RATIONAL POINTS ON ALGEBRAIC VARIETIES OVER LARGE NUMBER FIELDS[1]

BY MOSHE JARDEN

Communicated by Arthur Mattuck, January 13, 1969

Denote by Σ the class of all fields K which have the following property: For any nonvoid absolutely irreducible variety V defined by equations 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 [1] that if $\mathfrak{F} = \prod F_p/D$ is a nonprincipal ultra-product of the F_p then $\mathfrak{F} \in \Sigma$ (see [2, 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 $\mathfrak{F} \cap \tilde{Q} \in \Sigma$. Ax gave a counterexample in [3, §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, $\mathfrak{F} \cap \tilde{Q}$ does belong to Σ. To be more precise denote by $Q(\sigma)$ the fixed field in $\tilde{Q}$ of an automorphism $\sigma \in \mathcal{G}(\tilde{Q}/Q)$ ($\mathcal{G}(\tilde{Q}/Q)$ is the Galois group of $\tilde{Q}$ over Q). Ax showed ([2, Theorem 5]) that for every nonprincipal ultra-product $\mathfrak{F}$ of the F_p there exists $\sigma \in \mathcal{G}(\tilde{Q}/Q)$ such that $\mathfrak{F} \cap \tilde{Q} = Q(\sigma)$, and conversely, for each $\sigma \in \mathcal{G}(\tilde{Q}/Q)$ there exists a nonprincipal ultra-product $\mathfrak{F}$ of the F_p such that $\mathfrak{F} \cap \tilde{Q} \cong Q(\sigma)$. What we shall in fact prove is that for almost all $\sigma \in \mathcal{G}(\tilde{Q}/Q)$ (in the sense of Haar measure), $Q(\sigma) \in \Sigma$. More generally, let k be a field of characteristic zero. Denote by μ_k the normalized Haar measure defined on $\mathcal{G}(\tilde{k}/k)$ with respect to the Krull topology. For any positive integer s denote by μ_k^s the product measure defined on $\mathcal{G}(\tilde{k}/k)^s$. Then the following theorem is true.

THEOREM. *If k is a denumerable Hilbertian field of characteristic zero, then for almost all $(\sigma_1, \cdots, \sigma_s) \in \mathcal{G}(\tilde{k}/k)^s$ the fixed field of $\{\sigma_1, \cdots, \sigma_s\}$, $k(\sigma_1, \cdots, \sigma_s)$, belongs to Σ.*

Since it is well known that Q is a Hilbertian field (see e.g. [4]) we have in particular the following corollary.

[1] This note is to be part of the author's Ph.D. thesis, prepared at the Hebrew University under the supervision of Professor H. Furstenberg to whom the author wishes to express his thanks and appreciation.

COROLLARY. *$Q(\sigma_1, \cdots, \sigma_e) \in \Sigma$ for almost all $(\sigma_1, \cdots, \sigma_e) \in \mathcal{G}(\tilde{Q}/Q)^e$.*

In particular this corollary answers 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 [3, p. 269, Problem 2]). In addition, the corollary implies that there exists a subfield K of $\tilde{Q}$ such that $K \in \Sigma$ and $\mathcal{G}(\tilde{Q}/K)$ is not abelian. To see this, note that there exists a set B of pairs $(\sigma_1, \sigma_2) \in \mathcal{G}(\tilde{Q}/Q)^2$ 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, nonabelian extension N/Q and picks $\bar{\sigma}_1, \bar{\sigma}_2 \in \mathcal{G}(N/Q)$ such that $\bar{\sigma}_1\bar{\sigma}_2 \neq \bar{\sigma}_2\bar{\sigma}_1$, then the set of pairs $(\sigma_1, \sigma_2) \in \mathcal{G}(\tilde{Q}/Q)$ such that $\sigma_1 | N = \bar{\sigma}_1$, $\bar{\sigma}_2 | N = \bar{\sigma}_2$ 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 our K may be chosen as one of the $Q(\sigma_1, \sigma_2) \in \Sigma$ 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 is not pseudo finite and belong to Σ?" (If K is pseudo finite then $\mathcal{G}(\tilde{Q}/K)$ is abelian.)

The theorem follows from the lemmas given below. All fields are assumed to be of characteristic zeio.

LEMMA 1. *If K is a finite extension of a field k then*

$$\mu_k(\mathcal{G}(\tilde{k}/K)) = \frac{1}{[K:k]} \cdot$$

This corresponds to the well-known fact that for finite algebraic extension K/k, the index of the subgroup $\mathcal{G}(\tilde{k}/K)$ in the group $\mathcal{G}(\tilde{k}/k)$ is $[K:k]$.

DEFINITION. An infinite sequence $\{K_i\}_{i=1}^{\infty}$ of extensions of a field K is said to be "linearly disjoint over K" if every finite subsequence is linearly disjoint over K, or, equivalently, if for every $i \geq 1$ the field K_{i+1} is linearly disjoint from $K_1K_2 \cdots K_i$ over K.

If the sequence $\{K_i/K\}_{i=1}^{\infty}$ is linearly disjoint over K then the subsets $\{\mathcal{G}(\tilde{K}/K_i)\}_{i=1}^{\infty}$ of $\mathcal{G}(\tilde{K}/K)$ are independent in the probabilistic sense. From this fact it is not difficult to deduce the following lemma.

LEMMA 2. *Let K be a finite extension of a field k. Let $\{K_i\}_{i=1}^{\infty}$ be a linearly disjoint sequence of finite extensions of K for which*

$$\prod_{i=1}^{\infty}\left(1 - \frac{1}{[K_i:K]^e}\right) = 0$$

where s is a positive integer. Then

$$\mu_k^s\left(\bigcup_{i=1}^{\infty} \mathcal{G}(\tilde{k}/K_i)^s\right) = \frac{1}{[K:k]^s}\cdot$$

The main step in the proof is the following lemma.

LEMMA 3. *Let k be a Hilbertian field and let K/k be a finite extension. Let $F \in K[X_1, \cdots, X_n] (n \geqq 2)$ be an absolutely irreducible polynomial and let $m \geqq 1$ be the degree of X_n in F. Then for every algebraic set V, defined in the affine space S^n over K, which does not contain $V(F)$ (the set of zeros of F), there exists a linearly disjoint sequence of algebraic extensions $\{K_i/K\}_{i=1}^{\infty}$ of degree m, such that for every $i \geqq 1$ there exist $a_{i,1}, \cdots, a_{i,n} \in K_i$ such that $(a_{i,1}, \cdots, a_{i,n}) \notin V$ and $F(a_{i,1}, \cdots, a_{i,n}) = 0$.*

The crucial point in the proof of this lemma is the following: For any finite extension L of K, F is irreducible in $L[X_1, \cdots, X_n]$ and hence we can find $a_1, \cdots, a_{n-1} \in K$ such that $F(a_1, \cdots, a_{n-1}, X_n)$ is irreducible in $L[X_n]$ of degree m. If $a_n \in \tilde{k}$ is a root of $F(a_1, \cdots, a_{n-1}, X_n)$ then the field $K(a_n)$ will be linearly disjoint from L over K. So we can construct our desired sequence by induction.

Let V_1, V_2 be two algebraic sets defined over a finite extension K of k in the same space. Denote by $\Sigma_K^s(V_1, -V_2)$ the set of all $(\sigma_1, \cdots, \sigma_s) \in \mathcal{G}(\tilde{k}/K)^s$ for which there exists a point rational over $k(\sigma_1, \cdots, \sigma_s)$ which belongs to V_1 but not to V_2.

Lemmas 2 and 3 yield the following result.

LEMMA 4. *Let $F[X_1, \cdots, X_n]$ $(n \geqq 1)$ be an absolutely irreducible polynomial defined over a finite extension K of a Hilbertian field k. Then for every algebraic set V defined over K in S^n which does not contain $V(F)$*

$$\mu_k^s(\Sigma_K^s(V(F), - V)) = \frac{1}{[K:k]^s}\cdot$$

Lemma 4 refers to hypersurfaces $V(F)$ in S^n. The same result is valid for arbitrary absolutely irreducible varieties.

LEMMA 5. *Let V be an absolutely irreducible variety defined over a finite extension K of a Hilbertian field k in S^n. Then for every algebraic set V' defined over K in S^n which does not contain V*

$$\mu_k^s(\Sigma_K^s(V, - V')) = \frac{1}{[K:k]^s}\cdot$$

Lemma 5 follows from Lemma 4 because by a suitable rational transformation $V(F) - V''$ is taken into $V - V'$ ($F \in K[X_1, \cdots, X_n]$ is a suitable absolutely irreducible polynomial and V'' is an algebraic set defined in S^n over K which does not contain $V(F)$). We thus have

$$\Sigma_K^s(V(F), - V'') \subseteq \Sigma_K^s(V, - V').$$

Denote by Σ_k^s the set of all $(\sigma_1, \cdots, \sigma_s) \in \mathcal{G}(\tilde{k}/k)^s$ such that $k(\sigma_1, \cdots, \sigma_s) \in \Sigma$. If k is denumerable then the set of all algebraic sets defined over k is denumerable. By observing that if two algebraic sets V, V' are defined over $k(\sigma_1, \cdots, \sigma_s)$ then there exists a finite extension K/k such that V, V' are defined over K and by Lemma 5, we conclude that if k is a denumerable Hilbertian field then $\mu_k^s(\Sigma_k^s) = 1$. This is exactly the content of the theorem.

It may be noted that the theorem can be generalized to fields of arbitrary characteristic by considering the separable closure of a field instead of its algebraic closure.

References

1. A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, Paris, 1948.

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

3. ———, *The elementary theory of finite fields*, Ann. of Math. (2) (1968), 239–271.

4. S. Lang, *Diophantine geometry*, Interscience Tracts in Pure and Appl. Math., no. 11, Interscience, New York, 1962.

The Hebrew University, Jersualem