ELEMENTARY STATEMENTS OVER LARGE ALGEBRAIC FIELDS(1)

BY

MOSHE JARDEN

Abstract. We prove here the following theorems:

A. *If k is a denumerable Hilbertian field then for almost all $(\sigma_1, \ldots, \sigma_e) \in \mathscr{G}(k_s/k)^e$ the fixed field of $\{\sigma_1, \ldots, \sigma_e\}$, $k_s(\sigma_1, \ldots, \sigma_e)$, has the following property: For any nonvoid absolutely irreducible variety V defined over $k_s(\sigma_1, \ldots, \sigma_e)$ the set of points of V rational over K is not empty.*

B. *If E is an elementary statement about fields then the measure of the set of $\sigma \in \mathscr{G}(\tilde{Q}/Q)$ (Q is the field of rational numbers) for which E holds in $\tilde{Q}(\sigma)$ is equal to the Dirichlet density of the set of primes p for which E holds in the field F_p of p elements.*

Introduction. Denote by Σ the class of all fields K which have the following property: For any nonvoid absolutely irreducible variety V defined over K, the set of points of V rational over K is not empty.

For any prime p denote by F_p the field with p elements. Then it follows from the Riemann hypothesis for curves that if $\mathscr{F} = \prod F_p/D$ is a nonprincipal ultra-product of the F_p then $\mathscr{F} \in \Sigma$ (see [1, Theorem 6]). On the other hand, it follows from the Hilbert Nullstellensatz that if K is an algebraically closed field then $K \in \Sigma$. In particular it follows that the algebraic closure of Q (the field of rational numbers), $\tilde{Q}$, belongs to Σ. It is therefore natural to ask whether or not $\mathscr{F} \cap \tilde{Q} \in \Sigma$. Ax gave a counterexample in [2, §14], showing that this is not always the case. One can then ask whether Ax's example is exceptional and that, in general, $\mathscr{F} \cap \tilde{Q}$ does belong to Σ. To be more precise denote by $\tilde{Q}(\sigma)$ the fixed field in $\tilde{Q}$ of an automorphism $\sigma \in \mathscr{G}(\tilde{Q}/Q)$ ($\mathscr{G}(\tilde{Q}/Q)$ is the Galois group of $\tilde{Q}$ over Q). Ax showed [1, Theorem 5] that for every nonprincipal ultra-product $\mathscr{F}$ of the F_p there exists $\sigma \in \mathscr{G}(\tilde{Q}/Q)$ such that $\mathscr{F} \cap \tilde{Q} = \tilde{Q}(\sigma)$, and conversely, for each $\sigma \in \mathscr{G}(\tilde{Q}/Q)$ there exists a nonprincipal ultra-product $\mathscr{F}$ of the F_p such that $\mathscr{F} \cap \tilde{Q} = \tilde{Q}(\sigma)$. Furstenberg suggested to me to prove that, for almost all $\sigma \in \mathscr{G}(\tilde{Q}/Q)$ (in the sense of Haar measure), $\tilde{Q}(\sigma) \in \Sigma$. More generally, let k be any field. Denote by μ_k the normalized Haar measure

Received by the editors June 18, 1970.

AMS 1969 *subject classifications.* Primary 1440, 1245.

Key words and phrases. Hilbertian fields, global fields, residue fields of global fields, ultra-products of the above residue fields, the fixed fields $k_s(\sigma_1, \ldots, \sigma_e)$ of $(\sigma_1, \ldots, \sigma_e) \in \mathscr{G}(k_s/k)^e$, Krull topology, Haar measure, absolutely irreducible varieties, Hilbert irreducibility theorem, elementary statement, Dirichlet density, Riemann hypothesis for curves.

(1) This paper is a reproduction of the author's doctoral thesis done in The Hebrew University of Jerusalem (1969) under the supervision of Professor H. Furstenberg to whom the author wishes to express his sincere appreciation.

defined on $\mathscr{G}(k_s/k)$ with respect to the Krull topology. For any positive integer e denote by μ_k^e the product measure defined on $\mathscr{G}(k_s/k)^e$. Then the following theorem is true:

THEOREM. *If k is a denumerable Hilbertian field, then for almost all $(\sigma_1, \ldots, \sigma_e) \in \mathscr{G}(k_s/k)^e$ the fixed field of $\{\sigma_1, \ldots, \sigma_e\}$, $k_s(\sigma_1, \ldots, \sigma_e)$, belongs to Σ.*

Since it is well known that any global field is a Hilbertian field we have in particular the following corollary:

COROLLARY. *If k is a global field then $k_s(\sigma) \in \Sigma$ for almost all $\sigma \in \mathscr{G}(k_s/k)$.*

This corollary enables us to prove a theorem which we call "the translation theorem" which links the fields of the form $k_s(\sigma)$ with the finite fields. Let R be the ring of integers of the global field k and denote by $P(k)$ the set of all nonzero prime ideals of R. For each $\mathfrak{p} \in P(k)$ denote by $F_\mathfrak{p}$ the residue field $R/\mathfrak{p}$. An R-elementary statement is a mathematical statement which is equivalent to a sentence in the first-order language of rings which includes terms for every element of R. If E is an R-elementary statement, denote by $A(E)$ the set of all $\mathfrak{p} \in P(k)$ such that E holds in $F_\mathfrak{p}$, and by $\Sigma(E)$ the set of all $\sigma \in \mathscr{G}(k_s/k)$ such that E holds in $k_s(\sigma)^{1/p^\infty}$ ($k_s(\sigma)^{1/p^\infty}$ is the maximal purely inseparable extension of $k_s(\sigma)$, where p is the characteristic of k). In this terminology the translation theorem may be formulated as follows:

Let k be a global field with ring of integers R. If E is an R-elementary statement, then $\delta(A(E)) = \mu_k(\Sigma(E))$ where $\delta(A(E))$ is the Dirichlet density of $A(E)$. If, in addition, $A(E)$ is infinite then $\delta(A(E))$ and hence $\mu_k(\Sigma(E))$ are positive rational numbers.

The proof of this theorem uses the corollary as well as theorems and methods developed by J. Ax in [1] and [2]. At least one of these theorems uses Riemann hypothesis for curves proved by Weil.

In §3.8 we show that generally there is great difference between sets of the form $A(E)$ and sets of primes in a given arithmetical progression.

I wish to express to Furstenberg my great appreciation for his suggestion of this topic and for the continued encouragement he has given me in my work.

CHAPTER 1. PRELIMINARIES

1.1. **Pro-cyclic extensions.** We begin by recalling some facts about infinite Galois extensions of fields.

Let K/k be an infinite Galois extension. Denote by $\mathscr{G}(K/k)$ the Galois group of K/k. $\mathscr{G}(K/k)$ becomes a topological group if we take as a base for the topology the family of all subsets of the form

$$\{\tau \in \mathscr{G}(K/k) \mid \tau|N = \sigma|N\}$$

where $\sigma \in \mathcal{G}(K/k)$ and N/k is a finite Galois subextension of K/k. This topology is known as the Krull topology of $\mathcal{G}(K/k)$. We can also prove that $\mathcal{G}(K/k)$ is algebraically and topologically isomorphic to the inverse limit of the set of finite group $\mathcal{G}(N/k)$ (N/k as before) and conclude that $\mathcal{G}(K/k)$ is compact and totally disconnected. If we replace subgroups by closed subgroups we can translate all the basic theorems of finite Galois theory to infinite Galois theory.

We now pass to the description of pro-cyclic extensions. All the facts about these extensions which we formulate below are well known.

LEMMA 1.1. *The following conditions on a Galois extension K/k are equivalent*:

(i) *$\mathcal{G}(K/k)$ is the closure of the group generated by one element (which will be called "a generator of the group $\mathcal{G}(K/k)$").*

(ii) *There exists a $\sigma \in \mathcal{G}(K/k)$ such that $k = K(\sigma)$, where $K(\sigma)$ is the fixed field of σ.*

(iii) *Every finite subextension of K/k is cyclic.*

(iv) *There exists at most one subextension of K/k for each degree.*

If one of the conditions is fulfilled we call K/k "a pro-cyclic extension" and $\mathcal{G}(K/k)$ "a pro-cyclic group."

For every rational prime p denote by $\bar{Z}_p$ the ring of p-adic integers. If S is a set of prime numbers then by $\mathfrak{m}(S)$ we mean the set of those positive integers whose prime factors are all in S. Then it can be shown that $\prod_{p\in S} \bar{Z}_p$ is algebraically and topologically isomorphic to the inverse limit $\operatorname{proj\,lim}_{n\in\mathfrak{m}(S)} Z/nZ$ where the topology of Z/nZ is taken as the discrete topology. We add that the ring of integers Z can be imbedded in $\prod_{p\in S} \bar{Z}_p$ and this imbedding will be also topological if we take for Z the topology in which the neighborhoods of 0 will be all the sets of the form mZ where $m \in \mathfrak{m}(S)$. Z will then be dense in $\prod_{p\in S} \bar{Z}_p$.

LEMMA 1.2. *Let K/k be a pro-cyclic extension. Take a generator σ for $\mathcal{G}(K/k)$ and suppose that S is a set of primes such that $m \in \mathfrak{m}(S)$ for every positive integer for which K/k has a subextension of degree m. Then the mapping $n \mapsto \sigma^n$ of Z into $\mathcal{G}(K/k)$ can be extended to a continuous epimorphism $h: \prod_{p\in S} \bar{Z}_p \to \mathcal{G}(K/k)$ and so $\mathcal{G}(K/k) \cong \prod_{p\in S} H_p$ where H_p is a factor ring of $\bar{Z}_p$ and the isomorphism is group-theoretic as well as topological.*

If S contains every prime then we have the following lemma:

LEMMA 1.3. *The following conditions are equivalent for a Galois extension K/k*: (i) *K/k has exactly one subextension of each degree.* (ii) *$\mathcal{G}(K/k)$ is algebraically and topologically isomorphic to $\hat{Z}$* ($\hat{Z} = \operatorname{proj\,lim}_{n\in Z;\, n>0} Zn/Z$).

Following Lemma 1.3 we define:

A perfect field K is said to be "quasi-finite" if it fulfills one of the following equivalent conditions:

(i) K has exactly one extension of each degree in a fixed algebraic closure $\tilde{K}$.

(ii) $\mathcal{G}(\tilde{K}/K)$ is algebraically and topologically isomorphic to $\hat{Z}$.

We shall also need the following lemma:

LEMMA 1.4. *Let K/k be a Galois extension. Suppose that $\mathcal{G}(K/k)\cong\prod_{p\in S}\overline{Z}_p$ where S is a set of primes. If q is a prime that does not belong to S then K/k does not have a subextension of degree q.*

Proof. We must show that $\prod_{p\in S}\overline{Z}_p$ does not have any closed subgroup of index q. Suppose such a subgroup exists, say I. Then it is not difficult to see that in fact I is a closed ideal in the ring $\prod_{p\in S}\overline{Z}_p$. From the fact that the index of I is q we conclude that $q\in I$. But since q is invertible in $\overline{Z}_p$ for $p\neq q$ and, since $q\notin S$, q is invertible in $\prod_{p\in S}\overline{Z}_p$. Hence $I=\prod_{p\in S}\overline{Z}_p$ which is a contradiction.

1.2. **Linear disjointness of field extensions.**

DEFINITION. A family of field extensions $\{k_1/k,\ldots,k_n/k\}$ which are all contained in a common extension is said to be "linearly disjoint" if the natural epimorphism of $k_1\otimes\cdots\otimes k_n$ (product over k) onto the k-algebra generated by all the products $x_1\cdots x_n$ with $x_i\in k_i$ defined by

$$x_1\otimes\cdots\otimes x_n\to x_1\cdots x_n,\qquad x_i\in k_i,$$

is an isomorphism.

The following lemma is well known (e.g. see [9, p. 5, Proposition 6]):

LEMMA 1.5. (i) *A necessary and sufficient condition for a family $\{k_1/k,\ldots,k_n/k\}$ of finite extensions to be linearly disjoint is*

$$[k_1\cdots k_n:k]=\prod_{i=1}^{n}[k_i:k].$$

(ii) *Let K/k be a field extension. Suppose $f\in k[x]$ is an irreducible polynomial and let $\alpha\in\tilde{k}$ be a root of f. A necessary and sufficient condition for $k(\alpha)$ to be linearly disjoint from K over k is that f is irreducible over K.*

DEFINITION. An infinite sequence $\{k_i/k\}_{i=1}^{\infty}$ of field extensions which are all contained in a common extension is said to be "linearly disjoint" if every finite subfamily is linearly disjoint.

It is obvious that $\{k_i/k\}_{i=1}^{\infty}$ is linearly disjoint if and only if, for every n, $k_1\cdots k_n$ is linearly disjoint from k_{n+1} over k.

Moreover it is easy to see that if $\{k_i/k\}_{i=1}^{\infty}$ is a linearly disjoint sequence of proper extensions and if K is the field generated by all the k_i, then K/k is an infinite extension.

We remark that the notion of linear disjointness plays an essential role in our work.

1.3. **Haar measure of the Galois group.** Let K/k be a Galois extension. We have seen in §1.1 that $\mathcal{G}(K/k)$ turns out to be a compact group by the Krull topology. It follows that we can define in a unique way a measure $\mu_{K/k}$ on the Borel field of

$\mathcal{G}(K/k)$ such that $\mu_{K/k}(\mathcal{G}(K/k))=1$, $\mu_{K/k}$ is regular and $\mu_{K/k}$ is two-sided invariant, i.e., if E is a measurable subset and $\sigma \in \mathcal{G}(K/k)$ then $\mu_{K/k}(\sigma E)=\mu_{K/k}(E)=\mu_{K/k}(E\sigma)$. This measure is called the Haar measure of $\mathcal{G}(K/k)$. We shall sometimes write μ_k or even μ instead of $\mu_{K/k}$. We note that the condition $\mu(\mathcal{G}(K/k))=1$ means that μ is in fact a probability measure. This permits us to use the probabilistic notion "independent sets (events)" and in fact we use it in an essential way.

We shall sometimes be working within the product space $\mathcal{G}(K/k)^n$; then we shall use $\mu^n_{K/k}$ or μ again to denote the appropriate product measure.

If L/k is a finite subextension of K/k of degree n then it is known that the index of $\mathcal{G}(K/L)$ in $\mathcal{G}(K/k)$ is n. If we use the invariance of μ we get the following basic lemma.

LEMMA 1.6. *Let L/k be a subextension of a Galois extension K/k.*

(i) *If L/k is a finite extension then $\mu(\mathcal{G}(K/L))=1/[L:k]$.*

(ii) *If L/k is an infinite extension then $\mu(\mathcal{G}(K/L))=0$.*

From Lemma 1.6 and from the uniqueness of the Haar measure we get

LEMMA 1.7. *Let k'/k be a finite subextension of a Galois extension K/k. Then for every measurable set $A\subseteq\mathcal{G}(K/k')^e$ we have $\mu_k(A)=\mu_{k'}(A)/[k':k]^e$, where e is a positive integer.*

If L/k is a finite Galois subextension then we have the following generalization of Lemma 1.6:

LEMMA 1.8. *Let L/k be a finite Galois subextension of a Galois extension K/k. Let $\mathfrak{C}\subseteq\mathcal{G}(L/k)$ then*

$$\mu(\{\tau\in\mathcal{G}(K/k)\mid \tau|L\in\mathfrak{C}\}) = |\mathfrak{C}|/[L:k]$$

(by $|\mathfrak{C}|$ we mean the cardinality of the set $\mathfrak{C}$).

Proof. The lemma follows immediately from the invariance of μ and from Lemma 1.6 if we only notice that

$$\{\tau\in\mathcal{G}(K/k)\mid \tau|L\in\mathfrak{C}\} = \bigcup_{\bar{\sigma}\in\mathfrak{C}}\sigma\mathcal{G}(K/L)$$

where σ is any extension of $\bar{\sigma}$ to K.

The notions "linear disjointness of field extensions" and "independence of sets in a probability space" are quite close to each other. We formulate the connection between them in the following lemma:

LEMMA 1.9. *Let $\{k_i/k\}_{i=1}^{\infty}$ be an infinite sequence of finite subextensions of a Galois extension K/k. A necessary and sufficient condition for $\{k_i/k\}_{i=1}^{\infty}$ to be linearly disjoint is that the sequence $\{\mathcal{G}(K/k_i)\}_{i=1}^{\infty}$ of subsets of $\mathcal{G}(K/k)$ is independent in the probabilistic sense.*

Proof. The proof follows by a direct computation from the preceding lemmas.

We use Lemma 1.9 to prove the following lemma which will be one of our basic tools in the work.

LEMMA 1.10. *Let k'/k be a finite subextension of a Galois extension K/k. Let $\{k_i/k'\}_{i=1}^{\infty}$ be a linearly disjoint sequence of finite subextensions of K/k'. Suppose e is a positive integer for which $\prod_{i=1}^{\infty}(1-1/[k_i:k']^e)=0$. Then*

$$\mu_k^e\left(\bigcup_{i=1}^{\infty}\mathscr{G}(K/k_i)^e\right)=\frac{1}{[k':k]^e}.$$

Proof. We use two simple facts from probability theory.

(a) For $1\leqq j\leqq e$ let $\{A_{ji}\}_{i=1}^{\infty}$ be an independent sequence of sets in a probability space Ω_j. The set $\{\times_{j=1}^{e}A_{ji}\}_{i=1}^{\infty}$ is independent in the product space $\Omega_1\times\cdots\times\Omega_e$.

(b) If a sequence of sets $\{A_i\}_{i=1}^{\infty}$ is independent in a probability space then the sequence of complements $\{\Omega-A_i\}_{i=1}^{\infty}$ is also independent in Ω.

Now from Lemma 1.9 it follows that $\{\mathscr{G}(K/k_i)\}_{i=1}^{\infty}$ is independent in the space $\mathscr{G}(K/k')$. Hence, according to (a), $\{\mathscr{G}(K/k_i)^e\}_{i=1}^{\infty}$ is independent in $\mathscr{G}(K/k')^e$ and so, according to (b), $\{\mathscr{G}(K/k')^e-\mathscr{G}(K/k_i)^e\}_{i=1}^{\infty}$ is independent in $\mathscr{G}(K/k')^e$. If we use Lemma 1.6 we get for every n

$$\begin{aligned}1&\geqq\mu_{k'}^e\left(\bigcup_{i=1}^{\infty}(K/k_i)^e\right)\geqq\mu_{k'}^e\left(\bigcup_{i=1}^{n}\mathscr{G}(K/k_i)^e\right)\\&=1-\mu_{k'}^e\left(\bigcap_{i=1}^{n}(\mathscr{G}(K/k')^e-\mathscr{G}(K/k_i)^e)\right)=1-\prod_{i=1}^{n}\left(1-\frac{1}{[K:k_i]^e}\right)\end{aligned}$$

hence $\mu_{k'}^e(\bigcup_{i=1}^{\infty}\mathscr{G}(K/k_i))^e=1$. If we use Lemma 1.7 we get

$$\mu_k^e\left(\bigcup_{i=1}^{\infty}\mathscr{G}(K/k_i)^e\right)=\frac{1}{[k':k]^e}.\qquad\text{Q.E.D.}$$

1.4. **Hilbertian fields.** Let k be a field and let $(\boldsymbol{T},\boldsymbol{X})=(T_1,\ldots,T_m,X_1,\ldots,X_n)$ be $m+n$ independent variables. Let $f(\boldsymbol{T},\boldsymbol{X})$ be a polynomial in $(\boldsymbol{X})$ with coefficients in the field $k(\boldsymbol{T})$ which is irreducible in the ring $k(\boldsymbol{T})[\boldsymbol{X}]$. Denote by $U_{f,k}$ the set of all $(a_1,\ldots,a_m)\in k^m$ for which $f(\boldsymbol{a},\boldsymbol{X})$ is defined and irreducible in $k[\boldsymbol{X}]$. $U_{f,k}$ will be called "Hilbert basic set." The intersection of a finite number of Hilbert basic sets with a Zariski nonvoid open set in m variables will be called "a Hilbert set of k^m." k will be called "a Hilbertian field" if for every $m\geqq 1$ the Hilbert sets of k^m are not empty.

Hilbertian fields will be of great importance to us since we are able to build linearly disjoint extensions over them very easily.

Many fields are Hilbertian. Among them the most important are the global fields and the fields of algebraic functions of one variable. In particular Q is Hilbertian. Moreover, every finite separable extension k' of a Hilbertian field k is Hilbertian and what will be most important to us is the fact that every Hilbertian set of k' contains a Hilbertian set of k. For details consult Lang [6, Chapter VIII]. Recently Kuyk has found a large variety of infinite algebraic extensions of Hilbert-

ian fields which are themselves Hilbertian (see Kuyk [4] and [5]). In particular he proved that the maximal abelian extension k_{ab} and the maximal nilpotent extension k_{nil} of a Hilbertian field is Hilbertian.

On the other hand finite fields and algebraically closed fields are easily shown not to be Hilbertian. We shall see that if k_s is the separable closure of a field k and if $\sigma \in \mathcal{G}(k_s/k)$ then $k_s(\sigma)$ is not Hilbertian.

Chapter 2. Algebraic Points on Absolutely Irreducible Variety

2.1. **Σ-fields.** Denote by Σ the class of all fields K which have the following property: For any nonvoid absolutely irreducible variety V defined over K, the set of points of V rational over K is not empty. A field K which belongs to Σ will be called a Σ-field.

In fact, one can easily show that if V is an absolutely irreducible variety defined over a Σ-field K then the set of points of V rational over K is dense on V in the Zariski topology.

For any prime p denote by F_p the field with p elements. Then it follows from the Riemann hypothesis for curves [8] that if $\mathcal{F} = \prod F_p/D$ is a nonprincipal ultra-product of the F_p then $\mathcal{F} \in \Sigma$ (see Ax [1, Theorem 6]). On the other hand, it follows from the Hilbert Nullstellensatz that if K is algebraically closed then $K \in \Sigma$. In particular it follows that $\tilde{Q} \in \Sigma$. It is therefore natural to ask whether or not $\mathcal{F} \cap \tilde{Q} \in \Sigma$. Ax gave a counterexample in [2, 14], showing that this is not always the case. One can then ask whether Ax's example is the exception or the rule. We shall see, however, that Ax's example is exceptional and that in general $\mathcal{F} \cap \tilde{Q}$ does belong to Σ. To be more precise we note that Ax showed [1, Theorem 5] that for every nonprincipal ultra-product $\mathcal{F}$ of the F_p there exists $\sigma \in \mathcal{G}(\tilde{Q}/Q)$ such that $\mathcal{F} \cap \tilde{Q} \cong \tilde{Q}(\sigma)$, and conversely, for each $\sigma \in \mathcal{G}(\tilde{Q}/Q)$ there exists a nonprincipal ultra-product of the F_p such that $\mathcal{F} \cap \tilde{Q} \cong \tilde{Q}(\sigma)$. What we shall in fact prove is that for almost all $\sigma \in \mathcal{G}(\tilde{Q}/Q)$, $\tilde{Q}(\sigma) \in \Sigma$. More generally, we shall show that if k is a Hilbertian field and e a positive integer then for almost all $(\sigma_1, \ldots, \sigma_e) \in \mathcal{G}(k_s/k)^e$ the fixed field of $\{\sigma_1, \ldots, \sigma_e\}$, $k_s(\sigma_1, \ldots, \sigma_e)$, belongs to Σ.

The following Lemma is obvious:

Lemma 2.1. *If K is a Σ-field and* char $(K) = p$ *then K^{1/p^∞} is a Σ-field.*

Definition. (i) Let $V^{n,r}$ be an irreducible variety defined over a field k (by $V^{n,r}$ we mean a variety V defined in the affine space S^n of dimension r). Suppose $\{i_1, \ldots, i_r\}$ is a subset of $\{1, \ldots, n\}$. V is said to be transcendental and separable in the direction $\{i_1, \ldots, i_r\}$ if there exists a generic point $(x_1, \ldots, x_n)$ of V such that $\{x_{i_1}, \ldots, x_{i_r}\}$ is algebraically independent over k and such that the extension $k(x_1, \ldots, x_n)/k(x_{i_1}, \ldots, x_{i_r})$ is both algebraic and separable.

(ii) Let $f \in k[X_1, \ldots, X_n]$. f is said to be separable in X_t if X_t really appears in $f(X)$ and if $f(X)$ as a polynomial over the field $k(X_1, \ldots, X_{t-1}, X_{t+1}, \ldots, X_n)$ is separable.

For example, if f is separable in each X_i and absolutely irreducible then $V(f)$ is transcendental and separable in the direction of each subset of $n-1$ numbers of the set $\{1, \ldots, n\}$.

(iii) An extension K/k is said to be Σ-extension if for every absolutely irreducible variety $V^{n,r}$ defined over K, transcendental and separable in the direction $\{1, \ldots, r\}$ there exists a point $(a_1, \ldots, a_n)$ on V, rational over K, such that $a_1, \ldots, a_r \in k$.

It is obvious that if K/k is a Σ-extension then K is a Σ-field.

2.2. **The Nullstellensatz.** The main step toward the Nullstellensatz is the following lemma:

LEMMA 2.2. *Let k be a Hilbertian field and let l/k be a finite separable extension. Suppose $f \in l[T_1, \ldots, T_r, X]$ is an absolutely irreducible polynomial which is separable in X. Let $d \geqq 1$ be the degree of X in $f(\boldsymbol{T}, X)$. Let A be an algebraic set defined over l in S^r which is not the whole space. Then there exists a linearly disjoint infinite sequence, $\{l_i/l\}_{i=1}^{\infty}$, of separable extensions of degree d such that for every $i \geqq 1$ there exist $a_{i1}, \ldots, a_{ir} \in k$ such that $(\boldsymbol{a}_i) \notin A$ and $\alpha_i \in l_i$ such that $f(a_{i1}, \ldots, a_{ir}, \alpha_i) = 0$.*

Proof. We define by induction a sequence of separable extensions l_i/l of degree d having the following properties:

(i) $l_0 = l$.

(ii) l_i is linearly disjoint from $l_0 \cdots l_{i-1}$ over l, for every $i \geqq 1$.

(iii) For every $i \geqq 1$ there exist $a_{i1}, \ldots, a_{ir} \in k$ such that $(\boldsymbol{a}_i) \notin k$ and $\alpha_i \in l_i$ such that $f(\boldsymbol{a}_i, \alpha_i) = 0$.

Then the sequence $\{l_i/l\}_{i=1}^{\infty}$ will be linearly disjoint and so it will be the desired sequence.

Suppose we have already defined $l_0, \ldots, l_{i-1}$ such that they have the properties (i)–(iii). Denote $L = l_0 \cdots l_{i-1}$, then L/k is a finite separable extension. $f(\boldsymbol{T}, X)$ can be written in the form

$$f(\boldsymbol{T}, X) = f_0(\boldsymbol{T})X^d + f_1(\boldsymbol{T})X^{d-1} + \cdots + f_d(\boldsymbol{T}), \qquad f_0(\boldsymbol{T}) \not\equiv 0.$$

From the assumption that $f(\boldsymbol{T}, X)$ is separable in X it follows that there exists $1 \leqq \delta \leqq d$ such that $\operatorname{char} k \nmid \delta$ and such that $f_\delta(\boldsymbol{T}) \not\equiv 0$. Moreover, $f(\boldsymbol{T}, X)$ is absolutely irreducible, hence it is irreducible over L. We conclude that $U_{f,L} - A \cup V(f_0) \cup V(f_\delta)$ is a Hilbertian set of L^m. Since L/k is a finite separable extension it follows that there exists a nonvoid Hilbertian set H of k^m which is contained in $U_{f,L} - A \cup V(f_0) \cup V(f_\delta)$. We therefore choose $(a_{i1}, \ldots, a_{ir}) \in H$ and then $f(\boldsymbol{a}_i, X)$ will be a separable polynomial of degree d which is defined over k and irreducible over L. Let $\alpha_i \in k_s$ be a root of $f(\boldsymbol{a}_i, X)$ and denote $l_i = k(\alpha_i)$. Then l_i/l will be a separable algebraic extension of degree d which, according to Lemma 1.5, is linearly disjoint from L over k.

The induction is thereby complete.

Let l/k be a finite separable extension. Let $V^{n,r}$ be an absolutely irreducible variety defined over l, transcendental and separable in the direction $\{1, \ldots, r\}$. Denote by $\Sigma^e_{l/k}(V)$ the set of all $(\sigma_1, \ldots, \sigma_e) \in \mathscr{G}(k_s/k)^e$ for which there exist $a_1, \ldots, a_r \in k$ and $\alpha_{r+1}, \ldots, \alpha_n \in k_s(\sigma_1, \ldots, \sigma_e)$ such that $(\boldsymbol{a}, \boldsymbol{\alpha}) \in V$. If A is an algebraic set defined over l in the space S^r which is not the whole space then by $\Sigma^e_{l/k}(V, -A)$ we mean the set of all $(\sigma_1, \ldots, \sigma_e) \in \mathscr{G}(k_s/l)^e$ for which there exists a point $(\boldsymbol{a}, \boldsymbol{\alpha}) \in V$ such that $(\boldsymbol{a}) \in k^r - A$ and $\alpha_{r+1}, \ldots, \alpha_n \in k_s(\sigma_1, \ldots, \sigma_e)$.

LEMMA 2.3. *Let k be a Hilbertian field and let l/k be a finite separable extension. Suppose $f \in l[T_1, \ldots, T_r, X]$ is an absolutely irreducible polynomial, separable in X. Let A be an algebraic set defined over l in S^r which is not the whole space. Then* $\mu_k(\Sigma^e_{l/k}(V(f), -A)) = 1/[l:k]^e$.

Proof. Let $d \geqq 1$ be the degree of X in $f(\boldsymbol{T}, X)$. Take the sequence $\{l_i/l\}_{i=1}^{\infty}$ of extensions in accordance with Lemma 2.2. According to definitions we have

$$\bigcup_{i=1}^{\infty} \mathscr{G}(k_s/l_i)^e \subseteq \Sigma^e_{l/k}(V(f), -A) \subseteq \mathscr{G}(k_s/l)^e.$$

Moreover $\prod_{i=1}^{\infty}(1 - 1/[l_i/l]^e) = \prod_{i=1}^{\infty}(1 - 1/d^e) = 0$ hence, according to Lemmas 1.6 and 1.10 we have

$$1/[l:k]^e = \mu_k\left(\bigcup_{i=1}^{\infty} \mathscr{G}(k_s/l_i)^e\right) \leqq \mu_k(\Sigma^e_{l/k}(V(f), -A)) \leqq \mu_k(\mathscr{G}(k_s/l)^e) = 1/[l:k]^e.$$

Hence $\mu_k(\Sigma^e_{l/k}(V(f), -A)) = 1/[l:k]^e$. Q.E.D.

Lemma 2.3 refers to hypersurfaces $V(f)$. The same result is valid for arbitrary absolutely irreducible varieties.

LEMMA 2.4. *Let l/k be a finite separable extension of a Hilbertian field k. Then for every nonvoid absolutely irreducible variety V defined over l,* $\mu_k(\Sigma^e_{l/k}(V)) = 1/[l:k]^e$.

Proof. Suppose V is defined over l in S^n and is of dimension r. Without loss of generality suppose also that V is transcendental and separable in the direction $\{1, \ldots, r\}$. Then we can find a generic point $(x_1, \ldots, x_n)$ for V over l such that $\{x_1, \ldots, x_r\}$ are algebraically independent over l and $l(\boldsymbol{x})/l(x_1, \ldots, x_r)$ is a finite separable extension.

If $l(\boldsymbol{x}) = l(x_1, \ldots, x_r)$ then there exists a point on V, rational over l, and the lemma is certainly true, otherwise there exists a $\xi \in l(\boldsymbol{x})$ of positive degree over $l(x_1, \ldots, x_r)$ such that $l(\boldsymbol{x}) = l(x_1, \ldots, x_r, \xi)$. Let W be the hypersurface generated by the point $(x_1, \ldots, x_r, \xi)$ over l. Then $W = V(f)$ where $f \in k[X_1, \ldots, X_r, T]$ is an absolutely irreducible polynomial separable in T. W will be also birationally equivalent to V over l, hence there exists a rational transformation $\boldsymbol{\phi}: W \to V$, $\boldsymbol{\phi} = (\phi_1, \ldots, \phi_n)$, and an algebraic set U defined over l in S^r which is not the whole space such that $\boldsymbol{\phi}$ is defined for every $(w_1, \ldots, w_{r+1}) \in W$ for which $(w_1, \ldots, w_r) \notin U$. From the

definitions it follows that $\Sigma^e_{l/k}(V(f), -U) \subseteq \Sigma^e_{l/k}(V)$. Hence, using Lemmas 1.6 and 2.3, we get our lemma.

THEOREM 2.5 (THE NULLSTELLENSATZ). *If k is a denumerable Hilbertian field and e is a positive integer then $k_s(\sigma_1, \ldots, \sigma_e)/k$ is a Σ-extension for almost every*

$$(\sigma_1, \ldots, \sigma_e) \in \mathscr{G}(k_s/k)^e.$$

Proof. Denote by S the set of all $(\sigma_1, \ldots, \sigma_e) \in \mathscr{G}(k_s/k)^e$ for which $k_s(\sigma_1, \ldots, \sigma_e)/k$ is not a Σ-extension. Let $(\sigma_1, \ldots, \sigma_e) \in S$. Then, there exists an absolutely irreducible variety $V^{n,r}$, transcendental and separable in the direction $\{1, \ldots, r\}$, which is defined over $k_s(\sigma_1, \ldots, \sigma_e)$ for which there does not exist a point $(a_1, \ldots, a_r, \alpha_{r+1}, \ldots, \alpha_n)$ such that $a_1, \ldots, a_r \in k$ and $(\boldsymbol{a}, \boldsymbol{\alpha}) \in V \cap k_s(\sigma_1, \ldots, \sigma_e)^n$. Let l be a field of definition for V which is contained in $k_s(\sigma_1, \ldots, \sigma_e)$ and finite and separable over k. Then $(\sigma_1, \ldots, \sigma_e) \in \mathscr{G}(k_s/l)^e - \Sigma^e_{l/k}(V)$. Hence $S \subseteq \bigcup_V (\mathscr{G}(k_s/k)^e - \Sigma^e_{l/k}(V))$ where V ranges over all the absolutely irreducible varieties defined over k_s. According to Lemma 2.4 the measure of each of the summands in the right-hand side is zero. Since k is denumerable, the number of the above V's is denumerable, hence the measure of the right-hand side is zero, and so $\mu_k(S) = 0$. Q.E.D.

Since every global field is Hilbertian and denumerable we have the following corollary of the Nullstellensatz:

COROLLARY 2.6. *If k is a global field and e is a positive integer then $k_s(\sigma_1, \ldots, \sigma_e)/k$ is a Σ-extension for almost all $(\sigma_1, \ldots, \sigma_e) \in \mathscr{G}(k_s/k)^e$.*

In particular if $k = Q$ we have

COROLLARY 2.7. *$\tilde{Q}(\sigma_1, \ldots, \sigma_e)/Q$ is a Σ-extension for almost every $(\sigma_1, \ldots, \sigma_e) \in \mathscr{G}(\tilde{Q}/Q)^e$.*

By this we answer positively Ax's question: "Does any proper subfield K of $\tilde{Q}$ have the property that every absolutely irreducible variety defined over K has a K-valued point?" (See [2, p. 269, Problem 2].) In addition, the corollary implies that there exists a subfield K of $\tilde{Q}$ such that $K \in \Sigma$ and $\mathscr{G}(\tilde{Q}/K)$ is not abelian. To see this, note that there exists a set B of pairs $(\sigma_1, \sigma_2) \in \mathscr{G}(\tilde{Q}/Q)^2$ of positive measure such that $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$ for any $(\sigma_1, \sigma_2) \in B$. For if one takes any finite normal, non-abelian extension N/Q and picks $\bar{\sigma}_1, \bar{\sigma}_2 \in \mathscr{G}(N/Q)$ such that $\bar{\sigma}_1\bar{\sigma}_2 \neq \bar{\sigma}_2\bar{\sigma}_1$, then the set of pairs $(\sigma_1, \sigma_2) \in \mathscr{G}(\tilde{Q}/Q)$ such that $\sigma_1|N = \bar{\sigma}_1$, $\sigma_2|N = \bar{\sigma}_2$ is of positive measure and is included in B. (In fact it can be shown that B can be chosen to have measure 1.) It follows that K may be chosen as one of the $\tilde{Q}(\sigma_1, \sigma_2) \in \Sigma$ such that $(\sigma_1, \sigma_2) \in B$. By this remark we answer positively another question of Ax which may be formulated as follows: "Does there exist a subfield K of $\tilde{Q}$ which belongs to Σ such that $\mathscr{G}(\tilde{Q}/K)$ is not abelian?" (See [2, p. 269].)

From the Nullstellensatz and from Lemma 2.1 we have also the following corollary which will be of importance to us in the next chapter.

COROLLARY 2.8. *If k is a denumerable Hilbertian field of characteristic $p \neq 0$ (e.g., if k is a function field of characteristic $p \neq 0$) then $k_s(\sigma)^{1/p^\infty}$ is a perfect Σ-field for almost every $\sigma \in \mathcal{G}(k_s/k)$.*

2.3. **Fields which are not Σ-fields.** In this section we point out briefly some fields which are not Σ-fields and raise some questions about these fields.

In the first place, we note that the words "almost all" cannot be replaced in the formulation of the Nullstellensatz by the word "all." For example if σ is the automorphism of $\tilde{Q}$ which takes any $a+b\sqrt{-1}$ to $a-b\sqrt{-1}$ (a, b are real algebraic numbers) then $\tilde{Q}(\sigma)$ is the field of real algebraic numbers. It is not a Σ-field because it does not contain any zero of the absolutely irreducible polynomial X^2+Y^2+1. Ax constructs in [2, p. 269] a whole class of fields of the type $\tilde{Q}(\sigma)$ which are not Σ-fields. His fields are in fact quasi-finite fields. Ax's examples are based on the following lemma:

LEMMA 2.9. *If one can define a discrete valuation v on a field k whose residue field is finite, then k is not a Σ-field.*

Proof. Choose a $\pi \in k$ for which $v(\pi)>0$. Suppose that the residue field has q elements. Then the polynomial $(X^q-X-1)(Y^q-Y-1)-\pi$ is absolutely irreducible and does not have any zero in k.

COROLLARY. (i) *A global field is not a Σ-field.*

(ii) *If k is a global field and if $\mathfrak{p}$ is a prime ideal of its ring of integers then $\bar{k}_\mathfrak{p}$ (the completion of k under $\mathfrak{p}$) is not a Σ-field.*

Problem 1. What can be said regarding intermediate extensions of Q, i.e. infinite extensions of Q which do not contain any field of the form $\tilde{Q}(\sigma_1, \ldots, \sigma_e)$. (Ax showed in [2, p. 268] that any extension of a perfect Σ-field is again a Σ-field.) In particular we ask if the maximal abelian extension of Q, Q_{ab} belongs to Σ. We note that it can be shown that Q_{ab} is not a Σ-extension of Q because $3X^3+4Y^3+5Z^3$ is an absolutely irreducible polynomial and it does not have any zero (x, y, z) such that $y, z \in Q$ and $x \in Q_{ab}$. Does $3X^3+4Y^3+5Z^3$ have any abelian zero at all?

Problem 2. Does there exist a Hilbertian field which belongs to Σ?

We note that(2) the fields $k_s(\sigma_1, \ldots, \sigma_e)$ are not Hilbertian because otherwise Lemma 2.2 would imply that they have infinitely many quadratic extensions. Thus $\mathcal{G}(k_s/k_s(\sigma_1, \ldots, \sigma_e))$ is not finitely generated (in the sense of topological groups) which is a contradiction since $\sigma_1, \ldots, \sigma_e$ are clearly topological generators to it.

CHAPTER 3. THE TRANSLATION THEOREM

3.0. **The pseudo-finite fields theorem.** Let K be a field of characteristic p. The K^{1/p^∞} will denote the maximal purely inseparable extension of K, i.e. the field

(2) This observation was made by the referee.

generated over K by the p^mth roots of elements of K if $p \neq 0$ and K itself if $p=0$.

A perfect field K is said to be "pseudo-finite" if K is a Σ quasi-finite field.

Our aim in this section is to prove that if k is a Hilbertian field then $k_s(\sigma)^{1/p^\infty}$ is a pseudo-finite field for almost all $\sigma \in \mathcal{G}(k_s/k)$. We begin with some lemmas.

The first lemma follows from Galois theory of infinite extensions. It will let us pass from the fields $k_s(\sigma)$ which are not always perfect to the perfect fields $k_s(\sigma)^{1/p^\infty}$.

LEMMA 3.1. *If k is a field of characteristic p then*

$$\mathcal{G}(k_s/k_s(\sigma)) \cong \mathcal{G}(\tilde{k}/k_s(\sigma)^{1/p^\infty})$$

for every $\sigma \in \mathcal{G}(k_s/k)$.

LEMMA 3.2. *Let k be a Hilbertian field and let p be a prime. Then there exists an infinite Galois extension $k^{(p)}$ of k which is contained in every separable extension K of k which has no cyclic extension of degree p.*

Proof. If $p \neq \text{char}\,(k)$ then according to a result of Kuyk [4, p. 401] there exists, an infinite Galois extension $k^{(p)}$ of k such that $\mathcal{G}(k^{(p)}/k) \cong \overline{Z}_p$. According to Lemma 1.4 the finite subextensions of $k^{(p)}/k$ are cyclic of degrees p^m.

Suppose now that $p = \text{char}\,(k)$. Denote by $k^{(p)}$ the field generated over k by all the cyclic extensions of k of degree p. Consider the polynomial $X^p - X - Y$. It is absolutely irreducible. Hence, according to Lemma 2.2 we can find a sequence of pairs $\{(a_n, \alpha_n)\}_{n=1}^\infty$ such that $a_n \in k$, the polynomial $X^p - X - a_n$ is irreducible over k, $\alpha_n^p - \alpha_n - a_n = 0$ and the sequence of extensions $\{k(\alpha_n)/k\}_{n=1}^\infty$ is linearly disjoint. According to a theorem of Artin and Schreier (see Lang [7, p. 215]) $k(\alpha_n)/k$ are cyclic extensions of degree p. The extension generated by all the $k(\alpha_n)$ is therefore contained in $k^{(p)}$. But this is an infinite extension, hence $k^{(p)}/k$ is an infinite extension. Also in this case we get that the finite subextensions of $k^{(p)}/k$ are of degrees p^m.

It is not difficult to see now that if K is a separable extension of k that has no cyclic extension of degree p then $k^{(p)} \subseteq K$. Q.E.D.

LEMMA 3.3. *Let k be a Hilbertian field of characteristic different from 2. Denote by $k'^{(2)}$ the field generated by all the fields of the form $k(\sqrt{\alpha})$ where $\alpha \in k$, α is not a square in k but the sum of two squares of k. Then $k'^{(2)}/k$ is an infinite Galois extension.*

Proof. Consider the absolutely irreducible polynomial $X^2 + Y^2 - Z^2$. We shall build by induction a sequence of pairs $\{(x_i, y_i)\}_{i=1}^\infty$ such that

(i) $x_i, y_i \in k$.

(ii) If we denote $\alpha_i = x_i^2 + y_i^2$ then the polynomial $x_i^2 + y_i^2 - Z^2$ is irreducible in $k(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_{i-1}})[Z]$.

Suppose we have already built (x_i, y_i) for $i = 1, \ldots, n$. Denote $l = k(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_n})$. Then l/k is a finite Galois extension. The polynomial $X^2 + Y^2 - Z^2$ is absolutely irreducible, hence, in particular, it is irreducible over l. We can therefore find $x_n, y_n \in k$ such that $x_n^2 + y_n^2 - Z^2$ will be irreducible in $l[Z]$.

By this we have completed the induction.

α_n has the following properties: $\alpha_n \in k$, α_n is not a square in k but is the sum of two squares of k. Hence $k(\sqrt{\alpha_n}) \subseteq k'^{(2)}$. Furthermore, according to the construction the sequence $\{k(\sqrt{\alpha_n})/k\}_{n=1}^{\infty}$ is linearly disjoint. Hence $k'^{(2)}/k$ is an infinite Galois extension. Q.E.D.

LEMMA 3.4 (THE QUASI-FINITE FIELD LEMMA). *Let k be a Hilbertian field of characteristic p. Then $k_s(\sigma)^{1/p^\infty}$ is a quasi-finite field for almost all $\sigma \in \mathcal{G}(k_s/k)$.*

Proof. This lemma was proved by Ax for $k = Q$. (See [1, p. 177].) We repeat here briefly Ax's proof and indicate why arguments which were valid over the field Q remain valid for arbitrary Hilbertian field k.

First we note that $k_s(\sigma)^{1/p^\infty}$ is always a perfect field. Hence, according to Lemma 3.1 it is sufficient that we prove that $\mathcal{G}(k_s/k_s(\sigma)) \cong \hat{Z}$ for almost all $\sigma \in \mathcal{G}(k_s/k)$.

Now, let $\sigma \in \mathcal{G}(k_s/k)$. Then, according to Lemma 1.2, $\mathcal{G}(\sigma) \cong \prod_q H_q$, where H_q is a factor ring of $\bar{Z}_q$. From a theorem of Artin we deduce that the torsion elements of $\mathcal{G}(k_s/k_s(\sigma))$ are of order 2. From this fact it can be shown that there exists a set $S(\sigma)$ of primes such that exactly one of the following cases takes place.

(i) $\mathcal{G}(k_s/k_s(\sigma)) \cong \prod_{q \in S(\sigma)} \bar{Z}_q$,

(ii) $\mathcal{G}(k_s/k_s(\sigma)) \cong Z/2Z \times \prod_{q \in S(\sigma)} \bar{Z}_q$, $2 \notin S(\sigma)$.

We shall see that, for almost all $\sigma \in \mathcal{G}(k_s/k)$, $S(\sigma)$ is the set of all primes and this will complete the proof.

For every prime q denote by $k^{(q)}$ the extension of k which has been defined in Lemma 3.2. Also denote by $k'^{(2)}$ the extension of Lemma 3.3. Denote $H = \mathcal{G}(k_s/k'^{(2)}) \cup \bigcup_q \mathcal{G}(k_s/k^{(q)})$ where q ranges over all the primes. Using Lemma 1.4 on one side and the theory of real fields on the other side one can show that if $S(\sigma)$ is a proper subset of the set of all primes then $\sigma \in H$. Now, $k'^{(2)}/k$ and $k^{(q)}/k$ are infinite extensions, hence $\mu(H) = 0$. Hence, the set of all $\sigma \in \mathcal{G}(k_s/k)$ such that $S(\sigma)$ is not the set of all primes is of measure zero. Q.E.D.

From the Nullstellensatz and from the quasi-finite field lemma we get the following theorem:

THEOREM 3.5 (THE PSEUDO-FINITE FIELD THEOREM). *If k is a Hilbertian field of characteristic p then $k_s(\sigma)^{1/p^\infty}$ is a pseudo-finite field for almost all $\sigma \in \mathcal{G}(k_s/k)$.*

3.1. **The decomposition field of a prime ideal.** Let R be a Dedekind ring and let k be its quotients field. Denote by $P(k)$ the set of all nonzero prime ideals of R. For every $\mathfrak{p} \in P(k)$ denote by $R_\mathfrak{p}$ the local ring of R defined by $\mathfrak{p}$, i.e.

$$R_\mathfrak{p} = \{x/y | x, y \in R, y \notin \mathfrak{p}\}.$$

Denote by $v_\mathfrak{p}$ the $\mathfrak{p}$-adic valuation. On $R_\mathfrak{p}$ we define a congruence relation as follows

$$a \equiv b \pmod{\mathfrak{p}} \Leftrightarrow v_\mathfrak{p}(a-b) > 0.$$

Denote by $\bar{k}_\mathfrak{p}$ the completion of k with respect to $\mathfrak{p}$. $\bar{R}_\mathfrak{p}$ will denote the valuation ring of $\bar{k}_\mathfrak{p}$.

Let L be a finite Galois extension of k. Denote by S the integral closure of R in L. Then S is a Dedekind ring and L is its quotients field. For every $\mathfrak{p} \in P(L)$ denote by $\Gamma(L/k, \mathfrak{p}) = \{\gamma \in \mathcal{G}(L/k) \mid \gamma(\mathfrak{p}) = \mathfrak{p}\}$ the decomposition group of $\mathfrak{p}$ with respect to k. Its fixed field in L will be denoted by $L(k, \mathfrak{p})$ and will be called the decomposition field of k in L with respect to $\mathfrak{p}$. We denote also by $(\mathfrak{p}|k)$ the prime ideal of R which lies under $\mathfrak{p}$. If $\mathfrak{P} = (\mathfrak{p}|k)$ then there is an algebraic and topological imbedding $i_{\mathfrak{p}}: \bar{k}_{\mathfrak{P}} \to \bar{L}_{\mathfrak{p}}$. It can be shown that $L(k, \mathfrak{p}) = i_{\mathfrak{p}}\bar{k}_{\mathfrak{P}} \cap L$. Hence $L(k, \mathfrak{p})$ is the closure of k in L with respect to the $\mathfrak{p}$-adic topology.

The following lemma is a straightforward generalization of a lemma of Ax [1, p. 163]:

LEMMA 3.6. *Let R be a Dedekind ring with quotients field k. Let L/k be a finite Galois extension. Let S be the integral closure of R in L. Suppose that a polynomial $f \in S[X]$ splits over L into linear factors. Then there exists a finite subset A of $P(L)$ such that for every $\mathfrak{p} \in P(L) - A$ there exists an $a \in R$ such that $f(a) \equiv 0 \pmod{\mathfrak{p}}$ if and only if f has a root in $L(k, \mathfrak{p})$.*

3.2. **The algebraic numbers of ultra-products of the residue fields of a global field.** Denote by $\mathcal{L}_Z$ the first order language of the theory of rings. If R is an arbitrary ring denote by $\mathcal{L}_R$ a fixed language which includes $\mathcal{L}_Z$ and in which every element of R has a name. A model of $\mathcal{L}_R$ is a system which includes the ordinary binary functions $+, -, \cdot$ and a constant for every element of R. If R is an integral domain then by an R-field we mean a model of $\mathcal{L}_R$ which fulfills the ordinary axioms of fields and the relations

$$\bar{a} + \bar{b} = \bar{c}, \qquad \bar{a} - \bar{b} = \bar{c}, \qquad \bar{a} \cdot \bar{b} = \bar{c}$$

for every $a, b, c \in R$ for which $a + b = c$, $a - b = c$, $ab = c$ (where $\bar{a}, \bar{b}, \bar{c}$ are the constants of the model which correspond to the elements a, b, c).

In other words, an R-field is a field which contains a homomorphic image of R. Examples of R-fields include the quotients field of R, extensions of them and the residue fields of R.

If K_1 and K_2 are R-fields then by $K_1 \cong_R K_2$ we mean that they are R-isomorphic (i.e. that they are isomorphic as models of $\mathcal{L}_R$) and by $K_1 \equiv_R K_2$ we mean that they are R-elementary equivalent.

An R-elementary assertion is a mathematical statement which is equivalent to a sentence in $\mathcal{L}_R$. For example, if $f \in R[X]$ then the statement "f is irreducible" is an R-elementary statement.

Now, let R be a Dedekind ring with infinite number of prime ideals, and let k be its quotients field. Let $\mathcal{D}$ be a nonprincipal ultra-filter on $P(k)$. For every $\mathfrak{P} \in P(k)$ denote $F_{\mathfrak{P}} = R/\mathfrak{P}$. Let $\mathcal{F} = \prod F_{\mathfrak{P}}/\mathcal{D}$. Every $F_{\mathfrak{P}}$ is an R-field hence $\mathcal{F}$ is also an R-field. Moreover there is a natural imbedding of R and hence of k in $\mathcal{F}$. If $a \in R$ then a is mapped to the element of $\mathcal{F}$ a representative of which is the function which

maps every $\mathfrak{p} \in P(k)$ to the residue class of R modulo $\mathfrak{p}$ which contains a. We shall identify the image of k in $\mathscr{F}$ with k and denote by $\tilde{k} \cap \mathscr{F}$ the algebraic closure of k in $\mathscr{F}$.

In particular these definitions apply to the ring of integers R of a global field k.

3.3. **An elementary equivalence.**

DEFINITION. Let F be a field. A commutative F-algebra A is said to be "absolutely entire over F" if $\tilde{F} \otimes_F A$ is an integral domain.

A field F is said to be "hyper-finite" if F is uncountable, quasi-finite and for every entire K-algebra A, where K is a subfield of F, such that $|A| < |F|$ there exists a K-algebra homorphism $A \to F$.

For the remainder of this paper we assume the continuum hypothesis $2^{\aleph_0} = \aleph_1$. However, the translation theorem and its applications can be freed from this assumption.

LEMMA 3.7. *Let k be a global field and let $\mathscr{D}$ be a nonprincipal ultra-filter of $P(k)$. Then $\mathscr{F} = \prod F_{\mathfrak{p}}/\mathscr{D}$ is a hyper-finite field of cardinality $2^{\aleph_0}$.*

Proof. For every $\mathfrak{p} \in P(k)$, $F_{\mathfrak{p}}$ is a finite field. For every positive integer m there is only a finite number of $\mathfrak{p}$'s such that $|F_{\mathfrak{p}}| \leqq m$. Hence, according to Ax [2, p. 253] $\mathscr{F}$ is a pseudo-finite field. Again, according to Ax [1, p. 173], $\mathscr{F}$ is also a saturated field and its cardinality is $2^{\aleph_0}$ (see [3, p. 208]). Hence, according to Ax [2, p. 254], $\mathscr{F}$ is hyper-finite. Q.E.D.

LEMMA 3.8. *Let I be an infinite set. For every $i \in I$ let F_i be a pseudo-finite field. Let D be a nonprincipal ultra-filter of I. Then $\prod F_i/D$ is a hyper-finite field.*

Proof. According to Ax [2, p. 254] all the axioms for pseudo-finiteness are elementary statements. Hence $\prod F_i/D$ is pseudo-finite. Moreover it is an uncountable saturated field, hence, according to Ax [2, p. 254], $\prod F_i/D$ is hyper-finite. Q.E.D.

THEOREM 3.9 (THE ELEMENTARY EQUIVALENCE THEOREM). *Let k be a global field of characteristic p and let R be its ring of integers. Then for almost all $\sigma \in \mathscr{G}(k_s/k)$ there exists a nonprincipal ultra-product $\mathscr{F}$ of the $F_{\mathfrak{p}}$'s such that $\tilde{k} \cap \mathscr{F} \cong_k k_s(\sigma)^{1/p^\infty}$ and $\mathscr{F} \equiv_R k_s(\sigma)^{1/p^\infty}$.*

Proof. Let $\sigma \in \mathscr{G}(k_s/k)$ then, according to Lemma 3.1, $\tilde{k}/k_s(\sigma)^{1/p^\infty}$ is a pro-cyclic extension, hence, according to a straightforward generalization of a theorem of Ax [2, p. 260] there exists a nonprincipal ultra-product $\mathscr{F}$ of the $F_{\mathfrak{p}}$'s such that $\tilde{k} \cap \mathscr{F} \cong_k k_s(\sigma)^{1/p^\infty}$. Suppose now that $K = k_s(\sigma)^{1/p^\infty}$ is pseudo-finite (according to Theorem 3.5 this is the case for almost all $\sigma \in \mathscr{G}(k_s/k)$). Take an infinite set I and a nonprincipal ultra-filter D of it. Then, according to [3, p. 208], $|K^I/D| = |\mathscr{F}^I/D| = 2^{\aleph_0} > \aleph_0 = |K|$. It is easy to see that K is algebraically closed in K^I/D and in $\mathscr{F}^I/D$. Moreover, K and $\mathscr{F}$ are pseudo-finite fields hence, according to Lemma 3.8, K^I/D and $\mathscr{F}^I/D$ are hyper-finite fields. According to Ax [2, p. 246], $\mathscr{F}^I/D \cong_K K^I/D$ hence $\mathscr{F}^I/D \cong_k K^I/D$. But $\mathscr{F} \equiv_R \mathscr{F}^I/D$ and $K \equiv_R K^I/D$ hence $\mathscr{F} \equiv_R K$. Q.E.D.

3.4. **The Ax boolean algebra.** Let R be the ring of integers of a global field k. For every $f \in R[X]$ denote

$$A(f) = \{\mathfrak{p} \in P(k) \mid F_{\mathfrak{p}} \models \exists X : f(X) = 0\}.$$

($F_{\mathfrak{p}} \models \exists X : f(X)=0$ means that the statement "$\exists X : f(X)=0$" holds in the field $F_{\mathfrak{p}}$.) Denote by $\mathscr{A}=\mathscr{A}(k)$ the boolean algebra on $P(k)$ generated by all the sets $A(f)$ for which $f \in R[X]$ is a separable polynomial over k (i.e. that its roots are separable over k). $\mathscr{A}$ will be called "the Ax boolean algebra." Every element in $\mathscr{A}$ has the form $\Phi(A(f_1), \ldots, A(f_m))$ where Φ is a boolean polynomial in m variables and $f_1, \ldots, f_m$ are separable polynomials over k. It is not difficult to see that every finite subset of $P(k)$ belongs to $\mathscr{A}$.

If E is an R-elementary statement then we denote

$$A(E) = \{\mathfrak{p} \in P(k) \mid F_{\mathfrak{p}} \models E\}.$$

By a structure induction it is not difficult to prove the following lemmas:

LEMMA 3.10. *Let R be the ring of integers of a global field k. Suppose $E_1, \ldots, E_m$ are R-elementary statements and let Φ be a boolean polynomial in m variables. Then*

$$A(\Phi(E_1, \ldots, E_m)) = \Phi(A(E_1), \ldots, A(E_m)).$$

LEMMA 3.11. *Let k be a field and let $f_1, \ldots, f_m \in k[X]$. Let N be an extension of k which contains all the roots of $f_1, \ldots, f_m$. Let L be an arbitrary extension of k. Then for every boolean polynomial Φ*

$$L \models \Phi(\exists X[f_1(X) = 0], \ldots, \exists X[f_m(X) = 0]),$$
$$\Leftrightarrow N \cap L \models \Phi(\exists X[f_1(X) = 0], \ldots, \exists X[f_m(X) = 0]).$$

Following Lemma 3.11 we denote

$$E_{\Phi}(f_1, \ldots, f_m) = \Phi(\exists X[f_1(X) = 0], \ldots, \exists X[f_m(X) = 0])$$

and call this kind of statement "one variable statement" ($f_1, \ldots, f_m$ are taken here to be separable over k).

The following generalization of a theorem of Ax [2, p. 263] shows us that every R-elementary statement can be reduced in a certain sense to a one variable statement.

THEOREM 3.12. *If E is an R-elementary statement, where R is the ring of integers of a global field R then $A(E) \in \mathscr{A}(k)$.*

3.5. **A normal set of fields.** Let L be a finite Galois extension of a global field k. Let $L_1, \ldots, L_m$ be m subfields of L which contain k. The set $\mathscr{L}=\{L_1, \ldots, L_m\}$ is said to be L/k normal if $\mathscr{G}(L/k)\mathscr{L}=\mathscr{L}$. In this case we denote

$$B_{L/k}(\mathscr{L}) = \{\mathfrak{p} \in P(k) \mid \exists \mathfrak{P} \in P(L) : (\mathfrak{P}|k) = \mathfrak{p} \ \&\ L(k, \mathfrak{P}) \in \mathscr{L}\}.$$

It is easy to see that

$$B_{L/k}(\mathscr{L}) = \{\mathfrak{p} \in P(k) \mid \forall \mathfrak{P} \in P(L) : (\mathfrak{P}|k) = \mathfrak{p} \Rightarrow L(k, \mathfrak{P}) \in \mathscr{L}\}.$$

The following lemma follows by a structure induction:

LEMMA 3.13. *Let L be a finite Galois extension of a global field k. Let $\mathscr{L}_1, \ldots, \mathscr{L}_m$ be L/k normal sets of subfields of L which contain k. Let Φ be a boolean polynomial. Then $\Phi(\mathscr{L}_1, \ldots, \mathscr{L}_m)$ is again an $\mathscr{L}/k$ normal set and*

$$B_{L/k}(\Phi(\mathscr{L}_1, \ldots, \mathscr{L}_m)) = \Phi(B_{L/k}(\mathscr{L}_1), \ldots, B_{L/k}(\mathscr{L}_m)).$$

REMARK. In the same way that Ax proves in [1, Proposition 1, p. 103] we can prove that every set of the form $B_{L/k}(L)$ belongs to $\mathscr{A}(k)$ and for every set of $\mathscr{A}(k)$ there exists a set of the form $B_{L/k}(\mathscr{L})$ which differs from it only by a finite number of elements.

3.6. **The translation theorem for one variable statements.** If A and B are two subsets of $P(k)$ which differ from one another only by a finite number of elements then we shall write "$A \approx B$" and we shall say that "A is almost equal to B."

The following lemma does most of the work toward the translation theorem. Some of the following arguments appear implicitly in Ax [1].

LEMMA 3.14. *Let R be the ring of integers of a global field k of characteristic p. Let $f_1, \ldots, f_m \in R[X]$ be separable polynomials over k and let Φ be a boolean polynomial. Denote $E = E_\Phi(f_1, \ldots, f_m)$. Let L be a finite Galois extension of k which contains all the roots of $f_1, \ldots, f_m$. Then there exist conjugacy classes $\mathfrak{C}_1, \ldots, \mathfrak{C}_n$ $(n \geqq 0)$ in $\mathscr{G}(L/k)$ such that*

$$A(E) \approx \{\mathfrak{p} \in P(k) \mid ((L/k)/\mathfrak{p}) \in \{\mathfrak{C}_1, \ldots, \mathfrak{C}_n\}\} \tag{1}$$

$$\begin{aligned} &\{\sigma \in \mathscr{G}(k_s/k) \mid k_s(\sigma)^{1/p^\infty} \models E\} \\ &= \{\sigma \in \mathscr{G}(k_s/k) \mid \exists \mathfrak{P} \in P(L) : \sigma|L = [(L/k)/\mathfrak{P}] \ \&\ L(k, \mathfrak{P}) \models E\} \\ &= \left\{\sigma \in \mathscr{G}(k_s/k) \mid \sigma|L \in \bigcup_{i=1}^{n} \mathfrak{C}_i\right\} \end{aligned} \tag{2}$$

where $[(L/k)/\mathfrak{P}]$ and $((L/k)/\mathfrak{P})$ denote the Frobenius automorphism and Artin symbol respectively.

Proof. For every $1 \leqq \mu \leqq m$ let $\mathscr{L}_\mu$ be the set of all subfields of L which contain k and a root of f_μ. Then $\{\mathscr{L}_1, \ldots, \mathscr{L}_m\}$ is an L/k normal set of subfields. Then, according to Lemma 3.13, $\mathscr{L} = \Phi(\mathscr{L}_1, \ldots, \mathscr{L}_m)$ is also an L/k normal set of subfields.

Assertion A.

$$A(E) \approx B_{L/k}(\mathscr{L}).$$

In fact, Lemma 3.6 implies that $A(f_\mu) = B_{L/k}(\mathscr{L}_\mu)$ for every μ. Hence

$$\Phi(A(f_1), \ldots, A(f_m)) \approx \Phi(B_{L/k}(\mathscr{L}_1), \ldots, B_{L/k}(\mathscr{L}_m)).$$

This, together with Lemmas 3.10 and 3.13, imply the Assertion.

Consider now the set of conjugacy classes $\{((L/k)/\mathfrak{p}) \mid \mathfrak{p} \in B_{L/k}(\mathscr{L})\}$. This is of course a finite set (it might be empty). Let $\mathfrak{C}_1, \ldots, \mathfrak{C}_n$ be its elements.

Assertion B.

$$B_{L/k}(\mathscr{L}) \approx \{\mathfrak{p} \in P(k) \mid ((L/k)/\mathfrak{p}) \in \{\mathfrak{C}_1, \ldots, \mathfrak{C}_n\}\}.$$

In fact, it is clear that if a nonramified ideal belongs to the left-hand side then it belongs to the right-hand side. On the other hand, if $\mathfrak{p}$ is nonramified in L and there exists a $1 \leqq \nu \leqq n$ such that $((L/k)/\mathfrak{p}) = \mathfrak{C}_\nu$ then there exists a $\mathfrak{p}' \in B_{L/k}(\mathscr{L})$ such that $((L/k)/\mathfrak{p}) = ((L/k)/\mathfrak{p}')$. Let $\mathfrak{P}$ be a prime ideal of L which lies over $\mathfrak{p}$. Then $[(L/k)/\mathfrak{P}] \in ((L/k)/\mathfrak{p}')$ and hence there exists a $\mathfrak{P}' \in P(L)$ such that $(\mathfrak{P}'|k) + \mathfrak{p}'$ and $[(L/k)/\mathfrak{P}] = [(L/k)/\mathfrak{P}']$. But $[(L/k)/\mathfrak{P}]$, $[(L/k)/\mathfrak{P}']$ are generators of the cyclic groups $\Gamma(L/k, \mathfrak{P})$, $\Gamma(L/k, \mathfrak{P}')$, respectively, hence $L(k, \mathfrak{P}) = L(k, \mathfrak{P}') \in \mathscr{L}$. Hence $\mathfrak{p} \in B_{L/k}(\mathscr{L})$.

The Assertions A and B imply (1). We shall now prove (2).

Assertion C.

$$\{\sigma \in \mathscr{G}(k_s/k) \mid k_s(\sigma)^{1/p^\infty} \models E\}$$
$$= \{\sigma \in \mathscr{G}(k_s/k) \mid \exists \mathfrak{P} \in P(L) : \sigma|L = [(L/k)/\mathfrak{P}] \,\&\, L(k, \mathfrak{P}) \models E\}.$$

In fact, suppose that $\sigma \in \mathscr{G}(k_s/k)$ is an automorphism for which $k_s(\sigma)^{1/p^\infty} \models E$. According to Čebotarev density theorem (which is valid for every global field) there exists a $\mathfrak{P} \in P(L)$ such that $(\mathfrak{P}|k)$ is not ramified in L and $[(L/k)/\mathfrak{P}] = \sigma|L$. The fixed field of $[(L/k)/\mathfrak{P}]$ is $L(k, \mathfrak{P})$ hence $k_s(\sigma)^{1/p^\infty} \cap L = k_s(\sigma) \cap L = L(k, \mathfrak{P})$. Since L contains all the roots of $f_1, \ldots, f_m$ we get from Lemma 3.11 that $L(k, \mathfrak{P}) \models E$.

The opposite direction is obtained in an analogous way.

Assertion D.

$$A(E) \approx \{\mathfrak{p} \in P(k) \mid \exists \mathfrak{P} \in P(L) : (\mathfrak{P}|k) = \mathfrak{p} \,\&\, L(k, \mathfrak{P}) \models E\},$$
$$A(E) \approx \{\mathfrak{p} \in P(k) \mid \forall \mathfrak{P} \in P(L) : (\mathfrak{P}|k) = \mathfrak{p} \Rightarrow L(k, \mathfrak{P}) \models E\}.$$

In fact, Lemma 3.6 implies that

$$(4) \quad A(f_n) \approx \{\mathfrak{p} \in P(k) \mid \exists \mathfrak{P} \in P(L)[(\mathfrak{P}/k) = \mathfrak{p} \,\&\, L(k, \mathfrak{P}) \models \exists X : f_n(X) = 0]\}.$$

The assertion follows now by a structure induction.

Assertion E.

$$\{\sigma \in \mathscr{G}(k_s/k) \mid \exists \mathfrak{P} \in P(L)[\sigma|L = [(L/k)/\mathfrak{P}] \,\&\, L(k, \mathfrak{P}) \models E]\}$$
$$= \left\{\sigma \in \mathscr{G}(k_s/k) \mid \sigma|L \in \bigcup_{i=1}^{n} \mathfrak{C}_i\right\}.$$

Suppose $\sigma \in \mathscr{G}(k_s/k)$ is an automorphism for which there exists a $\mathfrak{P} \in P(L)$ such that $\sigma|L = [(L/k)/\mathfrak{P}]$ and $L(k, \mathfrak{P}) \models E$. According to Čebotarev density theorem $\mathfrak{P}$ might be chosen such that $\mathfrak{p} = (\mathfrak{P}|k)$ will not be in the extra ordinary finite sets that exist in Assertions A and D. According to D, $\mathfrak{p} \in A(E)$; hence, according to A, $\mathfrak{p} \in B_{L/k}(\mathscr{L})$. Hence $((L/k)/\mathfrak{p}) \in \{\mathfrak{C}_1, \ldots, \mathfrak{C}_n\}$ so that $\sigma|L = [(L/k)/\mathfrak{P}] \in \bigcup_{i=1}^{n} \mathfrak{C}_i$.

The opposite direction is obtained in an analogous manner.

Assertions C and E imply (2). Q.E.D.

We recall that if $B \subseteq P(k)$ then the "Dirichlet density of B" is defined as the limit (if it exists)

$$\delta(B) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in B} N(\mathfrak{p})^{-s}}{\log 1/(s-1)}$$

where $N(\mathfrak{p})$ is the absolute norm of $\mathfrak{p}$, i.e. $N(\mathfrak{p}) = (R:\mathfrak{p})$.

LEMMA 3.15 (THE TRANSLATION THEOREM FOR ONE-VARIABLE STATEMENTS). *Let R be the ring of integers of a global field k of characteristic p. Suppose $f_1, \ldots, f_m \in R[X]$ are separable polynomials over k and let Φ be a boolean polynomial. Denote*

$$E = E_\Phi(f_1, \ldots, f_m).$$

Then the numbers exist and the equality

$$\delta(A(E)) = \mu(\{\sigma \in \mathcal{G}(k_s/k) \mid k_s(\sigma)^{1/p^\infty} \models E\}) \tag{5}$$

holds. If $A(E)$ is an infinite set then these numbers are positive rational numbers.

Proof. We use the notation of Lemma 3.14. According to (1) and the Čebotarev density theorem,

$$\delta(A(E)) = \sum_{i=1}^{n} |\mathfrak{C}_i| \Big/ [L:k]. \tag{6}$$

By (2) and Lemma 1.8,

$$\mu(\{\sigma \in \mathcal{G}(k_s/k) \mid k_s(\sigma)^{1/p^\infty} \models E\}) = \sum_{i=1}^{n} |\mathfrak{C}_i| \Big/ [L:k]. \tag{7}$$

(6) and (7) imply (5).

Suppose now that $A(E)$ is an infinite set. Then Lemma 3.14(1) implies that $n \geqq 1$. Since $|\mathfrak{C}_i| \geqq 1$ are positive integers we conclude from (6) that $\delta(A(E))$ is a positive rational integer. Q.E.D.

REMARKS. (a) The only heavy theorem we have used to prove Lemma 3.15 was Čebotarev density theorem. In particular we have not used Weil's theorem and the continuum hypothesis. We shall need them in the reduction of the general translation theorem to that for one-variable statements.

(b) Ax has proved in [1, p. 161] "half" of the translation theorem. He proves (1) (though not explicitly) and deduces from it that $\delta(A(E))$ exists and equals a rational number. Moreover he deduces that if $A(E)$ is infinite then $\delta(A(E)) > 0$ (all this has been done only in the case when $k = Q$).

3.7. An isomorphism of boolean algebras.

DEFINITION. Let k be a global field and let $\Sigma_1, \Sigma_2 \subseteq \mathcal{G}(k_s/k)$ be two measurable subsets. Σ_1 is said to be "almost equal" to Σ_2 if Σ_1 differs from Σ_2 only by a set of measure 0. In this case we write $\Sigma_1 \approx \Sigma_2$.

Let R be the ring of integers of k and let p be the characteristic of k. Let E be an R-elementary statement. Denote

$$\Sigma(E) = \{\sigma \in \mathcal{G}(k_s/k) | k_s(\sigma)^{1/p^\infty} \models E\}.$$

By structure induction it is easy to prove the following lemma:

LEMMA 3.16. *Let k be a global field of characteristic p and with a ring of integers R. If Φ is a boolean polynomial then*

$$\Sigma(\Phi(E_1, \ldots, E_m)) = \Phi(\Sigma(E_1), \ldots, \Sigma(E_m)).$$

Lemma 3.16 tells us that the family of all subsets of $\mathcal{G}(k_s/k)$ of the form $\Sigma(E)$ is a boolean algebra which we denote by $\Sigma(k)$. The relation "almost an equality" which was defined above is clearly a congruence relation. We denote by $\bar{\Sigma}(k)$ the appropriate factor boolean algebra.

Similarly the relation "almost an equality" which was defined in §3.6 is a congruence relation and we denote by $\bar{\mathcal{A}}(k)$ the appropriate factor boolean algebra.

THEOREM 3.17 (THE TRANSLATION THEOREM). *Let k be a global field of characteristic p, with a ring of integers R. The mapping θ: $A(E) \mapsto \Sigma(E)$ where E ranges over the R-elementary statements induces an isomorphism of $\bar{\mathcal{A}}(k)$ onto $\bar{\Sigma}(k)$, i.e.*

$$A(E_1) \approx A(E_2) \Leftrightarrow \Sigma(E_1) \approx \Sigma(E_2) \tag{1}$$

and θ preserves the boolean operations. Moreover

$$\delta(A(E)) = \mu(\Sigma(E)) \tag{2}$$

and if $A(E)$ is an infinite set then both sides of (2) *are positive rational numbers.*

Proof. From Lemma 3.10 it follows that every $A \in \mathcal{A}(k)$ has the form $A = A(E_\Phi(f_1, \ldots, f_m))$ where $f_1, \ldots, f_m \in R[X]$ are separable polynomials and Φ is a boolean polynomial. Hence θ is defined on $\mathcal{A}(k)$. Moreover if E is an R-elementary statement then, according to Theorem 3.12, $A(E) \in \mathcal{A}(k)$. It follows that the domain of definition of θ is exactly $\mathcal{A}(k)$.

To show that θ induces the desired isomorphism we have to prove that if E_1 and E_2 are two R-elementary statements for which $A(E_1) \approx A(E_2)$ then $\Sigma(E_1) \approx \Sigma(E_2)$. In fact, let $\sigma \in \Sigma(E_1)$ be an element for which there exists a nonprincipal ultra-filter $\mathcal{D}$ of $P(k)$ such that $\tilde{k} \cap \prod F_\mathfrak{p}/\mathcal{D} \cong_k k_s(\sigma)^{1/p^\infty}$ and $\prod F_\mathfrak{p}/\mathcal{D} \equiv_R k_s(\sigma)^{1/p^\infty}$. (According to Theorem 3.9 almost every $\sigma \in \Sigma(E_1)$ has this property.) From the assumption it follows that $k_s(\sigma)^{1/p^\infty} \models E_1$. From the R-elementary equivalence we get that $\prod F_\mathfrak{p}/\mathcal{D} \models E_1$. Hence $A(E_1) \in \mathcal{D}$. Since $A(E_2)$ differs from $A(E_1)$ only by a finite number of elements and $\mathcal{D}$ is a nonprincipal ultra-filter, we have $A(E_2) \in \mathcal{D}$. $\Rightarrow \prod F_\mathfrak{p}/\mathcal{D} \models E_2$. $\Rightarrow k_s(\sigma)^{1/p^\infty} \models E_2$. $\Rightarrow \sigma \in \Sigma(E_2)$. Symmetrically we show that almost all $\sigma \in \Sigma(E_2)$ belong also to $\Sigma(E_1)$. Hence $\Sigma(E_1) \approx \Sigma(E_2)$.

Let now E be an R-elementary statement. Then, as we noted before there exists a one-variable statement E' such that $A(E)=A(E')$. Hence, from what we have just proved $\Sigma(E)\approx\Sigma(E')$. Hence

$$\delta(A(E)) = \delta(A(E')), \qquad \mu(\Sigma(E)) = \mu(\Sigma(E')).$$

But according to the translation theorem for one-variable statements, $\delta(A(E'))=\mu(\Sigma(E'))$. Hence $\delta(A(E))=\mu(\Sigma(E))$.

If $A(E)$ is an infinite set then $A(E')$ is also an infinite set hence $\delta(A(E))=\delta(A(E'))$ is a positive rational number.

The fact that θ preserves the boolean operations follows from Lemmas 3.10 and 3.16.

At last we prove that θ is almost injective. We prove the second direction of the implication (1).

$$\begin{aligned}
&\Sigma(E_1)\approx\Sigma(E_2)\Rightarrow\Sigma(E_1\leftrightarrow E_2)\approx\mathcal{G}(k_s/k).\\
&\qquad\Rightarrow\Sigma(\sim[E_1\leftrightarrow E_2])\approx\Phi. \qquad\Rightarrow\mu(\Sigma(\sim[E_1\leftrightarrow E_2]))=0.\\
&\qquad\Rightarrow\delta(A(\sim[E_1\leftrightarrow E_2]))=0. \qquad\Rightarrow A(\sim[E_1\leftrightarrow E_2])\approx\Phi.\\
&\qquad\Rightarrow A(E_1\leftrightarrow E_2)\approx P(k). \qquad\Rightarrow A(E_1)\approx A(E_2). \qquad \text{Q.E.D.}
\end{aligned}$$

REMARK. The translation theorem assures us that $\delta(A(E))$ is a rational number for every R-elementary statement E. The opposite assertion is false, i.e. there exist sets of prime ideals of rational Dirichlet density which cannot be represented in the form $A(E)$. Examples of such sets are infinite sets of prime ideals of zero density. In particular it follows that if there are infinitely many twin primes then they cannot be characterized by an elementary statement since their Dirichlet density is known to be zero. It is therefore interesting to ask if certain known sets of primes are characterizable by an elementary statement. In particular it is interesting to know when a set of all primes in a given reduced arithmetical progression can be characterized by an elementary statement. We discuss this problem in the next section.

3.8. **Čebotarev sets and Ax sets.** Let k be a global field. Any set which belongs to the boolean algebra generated in $P(k)$ by all the sets of the form

$$\{\mathfrak{p}\in P(k)\mid((L/k)/\mathfrak{p})=\mathfrak{C}\},$$

where L/k is finite Galois extension and $\mathfrak{C}$ is a conjugation class in $\mathcal{G}(L/k)$, will be called a Čebotarev set. An Ax set is a set which belongs to the Ax boolean algebra, i.e. a set which can be elementarily characterized. From Theorem 3.12 and Lemma 3.14 it is clear that every Ax set is also a Čebotarev set. The converse is not always true. In order to discuss the connections between these two kinds of sets of prime ideals we introduce the following definition from group theory.

DEFINITION. Let G be a finite group, let $\sigma\in G$ and let f be the order of σ in G. The subset of G consisting of all the elements which are conjugate to any of the

powers σ^i, for which i and f are relatively prime, will be called the Abteilung of G generated by σ.

It is clear that the Abteilungs generated by two elements of G are either coinciding or disjoint. Every Abteilung is the union of some conjugacy classes and it is generated by every one of its elements.

LEMMA 3.18. *Let k be a global field, L/k a finite Galois extension and $\mathfrak{D}$ an Abteilung in $\mathfrak{G}(L/k)$. Then the set $\{\mathfrak{p} \in P(k) \mid ((L/k)/\mathfrak{p}) \subseteq \mathfrak{D}\}$ is an Ax set.*

Proof. Let $\tau \in \mathfrak{D}$. Denote by $\tau_1, \tau_2, \ldots, \tau_m$ all the elements of $\mathfrak{G}(L/k)$ which are conjugate to τ. Let $L_1, L_2, \ldots, L_m$ be their fixed fields in L respectively and put $\mathfrak{L} = \{L_1, L_2, \ldots, L_m\}$. Then $\mathfrak{L}$ is an L/k normal set of fields. Noting that an element $\sigma \in \mathfrak{G}(L/k)$ generates the same cyclic group as τ_j if and only if it is a power of τ_j whose exponent is prime to the order of τ_j, we conclude that

$$\{\mathfrak{p} \in P(k) \mid ((L/k)/\mathfrak{p}) \subseteq \mathfrak{D}\} \approx B_{L/k}(\mathfrak{L}).$$

Our lemma follows now from the remark in §3.5.

THEOREM 3.19. *Let k be a global field, L/k a finite Galois extension and $\mathfrak{C}$ a conjugacy class in $\mathfrak{G}(L/k)$. A necessary and sufficient condition that*

$$\{\mathfrak{p} \in P(k) \mid ((L/k)/\mathfrak{p}) = \mathfrak{C}\}$$

is an Ax set is that $\mathfrak{C}$ coincides with the Abteilung it generates.

Proof. The sufficiency is a special case of Lemma 3.18. The necessity follows from the following qualitative theorem.

THEOREM 3.20. *Let k be a global field with a ring of integers R. Let L/k be a finite Galois extension and $\mathfrak{C}$ a conjugacy class in $\mathfrak{G}(L/k)$ which does not coincide with the Abteilung it generates. Then, for every R-elementary statement E, the Dirichlet density of the symmetric difference between $A(E)$ and $\{\mathfrak{p} \in P(k) \mid ((L/k)/\mathfrak{p}) = \mathfrak{C}\}$ is at least $1/[L:k]$.*

Proof. According to the remark in §3.5 there exists a finite Galois extension M and an M/k normal set $\mathfrak{M}$ of fields such that $A(E) \approx B_{M/k}(\mathfrak{M})$. Without loss of generality we can assume that M includes L.

Let $\tau \in \mathfrak{C}$ and let f be the order of τ in $\mathfrak{G}(L/k)$. According to the assumption there exists a positive integer i, relatively prime to f, such that $\tau^i \notin \mathfrak{C}$. Let r be a positive integer, relatively prime to $[M:k]$, such that $r \equiv i \pmod{f}$. Choose an extension ρ of τ to M. Let $m = [M:L]$ and denote by $\sigma_1, \ldots, \sigma_m$ the elements of $\mathfrak{G}(M/L)$. Then the set $\{\sigma_1\rho, \sigma_2\rho, \ldots, \sigma_m\rho; (\sigma_1\rho)^r, (\sigma_2\rho)^r, \ldots, (\sigma_m\rho)^r\}$ consists of $2m$ different elements of $\mathfrak{G}(M/k)$, since $\tau^i \notin \mathfrak{C}$. Let

$$\mathfrak{S} = \{\sigma \in \mathfrak{G}(M/k) \mid \text{The fixed field of } \sigma \text{ in } M \text{ belongs to } \mathfrak{M}\},$$
$$\mathfrak{F} = \{\sigma \in \mathfrak{G}(M/k) \mid \sigma|L \in \mathfrak{C}\}.$$

It is not difficult to see that for every $1 \leqq j \leqq m$ either $\sigma_j\rho$ or $(\sigma_j\rho)^r$ belongs to $(\mathscr{E}-\mathscr{F})\cup(\mathscr{F}-\mathscr{E})$. Hence $|(\mathscr{E}-\mathscr{F}) \cup (\mathscr{F}-\mathscr{E})| \geqq m$. On the other hand $(\mathscr{E}-\mathscr{F}) \cup (\mathscr{F}-\mathscr{E})$ is the union of some conjugacy classes in $\mathscr{G}(M/k)$, hence, if we let $C=\{\mathfrak{p} \in P(k) \mid ((L/k)/\mathfrak{p})=\mathfrak{C}\}$ we have according to the Čebotarev density theorem

$$\delta((A(E)-C) \cup (C-A(E))) = \delta(\{\mathfrak{p} \in P(k) | ((M/k)/\mathfrak{p}) \subseteq (\mathscr{E}-\mathscr{F}) \cup (\mathscr{F}-\mathscr{E})\})$$
$$\geqq m/[M:k] = 1/[L:k]. \qquad \text{Q.E.D.}$$

REMARK. This theorem expresses the fact that in the above situation C cannot even be approximated by sets of the form $A(E)$.

The following theorem is another generalization of the necessity part of Theorem 3.19.

THEOREM 3.21. *Let k be a global field with a ring of integers R. Let L/k be a finite Galois extension and let $\mathfrak{C}, \mathfrak{C}'$ be two conjugacy classes which are contained in the same Abteilung of $\mathscr{G}(L/k)$. Let*

$$C = \{\mathfrak{p} \in P(k) \mid ((L/k)/\mathfrak{p}) = \mathfrak{C}\}, \qquad C' = \{\mathfrak{p} \in P(k) \mid ((L/k)/\mathfrak{p}) = \mathfrak{C}'\}.$$

Then for every R-elementary statement E, $\delta(A(E) \cap C)=\delta(A(E) \cap C')$. Moreover, $\delta(A(E) \cap C)$ is a positive rational integer if and only if $A(E) \cap C$ is an infinite set. In particular, $A(E) \cap C$ is an infinite set if and only if $A(E) \cap C'$ is an infinite set.

Proof. As in the proof of Theorem 3.20 we have $A(E) \approx B_{M/k}(\mathscr{M})$ where M is finite Galois extension containing L. Put $B=B_{M/k}(\mathscr{M})$. It will be sufficient to prove that if $B \cap C$ is an infinite set then $\delta(B \cap C)$ is a positive rational number and $\delta(B \cap C)=\delta(B \cap C')$. Also, it will be sufficient to prove the assertion in the case where $\mathscr{M}$ is a minimal M/k normal set of fields, i.e. in the case where any two fields of $\mathscr{M}$ are conjugates.

Choose a prime ideal $\mathfrak{p}_0 \in B \cap C$ which is not ramified in M. Let $\mathfrak{P}_0 \in P(L)$ be an extension of $\mathfrak{p}_0$ to L and let $\overline{\mathfrak{P}}_0 \in P(M)$ an extension of $\mathfrak{P}_0$ to M. Let $M'=M(k, \overline{\mathfrak{P}}_0)$, $\rho=[(M/k)/\overline{\mathfrak{P}}_0]$ and $\tau=[(L/k)/\mathfrak{P}_0]$. Then $M' \in \mathscr{M}$, ρ generates the cyclic group $\mathscr{G}(M/M')$, $\rho|L=\tau$ and $\tau \in \mathfrak{C}$. Denote by m, f the orders of ρ, τ in $\mathscr{G}(M/k)$, $\mathscr{G}(L/k)$ respectively. Denote by $\overline{\mathscr{B}}$ the Abteilung generated by ρ in $\mathscr{G}(M/k)$. Let $\overline{\mathfrak{C}}$ be the set of all the elements of $\mathscr{G}(M/k)$ whose restriction to L belongs to $\mathfrak{C}$. Then $\overline{\mathscr{B}} \cap \overline{\mathfrak{C}}$ is a nonvoid union of conjugacy classes of $\mathscr{G}(M/k)$ and, hence, according to Čebotarev density theorem

$$\delta(\{\mathfrak{p} \in P(k) \mid ((M/k)/\mathfrak{p}) \subseteq \overline{\mathscr{B}} \cap \overline{\mathfrak{C}}\}) = |\overline{\mathscr{B}} \cap \overline{\mathfrak{C}}|/[M:k]. \tag{1}$$

This is, of course, a positive rational number. It is not difficult to see that

$$\{\mathfrak{p} \in P(k) \mid ((M/k)/\mathfrak{p}) \subseteq \overline{\mathscr{B}} \cap \overline{\mathfrak{C}}\} \approx B \cap C.$$

Hence $\delta(B \cap C)=|\overline{\mathscr{B}} \cap \overline{\mathfrak{C}}|/[M:k]$. Similarly we denote by $\overline{\mathfrak{C}}'$ the set of elements of $\mathscr{G}(M/k)$ whose restriction to L belongs to $\mathfrak{C}'$. According to the assumption there exists a positive integer b which is relatively prime to f such that $\tau^b \in \mathfrak{C}'$. We can

choose b such that it is also relatively prime to m. Let $\tau' = \tau^b$ and $\rho' = \rho^b$. Th. $\rho' \in \bar{\mathfrak{B}} \cap \bar{\mathfrak{C}}'$ (hence ρ' generates $\bar{\mathfrak{B}}$) and the orders of ρ', τ' in $\mathcal{G}(M/k)$, $\mathcal{G}(L/k)$ are m, f respectively. The mapping $\sigma \mapsto \sigma^b$ induces a one-to-one correspondenc between $\bar{\mathfrak{B}} \cap \bar{\mathfrak{C}}$ and $\bar{\mathfrak{B}} \cap \bar{\mathfrak{C}}'$, hence $|\bar{\mathfrak{B}} \cap \bar{\mathfrak{C}}| = |\bar{\mathfrak{B}} \cap \bar{\mathfrak{C}}'|$. As above we can deduce that $\delta(B \cap C') = |\bar{\mathfrak{B}} \cap \bar{\mathfrak{C}}'|/[M:k]$. Hence $\delta(B \cap C) = \delta(B \cap C')$. Q.E.D.

As a consequence of the last part of Theorem 3.21 we prove the following theorem:

THEOREM 3.22. *Let k, R, C and C' be as in Theorem* 3.21. *Then for every non-principal ultra-filter $\mathcal{D}$ of $P(k)$ which contains C there exists a nonprincipal ultra-filter $\mathcal{D}'$ of $P(k)$ which contains C' such that*

$$\prod F_\mathfrak{p}/\mathcal{D} \equiv_R \prod F_\mathfrak{p}/\mathcal{D}'.$$

Proof. Denote by $\mathcal{D}_0$ the family of all sets of the form $A(E)$ belonging to $\mathcal{D}$. From Theorem 3.21 it follows that the family $\mathcal{D}_0 \cup \{C'\}$ has the finite intersection property. Hence there exists a nonprincipal ultra-filter $\mathcal{D}'$ containing $\mathcal{D}_0 \cup \{C'\}$. $\mathcal{D}'$ has the desired property.

The most interesting case arises when $k = Q$ and $L = Q(\xi)$, where ξ is a primitive mth root of 1. In this case, as is well known, the Čebotarev sets are reduced to Dirichlet sets modulo m, i.e. to sets of all primes in a given reduced arithmetical progression whose constant difference is m. Moreover, the Galois group $\mathcal{G}(Q(\xi)/Q)$ is naturally isomorphic to Z_m^* (the multiplicative group of congruence classes modulo m whose elements are relatively prime to m). In this case, an Abteilung generated by an element $\bar{a} \in Z_m^*$ is the set of all its powers whose exponents are relatively prime to its order. In particular such an Abteilung consists of one conjugacy class if and only if the order of $\bar{a}$ is not greater than 2. We summarize all the results in this section in this special case in the following theorem:

THEOREM 3.23. *Let m be a positive integer. Let a be an integer relatively prime to m and let f be its order modulo m.*

(i) *Let $a_1, \ldots, a_n$ be all the powers of a modulo m whose exponents are relatively prime to the order of a modulo m. Then the set*

$$\{p \in P(Q) \mid \exists i : p \equiv a_i \pmod{m}\}$$

is an Ax set.

(ii)[3] *The set $A = \{p \in P(Q) \mid p \equiv a \pmod{m}\}$ is an Ax set if and only if the order of a modulo m is not greater than* 2.

(iii) *Suppose that the order of a modulo m is > 2. Then for every elementary statement E the Dirichlet density of the symmetric difference of $A(E)$ and A is at least $1/\varphi(m)$.*

(iv) *Suppose that $b \equiv a^i \pmod{m}$ and $(i, f) = 1$. Then for every elementary statement E, $\delta(A(E) \cap A) = \delta(A(E) \cap B)$ where $B = \{p \in P(Q) \mid p \equiv b \pmod{m}\}$.*

---

[3] This was suggested by the referee.

(v) *Let b be as in* (iv). *Then for every nonprincipal ultra-filter $\mathscr{A}$ of $P(Q)$ which contains A there exists a nonprincipal ultra-filter $\mathscr{B}$ which contains B such that* $\prod F_p/\mathscr{A} \equiv \prod F_p/\mathscr{B}$.

References

1. J. Ax, *Solving diophantine problems modulo every prime*, Ann. of Math. (2) **85** (1967), 161–183. MR **35** #126.

2. ———, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271. MR **37** #5187.

3. T. Frayne, A. C. Morel and D. S. Scott, *Reduced direct products*, Fund. Math. **51** (1962/63), 195–228. MR **26** #28.

4. W. Kuyk, *Generic approach to the Galois embedding and extension problem*, J. Algebra **9** (1968), 393–407. MR **38** #2128.

5. ———, *Extension de corps Hilbertiens*, J. Algebra **14** (1970), 112–124. MR **41** #1698.

6. S. Lang, *Diophantine geometry*, Interscience Tracts in Pure and Appl. Math., no. 11, Interscience, New York, 1962. MR **26** #119.

7. ———, *Algebra*, Addison-Wesley, Reading, Mass., 1965. MR **33** #5416.

8. A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Indust., no. 1041, Hermann, Paris, 1948. MR **10**, 262.

9. ———, *Foundations of algebraic geometry*, Amer. Math. Soc. Colloq. Publ., vol. 29, Amer. Math. Soc., Providence, R. I., 1946. MR **9**, 303.

Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem, Israel

Current address: Mathematisches Institut, Universität Heidelberg, West Germany