases X will be pathwise connected, and we omit reference to x without ambiguity. If $f: X \to Y$ is a continuous function between topological spaces and $x \in X$, denote the induced map $\pi_1(X, x) \to \pi_1(Y, f(x))$ by f_*.

Definition 5.1. Let U be a locally compact Hausdorff space. By a ramification constraint for U, we mean a non-empty connected closed subset $I \subseteq U$ such that for each $x \in I$ and each neighborhood V of x in U, there is a neighborhood W of x in U such that

$$(5.1)\qquad W \subseteq V \quad \text{and} \quad W - I \text{ is pathwise connected.}$$

We refer to a pair (U, I) of a topological space with a choice of (ramification) constraint as a space with constraint. Often we identify U with the pair, and denote I by ∞ or ∞_U.

For (U, I) and (V, J) spaces with constraint, a continuous function $f: U \to V$ is said to be almost l.h. (almost locally homeomorphic) if

$$f \text{ is locally homeomorphic at each } x \in U - I, \tag{5.2.a}$$

$$f(U - I) \subseteq V - J \quad \text{and} \quad f(I) \subseteq J, \tag{5.2.b}$$

$$f \text{ is proper and open.} \tag{5.2.c}$$

For $m \in \mathbf{N}$, we say f is an almost m-fold cover if $|f^{-1}\{v\}| = m$ for $v \in V - J$.

LEMMA 5.1. *Let X, Y and Z be locally compact Hausdorff spaces, let $D \subseteq Z$ be a dense subset and let $f: X \to Z$ and $\imath: Y \to Z$ be proper open maps.*

(A) *Suppose $m \in \mathbf{N}$ so $|f^{-1}\{u\}| \leqq m$ for each $u \in D$. Then $|f^{-1}\{z\}| \leqq m$ for each $z \in Z$.*

(B) *Let $F: f^{-1}D \to Y$ be a continuous function. Suppose*

$$\imath \circ F = f, \tag{5.3.a}$$

$$\imath^{-1}\{z\} \textit{ is a discrete subset of } Y \textit{ for } z \in Z, \tag{5.3.b}$$

$$\begin{array}{l} \textit{for } V \textit{ open in } X \textit{ and } x \in V, \\ \textit{there is an open set } W \subseteq V \textit{ so } x \in W \textit{ and } W \cap f^{-1}D \textit{ is connected.} \end{array} \tag{5.3.c}$$

Then F has a unique continuous extension to $F': X \to Y$, and $\imath \circ F' = f$.

PROOF. We sketch the argument.

(A) Let $z \in Z$ and let $x_1, \ldots, x_n$ be a list of distinct points in $f^{-1}\{z\}$. Let $V_1, \ldots, V_n$ be a list of pairwise mutually disjoint open subsets of X such that $x_j \in V_j$ for each $j \in \mathbf{N}(n)$. As f is an open map, $U = \bigcap_{j=1}^n f(V_j)$ is an open neighborhood of z. There is $u \in D \cap U$, and then $|f^{-1}\{u\}| \geqq n$. Consequently, $m \geqq n$.

(B) Let

$$\Gamma = \{(x, f(x)) : x \in \operatorname{dom}(f)\}, \tag{5.4}$$

and let Γ' be the closure of Γ in $X \times Y$. If $A \subseteq X$ is compact, then $F(A \cap D)$ is contained in the compact set $\imath^{-1}f(A)$. Point set topology states that if for each $x \in X$ there is no more than one $y \in Y$ so $(x, y) \in \Gamma'$, then Γ' is the graph of a continuous extension of F. All other claims follow easily.

Suppose $x \in X$. Index $\iota^{-1}\{f(x)\}$ as $y_1, \ldots, y_n$ where $n = |\iota^{-1}\{f(x)\}|$. Let $V_1, \ldots, V_n$ be a list of pairwise mutually disjoint open subsets such that $y_j \in V_j$ for $j \in \mathbf{N}(n)$. Since ι is proper and Z is locally compact and Hausdorff, there is a neighborhood U of $f(x)$ such that $\iota^{-1}U \subseteq \bigcup_{j=1}^{n} V_j$. Let W be a neighborhood of x such that $W \cap f^{-1}D$ is connected and $W \subseteq f^{-1}U$. Then $F(W)$ is connected, and there is an index $k \in \mathbf{N}(n)$ so $F(W) \subseteq V_k$. Clearly if $y \in Y$ so $(x, y) \in \Gamma'$, then y must be y_k. □

THEOREM 5.2. *Let $n \in \mathbf{N}$. Let $\lambda : \mathbf{C}^n \to \mathbf{C}^n$ be the polynomial function whose j-th coordinate is the j-th Newton symmetric polynomial. Let*

$$I = \{z \in \mathbf{C}^n : \exists j, k \in \mathbf{N}(n) \text{ so } j \neq k \text{ and } z_j = z_k\},$$
$$J = \lambda(I). \tag{5.5}$$

Then $(\mathbf{C}^n, I)$ and $(\mathbf{C}^n, J)$ are spaces with constraints and $\lambda : (\mathbf{C}^n, I) \to (\mathbf{C}^n, J)$ is an almost n-fold cover. Moreover, the Jacobian of λ is invertible at each $x \in \mathbf{C}^n - I$.

PROOF. Standard theory includes the relevant properties. □

DEFINITION 5.2. Let (U, I) be a space with constraint. Assume U is connected. A neatly holomorphic structure for (U, I) is a complex manifold structure $\mathscr{S}$ on U such that there is a function $\sigma : U \to \mathbf{C}$ for which

(5.6.a) σ is holomorphic with respect to $\mathscr{S}$,

(5.6.b) $I = \sigma^{-1}\{0\}$,

(5.6.c) the rank of the Jacobian of σ is 1 at each point in I,

(5.6.d) $\sigma_* : \pi_1(U - I) \to \pi_1(\mathbf{C} - \{0\})$ is a group isomorphism.

Such a map σ is referred to as "axial".

If U is a neatly holomorphic space, M is a complex manifold and $f: U \to M$ is a function, we say f is neat if f is holomorphic and the Jacobian of f is invertible at each $z \in U - \infty_U$.

For our next comments, fix U a neatly holomorphic space with constraint, and fix σ an axial function of U.

DEFINITION 5.3. Let $\infty = \infty_U$. The ring $\mathscr{O}_\infty$ is a domain and the set $\mathscr{P}$ of germs in $\mathscr{O}_\infty$ which vanish on ∞ form a principal prime ideal generated by σ.

The localization of $\mathcal{O}_\infty$ at $\mathcal{P}$ is a discrete valuation ring. For the rest of this paper, "∞-valuation" refers to any choice of valuation for this particular ring.

There is a unique subring $\mathcal{N} = \mathcal{N}_\infty \subseteq \mathcal{M}_\infty$ with the property that if $\gamma \in \mathcal{O}_\infty$ is axial, then $\mathcal{N} = \mathcal{O}[\gamma^{-1}]$. A germ $\alpha \in \mathcal{M}_\infty$ is said to have axial denominator if and only if $x \in \mathcal{N}$. The intersection of $\mathcal{N}$ with the ring of the ∞-valuation is exactly $\mathcal{O}_\infty$.

Let $x \in \infty_U$. There is a local holomorphic coordinate system $X_1, \ldots, X_n$ where $X_n = \sigma$. Therefore there is a basis of neighborhoods at x which, in appropriate coordinates, are products of open balls and in which I corresponds to the hyperspace $X_n = 0$. Consequently, there is a basis of open neighborhoods W of x such that $(W, \infty_U \cap W)$ is a neat holomorphic space with constraint. We may apply the theory of several complex variables within such charts. Consequently, if $\theta: U \to M$ is a continuous function into a complex manifold which is holomorphic on $U - \infty_U$, then θ is holomorphic on all of U. In particular, given the structure of an n-dimensional complex manifold on $U - \infty_U$ for some $n \in \mathbf{N}$, there is at most one extension to a neatly holomorphic structure on U.

The axioms assure existence of a non-canonical isomorphism $\pi_1(U - \infty_U) \approx \mathbf{Z}$. Let V be a neatly holomorphic space with constraint and let $\theta: V \to U$ be a neat almost m-cover. General nonsense implies that $\theta_*(\pi_1(V - \infty_V))$ is the unique subgroup of $\pi_1(U - \infty_U)$ of index m.

Let V_1 and V_2 be neatly holomorphic spaces with constraint. For $j \in \{1, 2\}$, let $m_j \in \mathbf{N}$, let $\theta_j: V_j \to U$ be a neat almost m_j-cover, let ∞_j denote ∞_{V_j}, and let $v_j \in V_j - \infty_j$. Assume $m_2 \mid m_1$ and $\theta_1(v_1) = \theta_2(v_2)$. Covering space theory and Lemma 5.1 assure existence of a unique holomorphic function $F: V_1 \to V_2$ so $\theta_2 \circ F = \theta_1$ and $F(v_1) = v_2$. If $m_1 = m_2$, then F is biholomorphic.

Next, fix $m \in \mathbf{N}$. Let

$$V = \{(u, r) \in U \times \mathbf{C} : \sigma(u) = r^m\}. \tag{5.7}$$

Assign to V the subset topology from $U \times \mathbf{C}$. It is simple to demonstrate existence and uniqueness of a complex manifold structure on V such that π_U and $\pi_{\mathbf{C}}$ are neat and $\pi_{\mathbf{C}}$ is axial for the choice $\infty_V = V \cap (U \times \{0\})$. Moreover, π_U is a neat almost m-cover. The m-th roots of unity act on V by $\xi \cdot (u, r) = (u, \xi r)$.

We have outlined several existence, uniqueness and lifting theorems. The following applications are simple consequences, and their proofs are left to the reader:

DEFINITION 5.4. Let U be a neatly holomorphic space with constraint. By a (geometric) shift on U, we mean a holomorphic ∞_U-germ α into U such that

(5.8.a) α determines the identity map on ∞_U,

(5.8.b) for $x \in \infty_U$, T_x the complex tangent space at x, and W the subspace tangent to ∞_U, the factoring of the differential of α at x to an endomorphism of T_x/W is the identity function.

If σ is axial and f represents a germ α which satisfies (5.8.a), then (5.8.b) is equivalent to requiring that the differential of $\sigma - (\sigma \circ f)$ vanish on ∞_U. Alternatively, if $\beta \in \mathcal{M} = \mathcal{M}_{\infty_U}$ is non-zero then $|\beta - \beta \circ \alpha| < |\beta|$ for $\|$ any ∞-valuation of $\mathcal{M}$; that is, $\alpha_* : \beta \mapsto \beta \circ \alpha$ is a shift in the sense of Definition 3.1. Observe that α_* maps the ring $\mathcal{N}_\infty$ to itself.

LEMMA 5.3. *Let $m \in \mathbf{N}$ and let $\theta : W \to U$ be a neat almost m-cover between two neatly holomorphic spaces with constraint. Let $\boldsymbol{\mu}_m$ be the set of m-th roots of unity and let $\mathcal{A}$ be the set of holomorphic ∞_W-germs α into W such that $\theta = \theta \circ \alpha$. Then $\mathcal{A}$ is a group under composition and there is a group isomorphism $\omega : \mathcal{A} \to \boldsymbol{\mu}_m$ such that for $\alpha \in \mathcal{A}$ and $x \in \infty_W$, the determinant of $d\alpha$ at x is $\omega(\alpha)$. Moreover, if f is a holomorphic function (respectively, holomorphic ∞_W-germ) which is invariant under $\mathcal{A}$, then f factors through a holomorphic function (respectively, holomorphic ∞_U-germ) on U.*

COROLLARY 5.3.1. *Let $m \in \mathbf{N}$ and let $\theta : W \to U$ be a neat almost m-cover between two neatly holomorphic spaces with constraint. If α is a shift on U, then there is a unique shift β on W such that $\alpha = \theta \circ \beta$.*

PROOF. Identify W with V of (5.7), in which case β is the restriction of $\alpha \times 1_{\mathbf{C}}$ to V.

DEFINITION 5.5. Let $n \in \mathbf{N}$ and fix a choice of homogeneous coordinates for $\mathbf{P}^n$. Let U be an open subset of $\mathbf{P}^n(\mathbf{C})$ such that (U, ∞_U) is neatly holomorphic for $\infty_U = U \cap \infty$. For $v \in \mathbf{Z}^n$, let sh_v be the ∞_U-germ determined by the affine function associated to $\boldsymbol{T} \mapsto \boldsymbol{T} + v$ on $\mathbf{Z}^n$. Then sh_v is a geometric shift. In general, if $m \in \mathbf{N}$ and $\theta : V \to U$ is a neat almost m-cover, define the v-shift (of V via θ) to be the shift β such that $\mathrm{sh}_v \circ \theta = \theta \circ \beta$, and denote β or its germ by sh_v or $\mathrm{sh}_{v,V}$.

DEFINITION 5.6. Finally, we need to lift the notion of a $\mathbf{Z}$-rational point in a manner consistent with shifting. Let m, n and $\theta : V \to U$ be as in the previous paragraph.

By a lattice structure on V, we mean a function $s : \mathbf{Z}^n \cap U \to V$ such that

(5.9.a) $\theta \circ s$ is the identity map,

(5.9.b) if $v \in \mathbf{Z}^n$ and f and g represent $\mathrm{sh}_{v,V}$ and $\mathrm{sh}_{v,U}$, respectively, then there is a neighborhood U' of ∞_U in U such that $(f \circ s)(x) = (s \circ g)(x)$ for $x \in s^{-1}U'$.

We claim that for each $x \in \infty(\mathbf{C}) \subseteq \mathbf{P}^n(\mathbf{C})$ there is a basis of neighborhoods U of x each of which admits an almost m-cover V on which is a lattice structure. To demonstrate this, it suffices to construct a lattice structure over the 1st chart.

Fix $n, m \in \mathbf{N}$ and $t_1, \dots, t_{n+1}$ a system of homogeneous coordinates for $\mathbf{P}^n$. Let U be the 1st coordinate chart, and put $T_j = t_{j+1}/t_1$ for $j \in \mathbf{N}(n)$. Put $\infty_U = \infty \cap U$, and then (U, ∞_U) with the submanifold structure is a neatly holomorphic space with constraint on which T_n is axial. Let $X_1, \dots, X_n$ be the usual coordinates on $\mathbf{C}^n$, and let ∞' denote the set determined by $X_n = 0$. In what follows, we regard $\mathbf{C}^n$ as the neatly holomorphic space with constraint $(\mathbf{C}^n, \infty')$.

Define $\theta : \mathbf{C}^n \to U$ by

$$T_j \circ \theta = X_j \qquad \text{for } j \in \mathbf{N}(n-1), \qquad T_n \circ \theta = (X_n)^m. \tag{5.10}$$

Then θ is a neat almost m-cover. For $v = (v_1, \dots, v_n)$, direct computation verifies that the germ of the v-shift on U in terms of coordinates $T_1, \dots, T_n$ is

$$T_j \circ \mathrm{sh}_{v,U} = \begin{cases} \dfrac{T_j + v_{j+1}T_n}{1 + v_1 T_n} & \text{if } j \neq n, \\[2ex] \dfrac{T_n}{1 + v_1 T_n} & \text{if } j = n. \end{cases} \tag{5.11}$$

Let γ be the unique holomorphic function on $B(0, 1)$ with the property that $\gamma(z)^m = 1 + z^m$ and $\gamma(0) = 1$.

Fix $\omega \in \mathbf{C}$ so $\omega^m = -1$. For $c \in \mathbf{R}$, put

$$\omega_C = \begin{cases} |c|^{1/m} & \text{if } c \geqq 0, \\ \omega |c|^{1/m} & \text{if } c < 0. \end{cases} \tag{5.12}$$

Let $v = (v_1, \dots, v_n) \in \mathbf{Z}^n$. The reader may verify by direct calculation that β, the v-shift on $\mathbf{C}^n$ via θ, is given in terms of the coordinates by

(5.13)
$$X_j \circ \beta = \begin{cases} \dfrac{X_j + v_{j+1} X_n^m}{1 + v_1 X_2^m} & \text{if } j \neq n, \\[2ex] \dfrac{X_n}{\gamma_m({}^{\omega} v_1 X_n)} & \text{if } j = n. \end{cases}$$

Let $s : \mathbf{Z}^n \cap U \to \mathbf{C}^n$ be the function

(5.14)
$$s([b_1, \ldots, b_{n+1}]) = (b_2/b_1, \ldots, b_n/b_1, {}^{\omega}(b_{n+1}/b_1)).$$

Then s is a lattice structure via θ.

Finally, we interpret roots of polynomials as both functions and germs.

Let $p \in \mathbf{Q}(T_1, \ldots, T_n)$. Let Q be the set of all subvarieties in the divisor of p *except* ∞, and let $V(p)$ be the union of $\mathbf{C}$-rational points over members of Q. Then p determines a non-vanishing function (also denoted by p) on $\mathbf{P}^n(\mathbf{C}) - V(p) - \infty(\mathbf{C})$. For X another indeterminate and $P(X)$ a polynomial over $\mathbf{Q}(\boldsymbol{T})$, define $V_1(P)$ to be the union of sets $V(p)$ where p varies over the non-zero coefficients of P and the discriminant of P.

Lemma 5.4. *Let U be an open subset of $\mathbf{P}^n(\mathbf{C})$ contained in some coordinate chart. Let $\infty_0 = \infty \cap U$, and assume (U, ∞_0) is a neatly holomorphic space with constraint. Put $\mathcal{M}_0 = \mathcal{M}_{\infty_0}$, and embed $\mathbf{C}(\boldsymbol{T}) \subseteq \mathcal{M}_0$ in the canonical manner.*

Let $P(X) \in \mathbf{Q}(\boldsymbol{T})[X]$ and suppose $V_1(P) \cap U = \varnothing$. Let m be the degree of P as a polynomial in X. Let $\theta : V \to U$ be a neat almost $m!$-cover, let $\mathcal{M}_1$ be the field of meromorphic germs at ∞_V, and regard $\mathcal{M}_0$ as a subfield of $\mathcal{M}_1$. Then P splits in $\mathcal{M}_1$, and its roots have axial denominator.

Proof. The assumption that U lies in a coordinate chart implies the existence of an axis σ for U in $\mathbf{Q}(\boldsymbol{T})$. Let q be the leading coefficient of P; then $P_1 = q^{-1}P$ has the same roots as P, and satisfies the hypothesis. Without loss of generality, assume P is monic. Furthermore, the assumption on $V_1(P)$ implies that there is $r \in \mathbf{N} \cup \{0\}$ such that the coefficients of $P' = \sigma^{r(m-1)} P(X/(\sigma^r))$ are non-vanishing holomorphic functions on U. It is clear that P' satisfies the hypothesis, and the conclusion for P' would imply the result for P. For the remainder of the argument, assume P is monic with coefficients holomorphic on U.

Let $\theta : V \to U$ be as hypothesized. Let λ, I and J be as stated in Theorem 5.2. Let $f : U \to \mathbf{C}^n$ be the function whose j-th coordinate is the $(j-1)$st coefficient of P. Our assumption on discriminant implies that $f(U - \infty_0) \subseteq \mathbf{C}^n - J$.

Let $z_1 \in V - \infty_1$ and $w = f(\theta(z_1))$. For $\gamma \in \pi_1(V - \infty_V, z_1)$, there is $\alpha \in \pi_1(\mathbf{C}^n - J, w)$ for which $\alpha^{m!} = (f \circ \theta)_*(\gamma)$. There is a canonical action by $\pi_1(\mathbf{C}^n - J, w)$ on $\lambda^{-1}\{w\}$, and $\lambda^{-1}\{w\}$ has m elements. Consequently, $(f \circ \theta)_*(\gamma)$ acts trivially. Choose $y \in \lambda^{-1}\{w\}$. Then there is a unique holomorphic function $F_0 : V - \infty_1 \to \mathbf{C}^n - I$ such that $\lambda \circ F_0 = f \circ \theta$ and $F_0(z_1) = y$. Lemma 5.1 implies that F_0 has a holomorphic extension F. For $j \in \mathbf{N}(n)$, let π_j be the j-th projection $\mathbf{C}^n \to \mathbf{C}$, and let $F_j = \pi_j \circ F$. Consequently,

$$P(X) = \prod_{j \in \mathbf{N}(n)} (X - F_j), \tag{5.15}$$

where expression (5.15) is expanded as polynomials in X over the ring of holomorphic functions on V. The analogue holds for germs. □

§6. Proof of Proposition 1.4

We are ready to prove Proposition 1.4. It is an easy consequence of the assembled machinery. Proof is by a series of reductions.

Fix $n \in \mathbf{N}$, fix a choice of homogeneous coordinates on $\mathbf{P}^n(\mathbf{C})$ and fix δ a $\mathbf{Q}$-diffuse n-dimensional density which satisfies the VW condition. Let X and $\boldsymbol{T} = T_1, \ldots, T_n$ be indeterminates.

First, consider an irreducible monic polynomial P of $\mathbf{Z}[X; \boldsymbol{T}]$ which depends on X, and suppose $\delta(I(P)) > 0$. Let x be a point of concentration for $I(P)$ which is not contained in $V_1(P)$. Choose an open neighborhood U of x such that

(6.1.a) U is contained in a chart associated with the choice of homogeneous coordinates,

(6.1.b) (U, ∞') is a neatly holomorphic space with constraint for $\infty' = \infty \cap U$,

$$U \cap V_1(P) = \varnothing. \tag{6.1.c}$$

Let $\theta : V \to U$ be a neat almost $m!$-cover, and let $\mathscr{M}$ denote the field of ∞_V-germs. Fix a lattice structure $s : \mathbf{Z}^n \to V$.

Suppose $\alpha \in \mathscr{M}$ has axial denominator. Then we may regard α as a class of functions whose domains are neighborhoods of ∞' minus a subset of ∞'. For $M \subseteq \mathbf{Z}^n$ such that $M \subseteq U \cap \mathbf{Z}^n$, we say α is integral on M if for one representative $f \in \alpha$ (and, consequently, for all representatives), f assumes values in $\mathbf{Z}$ on $s(M) \cap \operatorname{dom}(f)$ minus a finite set.

Let $\alpha_1, \ldots, \alpha_r$ be the roots of P in $\mathcal{M}$. Each α_j has axial denominator, and, for at least one index $k \in \mathbf{N}(r)$, α_k is integral on a set $M \subseteq \mathbf{Z}^n$ of positive δ-density such that $\overline{M} - M \subseteq U$. It is sufficient to prove that such an α_k must be in $\mathbf{Q}[\boldsymbol{T}]$.

For the rest of the argument, fix U, V, θ and s; we ignore P. For convenience, say $M \subseteq \mathbf{Z}^n$ is properly concentrated if $\overline{M} - M \subseteq U$.

Suppose $\alpha \in \mathbf{C}[\boldsymbol{T}]$ is integral on a properly concentrated set of positive δ-density. Express

$$\alpha = \sum_{j=1}^{t} g_j e_j, \tag{6.2}$$

where $t \in \mathbf{N}$, $e_1, \ldots, e_t$ are $\mathbf{Q}$-linearly independent complex numbers, $e_1 = 1$ and $g_1, \ldots, g_t \in \mathbf{Q}[\boldsymbol{T}]$. But for $j \in \mathbf{N}(t) - \{1\}$, $Z(g_j)$ must contain M which by Corollary 1.3.1 forces $g_j = 0$. Consequently, $\alpha \in \mathbf{Q}[\boldsymbol{T}]$.

Proposition 1.4 has been reduced to showing that if $\alpha \in \mathcal{M}$ is integral on a properly concentrated set and has axial denominator, then $\alpha \in \mathbf{C}[\boldsymbol{T}]$. Now $\mathcal{M}$ is closed under algebraic shifts, so we may use Theorem 3.2 for the choice $k = \mathbf{C}$. In particular, we are reduced to finding for each $r \in \mathbf{N}(n)$ a sequence $c_1, \ldots, c_m \in \mathbf{N}$ for which (3.17) holds with α in place of x.

Let $r \in \mathbf{N}(n)$ and suppose $\alpha \in \mathcal{M}$ is integral on a properly concentrated set M of positive δ-density and has axial denominator. Consider the geometric interpretation for shifts of $\mathcal{M}$. Then the VW condition states that there is $k \in \mathbf{N}$ and $N \subseteq M$ such that $\delta(N) > 0$ and $\alpha - \mathrm{sh}_{k;r}(\alpha)$ remains integral on N. Now the valuation on $\mathcal{M}$ is discrete. Thus there is a sequence $k_1, \ldots, k_m \in \mathbf{N}$ such that

$$\beta = \{\Delta_{k_1;r} \circ \cdots \circ \Delta_{k_m;r}\}(\alpha) \tag{6.3}$$

is in the intersection of $\mathcal{O}_{\infty_V}$ with the prime ideal of the ∞_V-valuation and is integral on a properly concentrated set of positive δ-density. We are reduced to proving that $\beta = 0$.

Let f represent β. Then $f^{-1}B(0, \frac{1}{2})$ is a neighborhood of ∞_V. Consequently, β actually vanishes on a properly concentrated set of positive δ-density. Let $\mathscr{A}$ be the group of holomorphic functions $\tau: V \to V$ such that $\theta \circ \tau = \theta$. Then $\gamma = \Pi_{\tau \in \mathscr{A}} \beta \circ \tau$ factors to a holomorphic germ on U which vanishes on a properly concentrated set of positive δ-density. By Theorem 4.2, $\gamma = 0$. But then, finally, β must be 0.

References

1. S. D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proc. London Math. Soc. (3) **43** (1981), 227–250.

2. M. Fried, *Arithmetic properties of function fields (II)*, Acta Arith. **25** (1974), 225–258.

3. M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory **6** (1974), 211–231.

4. M. Fried, *On the Sprindžuk–Weissauer approach to universal Hilbert subsets*, Isr. J. Math. **51** (1985), 347–363.

5. H. Furstenberg, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton University Press, Princeton, 1981.

6. H. Furstenberg and Y. Katznelson, *An ergodic Szemeredi theorem for commuting transformations*, J. Analyse Math. **34** (1978), 275–291.

7. D. Hilbert, *Über die irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. Reine Angew. Math. **110** (1892), 104–129.

8. S. Lang, *Diophantine Geometry*, Interscience, New York, 1966.

9. R. Narasimhan, *Several Complex Variables*, University of Chicago Press, Chicago, 1971.

10. C. L. Siegel, *Über einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys. Math. Kl. **1** (1929), 14–67.

11. V. G. Sprindžuk, *Reducibility of polynomials and rational points on algebraic curves*, Seminar on Number Theory, Paris, 1979–80.

12. V. G. Sprindžuk, *Diophantine equations involving unknown primes*, Trudy MIAN SSR **158** (1981), 180–196.