On the rationality of the zeta-function of a set definable over a finite field

A Dissertation presented

by

Catarina Isabel Kiefe

to

The Graduate School

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in

Mathematics

State University of New York

at

Stony Brook

June, 1973

STATE UNIVERSITY OF NEW YORK

AT STONY BROOK

THE GRADUATE SCHOOL

Catarina Isabel Kiefe

We, the thesis committee for the above candidate for the Ph. D. degree, hereby recommend acceptance of the Thesis.

Henry Laufer, Chairman

James Ax, Advisor

Stanley Osher

Chih Han Sah

John Cherniavsky, extra-departmental member

The thesis is accepated by the Graduate School.

Herbert Weisinger, Dean

Abstract of the Dissertation

On the rationality of the zeta-function of a set definable over a finite field

by

Catarina Isabel Kiefe

Doctor of Philosophy

in

Mathematics

State University of New York at Stony Brook

1973

Let k be a finite field, k_s its unique extension of degree s, $\bar{k}$ its algebraic closure. If $U \subseteq \bar{k}^r$ is a set definable over k, let $U_s = U \cap k_s{}^r$ and $N_s(U) = \# U_s$; then

$$\zeta_U(t) = \exp \sum_{s=1}^{\infty} \frac{N_s(U)}{s} t^s \quad \text{and}$$

$$\pi_U(t) = t \frac{d}{dt} \log \zeta_U(t) .$$

Dwork has proved the rationality of $\zeta_U(t)$, hence of $\pi_U(t)$, in case U is a variety. We prove that $\pi_U(t)$ is rational for any definable set U.

The result is achieved using model-theoretic tools: Shoenfield's Quantifier Elimination Theorem is generalized to yield a semantic characterization of the

elimination of quantifiers. This is then applied to:

1) Produce a first-order language in which the elementary theory of C((t)) admits elimination of quantifiers: the theory discussed is an extension by definitions of the theory of C((t)) in ordinary valued-field language.

2) Produce an extension by definitions of the elementary theory of finite fields which admits elimination of quantifiers. This yields a simple characterization of sets definable over a finite field, and allows us to obtain our main result.

Table of Contents

List of symbols

Q - rational numbers

Z - rational integers

$Z_{>a}$ - rational integers greater than a

C - complex numbers

L_τ - language of type τ

St_{L_τ} - sentences in language of type τ

$\mathfrak{A} \models \Sigma$ - $\mathfrak{A}$ is a model of the theory Σ

$|\mathfrak{A}|$ - domain of the strucuture $\mathfrak{A}$

$\mathfrak{A}_1 \subseteq \mathfrak{A}_2$ - $\mathfrak{A}_1$ is a substructure of $\mathfrak{A}_2$

$\mathfrak{A}_1 \preceq \mathfrak{A}_2$ - $\mathfrak{A}_1$ is an elementary substructure of $\mathfrak{A}_2$

$\mathfrak{A}_1 \equiv \mathfrak{A}_2$ - $\mathfrak{A}_1$ is elementarily equivalent to $\mathfrak{A}_2$

$\mathfrak{A} \models \varphi[a_1,\ldots,a_n]$ - $\mathfrak{A}$ satisfies φ at $(a_1,\ldots,a_n)$

$L_{\tau,\mathfrak{A}}$ - language of type $\langle\tau,\mathfrak{A}\rangle$, which means L_τ with a new constant for every element of $\mathfrak{A}$ adjoined

Diag $\mathfrak{A}$ - set of atomic formulae and negations of atomic formulae in $L_{\tau,\mathfrak{A}}$ satisfied by $\mathfrak{A}$.

$\mathfrak{A}^f$ - interpretation in the strucuture $\mathfrak{A}$ of the function, predicate or constant symbol f

$\mathfrak{F}^*$ - multiplicative group of units of the field $\mathfrak{F}$

$\bar{\mathfrak{F}}$ - residue class field of the valued field $\mathfrak{F}$

irred(a,F) - minimum polynomial of a over F

Acknowledgments

I wish to thank Professor Ax: he not only suggested this problem and was generous with his ideas, but also -quite unexpectedly - showed extreme patience with my shortcomings.

I also held several valuable conversations on related matters with Allan Adler; specifically, he found the counter-example in Chapter II.

I - Introduction

A semantic characterization of the first-order theories admitting elimination of quantifiers is given; this is done by generalizing Shoenfield's Quantifier Elimination Theorem to a necessary and sufficient condition, via ultraproducts. This si then used to prove the possibility of eliminating quantifiers in two cases:

1) The elementary theory of $C((t))$ (the field of formal power series over the complex numbers); the theory for which the existence of an elimination is established is an extension by definitions of the theory of $C((t))$ in ordinary valued-field language. The proof involves results found in the Ax-Kochen papers relative to the Artin conjecture.

2) The elementary theory of finite fields; here, the theory for which the existence of a quantifier-elimination is established, is an extension by definitions of the theory of finite fields in ordinary field language; the extension is obtained by adjoining a countable set of predicate symbols $\{\varphi_n | n \in Z_{>0}\}$, where each φ_n is a n+1-ary relation symbol; for each $n \in Z_{>0}$ we introduce a defining axiom which essentially says that for any model $\mathfrak{F}$ of our theory and for all $a_0, \ldots, a_n \in \mathfrak{F}$, we have

$$\mathfrak{F} \models \varphi_n[a_0, \ldots, a_n] \iff \text{the polynomial } a_n x^n + \ldots + a_0 \text{ has a root in } \mathfrak{F}.$$

This theory is then shown to be model-complete and to satisfy a weak isomorphism condition specified in our semantic characterization; this si done using methods contained in Ax's papers on finite fields.

The existence of an elimination of quantifiers as described in 2) is now used to establish the main result:

Let k be a finite field, and k_s its unique extension field such that $[k_s:k]=s$. Let φ be a formula with r free variables in ordinary field language and constants in k; let U be the set defined over k by φ. We define

$$U_s = \{(a_1,\ldots,a_r)\in {k_s}^r \mid k_s \models \varphi[a_1,\ldots,a_r]\} ,$$

$$N_s(U) = \# U_s ,$$

$$\zeta_U(t) = \exp \sum_{s=1}^{\infty} \frac{N_s(U)}{s} t^s ,$$

$$\pi_U(t) = (\frac{d}{dt} \log \zeta_U(t))\ t.$$

Dwork has proved that if U is a variety, $\zeta_U(t)$ is rational, hence so is $\pi_U(t)$. We prove that $\pi_U(t)$ is rational for any definable set U. This si achieved by first eliminating quantifiers from φ, i.e., considiering it reduced to its quantifier-free form in the extended field language; then, after various reductions, the main result boils down to to proving that $\pi_U(t)$ is rational in the case where U is defined by the atomic formula

$\varphi_n(p_0(x_1,\ldots,x_r),\ldots,p_n(x_1,\ldots,x_r)$, with $p_i \in k[x_1,\ldots,x_r]$.

The proof involves some moderately involved computations and Dwork's result.

As an illustration, the main result is used to establish the rationality of the Poincare series of the image of a variety under a morphism.

The terminology is standard, at least where not specifically defined in the text. In Chapter III, the terminology and notation is as in [10] and [11].

II - A semantic characterization of the elimination of quantifiers

Let τ be a type, L_τ the first-order language of type τ; let Λ be a theory in language L_τ.

Definition 1: We say that Λ satisfies the isomorphism condition if for every two models $\mathfrak{A}$ and $\mathfrak{A}'$ of Λ and every isomorphism θ of substructures of $\mathfrak{A}$ and $\mathfrak{A}'$, there is an extension of θ which is an isomorphism of a submodel of $\mathfrak{A}$ and a submodel of $\mathfrak{A}'$.

Definition 2: We say that Λ satisfies the submodel condition if for every model $\mathfrak{D}$ of Λ, every submodel $\mathfrak{A}$ of $\mathfrak{D}$, and every closed simply existential formula φ of $L_{\tau,\mathfrak{A}}$, we have

$$\mathfrak{A} \models \varphi \quad \Leftrightarrow \quad \mathfrak{D} \models \varphi \quad .$$

The following theorem is well-known [6, p. 85]:

Quantifier Elimination Theorem: If Λ satisfies the isomorphism condition and the submodel condition, then Λ admits elimination of quantifiers.

The Quantifier Elimination Theorem gives a sufficient condition for a theory to admit elimination of quantifiers. However, this condition is not necessary, as is established by the following counter-example, due to Allan Adler:

Counter-example: Let Γ denote the "theory of independent events", described as follows:

Language of Γ: no constant symbols

no function symbols

a countable set $\{\rho_n | n \in \omega\}$ of unary predicate symbols

Axioms of Γ: for every orderd pair (S,T) of finite subsets of ω such that $S \cap T$ is empty we have an axiom

$$A_{(S,T)} : \quad (\exists x)\Big(\bigwedge_{n\in S} \rho_n(x) \wedge \bigwedge_{n\in T} \neg\rho_n(x)\Big)$$

Γ admits elimination of quantifiers: indeed, by [6, p. 83], it suffices to show that if φ is a simply existential formula, φ is equivalent in Γ to an open formula; so let φ be of the form $(\exists x)\psi$, with ψ an open formula. By a standard reduction we may assume that ψ has a conjunctive matrix, i. e. ψ has the form

$$\bigwedge_{n\in S} \rho_n(x) \wedge \bigwedge_{i=1}^{r}\Big(\bigwedge_{n\in S_i} \rho_n(y_i)\Big) \wedge \bigwedge_{n\in T} \neg\rho_n(x) \wedge \bigwedge_{i=1}^{r}\Big(\bigwedge_{n\in T_i} \neg\rho_n(y_i)\Big)$$

where $y_1,\dots,y_r$ are the free variables of φ and S,T,S_i,T_i $(i=1,\dots,r)$ are finite sets of positive integers. If $S \cap T$ is empty, then by $A_{(S,T)}$ we have

$$\Gamma \vdash \varphi \leftrightarrow \bigwedge_{i=1}^{r}\Big(\bigwedge_{n\in S_i} \rho_n(y_i)\Big) \wedge \bigwedge_{i=1}^{r}\Big(\bigwedge_{n\in T_i} \neg\rho_n(y_i)\Big)$$

If $S \cap T$ is not empty then we have

$$\Gamma \vdash \varphi \leftrightarrow \rho_1(x) \wedge \neg\rho_1(x)$$

To establish our counter-example all that remains to be done is to show that

Γ does not satisfy the isomorphism condition: indeed, we define two subsets M, N of [0,1] as follows:

First, we define sequences $\{M_n\}_{n\in\omega}$, $\{N_n\}_{n\in\omega}$ of finite subsets of [0,1] inductively by:

$M_0=N_0=\{0\}$,

if $M_0,\ldots,M_n,N_0,\ldots,N_n$ are known, choose $\xi_1,\ldots,\xi_{2^{n+1}}$, $\eta_1,\ldots,\eta_{2^{n+1}}$ in [0,1] such that all are irrational,

$\xi_j,\eta_j \in[(j-1)/2^{n+1},j/2^{n+1}]$ $(j=1,\ldots,2^{n+1})$,

all are distinct and none are contained in M_n or N_n.

We put $M_{n+1}=M_n\cup\{\xi_1,\ldots,\xi_{2^{n+1}}\}$, $N_{n+1}=N_n\cup\{\eta_1,\ldots,\eta_{2^{n+1}}\}$.

We now define $M=\bigcup_{n\in\omega} M_n$, $N=\bigcup_{n\in\omega} N_n$

We make M, N models of Γ by interpreting $\rho_n(x)$ to mean that the n-th binary digit of x is 1. The axioms then simply require that M and N should each have non--empty intersection with each dyadic interval $[j/2^n,(j+1)/2^n]$ and are satisfied by construction.

$M_0=N_0=\{0\}$ are isomorphic substructures of M and N. However, any isomorphism of submodels of M and N must take an irrational number into itself. Since $M\cap N=\{0\}$, the isomorphism condition fails.

The Quantifier Elimination Theorem is now going to be extended to a necessary and sufficient condition, therewith yielding a semantic characterization of the elimination of quantifiers. We need

Definition 3: We say that Λ satisfies the weak isomorphism condition if for every two models $\mathfrak{a}$ and $\mathfrak{a}'$ of Λ and every isomorphism θ of a substructure of $\mathfrak{a}$ and a substructure of $\mathfrak{a}'$, there is an elementary extension $\mathfrak{a}''$ of $\mathfrak{a}'$ and an extension of θ which is an isomorphism of a submodel of $\mathfrak{a}$ and a submodel of $\mathfrak{a}''$.

We then have

Theorem 1: Λ admits elimination of quantifiers if and only if Λ is model-complete and Λ satisfies the weak isomorphism condition.

For the proof of Theorem 1 we need the following three Lemmas:

Lemma 1: Let φ be a closed formula in L_τ. Suppose that for every two models $\mathfrak{a}$ and $\mathfrak{a}'$ of Λ such that for every variable-free formula ψ in L_τ $\mathfrak{a} \models \psi \Leftrightarrow \mathfrak{a}' \models \psi$, we have $\mathfrak{a} \models \varphi \Leftrightarrow \mathfrak{a}' \models \varphi$. Then φ is equivalent in Λ to a variable-free formula.

Proof: Done in [6, P. 83].

Lemma 2: Let Λ' be obtained form Λ by adjoining a new constant. If Λ satisfies the weak isomorphism condition (is model-complete), then so does (is) Λ.

Proof: immediate.

Lemma 3: If Λ is model-complete and satisfies the weak isomorphism condition and contains a constant, then every closed formula in L_τ is equivalent in Λ to a variable-free formula.

Proof: Let φ be closed. By Lemma 1 it suffices to verify that for any $\mathfrak{A}_1, \mathfrak{A}_2 \models \Lambda$ such that for every variable-free formula ψ, $\mathfrak{A}_1 \models \psi \Leftrightarrow \mathfrak{A}_2 \models \psi$, we have $\mathfrak{A}_1 \models \varphi \Leftrightarrow \mathfrak{A}_2 \models \varphi$.

So assume $\mathfrak{A}_1 \models \Lambda$ and $\mathfrak{A}_2 \models \Lambda$ and that for any variable-free ψ we have $\mathfrak{A}_1 \models \psi \Leftrightarrow \mathfrak{A}_2 \models \psi$. For $i=1,2$, Let $\mathfrak{B}_i$ be a minimal substructure of $\mathfrak{A}_i$, i.e., a substructure obtained by closing up under the functions of $\mathfrak{A}_i$ the set obtained by interpreting in $\mathfrak{A}_i$ all the variable-free terms of L_τ; since Λ contains a constant, $\mathfrak{B}_i$ is non-empty; by the assumption on $\mathfrak{A}_1$ and $\mathfrak{A}_2$, it is clear that we can construct an isomorphism $\theta: \mathfrak{B}_1 \longrightarrow \mathfrak{B}_2$. By the weak isomorphism condition, θ can be extended to an isomorphism

$$\theta' : C_1 \longrightarrow C_2 \qquad \text{where}$$

$\mathfrak{B}_1 \subseteq C_1 \subseteq \mathfrak{A}_1$, $C_1 \models \Lambda$, $C_2 \models \Lambda$ and $\mathfrak{B}_2 \subseteq C_2 \subseteq \mathfrak{A}_2'$, with $\mathfrak{A}_2 \leq \mathfrak{A}_2'$.

Because Λ is model-complete

$$\mathfrak{G}_1 \models \varphi \quad \Leftrightarrow \quad \mathfrak{C}_1 \models \varphi \text{ and } \mathfrak{G}_2' \models \varphi \quad \Leftrightarrow \quad \mathfrak{C}_2 \models \varphi \quad \Leftrightarrow \quad \mathfrak{G}_2 \models \varphi$$

and because θ' is isomorphism $\mathfrak{C}_1 \models \varphi \quad \Leftrightarrow \quad \mathfrak{C}_2 \models \varphi$

q. e. d.

Proof of Theorem 1:

$\Leftarrow$: We want to show that every formula φ in L_τ is equivalent in Λ to an open formula. Let φ' be obtained from φ by replacing each variablr free in in φ by a new constant. and say Λ' is the theory obtained from Λ by adjoining these new constants (or by adjoining one new constant if φ is closed). From Lemmas 2 and 3 , φ' is equivalent in Λ to a variable-free formula; so by a Theorem on Constants [6, p. 33], φ is equivalent in Λ to an open formula.

$\Rightarrow$: Let $\mathfrak{G}_1, \mathfrak{G}_2 \models \Lambda$, $\mathfrak{G}_1 \subseteq \mathfrak{G}_2$;
to prove that Λ is model-complete, we need $\mathfrak{G}_1 \preceq \mathfrak{G}_2$;
so let φ be a formula in L_τ, with free variables $x_1, \ldots, x_n$;
we must show that given any $a_1, \ldots, a_n \in |\mathfrak{G}_1|$,

$$\mathfrak{G}_1 \models \varphi[a_1, \ldots, a_n] \quad \Leftrightarrow \quad \mathfrak{G}_2 \models \varphi[a_1, \ldots, a_n] \quad .$$

By hypothesis, Λ admits elimination of quantifiers, hence we can find a quantifier-free formula ψ equivalent in Λ to φ, i.e., such that

$$\Lambda \vdash \forall x_1 \ldots \forall x_n (\varphi \leftrightarrow \psi)$$

But then

$$\mathfrak{A}_i \models (\varphi \leftrightarrow \psi)[a_1, \ldots, a_n] \qquad (i=1,2) \quad , \text{ so}$$

$$\mathfrak{A}_i \models \varphi[a_1, \ldots, a_n] \quad \Leftrightarrow \quad \mathfrak{A}_i \models \psi[a_1, \ldots, a_n]$$

and since ψ is quantifier-free and $\mathfrak{A}_1 \subseteq \mathfrak{A}_2$,

$$\mathfrak{A}_1 \models \psi[a_1, \ldots a_n] \quad \Leftrightarrow \quad \mathfrak{A}_2 \models \psi[a_1, \ldots, a_n]$$

and hence

$$\mathfrak{A}_1 \models \varphi[a_1, \ldots, a_n] \quad \Leftrightarrow \quad \mathfrak{A}_2 \models \varphi[a_1, \ldots, a_n]$$

which establishes that Λ is model-complete.

We now show that Λ satisfies the weak isomorphism condition:

Let $\mathfrak{A}_1, \mathfrak{A}_2 \models \Lambda$ and let

$$\theta : \mathfrak{B}_1 \longrightarrow \mathfrak{B}_2$$

be an isomorphism, with $\mathfrak{B}_i \subseteq \mathfrak{A}_i \qquad (i=1,2)$

Let τ' be the type obtained from τ by adjoining as new constants a set enumerating $|\mathfrak{B}_1|$.

Then, if $|\mathfrak{B}_1| = \{b_j\}_{j \in |\mathfrak{B}_1|}$, and

$$|\mathfrak{B}_2| = \{\theta(b_j)\}_{j \in |\mathfrak{B}_1|} \quad ,$$

$< \mathfrak{A}_1, \{b_j\}_{j \in |\mathfrak{B}_1|} >$ and $< \mathfrak{A}_2, \{\theta(b_j)\}_{j \in |\mathfrak{B}_1|} >$

are structures of type τ'.

<u>Claim</u>: $< \mathfrak{A}_1, \{b_j\}_{j \in |\mathfrak{B}_1|} > \; \equiv \; < \mathfrak{A}_2, \{\theta(b_j)\}_{j \in |\mathfrak{B}_1|} >$

Indeed: let $\varphi \in St_{L_{\tau'}}$. Say the new constants occurring in φ are $b_{j_1},\ldots,b_{j_n}$.

Let φ^* be $\mathrm{Sub}^{x_1,\ldots x_n}_{b_{j_1},\ldots,b_{j_n}} \varphi$.

Since Λ admits elimination of quantifiers, we can find $\psi(x_1,\ldots,x_n)$ quantifier-free such that

$$\Lambda \vdash \varphi^* \longleftrightarrow \psi \quad , \text{ so}$$

$$\mathfrak{a}_i \models \forall x_1 \ldots \forall x_n(\varphi^* \longleftrightarrow \psi) \qquad (i=1,2)$$

In particular,

$$\mathfrak{a}_1 \models (\varphi^* \longleftrightarrow \psi)[b_{j_1},\ldots,b_{j_n}] \quad \text{and}$$

$$\mathfrak{a}_2 \models (\varphi^* \longleftrightarrow \psi)[\theta(b_{j_1}),\ldots,\theta(b_{j_n})]$$

but $\mathfrak{B}_i \subseteq \mathfrak{a}_i$ $(i=1,2)$, and since ψ is quantifier free

$$\mathfrak{a}_1 \models \psi[b_{j_1},\ldots,b_{j_n}] \Leftrightarrow \mathfrak{B}_1 \models \psi[b_{j_1},\ldots,b_{j_n}] \quad ,$$

$$\mathfrak{a}_2 \models \psi[\theta(b_{j_1}),\ldots,\theta(b_{j_n})] \Leftrightarrow \mathfrak{B}_2 \models \psi[\theta(b_{j_1}),\ldots,\theta(b_{j_n})]$$

and so

$$\mathfrak{a}_1 \models \varphi^*[b_{j_1},\ldots,b_{j_n}] \Leftrightarrow \mathfrak{a}_2 \models \varphi^*[\theta(b_{j_1}),\ldots,\theta(b_{j_n})]$$

which obviously implies

$$< \mathfrak{a}_1, \{b_j\}_{j\in|\mathfrak{B}_1|} > \models \varphi \Leftrightarrow < \mathfrak{a}_2, \{\theta(b_j)\}_{j\in|\mathfrak{B}_1|} > \models \varphi$$

and so the claim is established.

Now we peove our theorem by applying Frayne's Lemma [4, p. 161]:

we can find an ultrafilter pair < I, F > such that

$< \mathfrak{G}_1, \{b_j\}_{j \in |\mathfrak{B}_1|} >$ is elementarily embeddable in

$< \mathfrak{G}_2, \{\theta(b_j)\}_{j \in |\mathfrak{B}_1|} >^I / F$.

But this naturally means that we can embedd $\mathfrak{G}_1$ in $\mathfrak{G}_2{}^I / F$ by an embedding extending θ , and since $\mathfrak{G}_2{}^I / F$ is an elementary extension of $\mathfrak{G}_2$, the theorem is proved.

q. e.d ..

III - A language in which the theory of $C((t))$ admits elimination of quantifiers

Let τ be a type, Λ a theory in language L_τ.

Definition 4: Let $\{\varphi_i\}_{i\in A}$ be a collection of formulae in language L_τ; let n_i be the number of free variables of φ_i (we assume $n_i \geq 1$). Let τ' be obtained from τ by adjoining for every $i \in A$ an n_i-ary predicate symbol - say p_i. Let Λ' be the theory in language $L_{\tau'}$ obtained from Λ by adjoining the set of axioms

$$\{p_i(x_1,\dots,x_{n_i}) \longleftrightarrow \varphi_i(x_1,\dots,x_{n_i}) \mid i \in A\} .$$

Then Λ' is called an extension by definitions of Λ, and the axiom

$$p_i(x_1,\dots,x_{n_i}) \longleftrightarrow \varphi_i(x_1,\dots,x_{n_i})$$

is called the defining axiom for p_i.

Lemma 4: Let Λ' be an extension by definitions of Λ. Then Λ is complete $\Leftrightarrow$ Λ' is complete.

Proof: immediate, using an Equivalence Theorem as in [6, p. 34].

Let $C((t))$ denote the fields of formal power series (in t) over the complex numbers. We now describe a language and theory of $C((t))$ inthis language which admits elimination of quantifiers:

<u>Language</u>: function symbols: $+$ (field addition)

$\cdot$ (field multiplication)

$-$ (field subtraction)

$^{-1}$(field multiplicative inversion)

predicate symbols: $\mathfrak{O}$ (being an integer with respect to hte valuatio - unary relation)

φ_n (having order n - unary relation)

constant symbols: 0 (field zero)

1 (field unity)

<u>Axioms</u>: 1) valued field axioms

2) residue class field is algebraically closed and of characteristic zero

3) Hensel field axioms, i.e.,

a) value group is Z-group [9, p. 612]

b) Hensel's Lemma

4) Defining axioms for φ_n $(n \in Z_{>0})$:

a) $\varphi_1(x) \longleftrightarrow (x \neq 0 \wedge \mathfrak{O}(x) \wedge \neg\mathfrak{O}(x^{-1}) \wedge \forall y(\mathfrak{O}(y) \wedge \neg\mathfrak{O}(y^{-1}) \rightarrow \mathfrak{O}(x^{-1}y)))$

b) $\varphi_n(x) \longleftrightarrow \forall y(\varphi_1(y) \rightarrow \mathfrak{O}(y^{-1}{}^{n}x) \wedge \mathfrak{O}(x^{-1}y^n))$ $\qquad (n \in Z_{>1})$

It is a known fact that the theory of algebraically closed fields of characteristic zero is complete. It then follows from [3, p. 442, Thm 5] that the theory of Hensel fields whose residue class fields are algabraically closed of charactersitic zero is complete; i.e., the theory in the language of valued fields whose axioms are are 1), 2) and 3) above is complete. But the theory we have described above is an extension by definitions of the theory in the language of valued fields whose axioms are 1), 2) and 3) above, hence it also is complete. Let us call it Λ.

Since $C((t)) \models \Lambda$, Λ is the theory of $C((t))$ in the described language. Now we can proceed to prove

Theorem 2: Λ admits elimination of quantifiers.

Remark: Weissprenning [8] has exhibited an elimination of quantifiers for $C((t))$ in another language. However, this language contains a cross-section, which is a function not elementarily definable in the theory of valued fields; hence, his theory is not an extension by definitions of the theory of $C((t))$ in the language of valued fields.

Theorem 2 will be an immediate application of the Quantifier Elimination Theorem, once we have proved the following two Propositions:

Proposition 1: Λ is model-complete.

Proposition 2: Λ satisifies the isomorphism condition.

If $\mathfrak{F} \models \Lambda$, $|\mathfrak{F}|$ naturally becomes a Hensel field, which we shall denote F, where $\mathfrak{O}^{\mathfrak{F}}$ is the ring of integers; we shall designate by G the value group thus obtained (which is, of course, a Z-group), and by $\mathrm{ord}: F^* \longrightarrow G$ the valuation; $\overline{F}$ will denote the residue class field.

For the proof of Proposition 1 we shall use two Lemmas:

Lemma 5: Let $\mathfrak{F} \models \Lambda$; then then $\mathfrak{F}$ admits a cross--section, i.e., there exists a function $\pi: G \longrightarrow F^*$ which is a group homomorphism and such that $\mathrm{ord} \circ \pi = \mathrm{id}_G$.

Proof: Let U be the group of units in F, i.e., $U = \{u \in F \mid \mathrm{ord}\, u = 0_G\}$.

Claim: U is divisible as a multiplicative subgroup of F^*.

Indeed: let $a \in U$, $n \in Z_{>0}$; show $x^n - a = 0$ has a solution in U: this is an immediate consequence of Hensel's Lemma, since $\overline{F}$ has characteristic zero, and claim is established.

Now consider the short exact sequence

$$\{1\} \longrightarrow U \longrightarrow F^* \xrightarrow{\mathrm{ord}} G \longrightarrow \{0\}$$

Since U is divisible, the sequence splits, and we get a homomorphism $\pi : G \longrightarrow F^*$ such that $\mathrm{ord} \circ \pi = \mathrm{id}_G$

i.e., we get the required cross-section.

q.e.d.

Lemma 6: Let Λ be a theory without finite models in a language of cardinality $\aleph_0$. Then:

Λ is model-complete $\Leftrightarrow$ for any model $\mathfrak{A} \models \Lambda$ of cardinality $\aleph_0$ the Diagram of $\mathfrak{A}$ is complete .

Proof: $\Rightarrow$: obvious, from one of the current definitions of model-completeness.

$\Leftarrow$: let $\mathfrak{B}_1, \mathfrak{B}_2 \models \Lambda$, $\mathfrak{B}_1 \subseteq \mathfrak{B}_2$.

By Robinson's test for model-completeness, it suffices to show that if φ is a primitive sentence in the language of $\mathfrak{B}_1$ and $\mathfrak{B}_2 \models \varphi$, then $\mathfrak{B}_1 \models \varphi$. Indeed: in φ occurr only a finite set S of constants designating elements of $|\mathfrak{B}_1|$. By Skolem-Loewenheim, we can extend S to a model $\mathfrak{B}_3 \models \Lambda$ such that $S \subseteq |\mathfrak{B}_3|$ and $\mathfrak{B}_3 \leq \mathfrak{B}_1 \subseteq \mathfrak{B}_2$ and $\text{card}|\mathfrak{B}_3| = \aleph_0$. By hypothesis, Diag $\mathfrak{B}_3$ is complete. But

$\mathfrak{B}_2 \models \text{Diag } \mathfrak{B}_3$ and

$\mathfrak{B}_2 \models \varphi$, so

$\varphi \in \text{Diag } \mathfrak{B}_3$, i.e., $\mathfrak{B}_3 \models \varphi$

and $\mathfrak{B}_3 \leq \mathfrak{B}_1 \Rightarrow \mathfrak{B}_1 \models \varphi$.

q.e.d.

Proof of Proposition 1: By Lemma 6, it suffices

to show that $\mathfrak{F} \models \Lambda$, card$|\mathfrak{F}| = \aleph_0 \Rightarrow$ Diag $\mathfrak{F}$ complete.
So, assume $\mathfrak{F} \models \Lambda$, card$|\mathfrak{F}| = \aleph_0$. By Loewenheim-Skolem, it suffices to show that

$$\mathfrak{B}_1, \mathfrak{B}_2 \models \text{Diag } \mathfrak{F},\ \text{card}|\mathfrak{B}_1| = \text{card}|\mathfrak{B}_2| = \aleph_0 \quad \Rightarrow \quad \mathfrak{B}_1 \equiv \mathfrak{B}_2$$

We may assume $\mathfrak{F} \subseteq \mathfrak{B}_i$ $(i=1,2)$.

Let I be a countable set , D a non-principal ultrafilter (n.p.u.f.) on I; it now suffices to show that

$$\mathfrak{B}_1{}^I/_D \cong \mathfrak{B}_2{}^I/_D \qquad \text{(as valued fields)} .$$

It is certainly true that $\mathfrak{B}_1{}^I/_D$ and $\mathfrak{B}_2{}^I/_D$ have isomorphic value groups (say by [3, p. 438]); they obviously have isomorphic residue class fields of characteristic zero; then, assuming the Generalized Continuum Hypothesis, our proposition follows from the following version of the theorem in [, p. 491]:

"Let B_i $(i=1,2)$ be ω-pseudo-complete Hensel fields of cardinality $\aleph_1$ with isomorphic value groups G_i of cardinality $\aleph_1$ and isomorphic residue class fields of characteristic zero. Assume there exist normalized cross--sections $\pi_i : G_i \longrightarrow B_i$. Let $F \subseteq B_i$ be a Hensel field with ordF countable; then there exists an isomorphism $\theta : B_1 \longrightarrow B_2$ over F."

q.e.d.

<u>Remark</u>: Λ is thus proved to be model-complete,

and the φ_n are predicates in its language which are elementarily definable in terms of the remaining ones, for the theory of $C((t))$; however, this theory is no longer model-complete just in ordinary valued field language (hence does not admit elimination of quantifers in this language). In our proof of model-completeness we use the presence of the predicate φ_1 when we allow "let $F \subseteq B_i$ be Hensel fields" to signify that the prime elements of F must be prime elements of B_i. Similarly, the existence of the predicates φ_n will be strongly used in the proof that Λ satisfies the isomorphism condition. We need some more Lemmas:

Lemma 7: Let G be a Z-group. H a subgroup of G and $1 \in H$ (1 is the identity of G); then H is a Z-group $\Leftrightarrow$ H is pure in G.

Proof: $\Leftarrow$: want to show $(H:nH)=n$:

$\theta : H/nH \longrightarrow G/nG$ is a well-defined group-homomorphism and because H is pure in G, θ is injective, hence

$(H:nH) \leq (G:nG)=n$

But the diagram

$$\begin{array}{ccc} H & \xrightarrow{i} & G \\ {\scriptstyle \pi_H}\downarrow & & \downarrow{\scriptstyle \pi_G} \\ H/nH & \xrightarrow[\theta]{} & G/nG \end{array}$$

commutes, and since $1 \in H$, $k \in H$, for any $k=1,\dots,n$.

But $\pi_G(j) \neq \pi_G(k)$ for all $j,k=1,\ldots,n$, $j\neq k$

hence $\pi_H(j) \neq \pi_H(k)$ for all $j,k=1,\ldots,n$, $j\neq k$

so $(H:nH) \geq n$.

$\Rightarrow$: say H is a Z-group, $1\in H$, but H is not pure in G. Let $h\in H$ and $g\in G-H$, $h=ng$ $(n\in Z_{>0})$.

We have $(H:nH) = (G/nG) = n$.

By the Euclidean algorithm, we can find $h'\in H$ and $k\in Z_{\geq 0}$ such that $h=nh'+k$ with $0\leq k< n$.
But then $n(g-h')=k$, $g-h'\in G$;
since $k< n$, this is only possible with $k=0$, i.e., $g=h'$, which contradicts $g\in G-H$.

q.e.d.

<u>Lemma 8</u>: If $\mathfrak{F}\models\Lambda$, $a\in F$ then
a has n-th root in F $\Leftrightarrow$ $n|\text{ord } a$ in ord F^*.

<u>Proof</u>: $\Rightarrow$: obvious

$\Leftarrow$: take a cross-section π: ord $F^* \longrightarrow F$ and let $a'=\pi(\text{ord } a)$; we have that $\text{ord } a = n\beta$, for some $\beta\in\text{ord } F^*$; also, $\text{ord } a'=\text{ord } a$, so $a=ua'$, for some u such that $\text{ord } u =0$. By Hensel's Lemma, u has an n-th root, hence it suffices to show that a' has an n-th root. But this is so because $a'= \pi(n\beta) = (\pi\beta)^n$.

q.e.d.

Corollary: If $\mathfrak{F} \models \Lambda$, $a \in |\mathfrak{F}|$ and $\mathfrak{F} \models \varphi_n[a]$, then a has an n-th root in $\mathfrak{F}$.

Remark: If $\mathfrak{F} \models \Lambda$, $\mathfrak{F}$ is "more" than just a field; however, to simplify notation, we shall also denote by $\mathfrak{F}$ the value field which is underlying, by ord the valuation, by $\overline{\mathfrak{F}}$ the residue class field, etc.

Lemma 9: Let $\mathfrak{H} \models \Lambda$, $\mathfrak{F} \subseteq \mathfrak{H}$, and let $\mathfrak{F}$ contain a prime element of $\mathfrak{H}$; then

$\mathfrak{F} \models \Lambda \quad \Leftrightarrow \quad \mathfrak{F}$ is relatively algebraically closed in $\mathfrak{H}$.

Proof: $\Rightarrow$: since $\mathfrak{F}$ is Henselian, it suffices to show that ord $\mathfrak{F}^*$ is pure in ord $\mathfrak{H}^*$ and that $\overline{\mathfrak{F}}$ is relatively algebraically closed in $\overline{\mathfrak{H}}$; the latter is obvious, since $\overline{\mathfrak{F}}$ is algebraically closed. As for ord $\mathfrak{F}^*$ being pure in ord $\mathfrak{H}^*$, this is a direct consequence of Lemma 7.

$\Leftarrow$: $\mathfrak{F}$ is Henselian, $1 \in \text{ord}\,\mathfrak{F}^*$; so, by Lemma 7, it suffices to show that ord $\mathfrak{F}^*$ is pure in ord $\mathfrak{H}^*$: assume $\alpha \in \text{ord}\,\mathfrak{H}^*$, $\beta = n\,\alpha \in \text{ord}\,\mathfrak{F}^*$, $n \in Z_{>0}$;

let $\alpha = \text{ord}\ a$, $a \in \mathfrak{H}$

$\beta = n\alpha = \text{ord}\ b$, $b \in \mathfrak{F}$.

By Lemma 8 b has an n-th root in $\mathfrak{H}$, hence b has an n-th root in $\mathfrak{F}$, so $n \mid \text{ord}\ b$ in ord $\mathfrak{F}^*$.

q.e.d.

Definition 5: Let τ be the type of our language, let $\mathfrak{F}_1, \mathfrak{F}_2$ be two structures of type τ; a function $\theta : \mathfrak{F}_1 \longrightarrow \mathfrak{F}_2$ is defined to be a homo (epi, mono, iso)-morphism in the usual way; θ will be called a value-homo (epi, mono, iso)-morphism whenever it respects the functions in our structures and the $\mathfrak{G}$ relation, i.e., takes integers into integers. To be called a value-homomorphism θ need not take prime elements into prime elements or elements of order n into elements of order n, i.e., the concept of value-homomorphism is weaker than the concept of homomorphism. However, a value-isomorphism is the same thing as an isomorphism.

Lemma 10: suppose $\mathfrak{F} \subseteq \mathfrak{F}' \subseteq \mathfrak{H}_1$ and $\mathfrak{F}', \mathfrak{H}_1, \mathfrak{H}_2 \models \Lambda$ and $\theta : \mathfrak{F} \longrightarrow \mathfrak{H}_2$ is a monomorphism; then, if we can extend θ to a value-monomorphism $\theta' \mathfrak{F}' \longrightarrow \mathfrak{H}_2$, which takes at least one prime element of $\mathfrak{F}'$ (or $\mathfrak{H}_1$) into a prime element of $\mathfrak{H}_2$, then $\theta'(\mathfrak{F}') \models \Lambda$, with $\theta'(\mathfrak{F}')$ having the structure induced by $\mathfrak{H}_2$, i.e., $\theta'(\mathfrak{F}')$ is a submodel of $\mathfrak{H}_2$.

Proof: immediate.

Corollary: To establish the isomorphism condition for Λ, hence prove Proposition 2, we need only prove the following:

Given $\mathfrak{H}_i \models \Lambda$, $\mathfrak{F}_i \subseteq \mathfrak{H}_i$ $(i=1,2)$ and an isomorphism $\theta : \mathfrak{F}_1 \longrightarrow \mathfrak{F}_2$, we can find $\mathfrak{F}'$ and θ' such that:

a) $\mathfrak{F}_1 \subseteq \mathfrak{F}' \subseteq \mathfrak{H}_1$

b) $\mathfrak{F}'$ is relatively algebraically closed in $\mathfrak{H}_1$

c) $\theta' : \mathfrak{F}' \longrightarrow \mathfrak{H}_2$ is a value-monomorphism extending θ and taking some prime element of $\mathfrak{H}_1$ into a prime element of $\mathfrak{H}_2$.

Proof: Lemmas 9, 10.

We now prove three more Lemmas allowing us to carry out the different steps required to extend θ :

Lemma 11: Let $\mathfrak{F}_i$, $\mathfrak{H}_i$, θ be as in the Corollary to Lemma 10; then we can extend θ to a value-monomorphism $\theta' : \mathfrak{F}' \longrightarrow \mathfrak{H}_2$, where $\mathfrak{F}_1 \subseteq \mathfrak{F}' \subseteq \mathfrak{H}_1$ and where θ' takes some prime element of $\mathfrak{H}_1$ into a prime element of $\mathfrak{H}_2$.

Proof: $Z \subseteq \text{ord}\, \mathfrak{H}_i^*$.

Let $A_i = \{ k \in Z_{>0} \mid k \in \text{ord}\mathfrak{F}_i \}$ $(i=1,2)$

Case 1: $A_1 \neq \emptyset$.

Then let $n = \min A_1$ and say $\text{ord}\, r_1 = n$, with $r_1 \in \mathfrak{F}_1$ and let $r_2 = \theta(r_1)$.

If $n=1$ we are done, since θ is an isomorphism, not just a value-isomorphism. For the same reason, observe that $n = \min A_2$ and $\operatorname{ord} \theta(r_1) = \operatorname{ord} r_2 = n$.

So we may assume that $n>1$.

By the Corollary to Lemma 8, r_1 has an n-th root in $\mathfrak{H}_1$, i.e., $x^n - r_1 = 0$ has a solution in $\mathfrak{H}_1$ – say a_1.
But $a_1{}^n = r_1$ hence $\operatorname{nord} a_1 = n$ hence $\operatorname{ord} a_1 = 1$, i.e., a_1 is a prime element of $\mathfrak{H}_1$.

Also, $x^n - r_1$ is irreducible over $\mathfrak{F}_1$; indeed:

$$e(\mathfrak{F}_1(a_1)/\mathfrak{F}_1) \le [\mathfrak{F}_1(a_1):\mathfrak{F}_1] \le n \quad ,$$

but also the order of the equivalence class of $\operatorname{ord} a_1$ in $\operatorname{ord} \mathfrak{F}_1(a)^*/\operatorname{ord} \mathfrak{F}_1{}^*$ must be n (by minimality of n), hence $n|e$, i.e., $n \le e \le n$, so $n = e = [\mathfrak{F}_1(a_1):\mathfrak{F}_1]$.
But θ is an isomorphism, so
$x^n - r_1$ irreducible over $\mathfrak{F}_1 \Rightarrow x^n - r_2$ irreducible over $\mathfrak{F}_2$ and because $\operatorname{ord} r_2 = n$, $x^n - r_2 = 0$ has a solution in $\mathfrak{F}_2$ – – say a_2. We can now define

$$\theta' : \mathfrak{F}_1(a_1) \longrightarrow \mathfrak{H}_2 \quad \text{by}$$

$$\theta(a_1) = a_2 \quad ,$$

which is obviously an algebraic monomorphism.
It also is a value-monomorphism for the following reason:
let $b \in \mathfrak{F}_1(a_1)$: $b = \sum_{i=0}^{n-1} g_i a_1{}^i$, $g_i \in \mathfrak{F}_1$
and $i \ne j \Rightarrow \operatorname{ord}(g_i a_1{}^i) \ne \operatorname{ord}(g_j a_1{}^j)$;
indeed: $\operatorname{ord}(g_i a_1{}^i) = \operatorname{ord} g_i + i \operatorname{ord} a_1 = \operatorname{ord} g_i + i$

$\mathrm{ord}\,(g_j a_1{}^j) = \mathrm{ord}\, g_j + j$, and

$i \neq j \Rightarrow 0 < |i-j| < n$ so

$\mathrm{ord}\,(g_i a_1{}^i) = \mathrm{ord}\,(g_j a_1{}^j) \Rightarrow i-j = \mathrm{ord}\, g_i - \mathrm{ord}\, g_j \in \mathrm{ord}\, \mathfrak{F}_1{}^*$

which is a contradiction; hence

$\mathrm{ord}\, b = \min\,\{\mathrm{ord}\, g_i + i \mid i=0,\ldots,n-1\}$

and similarly $\mathrm{ord}\,\theta'(b) = \min\,\{\mathrm{ord}\,\theta(g_i)+i \mid i=0,\ldots,n-1\}$.

Say $\mathrm{ord}\, b = \mathrm{ord}\, g_{i_0} + i_0$; since θ is a value-monomorphism,

$\mathrm{ord}\, g_i + i > \mathrm{ord}\, g_{i_0} + i_0 \Rightarrow \mathrm{ord}\, g_i - \mathrm{ord}\, g_{i_0} > i_0 - i \Rightarrow$

$\Rightarrow \mathrm{ord}\,(g_i/g_{i_0}) > i_0 - i \Rightarrow \mathrm{ord}\,\theta(g_i/g_{i_0}) > i_0 - j \Rightarrow$

$\Rightarrow \mathrm{ord}\,\theta(g_i) + i > \mathrm{ord}\,\theta(g_{i_0}) + i_0$ so

$\mathrm{ord}\,\theta'(b) = \mathrm{ord}\,\theta\,(g_{i_0}) + i_0$

and since θ is a value-monomorphism so is θ'.

<u>Case 2</u>: $A_1 = \emptyset$.

In this case, because θ is a monomorphism , $A_2=\emptyset$

Hence, if t_1 is a prime element of $\mathfrak{K}_1$, t_1 is transcendental over $\mathfrak{F}_1$, and by a reasoning perfectly similar to Case 1 , we get θ'.

q.e.d.

<u>Remark</u>: Let $\mathfrak{K}_i \models \Lambda$, $(i=1,2)$, $\mathfrak{K}_1 \supseteq \mathfrak{F}$ Henselian, and $\theta : \mathfrak{F} \longrightarrow \mathfrak{K}_2$ a value-monomorphism. Since char $\bar{\mathfrak{F}}=0$, we

may assume $\overline{\mathfrak{F}} \subseteq \mathfrak{F}$ by identifying $\overline{\mathfrak{F}}$ with a subfield of $\mathfrak{F}$ maximal with respect to having trivial valuation. We can extend $\overline{\mathfrak{F}}$ to a subfield $\overline{\mathfrak{H}}_1$ of $\mathfrak{H}_1$ maximal with respect to the same property in $\mathfrak{H}_1$, hence isomorphic to the residue class field of $\mathfrak{H}_1$; so, we get

$$\overline{\mathfrak{F}} \subseteq \mathfrak{F} \subseteq \mathfrak{H}_1 \quad , \quad \overline{\mathfrak{F}} \subseteq \overline{\mathfrak{H}}_1 \subseteq \mathfrak{H}_1$$

Now $\theta(\overline{\mathfrak{F}})$ will have the trivial valuation, hence may be extended to $\overline{\mathfrak{H}}_2$, i.e., we write

$$\theta(\overline{\mathfrak{F}}) \subseteq \overline{\theta(\overline{\mathfrak{F}})} \subseteq \overline{\mathfrak{H}}_2 \subseteq \mathfrak{H}_2 \quad .$$

In this sense, we get

<u>Lemma 12</u>: With the above notation, let $a \in \overline{\mathfrak{H}}_1 - \overline{\mathfrak{F}}$, a algebraic over $\overline{\mathfrak{F}}$; then we extend θ to

$$\theta' : \mathfrak{F}(a) \longrightarrow \mathfrak{H}_2 \quad , \text{ a value-monomorphism.}$$

<u>Proof</u>: Let $f = \text{irred}(a, \mathfrak{F})$

$$g = \text{irred}(a, \overline{\mathfrak{F}})$$

then $f|g$; let f^θ be the transformed polynomial of f by θ: f^θ will be irreducible over $\theta(\mathfrak{F})$, $f^\theta | g^\theta$ and

$$g^\theta \in \theta(\overline{\mathfrak{F}})[x] \subseteq \overline{\mathfrak{H}}_2[x] \subseteq \mathfrak{H}_2[x] \quad ;$$

but $\overline{\mathfrak{H}}_2$ is algebraically closed, hence g^θ splits over $\overline{\mathfrak{H}}_2 \subseteq \mathfrak{H}_2$, hence f^θ, which is irreducible over $\theta(\mathfrak{F})$, has a root in $\mathfrak{H}_2$; let $b \in \mathfrak{H}_2$ be such that $f^\theta(b) = 0$. Now we can define $\theta' : \mathfrak{F}(a) \longrightarrow \mathfrak{H}_2$ by

$$\theta'(a) = b \quad ;$$

of course, θ' is an algebraic monomorphism. It is a value--monomorphism because $\mathfrak{F}$ is Henselian, hence has the uniqueness property.

q.e.d.

<u>Lemma 13</u>: Suppose $\overline{\mathfrak{F}} \subseteq \mathfrak{F} \subseteq \mathfrak{H}_1 \models \Lambda$, $\mathfrak{H}_2 \models \Lambda$, $\mathfrak{F}$ Henselian, $\overline{\mathfrak{F}}$ algebraically closed, and $\theta : \mathfrak{F} \longrightarrow \mathfrak{H}_2$ value- monomorphism. Suppose $\alpha \in$ divisible closure of ord $\mathfrak{F}^*$ in ord $\mathfrak{H}_1^*$; let n be the smallest positive integer such that $n\alpha \in$ ord $\mathfrak{F}^*$; then we can find $a \in \mathfrak{H}_1$ and θ' such that

a) a is algebraic over $\mathfrak{F}$

b) ord $a = \alpha$

c) $\theta' : \mathfrak{F}(a) \longrightarrow \mathfrak{H}_2$ is a value-monomorphism extending θ .

<u>Proof</u>: Say ord $b = n\alpha$, $b \in \mathfrak{F}$

then b has n-th root in $\mathfrak{H}_1$ - say $a^n = b$, $a \in \mathfrak{H}_1$

then ord $a = \alpha$, a algebraic over $\mathfrak{F}$.

<u>Claim</u>: $f(x) = x^n - b$ is irreducible over $\mathfrak{F}$.

Indeed: say $g = \text{irred}(a, \mathfrak{F})$, deg $g < n$.

Then, since $\overline{\mathfrak{F}}$ is algebraically closed, the field extension $\mathfrak{F}(a)/\mathfrak{F}$ is totally ramified and

$$1 \leq e = e(\mathfrak{F}_1(a)/\mathfrak{F}) = \deg g < n,$$

but $e \cdot \text{ord } a \in \text{ord } \mathcal{F}^*$,which is a contradiction.

So $\text{irred}(a,\mathcal{F}) = x^n - b$, but

$x^n - b$ irreducible over $\mathcal{F}$ $\Rightarrow$ $x^n - \theta(b)$ irreducible over $\theta(\mathcal{F})$

Claim: $x^n - \theta(b)$ has a solution in $\mathcal{H}_2$.

Indeed: $\text{ord } \theta(b) = \mu(\text{ord } b) = \mu(n\alpha) = n\mu(\alpha)$, where μ is the ordered group isomorphism induced by θ between $\text{ord } \mathcal{F}^*$ and $\text{ord } \theta(\mathcal{F})^*$.

So $\theta(b)$ has n-th root in $\mathcal{H}_2$, say c , and we can extend θ to $\theta' : \mathcal{F}(a) \longrightarrow \mathcal{H}_2$ by

$$\theta'(a) = c \ .$$

θ' is obviously an algebraic monomorphism. Again, it is a value-monomorphism because $\mathcal{F}$ is Henselian, hence has the uniqueness property.

q.e.d.

We are now ready to start the

Proof of Proposition 2: Let $\mathcal{F}_1 \subseteq \mathcal{H}_1 \models \Lambda$, and let $\theta : \mathcal{F}_1 \longrightarrow \mathcal{F}_2$ be an isomorphism. By Lemma 11 we can extend θ to $\theta_{\mathcal{G}} : \mathcal{G} \longrightarrow \mathcal{H}_2$, where $\mathcal{F}_1 \subseteq \mathcal{G} \subseteq \mathcal{H}_1$ and $\theta_{\mathcal{G}}$ takes some prime element of $\mathcal{H}_1$ into a prime element of $\mathcal{H}_2$. Since $\mathcal{H}_1$ and $\mathcal{H}_2$ are Henselian, we may extend $\theta_{\mathcal{G}}$ to the Henselization of $\mathcal{G}$, $\mathcal{E}$, i.e., we get

$$\theta_{\mathcal{E}} : \mathcal{E} \longrightarrow \mathcal{H}_2 \ ,$$

where $\theta_{\mathcal{E}}$ extends θ, $\mathcal{F}_1 \subseteq \mathcal{E} \subseteq \mathcal{H}_1$, and $\theta_{\mathcal{E}}$ takes a prime element in $\mathcal{H}_1$ to a prime element in $\mathcal{H}_2$, and $\mathcal{E}$ is Henselian.

Now, as in Lemma 12, we may consider

$\overline{\mathcal{E}} \subseteq \mathcal{E} \subseteq \mathcal{H}_1$, $\overline{\mathcal{E}} \subseteq \overline{\mathcal{H}}_1 \subseteq \mathcal{H}_1$ and let

$\tilde{\overline{\mathcal{E}}}^r$ denote the relative algebraic closure of $\overline{\mathcal{E}}$ in $\overline{\mathcal{H}}_1$.

Using Lemma 9, by an easy transfinite induction we can now extend $\theta_{\mathcal{E}}$ to

$$\theta_{\mathcal{L}} : \mathcal{L} \longrightarrow \mathcal{H}_2 \text{ , where}$$

$$\mathcal{L} = \mathcal{E} \cdot \tilde{\overline{\mathcal{E}}}^r \subseteq \mathcal{H}_1 \text{ .}$$

Note that $\mathcal{L}$ is algebraic over $\mathcal{E}$, hence $\overline{\mathcal{L}}$ is algebraic over $\overline{\mathcal{E}}$, and so $\overline{\mathcal{L}}$ is algebraically closed in $\overline{\mathcal{H}}_1$; but this implies that $\overline{\mathcal{L}}$ is algebraically closed. We may also assume that $\mathcal{L}$ is Henselian (otherwise, we simply take its Henselization).

We are now in a position to apply Lemma 13: well-order the divisible closure of ord $\mathcal{L}^*$ in ord $\mathcal{H}_1^*$, and by transfinite induction extend $\theta_{\mathcal{L}}$ to

$$\theta' : \mathcal{F}' \longrightarrow \mathcal{H}_2 \qquad \text{such that}$$

$\mathcal{F} \subseteq \mathcal{F}' \subseteq \mathcal{H}_1$, and $\overline{\mathcal{F}'}$ is algebraically closed, and ord $\mathcal{F}'^*$ is pure in ord $\mathcal{H}_1^*$, and $\mathcal{F}'$ is Henselian, and θ' takes some prime element of $\mathcal{H}_1$ into a prime element of $\mathcal{H}_2$.

But because $\mathcal{F}'$ is Henselian, $\overline{\mathcal{F}'}$ is algebraically closed and ord $\mathcal{F}'^*$ is pure in ord $\mathcal{H}_1^*$, $\mathcal{F}'$ must be relatively algebraically closed in $\aleph_1$. Hence, by the Corollary to Lemma 10, this proves the Proposition.

q.e.d.

V - A language in which the theory of finite fields admits elimination of quantifiers

We now describe a language and theory of finite fields in this language which admits elimination of quantifiers:

Language: function symbols: +(addition)

·(multiplication)

−(subtraction)

constant symbols: 0(additive identity)

1(unity)

predicate symbols: =(equality)

This language is the ordinary field language; henceforth, we denote it L_τ. Now, we introduce for every positive integer n an n+1-ary relation symbol: φ_n. L_τ, denotes the language obtained by adjoining the predicate symbols $\{\varphi_n | n \in Z_{>0}\}$ to L_τ.

We now denote

Σ - the theory of finite fields in L_τ (i.e., the set of sentences of L_τ satisfied by all finite fields)

π - the theory of pseudo-finite fields in L_τ (i.e., the set of sentences of L_τ satisfied by all the infinite models of Σ).

In [2, p. 255, Thm 5], we can find a recursive axiomatization for π.

Naturally, $\Sigma \subset \pi$, i.e., $\mathfrak{F} \models \pi \Rightarrow \mathfrak{F} \models \Sigma$.

Now, we let π' and Σ' be the theories in the language $L_{\tau'}$ obtained by taking for axioms respectively

$$\pi \cup \{\forall x_0 \ldots \forall x_n(\varphi_n(x_0,\ldots,x_n) \longleftrightarrow \exists y(x_n y^n + \ldots + x_0 = 0)) \mid n \in Z_{>0}\}$$

and

$$\Sigma \cup \{\forall x_0 \ldots \forall x_n((\neg \exists y_1 \ldots \exists y_n(\bigwedge_{\substack{i,j=1\\ i\neq j}}^{n} y_i \neq y_j \wedge \forall y(\bigvee_{i=1}^{n} y = y_i)) \rightarrow$$

$$\rightarrow (\varphi_n(x_0,\ldots,x_n) \leftrightarrow \exists y(x_n y^n + \ldots + x_0 = 0))) \wedge$$

$$\wedge (\exists y_1 \ldots \exists y_n(\bigwedge_{\substack{i,j=1\\ i\neq j}}^{n} y_i \neq y_j \wedge \forall y(\bigvee_{i=1}^{n} y = y_i)) \rightarrow$$

$$\rightarrow (\varphi_n(x_0,\ldots,x_n) \leftrightarrow \forall y(y = 0 \vee \bigvee_{i=1}^{n-1} y = x_0^{\,i})))) \mid n \in Z_{>0}\}$$

Remarks:

a) Σ' is an extension by definitions of Σ; given $\mathfrak{F} \models \Sigma$, $\mathfrak{F}$ becomes a model of Σ' in a canonical way:

Case 1: $\mathfrak{F}$ is infinite - then we define the n+1-ary relation $\varphi_n^{\mathfrak{F}}$ by

$(a_0,\ldots,a_n) \in \varphi_n^{\mathfrak{F}} \Leftrightarrow$ the polynomial $a_n y^n + \ldots + a_0$ has a root in $\mathfrak{F}$

Case 2: $\mathfrak{F}$ is finite with k elements - then $\varphi_n^{\mathfrak{F}}$ is defined as before if $n \neq k$, and $\varphi_k^{\mathfrak{F}}$ is defined by

$$(a_0, \ldots, a_k) \in \varphi_k^{\mathfrak{F}} \Leftrightarrow a_0 \text{ is a generator of } \mathfrak{F}^*.$$

b) $\mathfrak{F} \models \pi' \Leftrightarrow \mathfrak{F} \models \Sigma'$ and $\mathfrak{F}$ is infinite

c) $\mathfrak{F} \models \Sigma' \Rightarrow (\mathfrak{F}$ finite with k elements $\Leftrightarrow (1,0,\ldots,0,1) \in \varphi_k^{\mathfrak{F}})$

Lemma 14: π' admits elimination of quantifiers $\Leftrightarrow$ $\Leftrightarrow \Sigma'$ admits elimination of quantifiers.

Proof: $\Leftarrow$: obvious, since $\Sigma' \subset \pi'$.

$\Rightarrow$: by Theorem 1, it suffices to show that

i) π' model-complete $\Rightarrow$ Σ' model-complete and

ii) π' satisfies weak isomorphism condition $\Rightarrow$ Σ' satisfies weak isomorphism condition.

i): Let $\mathfrak{F}_j \models \Sigma'$ $(j=1,2)$ and $\mathfrak{F}_1 \subseteq \mathfrak{F}_2$.

If $\mathfrak{F}_1$ is infinite, $\mathfrak{F}_j \models \pi'$ $(j=1,2)$ and $\mathfrak{F}_1 \leq \mathfrak{F}_2$ follows from hypothesis.

If $\mathfrak{F}_1$ is finite with k elements,

$(1,0,\ldots,0,1) \notin \varphi_k^{\mathfrak{F}_1} = \varphi_k^{\mathfrak{F}_2} \cap \mathfrak{F}_1^{\,k} \Rightarrow (1,0,\ldots,0,1) \notin \varphi_k^{\mathfrak{F}_2} \Rightarrow$

$\Rightarrow \mathfrak{F}_2$ finite with k elements $\Rightarrow \mathfrak{F}_1 = \mathfrak{F}_2$.

ii) Let $\mathfrak{F}_j \models \Sigma'$ $(j=1,2)$ and θ an isomorphism of non-empty substructures:

If both $\mathfrak{F}_1$ and $\mathfrak{F}_2$ are infinite, $\mathfrak{F}_j \models \pi'$, and θ can be extended by hypothesis.

If $\mathfrak{F}_1$ is finite with k elements,

$(1,0,\ldots,0,1)\notin\varphi_k^{\mathfrak{F}_1} \Rightarrow (1,\ldots,0,1)\notin\varphi_k^{\mathfrak{F}_2}$ (because θ is an isomorphism) $\Rightarrow$ $\mathfrak{F}_2$ is finite with k elements.

Hence θ is an isomorphism of two subrings of two fields with k elements, the subrings containig the prime fields; so, obviously, θ can be extended to the fields with k elements.

If $\mathfrak{F}_2$ is finite with k elements a similar reasoning holds.

q.e.d.

<u>Theorem 3</u>: π' admits elimination of quantifiers.

<u>Proof</u>: by Theorem 1, this proof is immediately reduced to the proof of the following two Lemmas:

<u>Lemma 15</u>: π' is model-complete.

<u>Lemma 16</u>: π' satisfies the weak isomorphism condition.

For the proofs of Lemmas 15 and 16 we need

<u>Lemma 17</u>: Let $\mathfrak{F}_i \models \pi'$ $(i=1,2)$, and assume that $\mathfrak{F}_1$ is a subfield of $\mathfrak{F}_2$; then

$\mathfrak{F}_1 \subseteq \mathfrak{F}_2$ (i.e., for all $n\in Z_{>0}$, $\varphi_n^{\mathfrak{F}_1} = \varphi_n^{\mathfrak{F}_2} \cap \mathfrak{F}_1^{n+1}$) $\Leftrightarrow$

$\Leftrightarrow$ $\mathfrak{F}_1$ is relatively algebraically closed in $\mathfrak{F}_2$.

Proof: ⇒: say $\alpha \in \mathfrak{F}_2 - \mathfrak{F}_1$, α algebraic over $\mathfrak{F}_1$;
let $f = \text{irred}(\alpha, \mathfrak{F}_1) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathfrak{F}_1[x]$ $(n>1)$
then $(a_0, \dots, a_{n-1}) \notin \varphi_n^{\mathfrak{F}_1} = \varphi_n^{\mathfrak{F}_2} \cap \mathfrak{F}_1^{n+1}$ because f has no roots in $\mathfrak{F}_1$, but since $f(\alpha)=0$, $(a_0, \dots, a_{n-1}, 1) \in \varphi_n^{\mathfrak{F}_2} \cap \mathfrak{F}_1^{n+1}$ which is a contradiction.

⇐: $(a_0, \dots, a_n) \in \varphi_n^{\mathfrak{F}_1}$ ⇔ $a_n x^n + \dots + a_0 = f(x)$ has a root in $\mathfrak{F}_1$ ⇔ $f(x)$ has a root in $\mathfrak{F}_2$ (since $\mathfrak{F}_1$ is relatively algebraically closed in $\mathfrak{F}_2$ ⇔

⇔ $(a_0, \dots, a_n) \in \varphi_n^{\mathfrak{F}_2} \cap \mathfrak{F}_1^{n+1}$

q.e.d.

Proof of Lemma 15: since π' has no finite models, by Lemma 6, to prove that π' is model-complete it suffices to show that

$$\mathfrak{F} \models \pi' \text{ and card } \mathfrak{F} = \aleph_0 \Rightarrow \pi' \cup \text{Diag } \mathfrak{F} \text{ complete:}$$

Let $\mathfrak{F}_1, \mathfrak{F}_2 \models \pi' \cup \text{Diag } \mathfrak{F}$; we we want to show that

$$\mathfrak{F}_1 \equiv \mathfrak{F}_2 \quad (\text{in language } L_{\tau''} \text{ of } \pi' \cup \text{Diag } \mathfrak{F}).$$

We may assume that $\mathfrak{F} \subseteq \mathfrak{F}_i$ $(i=1,2)$, and by Loewenheim--Skolem, we amy assume card $\mathfrak{F}_i = \aleph_0$ $(i=1,2)$.

Now let D be a non-principal ultrafilter on the set of positive integers I; let

$$\mathfrak{E}_i = \mathfrak{F}_i^{I}/_D \qquad (i=1,2).$$

Since $\mathcal{E}_i$ is pseudo-finite, $\mathcal{E}_i$ is hyper-finite; so we have $\mathfrak{F} \subseteq \mathfrak{F}_i \leq \mathcal{E}_i$, with $\mathcal{E}_i$ hyper-finite; by Lemma 17, $\mathfrak{F}$ is relatively algebraically closed in $\mathcal{E}_i$ $(i=1,2)$; and also card $\mathcal{E}_1$ = card $\mathcal{E}_2$ > card $\mathfrak{F}$. Hence, by [2, p.247, Thm 1], $\mathcal{E}_1$ and $\mathcal{E}_2$ are isomorphic as fields over $\mathfrak{F}$; but this implies that they are isomorphic as structures of type τ'', since the $\varphi_n{}^{\mathcal{E}_i}$ relations are "algebraic", i.e., preserved under field-isomorphisms. Hence

$$\mathfrak{F}_1 \leq \mathcal{E}_1 \cong \mathcal{E}_2 \geq \mathfrak{F}_2 \quad , \text{ so}$$

$$\mathfrak{F}_1 \equiv \mathfrak{F}_2 \ .$$

q.e.d.

Proof of Lemma 16: Let $\mathcal{E}_i \models \pi'$ $(i=1,2)$, $\mathfrak{D}_i \subseteq \mathcal{E}_i$ and $\theta : \mathfrak{D}_1 \longrightarrow \mathfrak{D}_2$ be an isomorphism (of structures of type τ').

$\mathfrak{D}_i$ is a substructure of $\mathcal{E}_i$, hence an integral domain. Let $\mathfrak{F}_i$ be the quotient field of $\mathfrak{D}_i$: $\mathfrak{F}_i \subseteq \mathcal{E}_i$, and certainly θ extends to a field-isomorphism

$$\theta : \mathfrak{F}_1 \longrightarrow \mathfrak{F}_2 \ .$$

θ is also an isomorphism of structures of type τ', as can be easily checked; so θ has the following property:

$$a_n x^n + \ldots + a_0 \in \mathfrak{F}_1[x] \text{ has a zero in } \mathcal{E}_1 \iff \theta(a_n)x^n + \ldots + \theta(a_0) \in \mathfrak{F}_2[x] \text{ has a zero in } \mathcal{E}_2 \ .$$

Now let $\mathfrak{F}_i^r$ be the relative algebraic closure of $\mathfrak{F}_i$ in $\mathcal{E}_i$.
Of course, we again have that

$a_n x^n + \ldots + a_0 \in \mathfrak{F}_1[x]$ has a zero in $\mathfrak{F}_1^r \Leftrightarrow \theta(a_n)x^n + \ldots + \theta(a_0) \in \mathfrak{F}_2[x]$ has a zero in $\tilde{\mathfrak{F}}_1^r$.

Hence by [1, p. 172, Lemma 5], we can extend θ to a field-isomorphism

$$\theta : \mathfrak{F}_1^r \longrightarrow \tilde{\mathfrak{F}}_2^r .$$

θ is still an isomorphism of structuresof type τ' because now

$(a_0, \ldots, a_n) \in \varphi_n^{\mathfrak{F}_1^r} = \varphi_n^{\mathcal{E}_1} \cap \tilde{\mathfrak{F}}_1^{r\,n+1} \Leftrightarrow a_n x^n + \ldots + a_0$ has a zero in $\mathcal{E}_1 \Leftrightarrow a_n x^n + \ldots + a_0$ has a zero in $\mathfrak{F}_1^r \Leftrightarrow$

$\Leftrightarrow \theta(a_n)x^n + \ldots + \theta(a_0)$ has a zero in $\tilde{\mathfrak{F}}_2^r \Leftrightarrow$

$\Leftrightarrow \theta(a_n)x^n + \ldots + \theta(a_0)$ has a zero in $\mathcal{E}_2 \Leftrightarrow$

$\Leftrightarrow (\theta(a_0), \ldots, \theta(a_n)) \in \varphi_n^{\mathcal{E}_2} \cap \tilde{\mathfrak{F}}_2^{r\,n+1} = \varphi_n^{\mathfrak{F}_1^r}$.

Let $\alpha = \text{card } \mathcal{E}_2$. By upward Loewenhweim-Skolem, let $\mathcal{H}_2'$ be such that $\mathcal{E}_2 \leq \mathcal{H}'_2$ and card $\mathcal{H}'_2 = \alpha^+$.
Now, let $\mathcal{H}_2$ be such that $\mathcal{E}_2 \leq \mathcal{H}'_2 \leq \mathcal{H}_2$, card $\mathcal{H}_2 = \alpha^+$ and $\mathcal{H}_2$ is saturated.

Then we have that

$\mathcal{E}_2 \leq \mathcal{H}_2$, $\mathcal{H}_2$ is hyper-finite, card $\mathcal{H}_2 = \alpha^+$ and $\tilde{\mathfrak{F}}_2^r$ is relatively algebraically closed in $\mathcal{H}_2$ (because $\mathcal{E}_2 \leq \mathcal{H}_2$).

Let $\beta = \text{card } \tilde{\mathfrak{F}}_1^r = \text{card } \mathfrak{F}_2^r \leq \alpha < \alpha^+$;

By downward Loewenheim-Skolem, let $\mathfrak{H}_1$ be such that $\tilde{\mathfrak{F}}_1^r \subseteq \mathfrak{H}_1 \leq \mathcal{E}_1$ and card $\mathfrak{H}_1 = \beta$. Then we know that $\mathfrak{H}_1$ is quasi-finite (because $\mathfrak{H}_1 \leq \mathcal{E}_1 \Rightarrow \mathfrak{H}_1 \models \pi'$), card$\mathfrak{H}_1$ < card $\mathfrak{H}_2$, and $\tilde{\mathfrak{F}}_1^r$ is relatively algebraically closed in $\mathfrak{H}_1$.

So we can extend θ to a field-monomorphism

$\theta : \mathfrak{H}_1 \longrightarrow \mathfrak{H}_2$ such that

$\theta(\mathfrak{H}_1)$ is relatively algebraically closed in $\mathfrak{H}_2$.

If we take $\varphi_n^{\theta(\mathfrak{H}_1)}$ to be defined on $\theta(\mathfrak{H}_1)$ through θ, we get, since $\pi' \models \mathfrak{H}_1$, that $\pi' \models \theta(\mathfrak{H}_1)$.

But now $\mathfrak{H}_2, \theta(\mathfrak{H}_1) \models \pi'$, $\theta(\mathfrak{H}_1)$ is a subfield of $\mathfrak{H}_2$, and is relatively algebraically closed in $\mathfrak{H}_2$. Then Lemma 17 applies to show that $\theta(\mathfrak{H}_1) \subseteq \mathfrak{H}_2$, i.e., with $\varphi_n^{\theta(\mathfrak{H}_1)}$ defined as above, $\theta(\mathfrak{H}_1)$ is a submodel of $\mathfrak{H}_2$.

Hence we have proved the weak isomorphism condition.

q.e.d.

V - Sets definable over a finite field : the rationality of their Poincare series

In this chapter, we shall use the following

Notation: L_τ - ordinary field language, as described in Chapter IV

$L_{\tau'}$ - ordinary field language with all the $n+1$-ary relations φ_n adjoined ($n \in Z_{>0}$)

Σ - theory of finite fields in L_τ

Σ' - theory of finite fields with defining axioms for φ_n adjoined (as in Chapter IV)

k - finite field of cardinality q

k_s - unique extension of k of degree s

$\bar{k}$ - algebraic closure of k

Definition 5: Let $U \subseteq \bar{k}^r$; then U is called a definable r-set over k $\Leftrightarrow$ there exists a formula φ in $L_{\tau,k}$ with r free variables such that

$$U_s \overset{def}{=} k_s^r \cap U = \{(a_1,\ldots,a_r) \in k_s{}^r \mid k_s \models \varphi[a_1,\ldots,a_r]\} .$$

We then say that U is defined by φ .

Remark: If U is definable over k, the formula φ defining U is not unique: in fact, every formula representing the same element in the r-th Lindenbaum algebra of Σ will also define U.

<u>Definition 6</u>: Say $U \subseteq \bar{K}^r$ is definable, defined by φ. We have $U_s = \{(a_1,\ldots,a_r)\in k_s{}^r \mid k_s \models \varphi[a_1,\ldots,a_r]\}$;
The <u>zeta-function</u> of U is defined by

$$\zeta_U(t) = \exp \sum_{s=1}^{\infty} \frac{N_s(U)}{s} t^s ,$$

where $N_s(U) = \# U_s$ = cardinality of U_s.

The <u>Poincare series</u> of U is defined by

$$\pi_U(t) = t \frac{d}{dt} \log \zeta_U(t) = \sum_{s=1}^{\infty} N_s(U)\ t^s .$$

The main result of this section is

<u>Theorem 4</u>: The Poincare series of a definable set is rational.

To prove it, we first reduce Theorem 4 to

<u>Lemma 18</u>: Let U be a definable set, defined by φ over the field k with q elements; let $m = \max\{n\in Z_{>0} \mid \varphi_n$ occurrs in $\varphi\}$; if $q>m$, then the Poincare series of U is rational.

Theorem 4 is indeed a consequence of Lemma 18:

Suppose U is defined by φ, m is as in Lemma 18, but $q\le m$; say $q=p^t$, p a prime, amd let t' be the samallest positive integer such that $t \mid t'$ and $q'=p^{t'}>m$. Then $q' = p^{t'} = (p^t)^{t'/t} = q^{t'/t}$ and

$$\pi_U(t) = \sum_{s=1}^{\infty} N_s(U)\ t^s = \sum_{s=1}^{t'/t} N_s(U)\ t^s + \sum_{s=t'/t+1}^{\infty} N_s(U)\ t^s$$

Now, if U' is the set defined by φ over $k'=k_{t'/t}$, we naturally have $s > t'/t \Rightarrow N_s(U) = N_s(U')$, and by Lemma 18 $\pi_{U'}(t)$ is rational, i.e., $\sum_{s=t'/t+1}^{\infty} N_s(U)\ t^s$ is rational. But certainly $\sum_{s=1}^{t'/t} N_s(U)\ t^s$ is rational, being a finite sum; hence, assuming Lemma 18, $\pi_U(t)$ is rational, for any definable set U.

All our efforts will now be directed towards the proof of Lemma 18. It will be accomplished by succesive reductions and one final computation.

<u>Definition 7</u>: A definable set $V \subseteq k^r$ will be called a <u>variety</u> over k if it can be defined by a formula of type

$$\bigwedge_{i=1}^{n} p_i(x_1,\dots,x_r)=0 \qquad , \text{ with}$$

$p_i(x_1,\dots,x_r) \in k[x_1,\dots,x_r]$ $(i=1,\dots,n)$.

<u>Definition 8</u>: A definable set $P \subseteq k^r$ will be called <u>primitive</u> if it can be defined by a formula of type

$$\bigwedge_{i=1}^{n} p_i(x_1,\dots,x_r)=0 \ \wedge \ \bigwedge_{i=1}^{m} q_i(x_1,\dots,x_r)\neq 0$$

with $p_i(\overline{x}),\ q_j(\overline{x}) \in k[\overline{x}]$ $(i=1,\dots,n\ ;\ j=1,\dots,m)$.

Definition 9: A definable set will be called constructible if it can be defined by a formula which is quantifier-free in $L_{T,k}$.

Lemma 19 : If $U \subseteq k^r$ is a constructible set, then $\zeta_U(t)$ is a rational function. Hence, so is $\pi_U(t)$.

Proof: Dwork [5] showed that $\zeta_{V-W}(t)$ is rational, for V,W varieties.

Any primitive set P is a difference of varieties: in fact, if P is defined by $\bigwedge_{i=1}^{n} p_i(\overline{x})=0 \wedge \bigwedge_{j=1}^{m} q_j(\overline{x})\neq 0$, we have that $\Sigma \vdash (\bigwedge_{i=1}^{n} p_i(\overline{x}) \wedge \bigwedge_{j=1}^{m} q_j(\overline{x})\neq 0) \leftrightarrow (\bigwedge_{i=1}^{n} p_i(\overline{x})=0 \wedge \prod_{j=1}^{m} q_j \neq 0)$

So if V is defined by $\bigwedge_{i=1}^{n} p_i(\overline{x})=0$ and

W is defined by $(\prod_{j=1}^{m} q_j(\overline{x}))=0$, then

P = V-W. So the Lemma holds for primitive sets.

Now observe that the intersection of primitve sets is primitive; on the other hand, any constructible set is the union of primitive sets, i.e., if U is constructible, there exist primitive sets $P_1,\ldots,P_n$ such that $U = \bigcup_{i=1}^{n} P_i$ and so $U_s = \bigcup_{i=1}^{n} (P_i)_s$; it is easily verified that

$$\#\left(\bigcup_{i=1}^{n} (P_i)_s\right) = \sum_{B\subseteq\{1,\ldots,n\}} (-1)^{\#B}\, \#\left(\bigcap_{i\in B} (P_i)_s\right) \quad \text{, i.e.,}$$

$$N_s(U) = \sum_{B\subseteq\{1,\ldots,n\}} (-1)^{\#B}\, N_s\left(\bigcap_{i\in B} P_i\right) = \sum_{B\subseteq\{1,\ldots,n\}} (-1)^{\#B} N_s(P_B),$$

where $P_B = \bigcap_{i\in B} P_i$, for all $B\subseteq\{1,\ldots,n\}$.

But P_B is a primitive set, hence $\zeta_{P_B}(t)$ is rational,

and so $$\zeta_U(t) = \prod_{B\subseteq\{1,\ldots,n\}} \zeta_{P_B}(t)^{(-1)^{\#B}}$$

is rational.

q.e.d.

We shall now reduce the proof of Lemma 18 to

<u>Lemma 20</u>: Let $U\subseteq k^r$ be definable, defined by an atomic formula in $L_{\tau',k}$ of type

$$\varphi_n(p_0(x_1,\ldots,x_r),\ldots,p_n(x_1,\ldots,x_r)) \text{ , with}$$

$p_i(x_1,\ldots,x_r) \in k[x_1,\ldots,x_r]$ $(i=1,\ldots,n)$

(obviously, we mean that U is defined by a formula of $L_{\tau,k}$ equivalent to $\varphi_n(p_0(\overline{x}),\ldots,p_n(\overline{x}))$). Suppose $n>q=\#k$; then $\pi_U(t)$ is rational.

We state the reduction of Lemma 18 to Lemma 20 as

<u>Lemma 21:</u> Lemma 20 $\Rightarrow$ Lemma 18.

<u>Proof</u>: Let U be a definable set; it has been proved in Chapter IV that Σ' admits elimination of

quantifiers, hence we may assume U defined by a quantifier--free formula φ in the language $L_{T',k}$, i.e., U is the union of sets defined by formulae of type

$$(*) \qquad \bigwedge_{i=1}^{\mu} p_i(\overline{x})=0 \wedge \bigwedge_{j=1}^{\nu} \varphi_{n_j}(p_{n_j,0}(\overline{x}),\dots,p_{n_j,n_j}(\overline{x})) \wedge$$

$$\wedge \bigwedge_{k=1}^{\xi} q_k(\overline{x})\neq 0 \wedge \bigwedge_{m=1}^{\eta} \neg\varphi_{n_m}(p_{n_m,0}(\overline{x}),\dots,p_{n_m,n_m}(\overline{x})) \; .$$

Again, since intersections of sets defined by formulae of type (*) are again defined by formulae of type (*), it will suffice to prove that the ζ-functions of sets defined by formulae of type (*) have the required property.

As before, we amy assume $\xi\leq 1$ by replacing $\bigwedge_{k=1}^{\xi} q_k(\overline{x})\neq 0$ by $\prod_{k=1}^{\xi} q_k(\overline{x}) \neq 0$; similarly. we may assume $\eta\leq 1$; indeed:

$$\Sigma\vdash \bigwedge_{m=1}^{\eta} \neg \exists z(p_{n_m,0}(\overline{x})+\dots+p_{n_m,n_m}(\overline{x}) \; z^{n_m}) \leftrightarrow \neg\exists z(\prod_{m=1}^{\eta} (p_{n_m,0}(\overline{x})+$$

$$+\dots+p_{n_m,n_m}(\overline{x}) \; z^{n_m}) =0) \; .$$

Furthermore, we can always assume $\xi=0$:

$$\Sigma\vdash q(\overline{x})\neq 0 \wedge \neg\varphi_n(p_0(\overline{x}),\dots,p_n(\overline{x})) \leftrightarrow q(\overline{x})\neq 0 \wedge \neg\exists z(p_0(\overline{x})+\dots+$$

$$+p_n(\overline{x})z^n =0) \; ,$$

$$\Sigma\vdash q(\overline{x})\neq 0\wedge\neg\exists z(p_0(\overline{x})+\dots+p_n(\overline{x})z^n=0) \leftrightarrow \neg\exists z(q(\overline{x})(p_n(\overline{x})z^n+\dots+p_0(\overline{x}))=0),$$

$$\Sigma \vdash \neg\exists z(q(\overline{x})(p_n(\overline{x})z^n+\ldots+p_0(\overline{x}))=0 \leftrightarrow \neg\varphi_n(q(\overline{x})p_0(\overline{x}),\ldots,q(\overline{x})p_n(\overline{x})) .$$

Should $\eta=0$, we can always introduce the conjunct $\neg\varphi_1(1,0)$. So, we may assume $\xi=0$, $\eta\leq 1$. We are now reduced to showing our result for sets defined by formulae of type

$$(**) \qquad \bigwedge_{i=1}^{\mu} p_i(\overline{x})=0 \wedge \bigwedge_{j=\mu+1}^{\nu} \varphi_{n_j}(p_{n_j,0}(\overline{x}),\ldots,p_{n_j,n_j}(\overline{x})) .$$

Indeed, if we get it for this case, then if we consider the set U defined by

$$\bigwedge_{i=1}^{\mu} p_i(\overline{x})=0 \wedge \bigwedge_{j=1}^{\nu} \varphi_{n_j}(\ldots) \wedge \neg\varphi_n(\ldots) \text{ , we observe}$$

that U=V-W, where V is defined by a formula of type (**) and W by $\varphi_n(\ldots)$, so

$$N_s(U) = N_s(V)-N_s(V \cap W) \text{ ,where } V\cap W \text{ is again}$$

defined by a formula of type (**).

Now to prove the result for a set U defined by (**), it will suffice to show thw following:

<u>Claim</u>: Let V_i be defined by $p_i(\overline{x})=0$ $(i=1,\ldots,\nu)$. Then for all $B\subseteq\{1,\ldots,\nu\}$, $V_B=\bigcup_{i\in B} V_i$ is a set such that $\frac{d}{dt}\log \zeta_{V_B}(t)$ is rational.

Indeed: suppose we have proved the Claim: then

$$N_s(U) = \#(\bigcap_{i=1}^{\nu}(V_i)_s) = \sum_{B\subseteq\{1,\ldots,\nu\}} (-1)^{\#B}\,\#(V_B)_s =$$

$$= \sum_{B \subseteq \{1,\ldots,\nu\}} (-1)^{\#B} N_s(V_B) \quad .$$

Now to prove the claim:

Let $B_1 = B \cap \{1,\ldots,\mu\}$

$B_2 = B \cap \{\mu+1,\ldots,\nu\}$: $V_B = \bigcup_{i\in B_1} V_i \cup \bigcup_{i\in B_2} V_i$

but $\bigcup_{i\in B_1} V_i$ can be defined by $\prod_{i\in B_1} p_i(\overline{x})=0$, and

$\bigcup_{j\in B_2} V_j$ can be defined by $\exists z(\prod_{j\in B_2} (p_{n_j,n_j} z^{n_j}+\ldots+p_{n_j,0} =0)$,

i.e., by $\varphi_n(q_0(\overline{x}),\ldots,q_n(\overline{x}))$, where $n=\sum_{j\in B_2} n_j$ and the

$q_i(\overline{x})$ are adequately computed.

Hence V_B is defined by

$\prod_{i\in B_1} p_i(\overline{x}) =0 \vee \varphi_n(q_0(\overline{x}),\ldots,q_n(\overline{x}))$, hence by

$\exists z(\pi p_i(\overline{x})\ q_n(\overline{x})\ z^n+\ldots+\pi p_i(\overline{x})\ q_0(\overline{x}) = 0)$ hence by

$\varphi_n(\pi p_i(\overline{x}) q_0(\overline{x}),\ldots,\pi p_i(\overline{x}) q_n(\overline{x}))$,

and Lemma 21 is established.

q.e.d.

<u>Proof of Lemma 20</u>: Let U be defined by

$\varphi_n(p_0(x_1,\ldots,x_r),\ldots.p_n(x_1,\ldots,x_r))$:

$U_s = \{ (a_1,\ldots,a_r)\in k_s{}^r \mid$ there exists $b\in k_s$ such that

$p_n(\overline{a})b^n+\ldots+p_0(\overline{a}) =0 \}$.

Let $f(x_1,\ldots,x_r,z)=p_0(x_1,\ldots,x_r)+\ldots+p_n(x_1,\ldots,x_r)z^n \in k[x_1,\ldots,x_r,z]$

Let V be the variety in k^{r+1} defined by $f(\overline{x},z)=0$:

$$V_s = \{(\overline{a},b)\in k_s^{r+1} \mid f(\overline{a},b)=0\}.$$

Let $V_{s,i} = \{(\overline{a},b)\in k_s^{r+1} \mid p_n(\overline{a})z^n+\ldots+p_0(\overline{a})$ has i distinct roots in k_s and b is one of them$\}$ $(i=1,\ldots,n)$;

obviously, we have

$$V_s = \overset{\circ}{\bigcup_{i=1}^{n}} V_{s,i}$$ and we observe that

$$N_s(U) = \#U_s = \sum_{i=1}^{n} \frac{\#V_{s,i}}{i} \quad .$$

Now let H_i be the constructible set in r+i-space defined by

$$f(\overline{x},z_1)=0 \wedge\ldots\wedge f(\overline{x},z_i)=0 \wedge \bigwedge_{\substack{k,m=1\\k\neq m}}^{i} z_k-z_m\neq 0 \quad .$$

By Lemma 19, $\zeta_{H_i}(t)$ is rational. We also have

$(H_i)_s = \{(\overline{a},b)\in k_s^{r+i} \mid f(\overline{a},b_k)=0$ for $k=1,\ldots,i$ and $b_k\neq b_m$ if $k\neq m\}$

Our aim is to compute $\#V_{s,i}$ from $N_s(H_j)$. For this purpose,

let $E_{s,i} = \{(\overline{a},b)\in(H_i)_s \mid f(\overline{a},z)$ has exactly i distinct roots in $k_s\}$

$F_{s,i} = \{(\overline{a},b)\in(H_i)_s \mid f(\overline{a},z)$ has $>i$ distinct roots in $k_s\}$

Of course,

$$(H_i)_s = E_{s,i} \overset{\circ}{\cup} F_{s,i}$$

and also

$\#\{\bar{a}\in k_s^{\,r} \mid f(\bar{a},z)$ has exactly i roots in $k_s\} = \frac{1}{i!}\,\#E_{s,i} = \frac{\#V_{s,i}}{i}$

hence $\quad \#V_{s,i} = \frac{1}{(i-1)!}\,\#E_{s,i}$, and if we can compute

$\#E_{s,i} = N_s(H_i) - \#F_{s,i}$ adequately, we ar through.

Indeed, consider the map

$$\pi_i : \bigcup_{k=i+1}^{n} E_{s,k} \longrightarrow F_{s,i}$$

$$(\bar{a},b_1,\ldots,b_i,\ldots b_k) \longmapsto (\bar{a},b_1,\ldots,b_i)$$

π_i is certainly surjective and also

$$k\neq k' \Rightarrow \pi_i(E_{s,k}) \cap \pi_i(E_{s,k'}) = \emptyset$$

(indeed: $(\bar{a},b_1,\ldots,b_i)\in\pi_i(E_{s,k}) \Rightarrow f(\bar{a},z)$ has exactly k roots)

So

$$F_{s,i} = \bigcup_{k=i+1}^{n} \pi_i(E_{s,k}) \quad , \quad \text{hence}$$

$$\#F_{s,i} = \sum_{k=i+1}^{n} \#\pi_i(E_{s,k}) \;.$$

But for $\quad k=i+1,\ldots,n \qquad \frac{1}{(k-i)!}\,\#E_{s,k} = \#\pi_i(E_{s,k})$

hence $\quad \#E_{s,i} = N_s(H_i) - \#F_{s,i} = N_s(H_i) - \sum_{j=i+1}^{n} \frac{1}{(j-i)!}\,\#E_{s,j}$

but we also know that $\quad \#E_{s,n} = N_s(H_n) \quad$ (from the definitions)

and so we get

$$\#V_{s,n} = \frac{1}{(n-1)!}\,N_s(H_n)$$

$$\#V_{s,i} = \frac{1}{(i-1)!}\#E_{s,i} = \frac{1}{(i-1)!}\Big(N_s(H_i) - \sum_{j=i+1}^{n} (j-1)!\,\#V_{s,j}\Big)$$

$(i=1,\ldots,n-1)$

This certainly determines each $\#V_{s,i}$ as a linear combination of the $N_s(H_j)$ $(j=1,\ldots,n)$ with rational coefficients (independent of s); hence

$$N_s(U) = \sum_{i=1}^{n} \frac{\#V_{s,i}}{i}$$ is given by a linear

combination of the $N_s(H_j)$ with rational coefficients, independent of s, hence the rationality of $\Sigma\, N_s(U)t^s$ follows from the rationality of $\Sigma\, N_s(H_j)t^s$.

q.e.d.

Remark: This proof yields that $\pi_U(t)$ is rational for any definable set U. Certainly, $\zeta_U(t)$ may not be rational. However, this proof also shows that $\zeta_U(t)$ is always "algebraic" in the sense that it can be written as the radical of a rational function.

Example: Let us consider the following:

Definition 10: Let $\Theta : \tilde{k}^r \longrightarrow \tilde{k}^t$ be a function; suppose we can find a t-tuple of polynomials $f_1,\ldots,f_t \in k[x_1,\ldots,x_r]$ such that for all $(a_1,\ldots,a_r) \in \tilde{k}^r$, $\Theta(a_1,\ldots,a_r) = (f_1(a_1,\ldots,a_r),\ldots,f_t(a_1,\ldots,a_r))$; then Θ is called an r-t - morphism over k , and the t-tuple $(f_1,\ldots,f_t)$ is said to define Θ .

We can now state the following

Lemma 22: If $U \subseteq \tilde{k}^r$ is a definable r-set over k, and Θ is an r-t - morphism over k, then $\Theta(U)$ is a definable t-set over k.

<u>Proof</u>: Say U is defined by the formula $\varphi(x_1,\ldots,x_r)$ of $L_{\tau,k}$ and Θ by the t-tuple $(f_1(x_1,\ldots,x_r),\ldots,f_t(x_1,\ldots,x_r))$. Then it is trivial to check that $\Theta(U)$ can be defined by the formula $\psi(y_1,\ldots,y_t)$ given by

$$\exists x_1\ldots\exists x_r(y_1=f_1(x_1,\ldots,x_r)\wedge\ldots\wedge y_t=f_t(x_1,\ldots,x_r)\wedge\varphi(x_1,\ldots,x_r)).$$

q.e.d.

In particular, we get the following generalization of Dwork's result:

The logarithmic derivative of the zeta-function of the image of a variety by a morphism is rational.

References

1. J. Ax, "Solving diophantine problems modulo every prime" Ann. of Math., 85(1967), 161-183.
2. J. Ax, "The elementary theory of finite fields", Ann. of Math., 88(1968), 239-271.
3. J. Ax and S. Kochen, "Diophantine problems over local fields: III", Ann. of Math., 83(1966), 437-456.
4. J. Bell and A. B. Slomson, "Models and Ultraproducts", North-Holland, 1969.
5. B. Dwork, "on the rationality of the zeta-function of an algebraic variety", Amer. J. Math., 82 (1960), 631-648.
6. J. Shoenfield, "Mathematical Logic", Addison-Wesley, 1967.
7. E. Weiss, "Algebraic number theory", McGraw-Hill, 1963.
8. V. Weispfenning, "Elementary theories of valued fields", Thesis, Heidelberg 1971.
9. J. Ax and S. Kochen, "Diophantine problems over local fields: I", Amer. J. Math., 87(1965), 605-630.
10. J. Ax and S. Kochen, "Diophantine problems over local fields: II", Amer. J. Math. 87(1965), 631-648.
11. P. Ribenboim, "Theorie des Valuations", University of Montreal Press, 1964