



Sets Definable Over Finite Fields: Their Zeta-Functions

Author(s): Catarina Kiefe

Source: *Transactions of the American Mathematical Society*, Vol. 223 (Oct., 1976), pp. 45-59

Published by: American Mathematical Society

Stable URL: <http://www.jstor.org/stable/1997516>

Accessed: 21/04/2010 13:43

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=ams>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.



American Mathematical Society is collaborating with JSTOR to digitize, preserve and extend access to *Transactions of the American Mathematical Society*.

<http://www.jstor.org>

SETS DEFINABLE OVER FINITE FIELDS: THEIR ZETA-FUNCTIONS

BY

CATARINA KIEFE⁽¹⁾

ABSTRACT. Sets definable over finite fields are introduced. The rationality of the logarithmic derivative of their zeta-function is established, an application of purely algebraic content is given. The ingredients used are a result of Dwork on algebraic varieties over finite fields and model-theoretic tools.

1. Introduction. In [6] Dwork proved the rationality of the zeta-function of a variety over a finite field. The main result of this paper is to extend this as far as possible to sets definable over finite fields. In this case, the zeta-function need no longer be rational, as illustrated by the set defined over the finite field with p elements (p odd prime) by the formula

$$\exists x(x^2 - y = 0).$$

However, the logarithmic derivative of the zeta-function, i.e., the Poincaré series, turns out always rational.

The result is found using model-theoretic tools: an extension by definitions of the theory of finite fields in ordinary field language is given: this extension is shown to admit elimination of quantifiers (by virtue of a generalization of the Shoenfield Quantifier Elimination Theorem [8]), this yields a characterization of sets definable over finite fields, and the Poincaré series for these can now be proved to be rational by some computations; although the zeta-function need not be rational, from the computation one can conclude that it can always be expressed as the radical of a rational function.

Unexplained notation follows Shoenfield [7] and Bell and Slomson [4].

2. A semantic characterization of elimination of quantifiers. Let τ be a similarity type, L_τ the first-order language of type τ ; let Λ be a theory in language L_τ .

Received by the editors

AMS (MOS) subject classifications (1970). Primary 02H15, 12C99, 12L99.

Key words and phrases. Finite and pseudo-finite fields, varieties, definable sets, zeta-function, elimination of quantifiers.

⁽¹⁾ The results presented in this paper are part of the author's doctoral dissertation, written at the State University of New York at Stony Brook, under the supervision of James Ax; the author wishes to thank Professor Ax for encouragement and advice.

Copyright © 1976, American Mathematical Society

DEFINITION 1. We say that Λ satisfies the *isomorphism condition* if for every two models A and A' of Λ and every isomorphism θ of substructures of A and A' , there is an extension of θ which is an isomorphism of a submodel of A and a submodel of A' .

DEFINITION 2. We say that Λ satisfies the *submodel condition* if for every model B of Λ , every submodel A of B , and every closed simply existential formula φ of $L_{\tau, A}$, we have

$$A \models \varphi \iff B \models \varphi.$$

The following theorem is well known [8, 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 counterexample, due to Allan Adler.

COUNTEREXAMPLE. Let Γ denote the “theory of independent events”, described as follows:

LANGUAGE OF Γ : no constant symbols
no function symbols
a countable set $\{\rho_n \mid n \in \omega\}$ of unary predicate symbols.

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

$$A_{(S, T)}: (\exists x) \left(\bigwedge_{n \in S} \rho_n(x) \wedge \bigwedge_{n \in T} \neg \rho_n(x) \right).$$

Γ admits elimination of quantifiers as can be proved by applying Lemma 3 in [8, p. 83]. To establish the counterexample one shows that Γ does not satisfy the isomorphism condition: indeed, we define two subsets M, N of $[0, 1]$ as follows:

First, we define sequences $\{M_n\}_{n \in \omega}, \{N_n\}_{n \in \omega}$ by $M_0 = N_0 = \{0\}$, if $M_0, \dots, M_n, N_0, \dots, N_n$ are known, choose $\xi_1, \dots, \xi_{2^{n+1}}, \eta_1, \dots, \eta_{2^{n+1}}$ in $[0, 1]$ such that all are irrational,

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

all are distinct, and none are contained in M_n or N_n . We put $M_{n+1} = M_n \cup \{\xi_1, \dots, \xi_{2^{n+1}}\}, N_{n+1} = N_n \cup \{\eta_1, \dots, \eta_{2^{n+1}}\}$.

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 nonempty 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 A and A' of Λ and every isomorphism θ of a substructure of A and a substructure of A' , there is an elementary extension A'' of A' and an extension of θ which is an isomorphism of a submodel of A and a submodel of 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. (2)

PROOF. \Leftarrow : The techniques used in [8] to prove the Quantifier Elimination Theorem can easily be adapted to prove that quantifiers can be eliminated even with these weaker hypotheses. (2)

\Rightarrow : Model-completeness follows trivially.

3. 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)
 \cdot (multiplication)
 $-$ (subtraction)
 constant symbols: 1 (unity)
 0 (additive identity)
 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 predicate symbol: φ_n . L_τ denotes the language obtained by adjoining the predicate symbols $\{\varphi_n | n \in \mathbb{Z}_{>0}\}$ to L_τ .

(2) Conversely, the necessity of these hypotheses follows easily by, e.g., an application of Frayne's Lemma [4, p. 161].

It has been brought to my attention that Theorem 13.1 of [7, p. 63] yields a characterization of elimination of quantifiers very close to this one. However, the one presented here appears to be somewhat more convenient for the purpose of this paper.

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, Theorem 5], a recursive axiomatization for π can be found. Naturally, $\Sigma \subseteq \pi$, i.e., $F \models \pi \Rightarrow F \models \Sigma$.

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

$$\pi \cup \{ \forall x_0 \cdots \forall x_n (\varphi_n(x_0, \dots, x_n) \leftrightarrow \exists y (x_n y^n + \cdots + x_0 = 0)) \mid n \in \mathbb{Z}_{>0} \}$$

and

$$\begin{aligned} \Sigma \cup \left\{ \forall x_0 \cdots \forall x_n \left(\left(\neg \exists y_1 \cdots \exists y_n \left(\bigwedge_{\substack{i,j=1 \\ i \neq j}}^n y_i \neq y_j \wedge \forall y \left(\bigvee_{i=1}^n y = y_i \right) \right) \right) \right. \right. \\ \left. \rightarrow (\varphi_n(x_0, \dots, x_n) \leftrightarrow \exists y (x_n y^n + \cdots + x_0 = 0)) \right) \\ \wedge \left(\exists y_1 \cdots \exists y_n \left(\bigwedge_{\substack{i,j=1 \\ i \neq j}}^n y_i \neq y_j \wedge \forall y \left(\bigvee_{i=1}^n y = y_i \right) \right) \right) \\ \left. \rightarrow \left(\varphi_n(x_0, \dots, x_n) \leftrightarrow \forall y \left(y = 0 \vee \bigvee_{i=1}^{n-1} y = x_0^i \right) \right) \right) \mid n \in \mathbb{Z}_{>0} \right\} \end{aligned}$$

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

Case 1. F is infinite—then we define the $n + 1$ -ary relation φ_n^F by

$$(a_0, \dots, a_n) \in \varphi_n^F \iff \text{the polynomial } a_n y^n + \cdots + a_0 \text{ has a root in } F.$$

Case 2. F is finite with k elements—then φ_n^F is defined as before if $n \neq k$, and φ_k^F is defined by

$$(a_0, \dots, a_k) \in \varphi_k^F \iff a_0 \text{ is a generator of } F^* \text{ (multiplicative subgroup of } F).$$

(b) $F \models \pi' \iff F \models \Sigma'$ and F is infinite,

(c) $F \models \Sigma' \Rightarrow (F \text{ finite with } k \text{ elements} \iff (0, 0, \dots, 0, 1) \notin \varphi_k^F)$.

LEMMA 1. π' admits elimination of quantifiers $\iff \Sigma'$ admits elimination of quantifiers.

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

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

- (i) π' model-complete $\Rightarrow \Sigma'$ model-complete, and
- (ii) π' satisfies weak isomorphism condition $\Rightarrow \Sigma'$ satisfies weak isomorphism condition.

(i) Let $F_j \models \Sigma'$ ($j = 1, 2$) and $F_1 \subseteq F_2$.

If F_1 is infinite, $F_j \models \pi'$ ($j = 1, 2$) and $F_1 \leq F_2$ follows from hypothesis.

If F_1 is finite with k elements,

$$(1, 0, \dots, 0, 1) \notin \varphi_k^{F_1} = \varphi_k^{F_2} \cap F_1^k$$

$$\Rightarrow (1, 0, \dots, 0, 1) \notin \varphi_k^{F_2} \Rightarrow F_2 \text{ finite } k \text{ elements} \Rightarrow F_1 = F_2.$$

(ii) Let $F_j \models \Sigma'$ ($j = 1, 2$) and θ an isomorphism of nonempty-substructures:

If both F_1 and F_2 are infinite, $F_j \models \pi'$, and θ can be extended by hypothesis.

If F_1 is finite with k elements, $(1, 0, \dots, 0, 1) \notin \varphi_k^{F_1} \Rightarrow (1, \dots, 0, 1) \notin \varphi_k^{F_2}$ (because θ is an isomorphism) $\Rightarrow F_2$ is finite with k elements. Hence θ is an isomorphism of two subrings of two fields with k elements, the subrings containing the prime fields; so, obviously, θ can be extended to the fields with k elements.

If F_2 is finite with k elements a similar reasoning holds.

THEOREM 2. π' admits elimination of quantifiers.

PROOF. By Theorem 1, this proof is immediately reduced to the proof of the following two lemmas:

LEMMA 2. π' is model-complete.

LEMMA 3. π' satisfies the weak isomorphism condition.

For the proofs of Lemmas 2 and 3 we need

LEMMA 4. Let $F_i \models \pi'$ ($i = 1, 2$), and assume that F_1 is a subfield of F_2 ; then $F_1 \subseteq F_2$ (i.e., for all $n \in \mathbf{Z}_{>0}$, $\varphi_n^{F_1} = \varphi_n^{F_2} \cap F_1^{n+1}$) $\Leftrightarrow F_1$ is relatively algebraically closed in F_2 .

We also use

LEMMA 5. Let Λ be a theory without finite models in a language of cardinality \aleph_0 . Then: Λ model-complete \Leftrightarrow for any model $A \models \Lambda$ of cardinality \aleph_0 ,

$\Lambda \cup$ Diagram of A is complete.

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

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

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

$$\mathcal{B}_2 \models \text{Diag } \mathcal{B}_3 \cup \Lambda, \text{ and}$$

$$\mathcal{B}_2 \models \varphi, \text{ so}$$

$$\text{Diag } \mathcal{B}_3 \cup \Lambda \models \varphi, \text{ hence } \mathcal{B}_3 \models \varphi$$

$$\text{and } \mathcal{B}_3 \leq \mathcal{B}_1 \Rightarrow \mathcal{B}_1 \models \varphi. \text{ Q.E.D.}$$

PROOF OF LEMMA 2. Since π' has no finite models, by Lemma 5, to prove that π' is model-complete it suffices to show that $\mathcal{F} \models \pi'$ and $\text{card } \mathcal{F} = \aleph_0 \Rightarrow \pi' \cup \text{Diag } \mathcal{F}$ complete: Let $\mathcal{F}_1, \mathcal{F}_2 \models \pi' \cup \text{Diag } \mathcal{F}$; we want to show that

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

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

Now let D be a nonprincipal ultrafilter on the set of positive integers I ; let

$$\epsilon_i = \mathcal{F}_i^I / D \quad (i = 1, 2),$$

since ϵ_i is pseudo-finite, ϵ_i is hyper-finite; (cf. definition in [2, p. 246]) so we have $\mathcal{F} \subseteq \mathcal{F}_i \leq \epsilon_i$, with ϵ_i hyper-finite; by Lemma 4, \mathcal{F} is relatively algebraically closed in ϵ_i ($i = 1, 2$); and also $\text{card } \epsilon_1 = \text{card } \epsilon_2 > \text{card } \mathcal{F}$. Hence, by [2, p. 247, Theorem 1], ϵ_1 and ϵ_2 are isomorphic as fields over \mathcal{F} ; but this implies that they are isomorphic as structures of type τ'' , since the $\varphi_n^{\epsilon_i}$ relations are "algebraic", i.e., preserved under field-isomorphisms. Hence

$$\mathcal{F}_1 \leq \epsilon_1 \simeq \epsilon_2 \geq \mathcal{F}_2, \text{ so}$$

$$\mathcal{F}_1 \equiv \mathcal{F}_2. \text{ Q.E.D.}$$

PROOF OF LEMMA 3. Let $\epsilon_i \models \pi'$ ($i = 1, 2$), $\mathcal{D}_i \subseteq \epsilon_i$ and $\theta: \mathcal{D}_1 \rightarrow \mathcal{D}_2$ be an isomorphism (of structures of type τ').

\mathcal{D}_i is a substructure of ϵ_i , hence an integral domain. Let \mathcal{F}_i be the quotient field of \mathcal{D}_i : $\mathcal{F}_i \subseteq \epsilon_i$, and certainly θ extends to a field-isomorphism $\theta: \mathcal{F}_1 \rightarrow \mathcal{F}_2$. θ is also an isomorphism of structures of type τ' , as can be easily checked; so θ

has the following property:

$$\begin{aligned} a_n x^n + \cdots + a_0 \in F_1[x] \text{ has a zero in } \epsilon_1 \\ \iff \theta(a_n)x^n + \cdots + \theta(a_0) \in F_2[x] \text{ has a zero in } \epsilon_2. \end{aligned}$$

Now let \tilde{F}_i^r be the relative algebraic closure of F_i in ϵ_i . Of course, we again have that

$$\begin{aligned} a_n x^n + \cdots + a_0 \in F_1[x] \text{ has a zero in } \tilde{F}_1^r \\ \iff \theta(a_n)x^n + \cdots + \theta(a_0) \in F_2[x] \text{ has a zero in } \tilde{F}_2^r. \end{aligned}$$

Hence by [1, p. 172, Lemma 5], we can extend θ to a field-isomorphism $\theta: \tilde{F}_1^r \rightarrow \tilde{F}_2^r$. θ is still an isomorphism of structures of type r' because now

$$\begin{aligned} (a_0, \dots, a_n) \in \varphi_n \tilde{F}_1^r = \varphi_n^{\epsilon_1} \cap \tilde{F}_1^{r^{n+1}} &\iff a_n x^n + \cdots + a_0 \\ \text{has a zero in } \epsilon_1 &\iff a_n x^n + \cdots + a_0 \text{ has a zero in } \tilde{F}_1^r \\ \iff \theta(a_n)x^n + \cdots + \theta(a_0) &\text{ has a zero in } \tilde{F}_2^r \\ \iff \theta(a_n)x^n + \cdots + \theta(a_0) &\text{ has a zero in } \epsilon_2 \\ \iff (\theta(a_0), \dots, \theta(a_n)) \in \varphi_n^{\epsilon_2} \cap \tilde{F}_2^{r^{n+1}} &= \varphi_n \tilde{F}_2^r. \end{aligned}$$

Let $\alpha = \text{card } \epsilon_2$. By upward Loewenheim-Skolem, let H'_2 be such that $\epsilon_2 \leq H'_2$ and $\text{card } H'_2 = \alpha^+$. Now, let H_2 be such that $\epsilon_2 \leq H'_2 \leq H_2$, $\text{card } H_2 = 2^\alpha$ and H_2 is α^+ -saturated [4, Theorem 11.1.7].

Then we have that $\epsilon_2 \leq H_2$, H_2 is hyper-finite, $\text{card } H_2 = 2^\alpha$ and \tilde{F}_2^r is relatively algebraically closed in H_2 (because $\epsilon_2 \leq H_2$).

Let $\beta = \text{card } \tilde{F}_1^r = \text{card } \tilde{F}_2^r \leq \alpha < 2^\alpha$; by downward Loewenheim-Skolem, let H_1 be such that $\tilde{F}_1^r \subseteq H_1 \leq \epsilon_1$ and $\text{card } H_1 = \beta$. Then we know that H_1 is quasi-finite (because $H_1 \leq \epsilon_1 \Rightarrow H_1 \models \pi'$), $\text{card } H_1 < \text{card } H_2$, and \tilde{F}_1^r is relatively algebraically closed in H_1 . So by [2, Lemma 2] we can extend θ to a field-monomorphism $\theta: H_1 \rightarrow H_2$ such that $\theta(H_1)$ is relatively algebraically closed in H_2 .

If we take $\varphi_n^{\theta(H_1)}$ to be defined on $\theta(H_1)$ through θ , we get, since $H_1 \models \pi'$, that $\theta(H_1) \models \pi'$. But now $H_2, \theta(H_1) \models \pi'$, $\theta(H_1)$ is a subfield of H_2 , and is relatively algebraically closed in H_2 . Then Lemma 4 applies to show that $\theta(H_1) \subseteq H_2$, i.e., with $\varphi_n^{\theta(H_1)}$ defined as above, $\theta(H_1)$ is a submodel of H_2 . Hence we have proved the weak isomorphism condition. Q.E.D.

4. Sets definable over a finite field: the rationality of their Poincaré series.

In this section, we shall use the following

NOTATION. L_r —ordinary field language, as described in §3.

$L_{r'}$ —ordinary field language with all the $n + 1$ -ary predicate symbols φ_n adjoined ($n \in \mathbb{Z}_{>0}$).

Σ -theory of finite fields in L_τ .

Σ' -theory of finite fields with defining axioms for φ_n adjoined (as in §3).

k -finite field of cardinality q .

$L_{\tau,k}$ - L_τ with q new constant symbol adjoined.

k_s -unique extension of k of degree s .

\tilde{k} -algebraic closure of k .

DEFINITION 4. Let $U = \{U_s\}_{s \in \mathbf{Z}_{>0}}$ with $U_s \subset k_s^r, \forall s \in \mathbf{Z}_{>0}$; then U is called a *definable* r -set over $k \iff$ there exists a formula φ in $L_{\tau,k}$ with r free variables such that

$$U_s = \{(a_1, \dots, a_r) \in k_s^r \mid k_s \models \varphi[a_1, \dots, a_r]\}, \quad \forall s \in \mathbf{Z}_{>0}.$$

We then say that U is *defined* by φ .

REMARK. If U is definable over k , the formula 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 .

DEFINITION 5. Say U is a definable r -set, defined by φ . We have $U_s = \{(a_1, \dots, a_r) \in k_s^r \mid k_s \models \varphi[a_1, \dots, a_r]\}$; the *zeta-function* of U is defined to be the formal power series in t

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

where $N_s(U) = \#U_s =$ cardinality of U_s . Following terminology used in [5, p. 47] we let the *Poincaré series* of U be 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

THEOREM 3. *The Poincaré series of a definable set is rational.* ⁽³⁾

DEFINITION 6. A definable r -set V over k will be called a *variety* over k if it can be defined by a formula of type

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

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

DEFINITION 7. A definable r -set will be called *primitive* if it can be defined by a formula of type

⁽³⁾ As usual, a formal power series is called rational when it is the quotient of two polynomials.

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

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

DEFINITION 8. A definable set will be called *constructible* if it can be defined by a formula which is quantifier free in $L_{\tau, k}$.

DEFINITION 9. Let $U = \{U_s\}_{s \in \mathbb{Z}_{>0}}$ and $V = \{V_s\}_{s \in \mathbb{Z}_{>0}}$ be definable r -sets. We define the *union*, *intersection* and *difference* of U and V "pointwise", i.e., by

$$(U \cup V)_s = U_s \cup V_s, \quad (U \cap V)_s = U_s \cap V_s, \\ (U - V)_s = U_s - V_s, \quad \forall s \in \mathbb{Z}_{>0}.$$

LEMMA 6. If U is a constructible set, then $\zeta_U(t)$ is a rational function. Hence, so is $\pi_U(t)$.

PROOF. Dwork [6] showed that $\zeta_{V-W}(t)$ is rational, for V, W varieties.

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

$$\Sigma \vdash \left(\bigwedge_{i=1}^n p_i(\bar{x}) \wedge \bigwedge_{j=1}^m q_j(\bar{x}) \neq 0 \right) \leftrightarrow \left(\bigwedge_{i=1}^n p_i(x) = 0 \wedge \prod_{j=1}^m q_j \neq 0 \right).$$

So if V is defined by $\bigwedge_{i=1}^n p_i(\bar{x}) = 0$ and W is defined by $(\prod_{j=1}^m q_j(\bar{x})) = 0$, then $P = V - W$. So the Lemma holds for primitive sets.

Now observe that the intersection of primitive 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, \dots, 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

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

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

where $P_B = \bigcap_{i \in B} P_i$, for all $B \subseteq \{1, \dots, n\}$. But P_B is a primitive set, hence $\zeta_{P_B}(t)$ is rational, so

$$\zeta_U(t) = \prod_{\phi \neq B \subseteq \{1, \dots, n\}} \zeta_{P_B}(t)^{(-1)^{\#B+1}}$$

is rational. Q.E.D.

We shall now reduce the proof of Theorem 3 to

LEMMA 8. Let $U \subseteq k^r$ be definable, defined by an atomic formula in $L_{\tau',k}$ of type

$$\varphi_n(p_0(x_1, \dots, x_r), \dots, p_n(x_1, \dots, x_r)),$$

with $p_i(x_1, \dots, x_r) \in k[x_1, \dots, x_r]$ ($i = 1, \dots, n$) (obviously, we mean that U is defined by a formula of $L_{\tau,k}$ equivalent to $\varphi_n(p_0(\bar{x}), \dots, p_n(\bar{x}))$); then $\pi_U(t)$ is rational.

Before we prove Lemma 8, we shall reduce the proof of Theorem 3 to it, i.e., show that Theorem 3 follows from Lemmas 7 and 8.

Let U be a definable set; it has been proved in §3 that Σ' admits elimination of quantifiers, hence we may assume U defined by a quantifier-free formula φ in the language $L_{\tau',k}$, i.e., U is the union of sets defined by formulae of type

$$(*) \quad \bigwedge_{i=1}^{\mu} p_i(\bar{x}) = 0 \wedge \bigwedge_{j=1}^{\nu} \varphi_{n_j}(p_{n_j,0}(\bar{x}), \dots, p_{n_j,n_j}(\bar{x})) \wedge \bigwedge_{k=1}^{\xi} q_k(\bar{x}) \\ \neq 0 \wedge \bigwedge_{m=1}^{\eta} \neg \varphi_{n_m}(p_{n_m,0}(\bar{x}), \dots, p_{n_m,n_m}(\bar{x})).$$

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.

We are now reduced to sets U defined by formulae of type (*). To proceed, we start by freeing ourselves from the restrictions imposed by the defining axiom for φ_m in case we are interpreting this relation in a field with m elements.

LEMMA 9. Let U be defined by a formula φ of type (*). Let ψ' be obtained from U by replacing each occurrence of $\varphi_m(p_{m,0}(\bar{x}), \dots, p_{m,m}(\bar{x}))$ by $\exists z(p_{m,0}(\bar{x}) + \dots + p_{m,m}(\bar{x})z^m = 0)$. Let U' be the set defined by ψ' . Then, if $\pi_{U'}(t)$ is rational, so is $\pi_U(t)$.

PROOF. Let

$$A = \{m \in \mathbf{Z}_{>0} \mid \varphi_m \text{ occurs in } \varphi \text{ and } m = q^s, \text{ for some } s \in \mathbf{Z}_{>0}\},$$

$$B = \{s \in \mathbf{Z}_{>0} \mid q^s = m, \text{ for some } m \in A\}.$$

If $B = \emptyset$, $\forall s \in \mathbf{Z}_{>0}$, $U_s = U'_s$ hence $N_s(U) = N_s(U')$ and the result is obvious. But if $B \neq \emptyset$, it certainly is finite. Also, $\forall s \in \mathbf{Z}_{>0}$, $s \notin B \Rightarrow N_s(U) = N_s(U')$. Hence $\pi_U(t) = \sum_{s=1}^{\infty} N_s(U)t^s = \sum_{s=1}^{\infty} N_s(U')t^s - \sum_{s \in B} N_s(U')t^s + \sum_{s \in B} N_s(U)t^s$. From the finiteness of B and the rationality of $\sum_{s=1}^{\infty} N_s(U')t^s$

we immediately conclude the rationality of $\pi_U(t)$. Q.E.D.

So in everything that follows we may replace $\varphi_m(p_{m,0}, \dots, p_{m,m})$ by $\exists z(p_{m,0} + \dots + p_{m,m}z^m = 0)$.

As before, in formulae of type (*) we may assume $\xi \leq 1$ by replacing $\bigwedge_{k=1}^{\xi} q_k(\bar{x}) \neq 0$ by $\prod_{k=1}^{\xi} q_k(\bar{x}) \neq 0$; similarly. We may assume $\eta \leq 1$; indeed:

$$\begin{aligned} \Sigma \vdash \bigwedge_{m=1}^{\eta} \neg \exists z(p_{n_m,0}(\bar{x}) + \dots + p_{n_m,n_m}(\bar{x})z^{n_m} = 0) \\ \leftrightarrow \neg \exists z \left(\prod_{m=1}^{\eta} (p_{n_m,0}(\bar{x}) + \dots + p_{n_m,n_m}(\bar{x})z^{n_m}) = 0 \right). \end{aligned}$$

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

$$\begin{aligned} \Sigma \vdash q(\bar{x}) \neq 0 \wedge \neg \varphi_n(p_0(\bar{x}), \dots, p_n(\bar{x})) &\Leftrightarrow q(\bar{x}) \\ &\neq 0 \wedge \neg \exists z(p_0(\bar{x}) + \dots + p_n(\bar{x})z^n = 0), \\ \Sigma \vdash q(\bar{x}) \neq 0 \wedge \neg \exists z(p_0(\bar{x}) + \dots + p_n(\bar{x})z^n = 0) \\ &\Leftrightarrow \neg \exists z(q(\bar{x})(p_n(\bar{x})z^n + \dots + p_0(\bar{x}))), \\ \Sigma \vdash \neg \exists z(q(\bar{x})(p_n(\bar{x})z^n + \dots + p_0(\bar{x})) = 0) \\ &\Leftrightarrow \neg \varphi_n(q(\bar{x}), \dots, q(\bar{x})p_n(\bar{x})). \end{aligned}$$

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

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

Indeed, if we get it for this case, then if we consider the set U defined by $\bigwedge_{i=1}^{\mu} p_i(\bar{x}) = 0 \wedge \bigwedge_{j=1}^{\nu} \varphi_{n_j}(\dots) \wedge \neg \varphi_n(\dots)$, we observe that $U = V - W$, where V is defined by a formula of type (**) and W by $\varphi_n(\dots)$, so $N_s(U) = N_s(V) - N_s(V \cap W)$, where $V \cap W$ is again defined by a formula of type (**).

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

Claim. Let V_i be defined by $p_i(\bar{x}) = 0$ ($i = 1, \dots, \mu$) and by $\varphi_{n_i}(p_{n_i,0}(\bar{x}), \dots, p_{n_i,n_i}(\bar{x}))$ for $i = \mu + 1, \dots, \nu$. Then for all $B \subseteq \{1, \dots, \nu\}$, $V_B = \bigcup_{i \in B} V_i$ is a set such that $d/dt \log \zeta_{V_B}(t)$ is rational.

Suppose we have proved the Claim: then

$$\begin{aligned} N_s(U) &= \# \left(\bigcap_{i=1}^{\nu} (V_i)_s \right) = \sum_{B \subseteq \{1, \dots, \nu\}} (-1)^{\#B} \#(V_B)_s \\ &= \sum_{B \subseteq \{1, \dots, \nu\}} (-1)^{\#B} N_s(V_B). \end{aligned}$$

Now to prove the Claim:

Let

$$\begin{aligned} B_1 &= B \cap \{1, \dots, \mu\}, \\ B_2 &= B \cap \sum_{\{\mu+1, \dots, \nu\}} V_B = \bigcup_{i \in B_1} V_i \cup \bigcup_{i \in B_2} V_i \end{aligned}$$

but $\bigcup_{i \in B_1} V_i$ can be defined by $\prod_{i \in B_1} p_i(\bar{x}) = 0$, and $\bigcup_{j \in B_2} V_j$ can be defined by

$$\exists z \left(\prod_{j \in B_2} (p_{n_j n_j} z^{n_j} + \dots + p_{n_j, 0}) = 0 \right),$$

i.e., by $\varphi_n(q_0(\bar{x}), \dots, q_n(\bar{x}))$, where $n = \sum_{j \in B_2} n_j$ and the $q_i(\bar{x})$ are adequately computed.

Hence V_B is defined by

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

$$\exists z (\pi p_i(\bar{x}) q_n(\bar{x}) z^n + \dots + \pi p_i(\bar{x}) q_0(\bar{x}) = 0), \text{ hence by}$$

$$\varphi_n(\pi p_i(\bar{x}) q_0(\bar{x}), \dots, \pi p_i(\bar{x}) q_n(\bar{x})),$$

and the proof of Theorem 3 is actually reduced to Lemma 8.

PROOF OF LEMMA 8. Let U be defined by

$$\varphi_n(p_0(x_1, \dots, x_r), \dots, p_n(x_1, \dots, x_r));$$

by Lemma 9 we may assume $n > q$:

$$U_s = \{(a_1, \dots, a_r) \in k_s^r \mid \text{there exists } b \in k_s$$

$$\text{such that } p_n(\bar{a}) b^n + \dots + p_0(\bar{a}) = 0\}.$$

Let $f(x_1, \dots, x_r, z) = p_0(x_1, \dots, x_r) + \dots + p_n(x_1, \dots, x_r) z^n \in k[x_1, \dots, x_r, z]$. Let V be the variety in k^{r+1} defined by $f(\bar{x}, z) = 0$:

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

Let

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

($i = 1, \dots, n$); obviously, we have $V_s = \dot{\bigcup}_{i=1}^n V_{s,i}$ and we observe that

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

Now let H_i be the constructible $r + i$ set defined by

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

By Lemma 6, $\zeta_{H_i}(t)$ is rational. We also have $(H_i)_s = \{(\bar{a}, \bar{b}) \in k_s^{r+1} \mid f(\bar{a}, b_k) = 0 \text{ for } k = 1, \dots, i \text{ and } b_k \neq b_m \text{ if } k \neq m\}$. Our aim is to compute $\#V_{s,i}$ from $N_s(H_i)$. For this purpose, let

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

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

Of course, $(H_i)_s = E_{s,i} \dot{\cup} F_{s,i}$ and also

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

hence $\#V_{s,i} = \#E_{s,i}/(i - 1)!$, and if we can compute $\#E_{s,i} = N_s(H_i) - \#F_{s,i}$ adequately, we are through.

Indeed, consider the map

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

$$(\bar{a}, b_1, \dots, b_i, \dots, b_k) \longrightarrow (\bar{a}, b_1, \dots, b_i).$$

π_i is certainly surjective and also

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

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

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

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

But for $k = i + 1, \dots, n$, $\#E_{s,k}/(k - i)! = \#\pi_i(E_{s,k})$; hence $\#E_{s,i} = N_s(H_i) -$

$\#F_{s,i} = N_s(H_i) - \sum_{j=i+1}^n \#E_{s,j}/(j-i)!$ but we also know that $\#E_{s,n} = N_s(H_n)$ (from the definitions) and so we get

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

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

$$(i = 1, \dots, n-1).$$

This certainly determines each $\#V_{s,i}$ as a linear combination of the $N_s(H_j)$ ($j = 1, \dots, n$) 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 $\sum N_s(U) t^s$ follows from the rationality of $\sum N_s(H_j) t^s$. Q.E.D.

REMARK. The 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, indeed, it can always be written as the radical of a rational function.

5. Application. Let us consider the following:

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

We can state the following

LEMMA 10. *If U 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 .*

PROOF. Say U is defined by the formula $\varphi(x_1, \dots, x_r)$ of $L_{\tau, k}$ and θ by the t -tuple $(f_1(x_1, \dots, x_r), \dots, f_t(x_1, \dots, x_r))$. Then it is trivial to check that $\theta(U)$ can be defined by the formula $\Psi(y_1, \dots, y_t)$ given by

$$\exists x_1 \cdots \exists x_r (y_1 = f_1(x_1, \dots, x_r) \wedge \cdots \wedge y_t = f_t(x_1, \dots, x_r) \wedge \varphi(x_1, \dots, x_r)). \quad \text{Q.E.D.}$$

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. James Ax, *Solving diophantine problems modulo every prime*, Ann. of Math. (2) **85** (1967), 161–183. MR 35 #126.
2. ———, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271. MR 37 #5187.
3. James Ax and S. Kochen, *Diophantine problems over local fields. III. Decidable fields*, Ann. of Math. (2) **83** (1966), 437–456. MR 34 #1262.
4. J. L. Bell and A. B. Slomson, *Models and ultraproducts. An introduction*, North-Holland, Amsterdam, 1969. MR 42 #4381.
5. Z. I. Borevič and I. R. Šafarevič, *Number theory*, “Nauka”, Moscow, 1964; English transl., Pure and Appl. Math., vol. 20, Academic Press, New York, 1966. MR 30 #1080; 33 #4001.
6. B. M. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648. MR 25 #3914.
7. G. E. Sacks, *Saturated model theory*, Math. Lecture Notes, Benjamin, New York, 1972.
8. J. R. Shoenfield, *Mathematical logic*, Addison-Wesley, Reading, Mass., 1967. MR 37 #1224.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY,
CALIFORNIA 94720