An injective rational map of an abstract algebraic variety into itself

By *Moshe Jarden* in Jerusalem

Introduction

We begin by introducing some notations. For every prime p, F_p is the field with p elements and $\bar{F}_p$ is its algebraic closure.

Let U be a closed subset of an abstract algebraic variety; then by $\dim U$ we mean the maximal dimension of the components of U. If $r = \dim U$ we write $n_r(U)$ for the number of components of U of dimension r. If $s > \dim U$ we put $n_s(U) = 0$.

The aim of this paper is to prove the following results:

Theorem 1. *Let V be an abstract algebraic variety: let U, W be two closed subsets of V and let $\chi : V \to V$ be a rational map defined at every point of $V - U$ and which induces a bijective map of $V - U$ onto $V - W$. Then* $\dim U = \dim W$, *and if we put* $r = \dim U$ *then* $n_r(U) = n_r(W)$.

Corollary 1. 1. *Let V be an abstract algebraic variety; let U be a closed subset of V and let $\chi: V \to V$ be a rational map defined at every point of $V - U$ and which induces a bijective map of $V - U$ onto V. Then U is empty, i. e. χ is a morphism.*

Let $\chi : V \to V'$ be a rational map; let A and A' be subsets of V and V' respectively. Then by $\chi(A)$ and $\chi^{-1}(A')$ we understand in this paper the set theoretic image and the set theoretic inverse image under χ of A and A' respectively.

Theorem 2. *Let V be an abstract algebraic variety defined over a field k; let U be a k-closed subset of V and let $\chi : V \to V$ be a k-rational map defined at every point of $V - U$ and which induces an injective map of $V - U$ into V. Let* $r = \dim U$. *Then for every closed subset W of V such that $V - W \subseteq \chi(V - U)$ we have either* $\dim W > r$ *or* $\dim W = r$ *and $n_r(W) \geqq n_r(U)$. Furthermore, there exists a closed subset Z of V such that:*

(a) $V - Z \subseteq \chi(V - U)$

(b) $\dim Z = r$

(c) $n_r(Z) = n_r(U)$

(d) *For every* $Q \in \chi(V - U) \cap Z$ *we have* $\dim_k Q < r$.

The components of Z having dimension r are determined uniquely by (a), (b) and (c) disregarding possible permutations.

Furthermore, the intersection of all the Z's for which (a), (b) and (c) hold is itself such a set and it is k-closed.

Corollary 2. 1. *In the notation of Theorem 1, if V and χ are defined over a field k and U is k-closed, then W is also k-closed.*

Corollary 2. 2. *Let V be an abstract algebraic variety; let U be a finite subset of V and let $\chi: V \to V$ be a rational map defined at every point of $V - U$ and which induces an injective map of $V - U$ into V. Then the set theoretic image of $V - U$ by χ has the form $V - W$ where W is a finite set of V having the same number of elements as U.*

Corollary 2. 3. *Every injective morphism of an abstract algebraic variety into itself is surjective.*

In Section 1 we show that Theorem 1 is logically an elementary first-order predicate calculus sentence. This enables us in Section 2 to reduce the Theorem to one over $\bar{F}_p$. Then we can use the Weil-Lang Theorem about the number of rational points of varieties over finite fields to obtain the Theorem. In Section 3 we obtain Theorem 2 from Theorem 1. In the Corollaries we have formulated some interesting special cases of the theorems. We note that Corollary 2. 3 is well-known; it was originally proved by Ax [1]. Indeed, our proof of Theorem 1 makes use of Ax's method namely that of reducing a problem to one over finite fields. Thus, Theorem 2 can be considered as a generalization of Ax's result.

The author wishes to acknowledge his indebtedness to Professor H. Furstenberg for several useful conversations, and especially for suggesting Theorem 1; he also wishes to thank Professor O. Zariski for encouraging him to publish this paper.

§ 1. Elementary statements about an algebraically closed field

Let K be an algebraically closed field. Denote by $\mathscr{L}$ the language of the first-order predicate calculus of the theory of fields. Let $\mathscr{L}(K)$ be $\mathscr{L}$ with the addition of constants for all the elements of K. An elementary statement (about K) is a mathematical statement which is equivalent to a sentence in $\mathscr{L}$ (in $\mathscr{L}(K)$). In this section we shall be concerned with a fixed algebraically closed field K, so we shall frequently omit the reference to it.

Let Ω be a universal extension of K. It is well known that Ω is an elementary extension of K (see e. g. Robinson [7], p. 100). This means that a sentence in the language $\mathscr{L}(K)$ holds in K if and only if it holds in Ω. We can, therefore, interpret the sentences we write below as speaking either about K or about Ω and obtain the same truth value in both cases.

Our aim in this section is to show that some basic notions and statements of algebraic geometry are elementary ones. We shall constantly use the Weil-Lang language of algebraic geometry.

Algebraic Sets. Let $V = V(f_1, \ldots, f_t)$ be an algebraic set defined over K in S^n. Let $X_1, \ldots, X_n$ be variables for the coordinates of S^n, and let $(X) = (X_1, \ldots, X_n)$. Then the statement "$(X) \in V$" is an elementary formula. It is equivalent to the formula $\bigwedge_{\tau=1}^{t} f_\tau(X) = 0$.

The Ideal belonging to an Algebraic Set. Let V be as before, let $\mathfrak{a}$ be the ideal generated by $f_1, \ldots, f_t$ and let $\sqrt{\mathfrak{a}}$ be its radical. Then $\sqrt{\mathfrak{a}}$ is the ideal of all polynomials $f \in K[X]$ which vanish on V. Thus "$\sqrt{\mathfrak{a}}$" is an elementary notion. We also want to characterize in an elementary way a set of generators for $\sqrt{\mathfrak{a}}$. In order to do this we quote two results which appear in Eklof [2], §§ 1 and 2.

Lemma 1. *For any q, n there exists a positive number $m_1(q, n)$ such that if F is any field and $\mathfrak{a}$ is any ideal in $F[X_1, \ldots, X_n]$ generated by polynomials of degree $\leqq q$ then $\sqrt{\mathfrak{a}}$ is generated by polynomials of degree $\leqq m_1(q, n)$.*

Lemma 2. *For any t, q, n there exists a positive number $m_2(t, q, n)$ such that if F is any field and $g, f_1, \ldots, f_t$ are polynomials with $\deg f_\tau \leqq q$ for $\tau = 1, \ldots, t$ and $g \in \langle f_1, \ldots, f_t \rangle$, then there exist polynomials $h_1, \ldots, h_t \in F[X_1, \ldots, X_n]$ such that $\deg h_\tau \leqq \deg g + m_2(t, q, n)$ and $g = \sum_{\tau=1}^{t} h_\tau f_\tau$.*

Let $q = \max_{1 \leqq \tau \leqq t} \{\deg f_\tau(X)\}$ and let $F_1, \ldots, F_{\bar{t}} \in K(X]$. Then, Lemmata 1 and 2 show that the following elementary statements characterize $\{F_1, \ldots, F_{\bar{t}}\}$ as a set of generators for $\sqrt{\mathfrak{a}}$:

(a) $F_\tau(X) \in \sqrt{\mathfrak{a}}$ for $\tau = 1, \ldots, \bar{t}$.

(b) $\deg F_\tau(X) \leqq m_1(q, n)$ for $\tau = 1, \ldots, \bar{t}$.

(c) For every polynomial $f(X) \in \sqrt{\mathfrak{a}}$ such that $\deg f(X) \leqq m_1(q, n)$ there exist polynomials $G_1(X), \ldots, G_{\bar{t}}(X)$ for which $\deg G_\tau(X) \leqq m_1(q, n) + m_2(\bar{t}, q, n)$ for

$$\tau = 1, \ldots, \bar{t} \text{ and } f(X) = \sum_{\tau=1}^{\bar{t}} G_\tau(X) F_\tau(X).$$

Irreducible Algebraic Sets. The statement "V is irreducible" is also an elementary statement (see e. g. Robinson [8], p. 327—328 or Lambert [4], § 5).

Dimension of a Variety. Let V be as before and assume that it is irreducible, i. e. it is a variety. Let $0 \leqq r \leqq n$. The statement "$\dim V = r$" is equivalent to the conjunction of the following two elementary statements:

(a) $\exists (X)$: $(X) \in V$ and the rank of the matrix $\left(\frac{\partial f_\mu(X)}{\partial X_\nu}\right)$ equals $n - r$.

(b) $\forall (X)$: $(X) \in V \Rightarrow$ the rank of the matrix $\left(\frac{\partial f_\mu(X)}{\partial X_\nu}\right) \leqq n - r$.

In fact, every (X) for which (a) holds is a simple point of V (see e. g. Weil [9], p. 99).

The notions of a closed subset of a variety and of a cartesian product of two varieties are obviously also elementary ones.

Rational Maps. Let V and V' be two irreducible varieties defined over K in S^n and $S^{n'}$ respectively. Let Φ: $V \to V'$ be a rational map defined over K. Let (x) be a generic point of V over K so that $(x') = \Phi(x)$. Define $\mathfrak{A} = \left\{A \in K[X] \,\middle|\, \bigwedge_{\nu'=1}^{n'} A(x) x'_{\nu'} \in K[x]\right\}$. Then $\mathfrak{A}$ is an ideal in $K[X]$ and for every $(a) \in V$, Φ is defined at (a) if and only if (a) is not a zero of $\mathfrak{A}$ (see e. g. Weil [9], p. 172). In particular there exist polynomials $A_1(X)$, $B_{1\nu'}(X) \in K[X]$, $\nu' = 1, \ldots, n'$, such that

$$A_1(x) x'_{\nu'} = B_{1\nu'}(x), \qquad \nu' = 1, \ldots, n', \ A_1(x) \neq 0.$$

Let $\{F_1(X), \ldots, F_{\bar{t}}(X)\}$ be a set of generators for the ideal of all polynomials in $K[X]$ vanishing on V. Suppose that the maximal degree of $F_\tau(X)$, $A_1(X)$, $B_{1\nu'}(X)$ is d. Consider the following system of homogeneous equations:

$$(1) \qquad A(X) B_{1\nu'}(X) = B_{\nu'}(X) A_1(X) + \sum_{\tau=1}^{\bar{t}} G_{\tau\nu'}(X) F_\tau(X) \qquad 1 \leqq \nu' \leqq n'$$

in the unknowns $A(X)$, $B_{\nu'}(X)$, $G_{\tau\nu'}(X)$, $1 \leqq \nu' \leqq n'$, $1 \leqq \tau \leqq \bar{t}$.

The collection of all solutions of this system constitutes a module $\mathfrak{M}$ over $K[X]$. One can find a set of generators $(A_\varrho(X), B_{\varrho\tau\nu'}(X), G_{\varrho\tau\nu'}(X)\colon 1 \leqq \nu' \leqq n', 1 \leqq \tau \leqq \bar{t})$, $\varrho = 1, \ldots, r$ such that the degrees of the polynomials appearing in it do not exceed $m_3(n', d, n)$, where $m_3(n', d, n) = \sum_{i=0}^{n-1} (n' \cdot d)^{2i}$ (see Hermann [3], p. 745, Satz 2). Using Hermann's theorem once more one can see that every element in $\mathfrak{M}$, such that the degrees of the polynomials appearing in it do not exceed $m_3(n', d, n)$, can be expressed as a linear combination of that set of generators with coefficients whose degrees are

$$\leqq m_3(1 + n' + n'\bar{t}, m_3(n', d, n), n).$$

We thus obtain that the varieties V, V' and the polynomials $F_\tau(X)$, $A_\varrho(X)$, $B_{\varrho\nu'}(X)$, $G_{\varrho\tau\nu'}(X)$ fulfill the following elementary statements:

(a) V, V' are irreducible.

(b) $\{F_1(X), \ldots, F_{\bar{t}}(X)\}$ is a set of generators for the ideal of all polynomials vanishing on V.

(c) $\deg F_\tau(X),\ A_1(X),\ B_{1\nu'}(X) \leqq d$ for $\tau = 1, \ldots, \bar{t}$; $\nu' = 1, \ldots, n'$.

(d) $\exists (X)[(X) \in V \wedge A_1(X) \neq 0]$.

(e) $\forall (X, X')\left[\left[(X) \in V \wedge \bigvee_{\varrho=1}^{r} \left[A_\varrho(X) \neq 0 \wedge \bigwedge_{\nu'=1}^{n'} A_\varrho(X) X'_{\nu'} = B_{\varrho\nu'}(X)\right]\right] \Rightarrow (X') \in V'\right]$.

(f) $(A_\varrho(X), B_{\varrho\nu'}(X), G_{\varrho\tau\nu'}(X))$ is a solution of (1) for every $1 \leqq \varrho \leqq r$.

(g) If $(A(X), B_{\nu'}(X), G_{\tau\nu'}(X))$ is a solution of (1) such that $\deg A(X), B_{\nu'}(X), G_{\tau\nu'}(X) \leqq m_3(n', d, n)$ then it is a linear combination of the $(A_\varrho(X), B_{\varrho\nu'}(X), G_{\varrho\tau\nu'}(X))$, $\varrho = 1, \ldots, r$ with coefficients whose degrees are $\leqq m_3(1 + n' + n'\bar{t}, m_3(n', d, n), n)$.

Conversely, assume that the varieties V, V' and the polynomials $F_\tau(X)$, $A_\varrho(X)$, $B_{\varrho\nu'}(X)$, $G_{\varrho\tau\nu'}(X)$ are given and that they fulfill the statements (a)—(g). Let (x) be a generic point of V over K. Then $A_1(x) \neq 0$. Define $(x') \in S^{n'}$ by the equations

$$A_1(x) x'_{\nu'} = B_{1\nu'}(x).$$

Then $K(x') \subseteq K(x)$ and $(x') \in V'$. Hence there exists a rational map $V \to V'$ which maps (x) onto (x'). This map coincides with Φ and $\{A_1(X), \ldots, A_r(X)\}$ is a set of generators for $\mathfrak{A}$.

The formula "Φ is defined at a point (X) of V and $\Phi(X) = (X')$" is now seen to be equivalent to the elementary formula:

$$(X) \in V \wedge \bigvee_{\varrho=1}^{r} \left[A_\varrho(X) \neq 0 \wedge \bigwedge_{\nu=1}^{n'} A_\varrho(X) X'_{\nu'} = B_{\varrho\nu'}(X)\right].$$

We have thus characterized elementarily the notion of a rational map.

The Graph of a Rational Map. Let V, V', Φ be as above. The graph of the rational map Φ is a variety Γ_Φ defined in $S^n \times S^{n'}$ over K with the following elementary properties:

a) Γ_Φ is irreducible.

b) $\forall (X, X') \in V \times V'$: If Φ is defined at (X) and $\Phi(X) = (X')$ then $(X, X') \in \Gamma_\Phi$.

c) $\dim \Gamma_\Phi = \dim V$.

Composition of Rational Maps. Let V, V', Φ be as before. Let V'' be another variety and let Φ': $V' \to V''$ and Ψ: $V \to V''$ be two additional rational maps. Then the statement $\Psi = \Phi' \circ \Phi''$ is equivalent to the following conjunction of elementary statements:

a) For every $(X, X', X'') \in V \times V' \times V''$:
Φ is defined at $(X) \wedge \Phi(X) = (X')$,
Φ' is defined at $(X') \wedge \Phi'(X') = (X'')$
$\Rightarrow \Psi$ is defined at $(X) \wedge \Psi(X) = (X'')$.

b) $\exists\, (X, X') \in V \times V'$: Φ is defined at $(X) \wedge \Phi(X) = (X') \wedge \Phi'$ is defined at (X').

Birational Maps. Take V, V', Φ as before and let Φ': $V' \to V$ be an additional rational map defined over K. Then the statement "Φ and Φ' are birational maps which are inverse to each other" is equal to the following elementary statement:

$$\Phi \circ \Phi' = 1_{V'} \wedge \Phi' \circ \Phi = 1_{V}.$$

Coherent Birational Maps. Let V, V', Φ, Φ', Γ_Φ be as before. Then the statement "Φ is a coherent birational map" is equivalent to the following elementary statement: $\forall (X, X') \in \Gamma_\Phi$: Φ is defined at (X) and Φ' is defined at (X').

Abstract Varieties. Let A be a finite set. For every $\alpha \in A$ let V_α be an affine variety defined over K in S^{n_α} and let $X_{\alpha,1}, \ldots, X_{\alpha,n_\alpha}$ be variables for the coordinates of S^{n_α}. Denote $(X_\alpha) = (X_{\alpha,1}, \ldots, X_{\alpha,n_\alpha})$ and $(X) = (X_\alpha)_{\alpha \in A}$. For every $\alpha, \alpha' \in A$ let

$$\Phi_{\alpha\alpha'}\colon V_\alpha \to V_{\alpha'}$$

be a birational coherent map defined over K, the inverse of which is $\Phi_{\alpha'\alpha}$. Furthermore, we demand that if $\alpha, \alpha', \alpha'' \in A$ then $\Phi_{\alpha\alpha''} = \Phi_{\alpha'\alpha''} \circ \Phi_{\alpha\alpha'}$. On the basis of the previous discussion we see that one can formulate all of these conditions as elementary statements on a certain set of polynomials defined over K.

Two points (X_α) of V_α and $(X_{\alpha'})$ of $V_{\alpha'}$ are said to be equivalent if the following elementary statements holds: "$\Phi_{\alpha\alpha'}$ is defined at (X_α) and $\Phi_{\alpha\alpha'}(X_\alpha) = (X_{\alpha'})$".

A point of the abstract variety V will, in our terminology, be a set of variables (X) for which there exists a non-empty subset A_0 of A such that:

a) For every $\alpha \in A_0$, $(X_\alpha) \in V_\alpha$.

b) For every $\alpha, \alpha' \in A_0$, (X_α) is equivalent to $(X_{\alpha'})$.

c) If $\alpha \in A_0$ and $\alpha' \in A - A_0$ then $\Phi_{\alpha\alpha'}$ is not defined at (X_α).

This is, of course, an elementary description. Every (X_α) for which $\alpha \in A_0$ is said to be a "representative of (X)".

The dimension of V is the dimension of each of the V_α's. This, as we have seen, is an elementary notion.

Subvarieties of an Abstract Variety. Let $[V, \Phi_{\alpha\alpha'}]_{\alpha'\alpha \in A}$ be as before. Let B be a non-empty subset of A. For every $\beta \in B$ let $\psi_{\beta\beta'}$: $W_\beta \to W_{\beta'}$ be a coherent birational map defined over K. Suppose that $[W_\beta, \psi_{\beta\beta'}]_{\beta,\beta' \in B}$ define an abstract variety W. Then W is a subvariety of V if the following elementary statements hold:

a) For every $\beta, \beta' \in B$ and $\forall (X_\beta, X_{\beta'}) \in W_\beta \times W_{\beta'}$: $\Phi_{\beta\beta'}$ is defined at (X_β) if and only if $\psi_{\beta\beta'}$ is defined at (X_β) and in this case $\Phi_{\beta\beta'}(X_\beta) = (X_{\beta'})$ if and only if

$$\psi_{\beta\beta'}(X_\beta) = (X_{\beta'}).$$

b) There exists a $\beta \in B$ such that for all $\beta' \in B$, $\exists (X_\beta) \in W_\beta$ such that $\Phi_{\beta\beta'}$ is defined at (X_β), and such that for all $\alpha \in A - B$, $\sim \exists (X_\beta) \in W_\beta$ for which $\Phi_{\beta\alpha}$ is defined at (X_β).

In order to say in an elementary way that a point (X) of V belongs to W one has to demand that for every $\beta \in B$, if (X_β) is a representative of (X) then $(X_\beta) \in W_\beta$.

Closed Subsets. A subset C of V is said to be closed over K if it is the union of a finite number of subvarieties defined over K. It is clear that this is an elementary notion.

Rational Maps of Abstract Varieties. Let $V = [V_\alpha, \Phi_{\alpha\alpha'}]_{\alpha,\alpha' \in A}$ and $U = [U_\beta, \psi_{\beta\beta'}]_{\beta,\beta' \in B}$ be two abstract varieties defined over K. Let (Y) be a set of coordinates for U. Let B' be a non-empty subset of B. For every $\alpha \in A$ and $\beta \in B'$ let $\chi_{\alpha\beta}$: $V_\alpha \to U_\beta$ be a rational map defined over K. The $\chi_{\alpha\beta}$'s are said to define a rational map χ: $V \to U$ if

a) There exists a $\beta' \in B'$ such that B' is the subset of all $\beta \in B$ for which there exists a $(X_\alpha) \in V_\alpha$ such that $\psi_{\beta'\beta} \circ \chi_{\alpha\beta'}$ is defined. (See e. g. Lang [5], p. 110 for this definition.)

b) For every $\alpha, \alpha' \in A$ and $\beta, \beta' \in B$ $\chi_{\alpha\beta} = \psi_{\beta'\beta} \circ \chi_{\alpha'\beta'} \circ \Phi_{\alpha\alpha'}$.

If $(X) \in V$ and $(Y) \in U$ then the statement "χ is defined at (X) and $\chi(X) = (Y)$" is equivalent to the following elementary formula: "There exist $\alpha \in A$ and $\beta \in B'$ such that $\chi_{\alpha\beta}$ is defined at (X_α) and $\chi_{\alpha\beta}(X_\alpha) = (Y_\beta)$."

All of these preliminaries enable us to be convinced of the validity of the following lemma:

Lemma 3. *Denote by* $E_0(V, U, W, \chi; r, m, s, n)$ *the statement*: "*V is an abstract variety defined over K; U, W are K-closed subsets of V; χ: $V \to V$ is a rational map defined at every point of $V - U$ which induces a bijective map of $V - U$ onto $V - W$;* $r = \dim U$, $m = n_r(U)$; $s = \dim W$, $n = n_s(W)$".

Denote by $E(V, U, W, \chi; r, m, s, n)$ *the statement*: "$E_0(V, U, W, \chi; r, m, s, n)$ *implies that* $r = s$ *and* $m = n$".

Then $E_0(V, U, W, \chi; r, m, s, n)$ *and* $E(V, U, W, \chi; r, m, s, n)$ *are elementary statements about* K.

§ 2. Proof of Theorem 1

Lemma 4. *Let* $B_1, \ldots, B_n, B_{n+1}, \ldots, B_m$ *denote* m *different subvarieties of an abstract variety* V. *Suppose that they are defined over a finite field k with q elements. Assume that* $\max\limits_{1 \le i \le m} \{\dim B_i\} = r$ *and that exactly the first n B_i's have the dimension r. For every* $\nu \geqq 1$ *denote by k_ν the extension of k of degree ν. Let* $B = \bigcup\limits_{i=1}^{m} B_i$. *Denote by* $|B|_\nu$ *the number of rational points of B over k_ν. Then*

$$|B|_\nu = n q^{\nu r} + O\left(q^{\nu\left(r - \frac{1}{2}\right)}\right) \qquad \nu \to \infty.$$

Proof. Consider the inequality

$$(1) \qquad \sum_{i=1}^{n} |B_i|_\nu - \sum_{i \neq j} |B_i \cap B_j|_\nu \leqq |B|_\nu \leqq \sum_{i=1}^{m} |B_i|_\nu .$$

According to a theorem of Weil-Lang [6], § 2 we have

$$|B_i|_\nu = \begin{cases} q^{\nu r} + O\left(q^{\nu\left(r - \frac{1}{2}\right)}\right) & 1 \leqq i \leqq n \\ O\left(q^{\nu\left(r - \frac{1}{2}\right)}\right) & n + 1 \leqq i \leqq m. \end{cases}$$

Hence, $| B |_\nu \leqq nq^{\nu r} + O\left(q^{\nu(r-\frac{1}{2})}\right)$. On the other hand, for every $i \neq j$,

$$\dim(B_i \cap B_j) \leqq r - 1;$$

thus, by the same argument

$$| B_i \cap B_j | \leqq m_{ij} q^{\nu(r-1)} + O\left(q^{\nu(r-1-\frac{1}{2})}\right) = O\left(q^{\nu(r-\frac{1}{2})}\right)$$

where m_{ij} is the number of components of $B_i \cap B_j$. Therefore, (1) gives us the desired result.

Lemma 5. *Let p be a prime. Then the statement $E(V, U, W, \chi; m, r, s, n)$ holds for every V, U, W, χ defined over the field $\bar{F}_p$.*

Proof. We can find a finite subfield k of $\bar{F}_p$ over which V, U, W, χ as well as the components of U and W are defined. Let q be the number of elements of k. For every $\nu \geqq 1$ denote by k_ν the extension of k degree ν, and by $(V - U)_\nu$ and $(V - W)_\nu$ denote the sets of rational points of $V - U$ and $V - W$ respectively over k_ν. Suppose that $E_0(V, U, W, \chi; m, r, s, n)$ holds. Then it is clear that χ induces an injective map of $(V - U)_\nu$ into $(V - W)_\nu$. This map is also surjective. Indeed, let Q be a point of $(V - W)_\nu$. Then there exists a point P of $V - U$, rational over $\bar{F}_p$ such that $\chi(P) = Q$. Let σ be any automorphism of $\bar{F}_p$ over k_ν. Then $\chi(\sigma P) = Q$. Moreover, $\sigma P \in V - U$ and is rational over $\bar{F}_p$, hence $\sigma P = P$. Hence $P \in (V - U)_\nu$. It follows that $(V - U)_\nu$ and $(V - W)_\nu$ have the same number of elements. Hence, the same is true for U_ν and W_ν. From Lemma 4 it follows now that $nq^{\nu r} + O\left(q^{\nu(r-\frac{1}{2})}\right) = mq^{\nu s} + O\left(q^{\nu(s-\frac{1}{2})}\right)$, $\nu \to \infty$. Hence $r = s$ and $m = n$.

q. e. d.

Proof of Theorem 1. There are only a finite number of polynomials appearing in the definitions of the objects V, U, W, χ. Their degrees are, therefore, bounded by some natural number N which we can suppose to be greater than r, m, s, n. Denote by E_N the following statement: "For all V, U, W, χ such that $E_0(V, U, W, \chi; r, m, s, n)$ holds, and such that the degrees of all the polynomials involved in the definitions of V, U, W, χ, as well as r, m, s, n, are smaller than N, we have $r = s$ and $m = n$". Then, according to Lemma 3, E_N is an elementary statement. In Lemma 5 we have, in fact proved that for every prime characteristic there exists an algebraically closed field K having this characteristic such that E_N holds in K. By taking ultra products we can obtain also an algebraically closed field of characteristic 0 such that E_N holds in it. Hence, according to the result of Robinson mentioned at the beginning of § 1, E_N holds in every algebraically closed field.

This concludes the proof of the theorem.

§ 3. Proof of Theorem 2

Let W be a closed subset of V such that $V - W \subseteq \chi(V - U)$. Let $s = \dim W$. χ induces a continuous map of $V - U$ into V (see e. g. Weil [9], p. 171 theorem 2). It follows that $\chi^{-1}(V - W) \cap (V - U)$ is an open subset of $V - U$ which, therefore, has the form $V - A$ where A is a closed subset of V containing U. χ certainly induces a bijective map of $V - A$ onto $V - W$. Hence, according to Theorem 1, $\dim A = s$ and $n_s(A) = n_s(W)$. Since $U \subseteq A$ it follows that $r \leqq s$, and if $r = s$ then $n_r(U) \leqq n_r(W)$.

In order to find Z we start with any closed subset W of V such that $V - W \leqq \chi(V - U)$. (Take, for example, $W = V$.) Let $s = \dim W$ and let A be as before. If $r < s$, or if $r = s$ and $n_r(U) < n_r(A)$, there exists a component A_1 of A such that $\dim A_1 = s$ and $A_1 - U$ is a non-empty open set of A_1. Let P be a generic point of A_1 over $\bar{k}$. Then $P \notin U$. Hence $\chi(P) = Q$ is defined and belongs to W. The injectivity of χ implies that $\bar{k}(P)$ is a purely inseparable extension of $\bar{k}(Q)$. In particular, $\dim_k Q = \dim_k P = \dim A_1 = s$. Hence, the locus of Q over $\bar{k}$ is a subvariety of W of dimension s, i. e. it is a component of W. Denote this component by W_1 and let $W_2, \ldots, W_m$ be all the other components of W. χ induces a generically surjective rational map of A_1 into W_1. Hence, according to a well known theorem $\chi(A_1 - U)$ contains a non-empty open subset $W_1 - W_1'$ of W_1 (cf. Lang [5], p. 95). W_1 is a closed subset of V and $\dim W_1' < s$. Hence

$$n_s\left(W_1' \cap \bigcup_{i=1}^{m} W_i\right) < n_s(W) \text{ and } V - W_1' \cup \bigcup_{i=s}^{m} W_i \leqq (V - W) \cup (W_1 - W_1') \leqq \chi(V - U).$$

We can, therefore, replace W by $W^* = W_1' \cup \left(\bigcup_{i=s}^{m} W_i\right)$. After a finite number of such replacements we get, eventually, the desired closed subset Z of V.

Let $Q \in \chi(V - U) \cap Z$. If it were true that $\dim_k Q < r$, we could further contract Z to a closed subset Z^* for which both $V - Z^* \leqq \chi(V - U)$ and $n_r(Z^*) < n_r(U)$, in contradiction to the first part of the theorem.

Let $n = n_r(U)$ and let $Z_1, \ldots, Z_n$ be all the components of Z of dimension r. Let Z' be another closed subset of Z for which (a), (b), (c) hold and let $Z_1', \ldots, Z_n'$ be the components of Z' of dimension r. If the two sets are not equal then by the dimension theorem (see e. g. Lang [5], p. 36) $n_r(Z \cap Z') < n$. But $V - Z \cap Z' \leqq \chi(V - U)$, so that by the first part of the theorem $n_r(Z \cap Z') \geqq n$, which is obviously a contradiction.

The last part of the theorem follows immediately from the uniqueness property and from the fact that the intersection of all the Z's for which (a), (b) and (c) hold is invariant under all the automorphisms of the universal domain leaving k fixed.

Remark. Note that Theorem 1 can also be derived from Theorem 2.

References

[1] *J. Ax*, Injective endomorphisms of varieties and schemes, Pacific J. of Math. **31** (1969), 1—7.

[2] *P. C. Eklof*, Resolutions of singularities in prime characteristic for almost all primes. Trans. of A. M. S. **146** (1969), 429—438.

[3] *G. Hermann*, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, Math. Annalen **95** (1926), 736—788.

[4] *W. M. Lambert*, A notion of effectiveness in arbitrary structures, J. of Symbolic Logic **33** (1968), 577—602.

[5] *S. Lang*, Introduction to algebraic geometry, New York 1958.

[6] *S. Lang* and *A. Weil*, Number of points of varieties in finite fields, Amer. J. of Math. **76** (1954), 819—827.

[7] *A. Robinson*, Introduction to model theory and to the mathematics of algebra, Amsterdam 1965.

[8] *A. Robinson*, Application to field theory, Summer Institute for Symbolic Logic, Cornell Univ. (1957), 326—331.

[9] *A. Weil*, Foundation of algebraic geometry, Providence 1962.

Mathematisches Institut der Universität, 69 Heidelberg 1, Im Neuenheimer Feld 9

Mathematics Department, The Hebrew University, Jerusalem, Israel

Eingegangen 21. Januar 1972