Accepted to Journal of Number Theory in 1986. Will be rewritten for final publication when I get around to it.

L-SERIES ON A GALOIS STRATIFICATION

M. Fried, U.C. Irvine, Irvine, Ca., 92717*

Abstract: Galois stratifications are a tool for turning the art of Galois theoretic interpretation into an algorithm. Here they give explicit computation for Euler factors attached to arithmetic statements (e.g., elementary statements) over number fields. We proceed in stages. First, generalizing Kiefe [K], §3 builds on [FrS; §5] to give an effective computation for a sequence of zeta functions attached to an elementary statement over a finite field. Then §4 gives similar results for general L-series on a Galois stratification. These require Dwork's fredholm determinant method [D,1,2,3] as applied by Bombieri in [B,2]. Finally, we discuss p-adic generalizations based on [De] and [Me,1] that use p-adic integration (§5). This leads to a p-adic generalization of the Čebotarev density theorem. The goal is a general quantitative theory of "bad" primes based on Euler factors as illustrated by examples applying to zeros of forms and value sets of polynomials (§6).

§1. Introduction.

For a field F, fix an algebraic closure $\bar{F}$ of F. Galois stratifications first appear in [FrS] to provide an elimination of quantifier procedure for the theory of all residue class fields (and all p-adic completions) of a number field: a procedure as effective as the procedure for deciding when a set of polynomial equations defines a nonempty set. Since

*Partially supported by NSF Grant #DMS-8508962.

then they have appeared as a tool for special theories of subfields of $\mathbf{Q}$ (e.g., the theory of Frobenius fields in [FrHJ] and the theory of fields with listinguished automorphisms [HJ]). Here we return to the classical setting of finite and p-adic fields.

For a prime power $q = p^r$, denote the finite field of order q by $\mathbf{F}(q)$. Kiefe [K] has attached a zeta function $Z(P,t)$ to each elementary statement P (with both free and quantified variables). The main theorem (Theorem 3.2) is the existence of an integer u and polynomials $f_1, f_2, f_3 \in \mathbf{Z}[t]$ such that $Z(P,t)^u = e^{f_1(t)}(f_2(t)/f_3(t))$. The exponential factor, $e^{f_1(t)}$ - an important part of our concerns - was left out of [K]. Assume that u is minimal and that f_2 and f_3 are relatively prime polynomials. Define the total degree, $\deg_{tot}(Z(P,t)$ to be $\deg(f_1) + \deg(f_2) + \deg(f_3)$.

As the methods of [K] are model theoretic, they provide no hope of computing either u or $\deg_{tot}(Z(P,t))$. In theory [FrS;§5] makes such a computation possible [Fr,1]. The algorithm of Theorem 3.2 is realistically machine programable and, in simple cases, possible to effect by hand. Indeed, we generalize these results to Galois stratifications (reviewed in §2) over $\mathbf{F}(q)$. Reasonable enough, as the method forces us to consider a sequence of Galois stratifications even when we start from a relatively innocuous elementary statement P. Effective computation of $Z(P,t)$ is a corollary.

Additions to the theory of zeta functions on a Galois stratification over finite fields give analogous results for (Artin) L-series on a Galois stratification over a finite field (Theorem 4.3). An essential part of the effectiveness of Theorem 3.2 derives from Bombieri's aplication of Dwork's fredholm determinant method [B,2] to compute the total degree of the zeta function of a variety over a finite field. The analogous computation, however, for L-series is still, unfortunately, incomplete. Thus we give the

best general result that we know (based on [B,3] and [Fr,1]) in Theorems 4.3 and 4.4. Supplementary results by Bombieri [B,1,2,3] and Adolphson-Sperber [ASp] (§4) to compute the total degree of an L-series attached to exponential sums over finite fields aid in practical examples.

Based on ideas of Denef [De] and Meuser [Me,1] we suggest p-adic analogues, Zeta functions that involve information about an elementary statement over all unramified extensions of a given p-adic ring, and additions to the earlier theory for proving these (§5). The new concept here is a property, following Meuser, that we call invariance of these zeta functions. A p-adic analogue of the Čebotarev density theorem lies at the heart of these results, a developmemt campatible with the scope of [Se,2]. The exposition on using these L-series to find quantitative evidence for "bad" primes attached to an elementary statement (§6) includes examples.

Acknowledgement: Moshe Jarden reminded us of the significance of the exponential factor in $Z(P,t)$. Alan Adolphson pointed us in the direction of [B,2].

§2. Zeta functions.

Let $\mathbf{A}^n$ denote affine n-space over a field K. Denote the coordinates of $\mathbf{A}^n$ by $x_1,\cdots,x_n$. Use the notation $V(\mathbf{g};f)$ for the locally closed (or basic) set defined by

$$g_1(\mathbf{x}) = \cdots = g_t(\mathbf{x}) = 0 ,$$

and

$$f_1(\mathbf{x}) \neq 0, \cdots, f_s(\mathbf{x}) \neq 0$$

with $(g_1,\cdots,g_t) = \mathbf{g}$ and $g_1,\cdots,g_t,f_1,\cdots,f_s \in K[x_1,\cdots,x_n]$. We assume, of course, that f_i , $i = 1,\cdots,s$, is not a zero divisor in the ring $K[x_1,\cdots,x_n]/(g_1,\cdots,g_t)$. The coordinate ring of $V(\mathbf{g};\mathbf{f})$ is $K[V(\mathbf{g},\mathbf{f})] = K[x_1,\cdots,x_n, 1/f_1,\cdots,1/f_s]/(g_1,\cdots g_t)$ where the ideal $(g_1,\cdots,g_t)$ is regarded as in $K[x_1,\cdots,x_n,1/f_1,\cdots,1/f_s]$. Then $V(\mathbf{g},\mathbf{f})$ is K-normal if $K[V(\mathbf{g};\mathbf{f})]$ is integrally closed. Denote the points of any algebraic set $V \subseteq \mathbf{A}^n$ with coordinates in K by $V(K)$.

A Galois stratification over K is a structure $\mathcal{A} = \{C(V_i)/V_i, Con(V_i)\}_{i\in I}$ with these properties: V_i is an irreducible K-normal basic subset of $\mathbf{A}^n$ (Remark 2.2) and $\varphi_i : C(V_i) \to V_i$ is a finite Galois cover (Remark 2.3) of K-normal sets, $i \in I$; the sets V_i , $i \in I$, are pairwise disjoint and have union equal to all of $\mathbf{A}^n$; and for each $i \in I$, $Con(V_i)$ is a union of conjugacy classes of the Galois group $G(C(V_i)/V_i)$ of the cover $C(V_i) \to V_i$.

Note that V_i may be reducible over $\bar{K}$. The condition that V_i and $C(V_i)$ are K-normal sets guarantees that $G(C(V_i)/V_i)$ is canonically identified with the Galois group of the corresponding extension of function fields. But if we know a' priori that $C(V_i) \to V_i$ is a Galois cover (as in Part 2 of the proof of Theorem 3.2) the K-normal condition can sometimes be relaxed.

From a Galois stratification we obtain a Galois formula by choosing an integer k between 0 and n and $n-k$ quantifiers $Q_{k+1},\cdots,Q_n$ with Q_i either $\exists$ ("there exists") or $\forall$ ("for each"). Other than these abbreviations, little use of logic appears in this paper. Write the Galois formula as

$$(2.1)\qquad (Q_{k+1}x_{k+1})\cdots(Q_n x_n)[(x_1,\cdots,x_n) = \mathbf{x} \in \bigcup_{i\in I} \mathrm{Con}(V_i)] \ .$$

Here $x_1,\cdots,x_k$ are free variables.

For $K = \mathbf{F}(q)$, interpret the portion of (2.1) in brackets as follows. If $\mathbf{x} \in \mathbf{A}^n(\mathbf{F}(q))$, then $\mathbf{x} \in V_i(F(q))$ for some $i \in I$. Choose a point $y \in C(V_i)$ lying above $\mathbf{x} \in V_i$ (i.e., $\varphi_i(\mathbf{y}) = \mathbf{x}$). The group $G(\overline{\mathbf{F}(q)}/\mathbf{F}(q))$ acts on the fiber $C(V_i)_{\mathbf{x}}$, consisting of the points of $C(V_i)$ that lie over $\mathbf{x}$, by acting on the coordinates of the points. The frobenius generator F_q of $G(\overline{\mathbf{F}(q)}/\mathbf{F}(q))$ is defined by the formula

$$(2.2)\qquad F_q(\alpha) = \alpha^q \quad \text{for each} \quad \alpha \in \overline{\mathbf{F}(q)} \ .$$

Let $\hat{D}_{\mathbf{y}} = \{\sigma \in G(C(V_i)/V_i) \mid \mathbf{y}^\sigma = \mathbf{y}$ and σ induces F_q on the residue class field of $y\}$. From [ZS;p.69-82], $\hat{D}_{\mathbf{y}}$ is a (nonempty) coset of $I_{\mathbf{y}} = \{\sigma \in G(C(V_i)/V_i) \mid \mathbf{y}^\sigma = \mathbf{y}$ and σ induces the identity on the residue class field of $y\}$. The condition that $\hat{D}_{\mathbf{y}}$ be a subset of $\mathrm{Con}(V_i)$ is independent of the choice of $\mathbf{y}$: $\hat{D}_{\mathbf{y}'}$ and $\hat{D}_{\mathbf{y}}$ are conjugate sets if $\mathbf{y}'$ also lies over $\mathbf{x}$. To simplify notation denote $\cup\sigma\hat{D}_{\mathbf{y}}\sigma^{-1}$, where the union runs over $\sigma \in G(C(V_i)/V_i)$, by $F_{\mathbf{x}}$. Finally, in this notation, $x \in \bigcup_{i\in I} \mathrm{Con}(V_i)$ means that $F_{\mathbf{x}} \subseteq \mathrm{Con}(V_i)$.

We explain this complicated definition. Assume $k < n$. The elimination of quantifier procedure of [FrS;§4] effectively produces a Galois stratification $\mathcal{B} = \{C(W_j)/W_j \ , \ \mathrm{Con}(W_j)\}_{j\in J}$ with $\bigcup_{j\in J} W_j = \mathbf{A}^{n-1}$ and an integer $\ell(\mathcal{A},Q_n)$ with this property: For each $\ell \geq \ell(\mathcal{A},Q_n)$ and $(x_1,\cdots,x_{n-1}) = \mathbf{x}' \in \mathbf{A}^{n-1}(\mathbf{F}(q^\ell))$

(2.3) $[\mathbf{x}' \in \bigcup_{j\in J} \mathrm{Con}(W_j)]$ if and only if $(Q_n x_n)[(\mathbf{x}', x_n) = \mathbf{x} \in \bigcup_{i\in I} \mathrm{Con}(V_i)]$

with $x_n \in \mathbf{F}(q^{\ell})$.

Since [FrS] always dealt with the situation that $C(V_i)/V_i$ is unramified, there $F_{\mathbf{x}}$ always consisted of a single element. Thus the condition $F_{\mathbf{x}} \subseteq \mathrm{Con}(V_i)$ is a more relaxed condition that is compatible with Remark 2.3 below. It actually has practical value in specific problems to allow this (Ex.6.2).

Ex. 2.1. Galois formulas include elementary statements. Suppose in (2.1) that $C(V_i) = V_i$, so that $G(C(V_i)/V_i)$ is trivial, for each $i \in I$. Thus $\mathrm{Con}(V_i)$ is either empty or the identity element. Partition I as $I_1 \dot{\cup} I_2$ with $i \in I_1$ if and only if $\mathrm{Con}(V_i)$ is the identity element. Denote the union $\bigcup_{i\in I_1} V_i$ by $V(I_1)$. Then (2.1) is equivalent to

(2.4) $\quad (Q_{k+1}x_{k+1})\cdots(Q_n x_n)[\mathbf{x} \in V(I_1)]$,

an elementary statement in prenex normal form. Conversely, suppose that we are given (2.4) with an algebraic subset $V \subseteq \mathbf{A}^n$ replacing $V(I_1)$. We need only stratify V into $\bigcup_{i\in I_1} V_i$ (resp., $\mathbf{A}^n - V$ into $\bigcup_{i\in I_2} V_i$) , a disjoint union of irreducible K-normal sets. Then let $C(V_i) = V_i$ and $\mathrm{Con}(V_i)$ is empty or the identity element depending on whether $i \in I_2$ or $i \in I_1$. Since nonsingular sets are normal [M;p.390, Proposition 1], the stratification of V into K-normal sets can be achieved through a stratification into nonsingular sets. Because, however, we have a goal of minimizing the work of refining a stratification, we would want to take advantage of observations of

this kind: If V is an open subset of a hypersurface of $\mathbf{A}^n$ and the singular points of V are of codimension at least 2, then V is normal [M; p.391, Proposition 2]. ■

The main point is that, even if $\mathcal{A}$ is an elementary statement (as in Ex. 2.1), the Galois stratification $\mathcal{B}$ in (2.3) may not be. Suppose, however, that $\mathcal{A}$ satisfies this property: For each $i \in I$, $\sigma \in G(C(V_i)/V_i)$ and $\ell \in \mathbf{Z}$, $(\ell, \mathrm{ord}(\sigma)) = 1$,

(2.5) $\sigma \in \mathrm{Con}(V_i)$ if and only if $\sigma^\ell \in \mathrm{Con}(V_i)$.

We say that $\mathcal{A}$ is an elementary Galois stratification and (2.1) is an elementary Galois formula. In this case $\mathcal{B}$ is also an elementary Galois stratification.

Remark 2.2. K-rational points on $\bar{K}$-reducible K-normal sets. Since the basic concern of this paper is K-rational points on a K-algebraic set V, we have been free to reduce to the case that V is K-irreducible (and, as in [FrS], we assume that V is reduced). We note here that if $V \subseteq \mathbf{A}^n$ is K-normal and a union $V_1 \cup \cdots \cup V_s$ of varieties defined over $\bar{K}$ such that $s \geq 1$ and $G(\bar{K}/K)$ acts transitively on $V_1, \cdots, V_s$, then $V(K)$ is empty. Indeed, let L/K be the minimal Galois extension of K over which $V_1, \cdots, V_s$ are all defined. Choose $\alpha \in L$ such that $L = K(\alpha)$. Let $\mathbf{v}^{gen} \in V_1$ be a generic point for V_1 over L and let $V_1^* \subseteq \mathbf{A}^{n+1}$ be the variety whose points are $(\mathbf{v}, \alpha) \in \mathbf{A}^n \times \mathbf{A}^1$ with $\mathbf{v} \in V_1$. Then $(\mathbf{v}^{gen}, \alpha)$ can be regarded as a generic point for V_1^* over L, or it can also be regarded as a generic point for the union $V^* = V_1^* \cup \cdots \cup V_s^*$ of the conjugates of V_1^* over K.
Clearly, however, $V^*(K)$ is empty and V^* is normal. Since the natural map $V^* \to V$ is finite, from the uniqueness of normalization [M; p.396, Theorem 3]

V^* is K-isomorphic to V. Thus $V(K)$ is empty. ■

Remark 2.3. Comments on the use of the word "cover." In the notation for the Galois stratification $\mathcal{A}$, above, that $\varphi_i: C(V_i) \to V_i$ is a cover means only that φ_i is a finite morphism [M;243-5]. In [FrS], however, a cover was assumed to be (besides finite) étale (unramified in the present context) so that we could assert that the set $\hat{D}_y$ consists of a unique element. A concept in between these two calls a morphism a cover if it is both finite and flat [M;p.434]. Flatness adds the most geometric touch since, in this case, the points in the fiber over $x \in V_i$, $C(V_i)_x$, can be counted with multiplicity in such a way that the sum of the multiplicities always adds up to the degree of φ_i. For theoretical purposes (e.g., as in [FrS]) the restrictive definition, that covers are unramified, suffices. But, for practical purposes, given $\mathcal{A}$, we wish to do as little work as possible in forming a stratification $\mathcal{B}$ that satisfies (2.3). Therefore the stratification process prefers the least restrictive definition that can carry the concepts of Galois theory. ■

We conclude this subsection with the definition of the L-function, $Z(\mathcal{A},\mathbf{Q},t)$, attached to the Galois formula (2.1). For each integer $\ell \geq 1$, define N_ℓ to be the cardinality of the set

$$(2.6)\quad \Big|\{(x_1,\cdots,x_k) \in \mathbb{A}^k(\mathbf{F}(q^\ell)) \Big|$$

$$(Q_{k+1}x_{k+1})\cdots(Q_n x_n)[(x_1,\cdots,x_n) \in \bigcup_{i\in I} \mathrm{Con}(V_i)]\Big| \ .$$

Then $Z(\mathcal{A},\mathbf{Q},t)$ is defined by the formula

$$(2.7)\quad t\frac{d}{dt}\left(\log(Z(\mathcal{A},\mathbf{Q},t))\right) = \sum_{\ell=1}^{\infty} N_\ell t^\ell \ .$$

The right side of (2.7) is called the Poincaré series of the Galois formula. If $\mathcal{A}$ is elementary call $Z(\mathcal{A},\mathbf{Q},t)$ a zeta function.

Ex. 2.4. A value set example. Take

$$n = 2\ ,\ k = 1\ ,\ \mathcal{A} = \{V_i/V_i\ ,\ \mathrm{Con}\ (V_i)\}_{i\in\{1,2\}}$$

where

$$V_1 = V(x_2^q - x_2 - x_1)\ ,\ V_2 = \mathbf{A}^2 - V_1\ ,\ \mathrm{Con}(V_1) = \{\mathrm{Id.}\} \quad \text{and} \quad \mathrm{Con}(V_2)$$

is empty. Denote Q_2 by a subscript: $Q_2 = \Xi_2$ or V_2. Compute that $t\frac{d}{dt}(\log(Z(\mathcal{A},\Xi_2,t))) = t$: for $x_1 \neq 0$ or $\ell > 1$, there exists $x_2 \in \mathbf{F}(q^\ell)$ with $x_2^q - x_2 - x_1 \neq 0$. Thus $Z(\mathcal{A},V_2,t) = e^t$.

Now compute $t\frac{d}{dt}(\log(Z(\mathcal{A},\Xi_2,t))) = \sum_{\ell=1}^{\infty} q^{\ell-1}t^\ell$: the polynomial $x_2^q - x_2$ takes on $q^{\ell-1}$ distinct values on the field $\mathbf{F}(q^\ell)$. Thus $\frac{d}{dt}(\log(Z(\mathcal{A},\Xi_2,t))) = 1/(1-qt)$ and $Z(\mathcal{A},\Xi_2,t) = (1-qt)^{-1/q}$.

Finally, consider the $\mathcal{B}$ that corresponds to (2.3). For $Q_2 = \Xi_2$,

$$\mathcal{B} = \{C(W_1))/W_1\ ,\ \mathrm{Con}(W_1)\}$$

(i.e., $|J| = 1$), where $W_1 = \mathbf{A}^1$ and $C(W_1) = V(x_2^q - x_2 - x_1) \subseteq \mathbf{A}^2$ maps to W_1 by projection on the first coordinate $(x_1,x_2) \in C(W_1) \to x_1 \in W_1$. Thus $\ell(\mathcal{A},\Xi_2) = 1$; there are no exceptional values

of ℓ .

On the other hand, if $Q_2 = \forall_2$, then $\mathcal{B} = \{\mathbf{A}^1/\mathbf{A}^1 , \mathrm{Con}(\mathbf{A}^1)\}$ where $\mathrm{Con}(\mathbf{A}^1)$ is empty. But, now, in order for (2.3) to hold, $\ell \geq 2$ or $\ell(\mathcal{A},\forall_2) = 2$. ■

§3. The "near rationality" of zeta functions.

It is well known that upper and lower bounds on the cardinality of the $\mathbf{F}(q)$-points on a curve can be given in terms of q and the degree of the curve. The following are the most practical such bounds that we know of. If C is a curve, then C_{ns} denotes the nonsingular points on C .

LEMMA 3.1. *Let $C \subseteq \mathbf{A}^n$ be an affine algebraic curve of degree d defined over $\mathbf{F}(q)$. Then*

$$(3.1)\quad q+1 - (d-1)(d-2)\sqrt{q} - d \leq |C_{ns}(F(\mathbf{q}))| \leq q+1+(d-1)(d-2)\sqrt{q} \ . \ .$$

In particular, if $q > (d-1)^4$, then $|C_{ns}(\mathbf{F}(q))|$ is nonempty.

Proof. This is [FrJ;Theorem 4.9] if $n = 2$. For the general case apply projection from $\mathbf{A}^n$ into $\mathbf{A}^2$ from a linear subspace disjoint from C [H;p.310]. ■

Since explicit calculation is so significant in application of the proof of Theorem 3.2, many times it will be advantageous to revert (e.g., in Part 3 of the proof) to the best known estimates for the maximum number, $N_q(g)$, of points on a nonsingular curve of genus g over $\mathbf{F}(q)$. For fixed q put

$A(q) = \limsup N_q(g)/g$. The Riemann hypothesis estimte, $|N_q-(q+1)| \leq [g2q^{1/2}]$, with $[x]$ the greatest integer in x , implies that $A(q) \leq 2q^{1/2}$. Serre [Se,3] improved Weil's estimate (via interpretation of the Frobenius as an endomorphism on Jacobians) to give the bound $|N_q-(q+1)| \leq g[2q^{1/2}]$. Thus $A(q) \leq [2q^{1/2}]$. But [DrV1] obtained the much improved estimate, $A(q) \leq q^{1/2}-1$. When q is a square this is best possible ([I] and [TsV1Z]). Also, independent of q there exists a constant $c > 0$ such that $A(q) \geq c \log(q)$ [Se,3;Theorem 4] (e.g., $A(2) \geq 8/39$) , but the exact upper and lower bounds for $A(q)$ for general q are still unknown.

Assume that $\mathcal{A}$ is a Galois stratification that satisfies condition (2.5), and that $\mathbf{Q} = (Q_{k+1},\cdots,Q_n)$ is an $(n-k)$-tuple of quantifiers.

THEOREM 3.2. The Poincare series $t\frac{d}{dt}(\log(Z(\mathcal{A},\mathbf{Q},t)))$ is $m_1(t) + t\frac{d}{dt}(\log(Z(\mathcal{B}_{n-k},t)))$ with $Z(\mathcal{B}_{n-k},t)$ the zeta function of an elementary Galois formula in $\mathbf{A}^k$ with all variables free and $m_1(t) \in \mathbf{Z}[t]$. In addition, there is an integer u such that $Z(\mathcal{B}_{n-k},t)^u = f_2(t)/f_3(t)$ with $f_2,f_3 \in \mathbf{Z}[t]$. Therefore $Z(\mathcal{A},\mathbf{Q},t)^u$ is $e^{f_1(t)}(f_2(t)/f_3(t))$ with $f_1 \in \mathbf{Z}[t]$, and f_1,f_2,f_3 and u are explicitly computable.

Proof. In order to isolate the effectiveness computations we break the proof into 7 parts.

Part 1 . Elimination of quantifiers. Consider the discussion up to and

including (2.3). If $k = n$ take $\mathcal{B}_0 = \mathcal{A}$. Otherwise, let $\mathcal{B}$ in (2.3) be $\mathcal{B}_1$. From (2.3),

$$t \frac{d}{dt}(\log(Z(\mathcal{A},\mathbf{Q},t))) =$$

$$p_1(t) + t \frac{d}{dt}(\log(Z(\mathcal{B}_1,(Q_{k+1},\cdots,Q_{n-1}),t)))$$

where $p_1(t)$ is of degree less than $\ell(\mathcal{A},Q_n)$. An easy induction allows us to remove each of the quantifiers in order to finally obtain $\mathcal{B}_{n-k}$ and $p_1(t) + p_2(t) + \cdots + p_{n-k}(t) = m_1(t)$. This proves the first sentence. But an explicit estimate on $\ell(\mathcal{A},Q_n)$ gives an explicit bound on $\deg(p_1(t))$, and by induction, on $\deg(m_1(t))$.

Part 2. Analysis of exceptional ℓ's. In this part all constructions occur over $\mathbf{F}(q^\ell)$. Note that the dependence on ℓ can be quite complicated. Use the notation of (2.3) and let $L_{\mathbf{x}'} = \{(\mathbf{x}',x_n) \in \mathbf{A}^n | x_n \in \mathbf{A}^1\}$. Let $i \in I$ be an index for which $V_i \cap L_{\mathbf{x}'} = L'$ is a nonempty open subset of $L_{\mathbf{x}'}$. The points of $C(V_i)$ that lie over points of L' form a cover $C(V_i)|_{L'} \to L'$. Since, however, $C(V_i)|_{L'}$ may not be connected, this cover may not be Galois. Let C' be a connected component of $C(V_i)|_{L'}$ (as varieties over $\mathbf{F}(q^\ell)$) and let $G(C')$ be the subgroup of $G(C(V_i)/V_i)$ that maps C', by restriction to C', into itself. Clearly, $G(C')$ maps onto $G(C'/L')$. Denote $\mathrm{Con}(V_i) \cap G(C')$ by $\mathrm{Con}(L')$. But, below, identify $\mathrm{Con}(L')$ with its image in $G(C'/L')$.

Identify $G(C'/L')$ with $G(\mathbf{F}(q^\ell)(C')/\mathbf{F}(q^\ell)(L'))$ and let $\mathbf{F}(q')$ be the algebraic closure of $\mathbf{F}(q^\ell)$ in $\mathbf{F}(q^\ell)(C')$: C' is irreducible over $\mathbf{F}(q^\ell)$, but it may not be absolutely irreducible. Denote the elements

of $G(C'/L')$, whose restrictions to $\mathbf{F}(q')$ are the frobenius generator $F_q\ell$ (in §2), by $\hat{G}$. Again, note the dependence of $\hat{G}$ on ℓ. According to [FrS;§4], here is an explicit list of the values ℓ that are exceptional for (2.3).

Either: (i) $Q_n = \Xi_n$ and $Con(L') \cap \hat{G}$ is nonempty, but there exists no $\mathbf{x} \in L'(F(q^\ell))$ for which $F_{\mathbf{x}} \subseteq Con(L') \cap \hat{G}$; or (ii) $Q_n = \forall_n$ and $\hat{G} - Con(L') \cap \hat{G} \stackrel{def}{=} Con(L')^c \cap \hat{G}$ is nonempty, but there exists no $\mathbf{x} \in L'(\mathbf{F}(q^\ell))$ for which $F_{\mathbf{x}} \subseteq Con(L')^c \cap \hat{G}$. Since (i) and (ii) are clearly similar, for explicitness we conclude with case (i).

Part 3. Rephrase of (i) in terms of curves with points in $\mathbf{F}(q^\ell)$. Let $\tau \in G(C'/L')$. Consider a connected component C'' of $C' \otimes \mathbf{F}(q^{ord(\tau)\ell})$, a Galois extension of L' (over $\mathbf{F}(q^\ell)$) whose group we identify with

$$(3.2) \quad \{(\tau_1,\tau_2) \in G(C'/L') \times G(\mathbf{F}(q^{ord(\tau)\ell})/\mathbf{F}(q^\ell)) \mid \tau_1|_{\mathbf{F}(q'')} = \tau_2|_{\mathbf{F}(q'')}\}$$

where $\mathbf{F}(q'') = \mathbf{F}(q') \cap \mathbf{F}(q^{ord(\tau)\ell})$. With the assumption that $\tau|_{\mathbf{F}(q')}$ is $F_q\ell|_{\mathbf{F}(q')}$, let $\hat{\tau}$ be the extension of τ to C'' through the element $(\tau, F_q\ell)$. Denote the quotient of C'' by the group generated by $\hat{\tau}$ by $C'_{\hat{\tau}}$ (Remark 3.3). Then $C'_{\hat{\tau}}$ is an algebraic curve defined over $\mathbf{F}(q^\ell)$. The following statement comes from Part A of the proof of Theorem 1.1 of [Fr,1]. Let $\mathbf{y} \in C'_{\hat{\tau}}$ be an $F(q^\ell)$- rational point that lies over $\mathbf{x} \in L'$. Then $F_{\mathbf{x}}$, for the cover C'/L', contains τ. Furthermore, it is just τ if $\mathbf{y}$ is unramified over $\mathbf{x}$.

At this point we note that condition (2.5) has a complicated effect on whether or not ℓ is exceptional. In order to identify ℓ as unexceptional we have only for some $\tau \in \mathrm{Con}(L') \cap \hat{G}$ to find an integer r with $(r,\mathrm{ord}(\tau)) = 1$ and a point $\mathbf{y} \in C'_{\tau^r}(F(q^\ell))$, with $\mathbf{y}$ unramified over L'. If L' were $\mathbb{P}^1$ - it's not, L' is an open subset of $\mathbb{A}^1$ - having many values of r would not increase the chances for this to happen. Indeed, let C''_r be the normalization of C'_{τ^r}. Then, in this case $|C''_r(\mathbf{F}(q^\ell))|$ is independent of r (Remark 3.4). Thus our analysis is heavily dependent on the degree of $P^1 - L' = D$ as a divisor on $\mathbf{P}^1$. Also, we need not distinguish between the curves C'_{τ^r} for distinct values of r.

From this analysis, we have only to estimate the following quantities in order to apply Lemma 3.1 to complete an upper bound for exceptional ℓ's :

(3.3) a) the degree of $C'_{\hat{\tau}}$ as an open subset of some affine curve $\bar{C}'_{\hat{\tau}} \subseteq \mathbf{A}^{n'}$;

b) the degree of the natural map $C'_{\hat{\tau}} \to L'$; and

c) the number of points of $\bar{C}'_{\hat{\tau}}$ that do not lie over L'.

Indeed, b) and c) give a bound for the number of points of $\bar{C}'_{\hat{\tau}}(\mathbf{F}(q^\ell))$ that must be removed from the estimate of Lemma 3.1 in order to ascertain the existence of $\mathbf{y} \in C'_{\hat{\tau}}(F(q^\ell))$ that lies over $\mathbf{x} \in L'$ and for which $\tau \in F_{\mathbf{x}}$. Since the map of (3.3) b) extends to a map $\bar{C}'_{\hat{\tau}} \to L_{\mathbf{x}'}$, a bound for (3.3) c) is the product of a bounds for b) and for $\deg(L_{\mathbf{x}'}-L')$. Bounds for $\deg(L_{\mathbf{x}}-L')$ and (3.3) b) are quite practical in terms of the polynomials that appear in the description of $C(V_i)$ and V_i.

Part 4. Bounds on the degrees of the polynomials of $\mathcal{B}$. The analysis of

the items in (3.3) depended heavily on the degrees of the polynomials that appear in $C(V_i)$ and V_i. Thus, in order to continue the effective analysis, a key ingredient requires us to bound the degrees of polynomials $g_1',\cdots,g_t',f_1',\cdots,f_s'$, for which $W_j = V(\mathbf{g}';f')$ in the notation of (2.3). Theoretically such a bound, in terms of corresponding degrees for $C(V_i) \to V_i$ in the Galois stratification $\mathcal{A}$, appears in [FrS]. We add some points of explicitness here.

Suppose that $V_i = V(\mathbf{g};f)$ with polynomials $g_1,\cdots,g_t,f_1,\cdots,f_s$. The construction of W_j from V_i starts with the computation of the image $pr(V_i)$ of V_i under $pr:\mathbf{A}^n \to \mathbf{A}^{n-1}$, projection onto the first $n-1$ coordinates. A simple inductive procedure appears in [M;p.97] that reduces this to the computation of an explicit open nonempty subset of $pr(V)$ with $V = V(g_1,\cdots,g_t)$. That is, we want an open subset U of the $(x_1,\cdots,x_{n-1}) \in \mathbf{A}^{n-1}$ such that $g_1,\cdots,g_t$ have a common zero in x_n. Classical elimination theory provides the fundamental theorems to find U [Wae;§80]. For example, if $t = 2$, the classical resultant of g_1 and g_2, as polynomials in x_n, gives $pr(V)$ (and the degree of $pr(V)$ quite explicitly). Furthermore, [FrJ;§26.1] gives details for the complete algorithmic construction of $pr(V_i)$, but at the cost of some extra structural baggage that assumes a finer stratification than we would want in a practical problem (c.f., Remark 2.3).

The next ingredient in the construction of W_j, is the stratification of $pr(V_i)$ by the dimension (0 or 1) of the fibers of the map $V_i \to pr(V_i)$ [M;p.93-94]. For the sake of simplicity in the next comments we assume that these fibers (over $pr(V_i)$) are all of the same dimension and that $pr(V_i)$ is locally closed and normal - a reduction that is part of the stratification procedure. At this point, in the construction of $C(W_j)$,

it is necessary to construct the normalization Z of $pr(V_i)$ in $\mathbf{F}(q)[C(V_i)]$ [FrJ;§26.1]. Finally we must complete polynomials for the variety $C(W_j)$ where we assume that $pr(V_i) = W_j$ and $\mathbf{F}(q)(C(W_j))/\mathbf{F}(q)(W_j)$ is the maximal Galois extension inside the normal closure of the extension $\mathbf{F}(q)(Z)/\mathbf{F}(q)(W_j)$.

In general we can expect nothing less than an exponential growth in the degree computations at each stage. Only a small part of this information,however, gleaned from the classical elimination theory, may be used in any specific problem in order to actually compute $Z(\mathcal{A},\mathbf{Q},t)$. Thus, in practice, the tough tasks listed above may be feasible.

Part 5. Galois stratifications without quantifiers. Parts 2-4 give us an explicit bound on $\deg(m_1(t))$ where $m_1(t)$ appears in Part 1. Thus, in order to conclude the theorem we have only to find an integer u such that $Z(\mathcal{A},t)^u = f_2(t)/f_3(t)$ where $\mathcal{A}$ is a Galois stratification with no quantifiers.

From (2.7), for each $\ell \geq 1$.

$$(3.4)\quad N_\ell = \sum_{i\in I} \left|\{\mathbf{x} \in V_i(F(q^\ell)) \mid F_{\mathbf{x}} \subseteq Con(V_i)\}\right|$$

If we define $N_{\ell,i}$ to be the term on the right that corresponds to $i \in I$, then with $t\frac{d}{dt}(\log(Z_i(t))) = \sum_{\ell=1}^{\infty} N_{\ell,i}t^\ell$, $Z(\mathcal{A},t) = \prod_{i\in I} Z_i(t)$.

Furthermore, since we assume that (2.5) holds, a similar argument reverts us to the case that $I = \{1\}$, $V_1 = V$ and $Con(V) = \{\sigma^{-1}\tau^r\sigma \mid$ with $\quad \in G(C(V)/V)$ and $(r,ord(\tau)) = 1\}$ where τ is a given element of $G(C(V)/V)$.

Let $G = G(C(V)/V)$ and ψ the character of a representation of G . A

theorem of Artin [Se; 12.4] states that if χ is $\mathbb{Q}$-rational then χ is a linear combination of characters of the form 1_H^G, the character induced from the identity on some subgroup H of G. Indeed, Artin's theorem is even more explicit in identifying cyclic groups as the subgroups that occur in this representation. This allows us to write χ as $\sum_{i=1}^{\ell} (a_i/b_i)1_{H_i}^G$ with $a_i, b_i \in \mathbb{Z}$, $(a_i, b_i) = 1$, $i = 1, \cdots, \ell$. Example 6.2 illustrates a simple practical case that takes account of the possible nonregularily of the field extensions. Part 6 (below) of the proof is, therefore, unneccessary for the completion of the proof of this theorem, but it will be used in the proof of Theorem 4.4.

We have reduced the result to finding the L-series, $L(C(V)/V, 1_H^G, t)$ where 1_H^G is the (not necessarily irreducible) character induced from the identity character on a subgroup H of G. Actually, this L-series is $Z(C_H, t)$, the zeta function of the quotient of $C(V)$ by H [CF;p.222] (Remark 3.3). Thus the L-series for χ (above) is $\prod_{i=1}^{\ell} Z(C_{H_i}, t)^{a_i/b_i}$ and the least common multiple b of $b_1, \cdots, b_\ell$ gives an integer power of $L(C(V)/V, Con(V), t)$ that is rational, where χ is the support function for $Con(V)$ in $G(C(V)/V)$. The reader should go to Part 7 for completion of the proof.

Part 6. More on the field crossing argument. For simplicity we assume that $C(V)/V$ is unramified, an assumption that requires only a finer stratification of $\mathcal{A}$. Let $\mathbb{F}(q^d)$ be the algebraic closure of $\mathbb{F}(q)$ in $\mathbb{F}(q)(V)$. Remark 2.2 allows us to replace $\mathbb{F}(q)$ by $\mathbb{F}(q^d)$ (and t by t^d) in order to assume that V is absolutely irreducible over $\mathbb{F}(q)$.

Let $\widehat{\mathbb{F}(q)}$ be the algebraic closure of $\mathbb{F}(q)$ in $C(V)$. In order for there to be $\mathbf{x} \in V(\mathbb{F}(q^\ell))$ such that $F_{\mathbf{x}}$ contains τ^r it is necessary that

$$(3.5)\quad \tau^r\big|_{\widehat{F(q)}} = F_{q^\ell}\big|_{\widehat{F(q)}} .$$

Given (3.5), using Part 3 (the field crossing argument of [Fr,1] applies to any cover $C(V)/V)$) , we may construct algebraic varieties $C(V;\hat{\tau}^r,\ell)$, $\ell = 1,2,\cdots,(r,ord(\tau)) = 1$ and $1 \le r \le ord(\tau)$ with the following properties [Fr,1; Part B of the proof of Theorem 1.1]:

(3.6) a) $C(V;\hat{\tau}^r,\ell)$ is the quotient of a connected component of $C(V) \otimes F(q^{ord(\tau)\ell})$ by the group generated by (τ^r, F_{q^ℓ}) ;

b) for $\mathbf{x} \in V(F(q^\ell))$, $F_{\mathbf{x}}$ contains τ^r if and only if there exists $\mathbf{y} \in C(V;\hat{\tau}^r,\ell)(F(q^\ell))$ over $\mathbf{x}$; and

c) the map from the points $\mathbf{y}$ to the points $\mathbf{x}$ that satisfy b) is exactly $d_\ell = [\widehat{F(q)}F(q^{ord(\tau)\ell}) : \widehat{F(q)}F(q^\ell)]$ to 1 .

Since $F_{\mathbf{x}}$ is a conjugacy class in $G(C(V)/V)$, let c be the number of conjugacy classes in $Con(V)$ and let $\tau^{r(1)},\cdots,\tau^{r(c)}$ run over distinct representatives of the conjugacy classes that make up $Con(V)$.

Denote the cardinality of $C(V;\hat{\tau}^r,\ell)(F(q^\ell))$ by $N_\ell(\hat{\tau}^r)$. From (3.6),

$$(3.7)\quad N_\ell = (1/d_\ell)[\sum_{j=1}^{c} N_\ell(\hat{\tau}^{r(j)})] .$$

At this point we need to recognize that the right side of (3.7) can be written in terms of the coefficient of the ℓth terms of the Poincaré series for a finite set of varieties, $C_1,\cdots,C_s$ (independent of ℓ), $\ell = 1,2,\cdots$. When this is written out explicitly, then it becomes clear that the Poincare series

for $Z(\mathcal{A},t)$ is a linear combination with rational coefficients of the Poincaré series for the zeta functions of $C_1,\cdots,C_s$. To do this, we rephrase all this in terms of Galois theory in the proof of Theorem 4.4.

Part 7. Completion of the proof with Dwork's theorem. From the end of Part 5, we have found an integer u such that $Z(\mathcal{A},t)^u$ can be written as an explicit product of integer powers of zeta functions of the form $Z(C_H,t)$. In the case that C_H is hypersurface in $\mathbf{A}^N$ an explicit bound for the total degree of $Z(C_H,t)$ comes from [D,3; Lemma 14.1,p.489]. An explicit expression for C_H as a locally closed subset of $\mathbf{A}^N$ (see Remark 3.3), as in §2, gives an expression for $Z(C_H,t)$ in terms of zeta functions of hypersurfaces [D,3; equation (2.1) on p.518]. Unfortunately the argument of [D,3] takes quite a job of unraveling. As an alternative, a more explicit calculation appears in [B,2].

Indeed, here Bombieri takes $V = \mathbf{A}^n$, $f \in \mathbf{F}(q)[x_1,\cdots,x_n]$ and he shows that if Tr_k denotes the trace from $\mathbf{F}(q^k)$ down to $\mathbf{F}(p)$, $\psi_k(x) = e^{(2\pi i/p)Tr_k(x)}$, $S_k(\mathbf{A}^n,f) = \sum_{x\in\mathbf{A}^n(\mathbf{F}(q^k))} \psi_k(f(\mathbf{x}))$ and $L(t) =$

$= \sum_{k=1} S_k(\mathbf{A}^n,f)t^k/k$, then $(4\deg(f)+5)^n$ bounds the total degree of $L(t)$. Replace f by $x_0 f(x_1,\cdots,x_n)$ in $\mathbf{A}^{n+1}$. For any value of $x \in \mathbf{A}^n(\mathbf{F}(q^k))$ with $f(\mathbf{x}) \neq 0$, the sum over $x_0 \in \mathbf{F}(q^k)$ gives 0. But, if $f(\mathbf{x}) = 0$, the sum over $x_0 \in \mathbf{F}(q^k)$ gives q^k. Thus $L(t)$ in this case is just the zeta function of the hypersurface with qt replacing t. With an affine variety V of degree d in $\mathbf{A}^n$ [B,2;Theorem 2] gets an analogous result through the observation that, with a computable finite extension of $\mathbf{F}(q)$ replacing $\mathbf{F}(q)$, V can be written as an intersection of no more than $n+1$ hypersurfaces of degree d. Thus we determine a bound on

the total degree of the zeta function for V. For a locally closed subset V of $\mathbf{A}^n$, V can be written as $V_1 - V_2$ with V_1 and V_2 as closed subsets and the Poincaré series for V is the differences of the Poincaré series for V_1 and V_2.

This determines an explicit bound for the total degree of $Z(C_H,t)$. Putting this and the previous results together produces an explicit multiple u_o of u, and $\deg(f_1)$ and bounds on $\deg(f_2) + \deg(f_3)$ in the statement of the theorem. From this we can find f_1, f_2 and f_3 and the actual value of u by explicitly computing the coefficients $N_1, \cdots, N_v$ of $t\frac{d}{dt}\log(Z(\mathcal{A},\mathbf{Q},t))$ for suitably large v. We now show that it suffices to take v to be any integer exceeding $(1+\deg(f_1))(1+\deg(f_2)+\deg(f_3))$. That is, in this case $N_1, \cdots, N_v$ effectively determine $Z(\mathcal{A},\mathbf{Q},t)$.

Without loss we may assume that $f_1(0) = 0$ and that $(f_2/f_3)(0) = 1$. Thus

$$(3.8)\quad a)\quad (f_2/f_3)(t) = \prod_{i=1}^{r}(1-\alpha_i t)/\prod_{j=1}^{s}(1-\beta_j t)\ ,\ \text{and}$$

$$b)\quad u_o N_k = \sum_{i=1}^{r}\alpha_i^k - \sum_{j=1}^{s}\beta_j^k \overset{\text{def}}{=} S(\boldsymbol{\alpha},\boldsymbol{\beta},k) \text{ for}$$

$$k > \deg(f_1)\ ,$$

where u_o is the multiple of u determined at the end of Part 5. Consider $u_o \frac{d^w}{dt^w}(\log(Z(\mathcal{A},\mathbf{Q},t)) =$

$$(3.9)\quad \sum_{i=1}^{r}(\alpha_i)^w/(1-\alpha_i t)^w - \sum_{j=1}^{s}(\beta_j)^w/(1-\beta_j t)^w$$

for $w = \deg(f_1)+1$. Clearly f_2/f_3 is determined by the right side of (3.9), which, being a rational function of degree at most $(\deg(f_1)+1)(s+r)$, is determined by the first $(\deg(f_1)+1)(s+r)+1$ coefficients. These, calculated by hand, are $u_o N_{\deg(t_1)+1}, \cdots, u_o N_v$. In particular, we can calculate $S(\alpha,\beta,k)$ for any specific value of k .

Since the coefficients $\frac{d}{dt}(f_1(t))$ are given by $N_k - S(\alpha,\beta,k)$, $k = 0,\cdots,\deg(f_1)-1$, we have an explicit procedure for computing $f_1(t)$. This concludes the proof of the theorem. ∎

Remark 3.3. Quotients. Parts 2 and 5 of the proof of Theorem 3.2 consider Galois covers $C' \to V'$ and the quotient C'_H of C' by a subgroup H of the Galois group $G(C'/V') = G$. Here V' is a locally closed subset of an affine variety, and thus a union of (not necessarily disjoint) affine varieties. The covering map is finite, and therefore affine [M;p.243, Proposition 5]. Thus, in computing C'_H we are reduced to the case that C' and V' are affine and to the problem of computing the subring of the coordinate ring of C' consisting of elements invariant under H . In the case that C' and V' are both normal varieties (as in Part 5), then C'_H is the normalization of V' in the field of invariants of the function field $\mathbf{F}(q)(C')$ under H . This field of invariants can be computed from explicit generators of $\mathbf{F}(q)(C')$, and the normalization process is explicit from [St]. But, for truly effective calculation, this normalization process can be a bottleneck unless the coordinate ring of C' is generated by a single element over the coordinate ring of V' . This is the condition for

$C' \to V'$ being a basic cover in [FJ;Chapter 5], and this can always be achieved by refining the original stratification. So too, a refinement of the stratification allows us always to assume that C' and V' are normal (and, if desired, that $C' \to V'$ is a basic cover). ■

Remark 3.4. Arithmetically similar curves. Use the notation of Part 3 of the proof of Theorem 3.2. With $(r,\mathrm{ord}(\tau)) = 1$ we compare arithmetic properties of C'' and C''_1, the respective normalizations of C' and $C'_{\hat{\tau}}$. The two curves are isomorphic upon an extension of the coefficient field K $(= \mathbf{F}(q^{\ell}))$. Assume, also, as in Part 3 that $L' = P^1$: that is, the curves are complete (projective).

For a general K it could be that C'' has a K-rational point and C''_1 has none. But, if K is a finite field they both have the same number of K-rational points. The argument goes like this. The respective Picard varieties, $\mathrm{Pic}(C'')$ and $\mathrm{Pic}(C''_1)$, of C'' and C''_1 are abelian varieties defined over K that are isomorphic over an extension of K. Thus [LT] they are isomorphic over K. The cardinality of $C''(\mathbf{F}(q^{\ell}))$ is determined by the zeta function of C'', and the zeta function of C'' is determined by $\mathrm{Pic}(C'')$. Thus $|C''(\mathbf{F}(q^{\ell}))| = |C''_1(\mathbf{F}(q^{\ell}))|$. ■

Remark 3.5. Absolute irreducibility and the definition of Galois stratifications. In the basic definition of Galois stratification for the covers $C(V_i)/V_i$, $i = I$, it is not possible to assume that that V_i is absolutely irreducibility. Part 6, however, of the proof has an important reduction assumption to this case. An alternative to this would have been a slight adjustment in the statement and proof of [Fr,1;Theorem 1.1]. One can foresee practical situations where there would be an algorithmic advantage in avoiding the return to the assumption of absolute irreducibility of V_i,

especially since we have no choice but to consider the possibility that $C(V_i)$ is reducible over $\overline{F(q)}$. ∎

Part 7 of the proof of Theorem 3.2 effectively determines u, f_1, f_2 and f_3 from an explicit multiple u_o of u, a bound on $\deg(f_1)$ and on $\deg(f_2)+\deg(f_3)$. Indeed, since [B,2;loc.sit.] has such an explicit bound on $\deg(f_2)+\deg(f_3)$ in terms of the degrees of the polynomials generating the ideal of the variety, the proof of Theorem 3.2 includes an outline of how to obtain a bound for the computations strictly in terms of the degrees of the polynomials that describe the varieties that appear in the Galois stratification $\mathcal{A}$. The proof essentially reverts this to an effective computation for a bound on the degrees of the polynomials that describe the varieties thast appear in the Galois stratification $\mathcal{B}_{n-k}$.

Besides the problems discussed in Remark 3.3, the key effectiveness computation is of the degrees and dimensions of the locally closed constituants of the image of a variety V in $\mathbf{A}^n$ under projection on the first $n-1$ coordinates (as in Part 4 of the proof).

With [B,2] as a model we propose the following addition to Theorem 3.2.

PROBLEM 3.6. <u>Find an explicit bound for</u> $u + \sum_{i=1}^{3} \deg(f_i)$ <u>in Theorem</u> 3.2 <u>in terms of the degrees and dimensions of the polynomials that appear in the varieties of the Galois stratification.</u>

The main construction of [FrS;p.226, expression (4.1)] starts with an elementary statement (or, more generally, a Galois stratification) over $\mathcal{O}_K[1/a]$, the ring of integers of a number field K localized away from the primes dividing an integer a. Note: Galois stratification here means that the properties given in Section 1 hold over the number field K, but

the coefficients of the defining polynomials are in $\mathcal{O}_K[1/a]$. As in the previous work we assume that this is a Galois stratification in n variables, $x_1,\cdots,x_n$. Given a set of quantifiers $Q_n,Q_{n-1},\cdots,Q_{k+1}$, it then produces Galois stratifications $\mathcal{B}_i = \{C(W_j^i)/W_j^i\ ,\ Con(W_j^i)\}_{j\in J_i}$ over $\mathcal{O}_K[1/a_i]$ with underlying space $\mathbf{A}^{n-i}$, $i = 1,\cdots,k$, and an integer a_o where $a|a_o$ and $a_i|a_{i+1}$, $i = 0,\cdots,k-1$. We now explain further properties.

The key property is that $\mathcal{A}$ (resp. $\mathcal{B}_i$) is a Galois stratification over $\mathrm{Spec}(\mathcal{O}_K[1/a_o])$ (resp., $\mathrm{Spec}(\mathcal{O}_K[1/a_i])$, $i = 1,\cdots,k$) . This means that for each prime $\mathfrak{p}$ of $\mathcal{O}_K[1/a_o]$ the reduction modulo $\mathfrak{p}$ of the data $\{C(V_i)/V_i\}_{i\in I}$ (as in §1) is a Galois stratification over $\mathcal{O}_K[1/a_o]/\mathfrak{p}$ with natural isomorphisms of $G(C(V_i)/V_i)$ and $G(C(V_i)\mathrm{mod}(\mathfrak{p})/V_i\mathrm{mod}(\mathfrak{p}))$, $i \in I$. Similarly, $\mathcal{B}_i$ is a Galois stratification over $\mathrm{Spec}(\mathcal{O}_K[1/a_i])$, $i = 1,\cdots,k$. Furthermore, for each prime $\mathfrak{P}$ of $\mathcal{O}_K[1/a_i]$, for each finite field extension $\mathbf{F}(q^\ell)$ of $\mathbf{F}(q) = \mathcal{O}_K[1/a_i]/\mathfrak{P}$ and for each $\mathbf{y} \in \mathbf{A}^{n-i}(\mathbf{F}(q^\ell))$

(3.10) $[\mathbf{y} \in \bigcup_{j\in J_i} Con(W_j^i \mathrm{mod}(\mathfrak{p}))]$ if and only if

$$(Q_{n-i+1}x_{n-i+1})\cdots(Q_n x_n)[(\mathbf{y},x_{n-i+1},\cdots,x_n) \in \bigcup_{i\in I} Con(V_i\mathrm{mod}(\mathfrak{p}))]$$

with $x_{n-i+1},\cdots,x_n \in \mathbf{F}(q^\ell)$.

In particular, in the analysis of Part 2 of the proof of Theorem 3.2, for each prime $\mathfrak{p}$ of $\mathcal{O}_K[1/a_k]$ there are no exceptional ℓ's . From this we conclude that the zeta function, $Z(\mathcal{A}\mathrm{mod}(\mathfrak{p}),\mathbf{Q},t)$ has no exponential factor:

THEOREM 3.7. *In the notation above, for each prime $\mathfrak{p}$ of $\mathcal{O}_K[1/a_k]$, there exists an explicitly computable integer u (independent of $\mathfrak{p}$) such that*

$Z(\mathcal{A} \bmod(\mathfrak{p}),\mathbb{Q},t)^u = f_2(t)/f_3(t)$ with $f_2,f_3 \in \mathbb{Z}[t]$ where $\deg(f_2)+\deg(f_3)$ is bounded by an explicitly computable integer (independent of p).

Of course, the minimal integer u , the actual degree of the rational function f_2/f_3 and the polynomials f_2 and f_3 in Theorem 3.7 are expected to be dependent on p in most cases.

Although it is premature for us to discuss "good" and "bad" primes, any such discussion must ultimately be concerned with effective computation of the primes that divide the integer a_k that appears in Theorem 3.7. We conclude this section with an example and discussion that relates Theorem 3.2 and 3.7 through their most elementary aspects: the respective factorizations of a polynomial over a finite field and over $\mathbb{Z}$.

Ex 3.8. Factorization of a polynomial. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree n and denote by P the elementary statement that expresses that $f(x)$ is irreducible: P is the disjunction of P_j , the existential statement in the "variable" coefficients of $g(x)$, $h(x)$ with g monic and of degree j , that expresses the equating of the coefficients on the left and right sides of $g(x)h(x) = f(x)$, $j = 1,\cdots,[n/2]$. That is, P_j is of the form $(\exists \mathbf{x}_j)[\mathbf{x}_j \in V_j]$ where V_j is an algebraic set of dimension 0 . Even to start the Galois stratification procedure on V_j , as in Ex. 2.1, either over $\mathbb{F}(q)$ or over $\mathbb{Z}$, requires us to decompose V_j into K-irreducible components with $K = \mathbb{F}(q)$ or $\mathbb{Q}$, respectively. In other words, the introduction of $V_1,\cdots,V_{[n/2]}$, while of theoretical value, provides no finesse around the problem of finding the K-components of the set $W - W(f) \subseteq \mathbb{A}^1$. ∎

The details of the proofs of Theorems 3.2 and 3.7 ultimately depend,

respectively, on a procedure to find the K-irreducible components of $W(f)$ for $K = F(q)$ or $\mathbb{Q}$ and Example 3.8 shows this to be a special case of our considerations. An elementary but extensive discussion, with many examples, of Berlekamp's deterministic algorithm [Be] in the case $K = F(q)$ appears in [LiP;Chapter 3, §4]. Starting with [CaZ], the last few years have seen the development of probabilistic algorithms for factorization over finite fields: the time of computation depends on random choices, but with high probability the computation will be complete in a time that is feasible for serious examples of the kind for which Theorem 3.2 is intended.

It is well known that a check for the $\mathbb{Q}$-irreducible components of $W(f)$ that depends on computation of the $Z/(p)$-irreducible components of $W(f)$ mod(p) may require an inspection of an enormous number of primes p. Apparently [LeLeLo] is the most practical procedure for this computation.

§4. (Artin) L-series on a Galois stratification.

Let $\varphi: C(V) \to V$ be a Galois cover of $\mathbf{F}(q)$-normal sets as in §2. Suppose that χ is a (complex) character of $G(C(V)/V)$ (i.e., the trace function composed with a complex representation of G). The (Artin) L-series, $L(C(V)/V,\chi,t)$, associated to χ can be defined by its Poincaré series as follows. Let $N_\ell = N_\ell(\chi)$ be the sum $\sum_{x \in V(F(q^\ell))} \chi(F_x)$, $\ell = 1,2,\cdots$, where

F_x is the Frobenius set explained between expressions (2.2) and (2.3): $\chi(F_x) = \chi(\sigma)$ for $\sigma \in F_x$ if χ is constant on F_x and $\chi(\sigma) = 0$ otherwise. Then $L(C(V)/V,\chi,t)$ is defined by the formula

$$t\frac{t}{dt}(L(C(V)/V,\chi,t)) = \sum_{\ell=1}^{\infty} N_\ell t^\ell \tag{4.1}$$

and $L(C(V)/V,\chi,0) = 1$. It is well known that $L(C(V)/V,\chi,t)$ is rational. Furthermore, even if χ is only a virtual character (i.e., a linear combination with coefficients in $\mathbf{C}$ of actual characters of G) , the Poincaré series is rational.

In this section we generalize §3 by defining L-series on a Galois stratification. Much of the work for the explicit computation analogue of Theorem 3.2 has already been done in the proof of Theorem 3.2. Explicit computation, however, of the total degree of a general (Artin) L-series cannot be reverted to the computation for zeta functions, say, from the simple observation that the product of this with other L-series related to the same cover is a zeta function. The problem is that there is possible cancellation of zeros or poles of one series by those of another. Thus Theorem 4.3 is based on a natural, but difficult to check hypothesis which evolves from a representation theory result (Lemma 4.2). Theorem 4.4 is a bit of a grab bag: it gives situations where [ASp] and [B,2] can be applied to show that the hypothesis of Theorem 4.3 holds; and it follows ideas of [B,3] and [Fr,1] to give a possible alternative approach to establishing Theorem 4.3 without the additional hypothesis. As Adolphson, Sperber and others continue their work the incompleteness of these results may disappear.

In some applications we might expect L-series to aid in the identification of the zeta functions of §3 with an Euler factor arising from some classical function (e.g., a modular function). In such cases we would have especially precise information on the variation of $Z(\mathcal{A} \bmod(p),\mathbf{Q},t)$ with p in Theorem 3.7 and an understanding of "exceptional p ." Such applications, however, lie in the future.

Let $\mathcal{A}^j = \{C(V_i^j)/V_i^j\ ,\ \mathrm{Con}(V_i^j)\}_{i\in I(j)}$ be a Galois stratification of

$\mathbf{A}^n$ over $\mathbf{F}(q)$, $j = 1,2$. The process of <u>amalgamation</u> [FrS;p.212] produces from $\mathcal{A}^1$ and $\mathcal{A}^2$ a new Galois stratification of $\mathbf{A}^n$ over $\mathbf{F}(q)$. It is denoted $\mathcal{A}^1 \times_{\mathbf{A}^n} \mathcal{A}^2 = \{C(W_k)/W_k, Con(W_k)\}_{k\in J}$ where the data has the following properties: $\dot{\bigcup}_{k\in J} W_k$ is a stratification of $\mathbf{A}^n$ (by $\mathbf{F}(q)$-irreducible normal subsets) that is finer than the stratification $\dot{\bigcup}_{i\in I(j)} V^j_i$, $j = 1,2$; if $W_k \subseteq V^1_{i(1)}$ and $W_k \subseteq V^2_{i(2)}$, then $C(W_k)$ is an $\mathbf{F}(q)$-irreducible component of the fiber product $C(V^1_{i(1)}) \times_{W_k} C(V^2_{i(2)})$ via the embedding of W_k in $V^j_{i(j)}$ and the maps $C(V^j_{i(j)}) \to V^j_{i(j)}$, $j = 1,2$; and, in the identification of $G(C(W_k)/W_k)$ with a subgroup of $G(C(V^1_{i(1)})/V^1_{i(1)}) \times G(C(V^2_{i(2)})/V^2_{i(2)})$, $Con(W_k)$ consists of the conjugacy classes of elements $(\sigma_1,\sigma_2) \in G(C(W_k)/W_k)$ such that σ_j represents an element of $Con(V^j_{i(j)})$, $j = 1,2$.

For a given Galois cover $C(V) \to V$ equipped with a union, $Con(V)$, of conjugacy classes of the Galois group, we may regard the support function $1_{Con(V)}$, as a virtual character. Suppose that, in place of $Con(V^j_i)$ above, we are given a virtual character χ^j_i of the Galois group of $C(V^j_i) \to V^j_i$. In this case call $\mathcal{A}^j$ a <u>Galois stratification with</u> (virtual <u>characters</u>. Then define $\mathcal{A}^1 \times_{\mathbf{A}^n} \mathcal{A}^2$ as above except that (in the notation above) we replace $Con(W_k)$ by the virtual character that takes the value $\chi^1_{i(1)}(\sigma_1)\chi^2_{i(2)}(\sigma_2)$ on the conjugacy class of $(\sigma_1,\sigma_2) \in G(C(W_k)/W_k)$.

Finally let $\mathcal{A} = \{C(V_i)/V_i, Con(V_i)\}_{i\in I}$ be a Galois stratification on $\mathbf{A}^n$ over $\mathbf{F}(q)$, let k be an integer between 0 and n , let $Q_{k+1},\cdots,Q_n$ be quantifiers and let $\mathcal{B} = \{C(W_j)/W_j\ ,\ \chi_j\}_{j\in J}$ be a Galois stratification with characters of $\mathbf{A}^k$ over $\mathbf{F}(q)$. For each integer $\ell \geq 1$, define $N_\ell = N_\ell(\mathcal{A},\chi,Q)$ to be

(4.2) a)
$$\sum_{\mathbf{x}'\in\mathbf{A}^k(\mathbf{F}(q^\ell))} \chi(F_{\mathbf{x}'})$$

where the sum is over $\mathbf{x}' = (x_1,\cdots,x_k) \in \mathbb{A}^k(\mathbf{F}(q^\ell))$ such that

(4.2) b) $$(Q_{k+1}x_{k+1})\cdots(Q_n x_n)[(\mathbf{x}',x_{k+1},\cdots,x_n) = \mathbf{x} \in \dot{\bigcup_{i\in I}} \mathrm{Con}(V_i)]$$

holds in $\mathbf{F}(q^\ell)$ and $\chi(F_{\mathbf{x}'})$ is defined to be $\chi_j(F_{\mathbf{x}'})$ if $\mathbf{x}' \in W_j$.

As in §2, define $L(\mathcal{A},\chi_{\mathcal{B}},\mathbf{Q},t)$ by its Poincaré series:

(4.3) $$t\frac{d}{dt}(\log(L(\mathcal{A},\chi_{\mathcal{B}},\mathbf{Q},t))) = \sum_{\ell=1}^{\infty} N_\ell t^\ell .$$

Note, too, as in §3, given $\mathcal{A}$ and quantifiers $Q_1,\cdots,Q_n$, each integer k between 0 and n and each stratification with characters $\mathcal{B}$ of $\mathbb{A}^k$ gives an L-series.

Def. 4.1. Let G be a group, let χ be a character of G and let q_0 be a fixed power of p. Suppose that if $\varphi:C(V) \to V$ is any galois cover of $\mathbf{F}(q)$ - normal sets where $q_0|q$ and $G(C(V)/V)$ is isomorphic to a subgroup of G, then the total degree of $t\frac{d}{dt}\log(L(C(V)/V,\chi,t))$ is explicitly computable. In the L-series here, χ denote the restriction of the original character to $G(C(V)/V)$. We say that χ is (explicitly) computable as an L-series character.

If, in the Galois stratification $\mathcal{B} = \{C(W_j)/W_j,\chi_j\}_{j\in J}$, each of the χ_j is computable as an L-series character, we say that $\mathcal{B}$ has (explicitly) computable characters. Note that we suppress the dependence of this definition on q_0. We now start the discussion of the representation theory observation which concludes the proof of Theorem 4.3.

Let $u:G \to K$ and $u_1:G_1 \to K$ be surjective homomorphisms of finite groups. Consider the fiber product $\bar{G} = \{(\sigma,\sigma_1) \in G \times G_1 \mid u(\sigma) = u_1(\sigma_1)\}$.

Let H_1 be a subgroup of G_1 and let χ be a character of G. Define $\chi \times 1_{H_1}^{G_1}$ to be the character of $\bar{G}$ defined by the formula

$$\chi \times 1_{H_1}^{G_1}(\sigma,\sigma_1) = \chi(\sigma)1_{H_1}^{G_1}(\sigma_1) \quad \text{for} \quad (\sigma,\sigma_1) \in \bar{G}. \tag{4.5}$$

Finally, let $\bar{H}$ be $\bar{G} \cap G \times H_1$ and denote the projections of $\bar{G}$ to G and G_1, respectively, by pr and pr_1.

LEMMA 4.2. *The representation induced on $\bar{G}$ by the representation $\chi \times 1_{H_1}$ on $\bar{H}$ is $\chi \times 1_{H_1}^{G_1}$:*

$$\chi \times 1_{H_1}^{G_1} = (\chi \times 1_{H_1})_{\bar{H}}^{\bar{G}} \tag{4.6}$$

Proof. Let $\alpha_1,\cdots,\alpha_r$ be representatives of the cosets of H_1 in G_1. Since the projection of $\bar{G}$ into G_1 is surjective, there exist $\bar{\alpha}_1,\cdots,\bar{\alpha}_r \in \bar{G}$ that project, respectively, to $\alpha_1,\cdots,\alpha_r$. Thus $\bar{\alpha}_1,\cdots,\bar{\alpha}_r$ are coset representatives of $\bar{H}$ in $\bar{G}$, and for $\bar{\sigma} \in \bar{G}$, then $\bar{\alpha}_i\bar{\sigma}\bar{\alpha}_i^{-1} \in \bar{H}$ if and only if $\alpha_i pr_1(\bar{\sigma})\alpha_i^{-1} \in H_1$, $i = 1,\cdots,r$. By definition of the induced representation, for $(\sigma,\sigma_1) \in \bar{G}$,

$$1_{H_1}^{G_1}(\sigma_1) = \sum_{i=1}^{r} 1_{H_1}(\alpha_i\sigma_1\alpha_i^{-1}), \quad \text{and} \tag{4.7 a)}$$

$$(\chi \times 1_{H_1})_{\bar{H}}^{\bar{G}}(\sigma,\sigma_1) = \sum_{i=1}^{r} 1_{\bar{H}}(\bar{\alpha}_i(\sigma,\sigma_1)\bar{\alpha}_i^{-1})1_{H_1}(\alpha_i\sigma_1\alpha_i^{-1})\chi(\sigma) \tag{4.7 b)}$$

where 1_{H_1} (resp., $1_{\bar{H}}$) in this context denotes the support function for H_1 (resp., $\bar{H}$). From the above comment, the right side of (4.7) b) is just $\sum_{i=1}^{r} 1_{H_1}(\alpha_i\sigma_1\alpha_i^{-1})\chi(\sigma) = \chi(\sigma)1_{H_1}^{G_1}(\sigma_1)$. This establishes (4.6). ∎

THEOREM 4.3. Let $\mathcal{A}$ be a Galois stratification of $\mathbf{A}^n$ over $\mathbf{F}(q)$, and, with $0 \le k \le n$, let $\mathcal{B}$ be a Galois stratification with computable characters of $\mathbf{A}^k$ over $\mathbf{F}(q)$. Then $t\frac{d}{dt}(\log(L(\mathcal{A},\chi_{\mathcal{B}},\mathbf{Q},t)))$ is an explicitly computable element of $\mathbf{Q}(t)$.

Proof. Theorem 3.2 produces from $\mathcal{A}$ a Galois stratification $\mathcal{B}_1 = \{C(U_s)/U_s, \mathrm{Con}(U_s)\}_{s\in S}$ of $\mathbf{A}^k$ over $\mathbf{F}(q)$ and an integer ℓ_o with the following properties. Suppose that $\ell \ge \ell_o$ and $x' \in \mathbf{A}^k(\mathbf{F}(q^\ell))$. Then $x' \in \dot{\bigcup}_{s\in S} \mathrm{Con}(U_s)$ if and only if (4.2) b) holds. Conclude that the sum (4.2) a) is the same as the sum

$$\sum''_{x'\in\mathbf{A}^k(\mathbf{F}(q^\ell))} \chi(F_{x'}) \tag{4.7}$$

where Σ'' signifies a sum over elements $x' \in \bigcup_{s\in S} \mathrm{Con}(U_s)$. Therefore for $\ell \ge \ell_o$, N_ℓ is

$$\sum_{x'\in\mathbf{A}^k(\mathbf{F}(q^\ell))} \chi(F_{x'})\chi_1(F_{x'}) \tag{4.8}$$

where χ_1 is the character representing the support function for $\dot{\bigcup}_{s\in S} \mathrm{Con}(U_s)$. Thus we are reduced to proving that the Poincaré series (with no quantifiers) for the Galois stratification with characters, $\mathcal{B}_{\mathbf{A}^k} \times \mathcal{B}_1$, is an explicitly computable rational function.

From this point follow Part 5 of the proof of Theorem 3.2. We have only to show that a Poincaré series $t\frac{d}{dt}(\log(L(C(W)/W,\chi',t)))$ is an explicitly computable rational function of t where the following conditions hold: W

is a locally closed normal subset of $\mathbf{A}^k$ over $\mathbf{F}(q)$; $C(W)/W$ is a Galois cover (as previously) whose group is identified with a subgroup $\bar{G}$ of $G \times G_1$ where G is the Galois group of one of the covers that appears in $\mathcal{B}$; projection of $\bar{G}$ on each of the factors G and G_1 is surjective, and the situation prior to Lemma 4.2 holds; and χ' is a virtual character that takes the value $\chi(\sigma)\chi_1(\sigma_1)$ on $(\sigma,\sigma_1) \in G \times G_1$ where χ is computable as an L-series character and χ_1 is a support character for a union of conjugacy classes of G_1 that satisfies condition (2.5).

From Artin's theorem, as in Part 5 of the proof of Theorem 3.2, we may assume that χ_1 is $1_{H_1}^{G_1}$. Now apply Lemma 4.2 to replace χ' by $(\chi \cdot 1_{H_1})_{\bar{H}}^{\bar{G}}$. Then [CF;p.222] shows that $t\frac{d}{dt}(\log(L(C(W)/W,\chi',t)))$ is the same as $t\frac{d}{dt}(\log(L(C(W')/W',\chi,t)))$ where $C(W')/W'$ is a Galois cover with group isomorphic to the projection H of $\bar{H}$ onto G. Here χ again denotes restriction of χ on G to H. By the assumptions, this latter Poincaré series is explicitly computable. This concludes the proof of the theorem. ■

Let $C(V) \to V$ be a Galois cover, as above, over $\mathbf{F}(q)$ and let χ be a character of $G(C(V)/V)$. A well known formula relates the L-series over $\mathbf{F}(q)$ to that over $\mathbf{F}(q^m)$:

$$(4.9) \qquad L((C(V)/V)\otimes\mathbf{F}(q^m),\chi,t^m) = \prod_{k=0}^{m-1} L(C(V)/V,\chi,e^{2\pi ki/m}t) .$$

Thus, if we could be certain that none of the zeros or poles of $L(C(V)/V,\chi,t)$ are canceled by those of another factor on the right side of (4.9), then we could assert tht the total degree of the left side gives a bound on the total degree of $L(C(V)/V,\chi,t)$. Unfortunately, the noncancellation statement is false in general. Thus in Definition 4.1 (and Theorem 4.4) we are not free to

extend the base finite field.

THEOREM 4.4. Let $\mathcal{A}$ be a Galois stratification of $\mathbf{A}^n$ over $\mathbf{F}(q)$ and, with $0 \leq k \leq n$, let $\mathcal{B}$ be a Galois stratification with the following property: For $C(W)/W$ a cover that appears in $\mathcal{B}$, the order m of the group satisfies either $m|q-1$ or $m = pm_o$ where $m_o|q-1$. Then $t\frac{d}{dt}(\log(L(\mathcal{A},\chi_{\mathcal{B}},\mathbf{Q},t)))$ is an explicitly computable element of $\mathbf{Q}(t)$.

Even without the hypothesis on $|G(C(W)/W)|$ there exists an integer $r_o = r_o(\mathcal{B})$ such that if ρ is a characteristic root of $L(C(W)/W,\chi,t)$ then ρ^r/ω is a root of 1 with r an integer dividing r_o and ω is a characteristic root of an explicitly computable zeta function. If r_o is explicitly computable, then $t\frac{d}{dt}(\log(L(\mathcal{A},\chi_{\mathcal{B}},\mathbf{Q},t)))$ is an explicitly computable element of $\mathbf{Q}(t)$.

Proof (with a proviso from [ASp]). The 1st paragraph of the statement follows from Theorem 4.3 once we demonstrate that $\mathcal{B}$ has computable characters (relative to q_o). For this we need to know that each character of G is a linear combination with rational coefficients of characters induced from characters of cyclic subgroups of G [Se;p.87]. Again from [CF;p.222], this reduces the 1st paragraph of the statement of the theorem to the case where $C(W)/W$ is a cyclic cover whose degree m has the stated properties. If $m = p$, then [B,2], as recounted in Part 7 of the proof of Theorem 3.2 shows, for χ any character of $G(C(V)/V)$, that χ is (explicitly) computable as an L-series character. On the other hand, if $(m,p) = 1$, the condition $m|q-1$ allows us to express $C(W)/W$ as a Kummer cover. In the case that $W = \mathbf{A}^n$, [ASp] give an explicit bound on the total degree of $L(C(W)/W,\chi,t)$. They then say [Asp;p.327]: "We believe the methods of this paper will lead to

similar treatment of 'mixed' sums of the type $\sum_{x\in(\mathbf{F}(q)^x)^n} \chi(\mathbf{g}(x))\psi(\mathbf{f}(x))$, where $f,g \in \mathbf{F}(q)[x_1,\cdots,x_n]$, χ is a multiplicative character of $\mathbf{F}(q)^x$, and Ψ is an additive character on $\mathbf{F}(q)$." If this statement holds, then the trick used in [B,2] to go from $W = A^n$ to a general subvariety of $\mathbf{A}^n$ applies here also. That is, if W is the locus of $f_1(\mathbf{x}) = 0,\cdots,f_n(\mathbf{x}) = 0$, replace $\Psi(f(\mathbf{x}))$ in the above sum by $\Psi(y_1f_1(\mathbf{x})+\cdots+ y_mf_n(\mathbf{x}))$ and replace $\sum_{x\in(F(q)^x)^n}$ by $\sum_{x\in(F(q)^x)^n}\sum_{y\in(F(q)^x)^m}$ to obtain an expression for the sum over $W(F(q))$ with the coordinate hyperplanes removed. From this to the desired solution is a well known combinatorial step.

The rest of the proof concentrates on the last paragraph of the statement of the theorem, and, as above, we are reduced to the case that $C(W)/W$ is a cyclic cover (and χ is an actual, not virtual, character). The statement on the characteristic roots is the last corollary of [B,3;p.29]. If r_o is explicitly computable, this gives a bound on the degrees of the Poincaré series from a bound on the degrees of zeta functions, and thus concludes the theorem.

Since [B,3] relies on a fairly sophisticated discussion, is missing many details and is not readily available, we give an alternative discussion that follows readily from Part 6 of the proof of Theorem 3.2, whose notation we now use: $C(V)/V$ is a cyclic cover with group generated by τ . The adjustments for the case when $\widehat{\mathbf{F}(q)}$ differs from $\mathbf{F}(q)$ are easy, but the notation simplifies if we assume $\widehat{F(q)} = F(q)$. Throughout we supress V whenever possible. The remaining argument has 4 parts.

Part 1: Introduction of a special subseries of the Poincaré series.

Designate $\mathrm{ord}(\tau)$ by $s = \prod_{i=1}^{t} p_i^{e_i}$, $p_1,\cdots,p_t$ distinct primes, $e_i \geq 1$, $i = 1,\cdots,t$. Let u be any positive integer that is a product of nonegative powers of $p_1,\cdots,p_t$ (e.g., $u = 1$). For a given u let $I_u = \{ku \mid (k,s)=1\}$. Our first goal is to show that if

$$\sum_{\ell=1}^{\infty} N_\ell t^\ell = t\frac{d}{dt}\log(L(C(V)/V,\chi,t)) \text{ , then}$$

$$s\Big(\sum_{\ell\in I_u} N_\ell t^\ell\Big) = \sum_{j=1}^{s} P_u(V_{j,u}\omega_j t^u) \tag{4.10}$$

where $V_{j,u}$ is an explicitly computable variety defined over $\mathbf{F}(q^u)$, ω_j is an sth root of 1, $P(V_j,t)$ is the Poincaré series for $V_{j,u}$ over $\mathbf{F}(q^u)$ and $P_u(t^u)$ denotes the sum over terms of $P_u(t^u)$ whose degrees are in I_u, $j = 1,\cdots,s$.

Consider first a Poincaré series related to the left side of (4.10), $\sum_{\ell\in I_u} N_\ell(\tau)t^\ell$, where $N_\ell(\tau) = \left|\{\mathbf{x} \in V(F(q^\ell)) \mid F_{\mathbf{x}} = \tau\}\right|$. We want an expression for this of the form of the right side of (4.10). As in (3.6), for any given ℓ, consider the variety $C(V;\hat{\tau},\ell) \overset{\text{def}}{=} C_{\tau,\ell}$ formed from a quotient of a connected component of $C(V) \otimes \mathbf{F}(q^{\mathrm{ord}(\tau)\ell})$ by the group generated by (τ,F_q^ℓ). Then, with our assumption that $\widehat{\mathbf{F}(q)} = \mathbf{F}(q)$, we have $[\mathbf{F}(q^{\mathrm{ord}(\tau)\ell}):\mathbf{F}(q^\ell)] = s$ and

$$N_\ell(\tau) = \left|C_{\tau,\ell}(\mathbf{F}(q^\ell))\right|/s \text{ .} \tag{4.11}$$

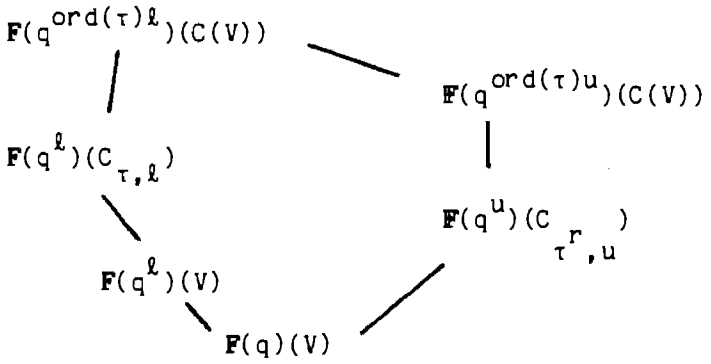
Part 2. A Galois Theoretic diagram. We now show that for r such that $r(\ell/u) \equiv 1 \bmod(s)$,

$$C_{\tau,\ell} = C_{\tau^r,u} \otimes \mathbf{F}(q^\ell) \quad \text{(recall } C_{\tau,u} \text{ is defined over} \tag{4.12}$$

$$\mathbf{F}(q^u)) \ .$$

As this is Galois theoretic, we do it on the level of function fields:

(4.13)



By degree computation, (4.12) follows if and only if the subgroup generated by (τ, F_q^{ℓ}) maps surjectively (by restriction to $\mathbf{F}(q^{ord(\tau)u})(C(V))$) to the subgroup of $G(\mathbf{F}(q^{ord(\tau)u})(C(V))/\mathbf{F}(q)(V))$ generated by (τ^r, F_q^u) . Identify (τ, F_q^{ℓ}) with $(1,\ell) \in \mathbf{Z}/(s) \times \mathbf{Z}/(\ell s)$ (and $(r,u) \in Z/(s) \times Z/(us)$) where restriction maps $(1,\ell)$ to $(1,\ell) \in \mathbf{Z}/(s) \times \mathbf{Z}/(us)$ via the canonical map $\mathbf{Z}/(\ell s) \to \mathbf{Z}/(us)$. Since $r\ell \equiv u \bmod(us)$, (4.12) follows.

From (4.11) and (4.12) (after the substitution of τ for τ^r) :

(4.14)
$$sN_{\ell} = \sum_{j=1}^{s} \chi(\tau^j)^{\ell/u} |C_{\tau^j,u}(\mathbf{F}(q^{\ell}))| \ .$$

This concludes (4.10) with $C_{\tau^j,u} = V_{j,u}$, $\omega_j = \chi(\tau^j)$, $j = 1,\cdots,s$.

Part 3: Convolution with the Mobius function. With $s' = p_1 \cdots p_t$, consider the classical identity

$$\sum_{k=1}^{\infty} \sum_{m|s'} \mu(m) a_{mk} t^{mk} = \sum_{(\ell,s')=1} a_\ell t^\ell ,$$

where $\mu(m)$ is the Mobius function evaluated at m. Apply this to both sides of (4.10):

$$(4.15) \qquad s\Big(\sum_{k=1}^{\infty} \sum_{m|s'} \mu(m) N_{ukm} t^{ukm}\Big) =$$

$$\sum_{j=1}^{s} \sum_{k=1}^{\infty} \sum_{m|s'} \mu(m) \omega_j^{km} N_{ukm}(V_{j,u}) t^{ukm} .$$

In terms of L-series, this becomes (cf., (7) in Theorem 2 of [B,3])

$$(4.16) \qquad \prod_{m|s'} L(C(V)/V \otimes \mathbf{F}(q^{mu}), \chi, t^{mu})^{s\mu(m)/mu}$$

$$\prod_{j=1}^{s} \prod_{m|s'} Z(V_{j,u} \otimes \mathbf{F}(q^{mu}), \omega_j^m t^{mu})^{\mu(m)/mu} .$$

Denote the uth power of the right side of (4.16) by $Z_u^*(t^u)$. On the other hand, the sum (4.10) (as given on the right side of (4.15)) over positive integers u that are products of nonnegative powers of $p_1, \cdots, p_t$ gives this L-series interpretation (cf., (8) of Theorem 3 of [B,3]):

$$(4.17) \qquad L(C(V)/V, \chi, t)^s = \prod_{u = \prod_{i=1}^{t} p_i^{z_i}} (Z_u^*(t^u))^{1/u} , \quad z_i \geq 0, i = 1, \cdots, t .$$

Part 4: Computation of r_o (in the statement of the theorem). Let a be a positive integer. An induction on a using (4.16) gives

$$(4.18) \qquad \prod_{m|s'} L(C(V)/V \otimes \mathbf{F}(q^{m^a}), \chi, t^{m^a})^{s\mu(m)(s'/m)^a} =$$

$$\prod_{u|(s')^a}{}' \; Z_u^*(t^u)^{(s')^a/u}$$

where π' indicates that the product excludes u if it is a multiple of m^a for $m|s'$, $m > 1$. For example, if we put both sides of (4.16) to the s' power, then $u = 1$ gives the case $a = 1$ in (4.18). Note that the term corresponding to $m = 1$ in the left side of (4.18) is $L(C(V)/V,\chi,t)^{s(s')^a}$.

We choose r_o to be the smallest integer of the form $(s')^a$ such that $L(C(V)/V,\chi,t) = L(t)$ and $L(C(V)/V \otimes \mathbf{F}(q^{m^a}),\chi,t^{m^a}) = L(t,m^a)$ have no common characteristic factors for each $m|s'$, $m > 1$. For example, chose a so that each of p_i^a, $i = 1,\cdots,t$, exceeds $\deg(L(t))$ (the usual degree for a rational function). Then a common characteristic factor, $1 - \theta t$, of $L(t)$ and $L(t,m^a)$ would produce the collection $\{1 - \zeta\theta t\}$, where ζ runs over m^a th roots of 1, of distinct common characteristic factors, contrary to our assumption on $\deg(L(t))$. Since, of course, we are trying to estimate $\deg(L(t))$, this only shows the existence of r_o. Indeed, additional arguments using the multiplicities of factors in the left side of (4.18) suggest that, perhaps, any $(s')^a$ exceeding s might work for r_o.

§5. Zeta functions for p-adic problems.

For p a prime, denote the p-adic numbers by $\mathbf{Q}_p$, its ring of integers by Z_p, and the ring of integers of the unique unramified extension of $\mathbf{Q}_p$ of degree ℓ by R_ℓ, $\ell = 1,2,\cdots$. Everything in this section works as well, excluding perhaps the notation, when $\mathbf{Q}_p$ is replaced by any completion of a number field K at a prime over p. We let p denote a generator of the maximal ideal of each of the local rings R_ℓ, $\ell = 1,2,\cdots$.

Fix an integer $e \geq 1$ and let V be an algebraic subvariety of $\mathbf{A}^n$

defined over Z. Meuser [Me,1] has defined the following zeta function:

$$(5.1) \qquad Z(V,t)_e = \exp\Big(\sum_{\ell=1}^{\infty} N(V)_\ell^e t^\ell/\ell\Big)$$

with $N(V)_\ell^e = |V(R_\ell/p^e)|$, $\ell = 1,2,\cdots$. The case $e = 1$ gives the ordinary (Weil) zeta function of V over Z/p. She shows that $Z(V,t)_e = Z(V_1,t)_1$ [M,1; Theorem 1] for some algebraic set V_1 (dependent on e). Thus it is rational.

Then Meuser introduces the function $H(V,w)_\ell = \sum_{e=1}^{\infty} N(V)_\ell^e w^e$ for each fixed ℓ. It is a standard argument (as in (3.8)) that rationality of $Z(V,t)_e$ implies the existence of $\alpha_1,\cdots,\alpha_r,\beta_1,\cdots,\beta_s \in \mathbf{C}$ such that

$$(5.2) \qquad N(V)_\ell^e = \sum_{i=1}^{r} (\alpha_i)^\ell - \sum_{j=1}^{s} (\beta_j)^\ell = \sum_i p^{\log_p(\alpha_i)\ell} - \sum_j p^{\log_p(\beta_j)\ell}$$

for all ℓ. But, as e varies, the elementary argument that $Z(V,t)_e = Z(V_1,t)_1$ requires a change in r and s. Nevertheless, these changes are suitably regular for Meuser to show that there exists an integer u, polynomials $G_1,G_2 \in \mathbf{C}[x_o,\cdots,x_u]$ and complex numbers $\lambda_1,\cdots,\lambda_u$ such that for each $\ell \geq 1$,

$$(5.3) \qquad H(V,W)_\ell = G_1(w,p^{\lambda_1\ell},\cdots,p^{\lambda_u\ell})/G_2(w,p^{\lambda_1\ell},\cdots,p^{\lambda_u\ell}) .$$

We say that $H(V,w)_\ell$ is an <u>invariant function of</u> ℓ.

In the remainder of this section we prove an analogous result to Meuser's for the generalization to elementary statements of the function $Z(V,t)_e$, and we discuss the property analogous to invariance fo the generalization of the function $H(V,w)_\ell$. For simplicity we start with elementary statements over

$\mathbf{Z}$.

As in (2.4), with $0 \leq k \leq n-1$, consider a collection of quantifiers $Q_{k+1},\cdots,Q_n$ and let V be a union of (not necessarily disjoint) locally closed subsets of $\mathbf{A}^n$ defined over Z . That is, V is a constructible set over $\mathbf{A}^n_Z$. Define $N^e_\ell = N^e_\ell(V)$ to be the cardinality of the set

$$\{(x_1,\cdots,x_k) \in \mathbf{A}^k(R_\ell/(p^e))\mid (Q_{k+1}x_{k+1})\cdots(Q_n x_n)[\mathbf{x} \in V(R_\ell/(p^e))]\} .$$

Then $Z(V,\mathbf{Q},t)_e$ is defined by the formula

$$t\frac{d}{dt}(\log(Z(V,\mathbf{Q},t))_e) = \sum_{\ell=1}^{\infty} N^e_\ell t^\ell \tag{5.4}$$

(and $Z(V,\mathbf{Q},0) = 1$) .

THEOREM 5.1. <u>There exist explicitly computable</u> $f_1,f_2,f_3 \in \mathbf{Z}[t]$ <u>and an explicitly computable integer</u> u <u>such that</u> $(Z(V,\mathbf{Q},t)_e)^u = e^{f_1(t)}(f_2(t)/f_3(t))$.

<u>Proof</u>. The argument amounts to introducing new variables to obtain a constructible subset V_1 of $\mathbf{A}^{ne}$ defined over Z such that $N^e_\ell(V) = N^1_\ell(V_1) = N_\ell(V_1)$ so that $Z(V,\mathbf{Q},t)_e = Z(V_1,\mathbf{Q}',t)$ for an appropriate set of quantifiers $\mathbf{Q}'$. Thus the theorem is an immediate corollary of Theorem 3.2.

For each $\ell \geq 1$, denote the Teichmuller representatives for R_ℓ by M_ℓ That is, M_ℓ is the set of coset representatives for such that $\alpha^{p^\ell} = \alpha$ for each $\alpha \in M_\ell$. In order to lower confusion, we denote the cartesian product of M_ℓ with itself n times by $M_\ell^{(n)}$.

Lemma 4 of [Me,1] makes the following observation: For $e > 1$ and for $f(\mathbf{x}) \in \mathbf{Z}_p[x_1,\cdots,x_n]$,

(5.5) a) $$f(\alpha) \equiv 0 \bmod(p^e) \quad \text{for} \quad \alpha \in M_\ell^{(n)}$$

if and only if

b) $$f(\alpha) \equiv 0 \bmod (p^{e-1}) \quad \text{and} \quad g(\alpha) \equiv 0 \bmod (p^{e-1})$$

with $g(\mathbf{x}) = (f(x_1^p,\cdots,x_n^p) - f(x_1,\cdots,x_n)^p)/p$. Note that with the replacement of $\mathbf{Z}_p$ by another p-adic ring with residue class field $F(q)$ and with maximal ideal generated by, say , π , we would replace $g(\mathbf{x})$ by $(f(x_1^q,\cdots,x_n^q) - f(x_1,\cdots,x_n)^q)/\pi$. From (5.5), an inequality $f(\alpha) \not\equiv 0 \bmod(p^e)$ would be equivalent to

(5.6) $$f(\alpha) \not\equiv 0 \bmod(p^{e-1}) \quad \text{or} \quad g(\alpha) \not\equiv 0 \bmod(p^{e-1}) .$$

Replace x_i by the expression $x_{i1}p + \cdots + x_{ie}p^{e-1}$ in the equalities and inequalities that define V , $i = 1,\cdots,n$. From this we produce a constructible subset V^* in $\mathbf{A}^{ne}$ where the coordinate variables are $(x_{11},\cdots,x_{1e},x_{21},\cdots,x_{ne}) = x^*$. Continuing this process, replace the quantification $(Q_i x_i)$ by the block of quantified variables $(Q_i x_{i1})(Q_i x_{i2})\cdots(Q_i x_{ie})$. Then $N_\ell^e(V)$ is equal to the cardinality of the set $S(V^*)_\ell^e =$

$$\{(x_{11},\cdots,x_{1e},\cdots,x_{ke}) \in \mathbf{A}^{ke}(M_\ell) \mid (Q_{k+1}x_{k+1})\cdots$$

$$(Q_n x_{ne})[\mathbf{x}^* \in V^*(M_\ell) \bmod(p^e)]\}$$

where $V^*(M_\ell)$ denotes the points in V^* whose coordinates are in M_ℓ, and $V^*(M_\ell)\bmod(p^e)$ denotes the reduction of the coordinates of these points modulo p^e.

Let $W_o = V^*$. Replace each equality $f(\mathbf{x}^*) \equiv 0 \bmod(p^e)$ by the equalities

$$[f(\mathbf{x}^*) \equiv 0 \bmod(p^{e-1})] \wedge [g(\mathbf{x}^*) \equiv 0 \bmod(p^{e-1})]$$

given by (5.5)b). Similarly replace each inequality $f(\mathbf{x}^*) \not\equiv 0 \bmod(p^e)$ by the inequalities

$$[f(\mathbf{x}^*) \not\equiv 0 \bmod(p^{e-1})] \vee [g(\mathbf{x}^*) \not\equiv 0 \bmod(p^{e-1}))$$

given by (5.6). The result is production of a new constructible subset W_1 of $\mathbf{A}^{ne}$ such that $S(W_o)_\ell^e = S(W_1)_\ell^{e-1}$, $\ell \geq 1$. Continue, inductively, to produce a constructible subset W_{e-1} of $\mathbf{A}^{ne}$ such that $S(V^*)_\ell^e = S(W_{e-1})_\ell^1$, $\ell \geq 1$. Since

$$N_\ell^1(W_{e-1}) = |S(W_{e-1})_\ell^1|$$

for $\ell \geq 1$, conclude the theorem by taking V_1 in the first paragraph of the proof to be W_{e-1}. ∎

Now we are prepared to consider the function $H(V,\mathbb{Q};w)_\ell = \sum_{e=1}^{\infty} N(V)_\ell^e w^e$ for each $\ell = 1,2,\cdots$, where $N(V)_\ell^e = N_\ell^e$ is defined just prior to Theorem 5.1. Following Denef [De;p.7], we define $\tilde{D}_\ell = \tilde{D}_{V,\mathbb{Q},\ell}$ to be the

set

$$\{(x_1,\cdots,x_k,w) = (\mathbf{x}_k,w) \in R_\ell^k \times R_\ell \mid (Q_{k+1}x_{k+1})\cdots(Q_n x_n)$$

$$[(\mathbf{x},w) \in \tilde{V}(R_\ell)]\}$$

where $\tilde{V}(R_\ell)$ is the subset of $R_\ell^n \times R_\ell$ defined by replacing every occurance of $=$ (resp., $\neq$) by $\equiv \bmod(w)$ (resp., $\not\equiv \bmod(w)$). A classical trick [De; p.2] allows us to replace $\tilde{V}(R_\ell)$ by a constructible subset (of some higher dimensional affine space). Indeed, a set of the form

$$\{\mathbf{x} \in R_\ell^n \mid \operatorname{ord}(f(\mathbf{x})) \geq \operatorname{ord}(g(\mathbf{x}))\}$$

can be rewritten (if $p \neq 2$, another formula works for $p = 2$) as

$$\{\mathbf{x} \in R_\ell^n \mid \exists y \in R_\ell\ ,\ (g(\mathbf{x}))^2 + p(f(\mathbf{x}))^2 = y^2\}\ .$$

Interpret $f_1(\mathbf{x}) \equiv 0 \bmod(w)$ as $\operatorname{ord}(f_1(\mathbf{x})) \geq \operatorname{ord}(w)$ to rewrite $\tilde{D}_{V,\mathbf{Q},\ell}$, for some integer m, as

$$(5.7) \qquad \{(\mathbf{x},w) \in R_\ell^k \times R_\ell \mid (Q_{k+1}x_{k+1})\cdots(Q_n x_n)(\exists \mathbf{y}_m)[(x,w,y) \in V^*(R_\ell)]\}$$

where V^* is a constructible subset of $\mathbb{A}^{n+m+1}$.

The next lemma slightly generalizes [De;Lemma 3.1]. For $x \in K_\ell$, denote $p^{-\operatorname{ord}(x)}$ by $|x|$. Let $|d\mathbf{x}_k|$ be the Haar measure on K_ℓ^k that has been normalized so that the measure of R_ℓ^k is 1.

LEMMA 5.2. For $s \in \mathbb{R}$, $s > 0$, consider $\tilde{I}_\ell(s) = \int_{\tilde{D}_{V,\mathbf{Q},\ell}} |w|^s |dx_k||dw|$. Then $\tilde{I}_\ell(s) = (p-1)H(V,\mathbf{Q};p^{-k-1}p^{-s})/p$.

Proof. By direct computation: With $\tilde{D}_{e,\ell} = \{(\mathbf{x}_k,w) \in \tilde{D}_\ell \mid \mathrm{ord}(w) = e\}$,

$$\tilde{I}_\ell(s) = \sum_{e=0}^{\infty} \int_{\tilde{D}_{e,\ell}} p^{-es} |dx_k||dw| = \sum_{e=o}^{\infty} p^{-es}(p^{-e}-p^{-e-1}) \int_{(\mathbf{x},p)\in\tilde{D}_{e,\ell}} |\mathbf{dx}_k| ,$$

where we identify the set of integration in the last integral with its projection into R_ℓ^k. But each $\mathbf{x}_k \bmod p^e$ that contributes to N_ℓ^e contributes a subset of $(\mathbf{x},p^e) \in \tilde{D}_{e,\ell}$ whose projection to R_ℓ^k has measure p^{ke}. Thus

$$\tilde{I}_\ell(s) = (p-1)\Big(\sum_{e=o}^{\infty} N_\ell^e (p^{-s}p^{-k-1})^e\Big)/p . \qquad (5.8)$$ ∎

From Lemma 5.2, the existence of ℓ_o such that $H(V,\mathbf{Q};w)_\ell$ is an invariant function of ℓ is equivalent to the same statement for the function $\tilde{I}_\ell(s)$ with p^{-s} replaced by w. Denef's treatment replaces an expression $f(\mathbf{x}) = 0$ by $(\exists y)[p(f(\mathbf{x}))^2 = y^2]$, as we did to get expression (5.7) (and he replaces the inequalities $\mathrm{ord}(x_i) \geq 0$ by $(\exists y_i)[px_i^2 = y_i^2]$, $i = 1,\cdots,n$) to note that the set $\tilde{V}(R_\ell)$ can be written as a Boolean combination of sets of type III:

$$\{(\mathbf{x},w) \in K_\ell^n \mid (\exists y)(f(\mathbf{x},w) = y^n\} \text{, with } n \text{ a positive integer.} \qquad (5.9)$$

For each fixed ℓ, he can then apply Macintyre's elimination theory [Mac] to state that $\tilde{D}_{V,\mathbf{Q},\ell}$ is a Boolean combination of sets of type III (in

$k+1$ variables). We now comment on why the theory of [Mac] is not yet adequate for investigating invariance properties relative to $\{R_\ell\}_{\ell=1,2,\dots}$.

First an explanation of why the elimination of quantifiers absolutely requires n to be an arbitrary positive integer in (5.9). Consider the statement

$$P_\ell\colon (\forall x)(\exists y)[(x,y) \in V(R_\ell)]$$

where $V \subseteq \mathbf{A}^2$ is defined by $f(x,y) \in \mathbf{Z}_p[x,y]$, an absolutely irreducible polynomial. As in the finite field case we would consider

$$M_\ell\colon (\exists y)[(x,y) \in V(R_\ell)] .$$

and we might like to free the dependence of M_ℓ of the appearance of y. For example, it would suffice, for each ℓ to describe the $x \in R_\ell$ for which M_ℓ holds as an explicit union of balls in R_ℓ.

Ex. 5.3. No simple removal of y. Let $f(x,y) = y^n - x$ in M_ℓ, $n > 1$. Suppose that the $x \in R_\ell$ such that M_ℓ holds is a union W_1 of balls. Since $0 \in W_1$, there is a neighborhood of 0 in W_1. But, in every neighborhood of $x = 0$ there are points $x_1, x_2 \in \mathbf{Z}_p$ for which $(\exists y)[y^n - x_1 = 0]$ is false (e.g., $x_1 = p^{kn+1}$ for suitably large k) and for which $(\exists y)[y^n - x_2 = 0]$ is true (e.g., $x_2 = p^{kn}$ for suitably large k).

Even though Ex. 5.3 shows that you can't eliminate $(\exists y)$ from M_ℓ in a simple manner, this example does fit into the Galois stratification ideas. Since $V \to \mathbf{A}^1_x$ by $(x,y) \to x$ defines a cover, we may go to the Galois closure

of this cover to get

$$\hat{V} \to \mathbb{A}^1_x \,, \tag{5.10}$$

where the function field of $\hat{V}$ over K_ℓ is $K_\ell(\hat{V}) = K_\ell(\zeta_n, x^{1/n})$ with $\zeta_n = e^{2\pi i/n}$, an extension of $K_\ell(x)$. Thus we may interpret the $x_o \in R_\ell$ that satisfy M_ℓ as a condition on the conjugacy class of subgroups of $G(K_\ell(\hat{V})/K_\ell(x))$ defined by decomposition groups of valuations of $K_\ell(\hat{V})$ that lie over the valuation $x \to x_o$ of $K_\ell(x)$.

From Macintyre's theorem it suffices, even for general $f(x,y)$, to define the $x \in R_\ell$ that satisfy M_ℓ by a finite number of conditions:

(5.11) $g_{j,\ell}(x)$ is an $n_{j,\ell}$ power in K_ℓ, $j = 1,\cdots,u_\ell$ and

$h_{j,\ell}(x)$ is not an $m_{j,\ell}$ power in K_ℓ, $j = 1,\cdots,v_\ell$.

The problem with Macintyre's theorem is not only that the production of $g_{j,\ell}$, $h_{j,\ell}$, $n_{j,\ell}$ and $m_{j,\ell}$ in (5.11) is not explicit, but that the dependence of these on ℓ is a complete mystery.

Both of these problems are remedied by the full Galois stratification procedure of [Fr,3]. Indeed [Fr,3; Section 2] has a weak Cebotarev property sufficient for the theory of elimination of quantifiers over all the rings $\{R_\ell\}_{\ell=1,2,\cdots}$. But it is insufficient to show the invariance (for suitably large ℓ) of the integral $\int_{D_\ell} |w|^s |dx||dw|$. For this we must consider a generalization of the following situation.

Let $\varphi: C \to \mathbb{A}^n$ be a Galois (finite normal) cover over $\mathbb{Q}_p$. Let W be a compact open subset of $\mathbb{A}^n(Z_p)$. Let H be a subgroup of $G(C/\mathbb{A}^n)$ and let

$W'_\ell = \{x \in W \wr R_\ell |$ the decomposition groups associated to x give the conjugacy class of $H\}$. We need to show that $\int_{W'_\ell} |m(x)|^s |dx|$ is an invariant function, where $m(x)$ is a function on $\mathbb{A}^n$ ($n = k+1$ and $m(x) = w$ in the original problem). This is a Frobenius density analogue for p-adic extensions. We'll now state an elementary rephrasing of this.

Let H be a subgroup of $G(C/\mathbb{A}^n)$ and let C_H be the quotient of C by H . Let $W_{H,\ell}$ be $\varphi(C_H(K_\ell)) \cap (W \wr R_\ell)$. Similarly for $W_{H',\ell}$ with H' a subgroup of $G(C/\mathbb{A}^n)$ containing H . Finally, let

$$W^*_{H,\ell} = W_{H,\ell} - \bigcup_{H \subsetneq H'} W_{H',\ell} .$$

BASIC THEOREM. With the notation above,

$$\int_{\bigcup_{\sigma \in G(C/\mathbb{A}^n)} W^*_{\sigma H \sigma^{-1},\ell}} |m(x)|^s |dx|$$

is an invariant function.

Along with a proof of the Basic Theorem, and discussion of a full-fledged Čebotarev analogue, a later paper will present for publication the Galois stratification procedure of [Fr,3] relative to $\{R_\ell\}_{\ell=1,2,\dots}$. Obviously a proof of this (and its necessary generalizations) generalizes the main theorem of [Me,1].

In analogy to [De] we intend also to consider the function $\sum_{e=1}^{\infty} N^*(V)^e_\ell w^e = H^*(V,\mathbb{Q};w)_\ell$ where $N^*(V)^e_\ell$ is defined from the set

$$D_\ell = D_{V,\mathbb{Q},\ell} =$$

$$\{(\mathbf{x}_k, w) \in R_\ell^k \times R_\ell \mid \exists \mathbf{z} \in R_\ell^k \text{ with } x \equiv \mathbf{z} \bmod w \text{ and}$$

$$(Q_{k+1} z_{k+1}) \cdots (Q_n x_n)[(\mathbf{z}, w) \in V(R_\ell)]\} ,$$

where $\mathbf{z} = (z_1, \cdots, z_n)$. As in the previous discussion, the invariance of $H^*(V, \mathbf{Q}; w)_\ell$ for ℓ suitably large is equivalent to this property for $I_\ell(s) = \int_{D_\ell} |w|^s |dx_k| |dw|$.

Indeed, it is the difference $H(V, \mathbf{Q}; w)_\ell - H^*(V, \mathbf{Q}; w)_\ell$, a kind of measure of "persistent phenomena" with respect to the e variable, that might be one of the more attractive invariants.

6. Examples.

In contrast to Ex. 2.4, the main point of the two examples here is to emphasize the Galois theoretic part of the elimination of quantifiers that effectively produces the zeta function of an elementary statement over a finite field $\mathbf{F}(q)$.

Ex. 6.1. Relations among the zeros of a finite set of polynomials. Let $f_1, \cdots, f_r \in \mathbf{F}(q)[x]$ be any finite collection of irreducible polynomials. Let $\widehat{\mathbf{F}(q)} = F(q^s)$ be the splitting field of $f_1 \cdots f_r$ over $\mathbf{F}(q)$. Consider a sentence M made entirely from the connectives $\wedge$ ("and") , $\vee$ ("or") and $\sim$ ("not"), and the atomic formulae "$f_i(x)$ has a solution," $i = 1, \cdots, r$. Interpret $M(q^\ell)$ to be M with the variables regarded as in $\mathbf{F}(q^\ell)$. For example, let M^0 be

(6.1) $$[(f(x) \text{ has a solution}) \wedge (g(x) \text{ has a solution})]$$
$$[\sim(f(x) \text{ has a solution}) \wedge \sim(g(x) \text{ has a solution})] ,$$

where $f(x) = f_1 \cdots f_{r_1}$ and, for example "$f(x)$ has a solution" is equivalent to $\overset{r_1}{\underset{i=1}{V}}[f_i(x)$ has a solution]. Thus $M^o(q^\ell)$ is equivalent to the statement that $f(x)$ has a solution in $\mathbf{F}(q^\ell)$. if and only if $g(x)$ has a solution in $\mathbf{F}(q^\ell)$.

Consider the zeta function $Z(M,t)$ defined by the Poincare series $t\frac{d}{dt}(\log(Z(M,t))) = \sum_{\ell=1}^{\infty} N_\ell t^\ell$ where $N_\ell = 1$ if $M(q^\ell)$ is true, 0 otherwise. We show how to compute $Z(M,t)$ as a near rational function (as in §3).

The restriction of F_{q^ℓ} to $\mathbf{F}(q^s)\mathbf{F}(q^\ell) = \mathbf{F}(q^{[s,\ell]})$ is a generator of $G(\widehat{\mathbf{F}(q)}\mathbf{F}(q^\ell)/\mathbf{F}(q^\ell))$. Denote the permutation action of this on the zeros of $f_i(x)$ by $T_i)F_q)^\ell$, $i = 1,\cdots,r$. Thus the atomic statement "$f_i(x)$ has a solution" holds in $\mathbf{F}(q^\ell)$ if and only if $T_i(F_q)^\ell$ is the identity. This is equivalent to the statement that the restriction of $T_i(\mathbf{F}_q)^\ell$ is in $G(\mathbf{F}(q)/\mathbf{F}_i)$ where $\mathbf{F}_i$ is the splitting field of $f_i(x)$ over $\mathbf{F}(q)$.

Identify $G(\widehat{\mathbf{F}(q)}/\mathbf{F}(q))$ with $\mathbf{Z}/(s)$, F_q with the generator 1 and $G(\widehat{\mathbf{F}(q)}/\mathbf{F}_i)$ with the subgroup generated by s_i , $i = 1,\cdots,r$. Finally, denote the support function for the subgroup of $\mathbf{Z}/(s)$ generated by an integer m by $\mathbf{1}_m$. Thus the atomic statement "$f_i(x)$ has a solution" holds in $\mathbf{F}(q^\ell)$ if and only if $\mathbf{1}_{s_i}(\ell) = 1$ where we regard ℓ as in $\mathbf{Z}/(s)$, $i = 1,\cdots,r$. With $\mathbf{1}_1$ denoted by $\mathbf{1}$, we may write N_ℓ as $u(\ell)$ where u is a function on $\mathbf{Z}/(s)$ given by

$$(6.2) \qquad -\sum_{m|s} u_m m \mathbf{1}_m \quad \text{with} \quad u_m = v_m/w_m \quad \text{and} \quad v_m, w_m \in \mathbf{Z}\ ,\ (v_m, w_m) = 1\ ,$$

(and if $v_m = 0$, then $w_m = 1$) . Indeed, this is a special case of Artin's theorem (cf., Part 5 of proof of Theorem 3.2). For example, when M is M^o , we may take u to be the function

$$(6.3)\qquad (1 - \prod_{i=1}^{r_1}(1 - 1_{s_i}))(1 - \prod_{i=r_1+1}^{r_1+r_2}(1 - 1_{s_i}) + \prod_{i=1}^{r_1+r_2}(1 - 1_{s_i}) ,$$

where we multiply it out to get an expression of the form (6.2). Use $1_{m_1} \cdot 1_{m_2} = 1_{[m_1,m_2]}$ for m_1 and m_2 integers that divide s.

Now use (6.2) to compute $Z(M,t)$:

$$(6.4)\qquad -\sum_{\ell=1}^{\infty}\sum_{m|s}(v_m/w_m)m1_m(\ell)t^{\ell} = -\sum_{m|s}v_m/w_m(\sum_{\ell=1}^{\infty}m1_m(\ell)t^{\ell})$$

$$= -\sum_{m|s}v_m/w_m(\sum_{k=1}^{\infty}mt^{km}) = -\Sigma(v_m/w_m)t^m m/(1-t^m) .$$

Thus, $Z(M,t) = \prod_{m|s}(1-t^m)^{v_m/w_m}$. In this case if w is the least common multiple of w_m, $m|s$, then $Z(M,t)^w$ is a rational function of t, and w is the minimal integer with this property. ∎

The next example illustrates a diophantine situation around which there has been a voluminous literature; it demonstrates the value of applying the Galois stratification procedure so that the covers involved may be ramified (i.e., $F_{\mathbf{x}}$ may not be a single element in the discussion prior to Ex. 2.1); and it illustrates the value, on occasion, of eliminating quantifiers in blocks (as is systematically done in [FrS]). Indeed, the situation of the example arises often in practical problems over finite fields.

Ex. 6.2. The diophantine covering property. For this example we change the notation of §3 for the variables. Let $V \subseteq \mathbf{A}^{2n}$ be an algebraic variety defined over $\mathbf{F}(q)$ such that V is of dimension n. Denote the coordinate variables by $x_1,\cdots,x_n,y_1,\cdots,y_n$ and consider the elementary statement M,

$$(6.5)\qquad (\forall \mathbf{x})(\exists \mathbf{y})[(\mathbf{x},\mathbf{y}) \in V] ,$$

where, for example, $(\forall \mathbf{x})$ is an abbreviation for $(\forall x_1)\cdots(\forall x_n)$.

Denote the projection of $\mathbb{A}^{2n}$ onto the first n coordinates by $pr_n: \mathbb{A}^{2n} \to \mathbb{A}^n$. We assume from this point that restriction of pr_n to V gives a <u>finite</u> map $V \to \mathbb{A}^n$ [M;243-5]. Denote the degree of this map by k . In particular $pr_n(V) = A^n$. As in Ex. 6.1, interpret $M(q^\ell)$ to be M with the variables regarded as in $\mathbf{F}(q^\ell)$. We will give an exact condition that implies that $M(q^\ell)$ is true for infinitely many integers ℓ . Then we'll use this to compute $Z(M,t)$ where $t\frac{d}{dt}(\log(Z(M,t)) = \sum_{\ell=1}^{\infty} N_\ell t^\ell$ with $N_\ell = 1$ if $M(q^\ell)$ is true, and 0 otherwise. As a practical example (as we'll show if q satisfies certain conditions), consider the case $n = 1$ and the statement

M^o ,

$$(6.6) \qquad (\forall x)(\exists y)[(x,y) \in V_o]$$

where V_o is the variety defined by $T_k(y) - x = 0$ where $T_k(y)$ is the kth chebychev polynomial:

$$(6.7) \qquad T_k(z + 1/z) \equiv z^k + 1/z^k \ .$$

In the general case let $\mathbf{F}(q)(V)$ be the function field of V . It is a degree k extension of $\mathbf{F}(q)(A^n)$, a rational function field in n variables. And with no loss we assume [FrS;p.231] that it is a separable extension. Let $\widehat{\mathbf{F}(q)(V)}$ be the Galois closure of this extension and let $\widehat{\mathbf{F}(q)}$ be the algebraic closure of $\mathbf{F}(q)$ in $\mathbf{F}(q)(V)$. Denote $G(\widehat{\mathbf{F}(q)(V)}/\mathbf{F}(q)(\mathbb{A}^n))$ by $\hat{G}$, and the normal subgroup

$G(\widehat{\mathbf{F}(q)(V)}/\widehat{\mathbf{F}(q)}(\mathbb{A}^n))$ by G. We state our condition in terms of the natural permutation representation $T:\hat{G} \to S_k$ of degree k. Identify $\hat{G}_1 = G(\widehat{\mathbf{F}(q)(V)}/\mathbf{F}(q)(V))$ (resp., G_1) with the stabilizer in $\hat{G}$ (resp., G) of the integer 1 under T.

Let $Y_1,\cdots,Y_r$ be the orbits of G_1 on $\{2,\cdots,k\}$. Then $M(q^\ell)$ is true for infinitely many ℓ if and only if

(6.8) Y_i breaks up into at least 2 orbits under G_1 for each $i = 1,\cdots,r$.

Much about the case $n = 1$ is characterized in great detail in [Fr,4; p.153-159]. This refers to [Fr,3;proof of Theorem 1] for the proof of this statement in a special case, which easily extends to our case. We now explain the conditions on q that imply that $M^o(q^\ell)$ is true for infinitely many ℓ.

Let ζ_k be a primitive kth root of 1 over $\mathbf{F}(q)$. To quarantee that there are k unequal kth roots of 1, assume that $(k,q) = 1$. Let z be a solution of $Z + 1/Z = y_1$ where y_1 is a solution of $T_k(Y) = x$ (with x an indeterminate). From (6.7) the complete set of solutions to $T_k(Y) = x$ is clearly

(6.9) $$\zeta_k^i z + 1/\zeta_k^i z \ , \ i = 0,\cdots,k-1 \ .$$

Thus $\widehat{\mathbf{F}(q)(V_o)} = \mathbf{F}(q)(z,\zeta_k)$ and $\widehat{\mathbf{F}(q)} = \mathbf{F}(q)(\zeta_k)$. In particular, the group G_1 (in the notation above) is generated by an element σ where $\sigma(z) = 1/z$. It will be clear below that we must assume $(k,2) = 1$. Thus, the action of σ on $2,\cdots,k$ is a product of $(k-1)/2$ cycles of length 2:

(6.10) $$\sigma(\zeta_k^i z + 1/\zeta_k^i z) = \zeta_k^{-i} z + 1/\zeta_k^{-i} z \ , \ i = 0,\cdots,k-1 \ .$$

Furthermore, $\hat{G}_1$ is generated by σ and the restriction of F_q to $\widehat{F(q)(V_o)}$ (determined by $F_q(\zeta_k) = (\zeta_k)^q$) . Thus, a restatement of (6.8) is that

(6.11) $$qi \neq i \bmod(k) \ , i = 1,\cdots,k-1 \ .$$

That is, both $q+1$ and $q-1$ must be invertible modulo k . Finally, we have deduced the equivalence of (6.8) and

(6.12) $$(2(q^2-1)q,k) \ .$$

Thus [Fr,3] (slightly generalized) shows that $M^o(q)$ is true.

By the same argument, the integers ℓ for which $M^o(q^\ell)$ is true are those for which $(q^{2\ell}-1,k) = 1$. Identify the cyclic group generated by q^2 in $(\mathbf{Z}/(k))^*$ with $\mathbf{Z}/(u)$. Then, $N_\ell = 1$ if and only if $\ell \bmod(u)$ is represented by ℓ_1 , between 1 and $u-1$, such that $(q^{2\ell_1}-1,k) = 1$. ∎

Bibliography

[ASp] A. Adolphson and S. Sperber, Character sums in finite fields, Compositio Mathematica 52 (1984), 325-354.

[Be] E. R. Berlakamp, Algebraic Coding Theory, Mcgraw Hill, New York, 1968.

[B,1] E. Bombieri, On exponential sums in finite fields, Amer. J. Math. 88 (1966), 71-105.

[B,2] E. Bombieri, On exponential sums in finite fields, II, Invent. Math. 47 (1978), 29-39.

[B,3] E. Bombieri, On Galois coverings over finite fields, Publicado en "Actas del Coloquio Internacional Geometria Algebraica" Madrid, Septiembre 1965

[CaZ] D. G. Cantor and H. Zassenhaus, A new algorithm for factoring polynomials over finite fields, Math. Comput. 36 (1981), 587-592.

[CF] J. W. S. Cassels and A. Frohlich, Algebraic Number Theory, Academic Press, London, 1967.

[D,1] B. Dwork, On the zeta function of a hypersurface, Pub. Math. IHES 12 (1962).

[D,2] B. Dwork, On the zeta function of a hypersurface II, Annals of Math. 80 (1964), 227-239.

[D,3] B. Dwork, On the zeta function of a hypersurface III, Ann. of Math. 83 (1966), 457-519.

[De] J. Denef, The rationality of the Poincare series associated to the p-adic points on a variety, Invent. Math. 77 (1984), 1-23.

[DrVl] V.G. Drinfel'd and S.G. Vladut, Number of points of an algebraic curve, Functional analysis and its applications, Russian original, Vol. 17 (1983), 53-54.

[Fr,1] M. Fried, The nonregular analogue of Tchebotarev's theorem, Pac. J. Math. 112 (1984), 303-311.

[Fr,2] M. Fried, Review of [K] in Math. Reviews.

[Fr,3] M. Fried, Toward a general theory of diophantine problems with application to p-adic fields and fields of finite corank, 102 pages of Notes available from U.C. Irvine, Spring, 1978.

[Fr,4] M. Fried, On a theorem of MacCluer, Acta Arith. 25 (1974), 121-126.

[Fr,5] M. Fried, Galois groups and complex multiplication, TAMS 235 (1978), 141-163.

[FrHJ] M. Fried, D. Haran and M. Jarden, Galois stratification over Frobenius fields, Advances in Math. 51 (1984), 1-35.

[FrJ] M. Fried and M. Jarden, Field Arithmetic, Springer Verlag, to appear.

[FrS] M. Fried and G. Sacerdote, Solving diophantine problems over all residue class fields of a number field and all finite fields, Annals of Math. 104 (1976), 203-233.

[HJ] D. Haran and M. Jarden, Bounded statements in the theory of algebraically closed fields with distinguished automorphisms, J. fur die reine und angewandte Math. 387 (1982), 1-17.

[I] Y.Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo 28 (1981), 721-724.

[K] U. Kiefe, Sets definable over finite fields: their zeta-functions, TAMS 223 (1976), 45-59.

[LT] S. Lang and J. Tate, Principal homogeneous spaces over abelian varieties, Amer. J. Math. 80 (1958), 659-684.

[LeLeLo] H. Lenstra, J. Lenstra, K. Lovasz, Factoring polynomials with rational coefficients, Math. Ann. 261 (1982), 515-534.

[LiP] R. Lidl and J. Pilz, Applied Abstract Algebra, Undergraduate texts in mathematics, Springer-verlag, 1984.

[Mac] A. Macintyre, On definable subsets of p-adic fields, J. Symbolic Logic 41 (1976), 605-610.

[Me,1] D. Meuser, The meromorphic continuation of a zeta function of Weil and Igusa type, preprint.

[Me,2] D. Meuser, On the poles of a local zeta function for curves, Invent. Math. 73 (1983), 445-465.

[M] D. Mumford, Introduction to Algebraic Geometry, Harvard University Notes, Cambridge Mass., 1966.

[Se] J. P. Serre, Representations Lineaires, des groupes finis, Deuxieme edition, 1971, Hermann, Paris.

[Se,2] J.P. Serre, Quelques applications du théorème de densite de Chebotarev, Publ. Math. IHES 54 (1981).

[Se,3] J.P. Serre, Sur le nombre des points rationnels dúne courbe algebrique sur un corps fini, C.R. 296(1983), 397-403.

[St] G. Stolzenberg, Constructive normalization of an algebraic variety, BAMS (1968), 595-599.

[TsVlZ] M.A. Tafasman, S.G. Vlâdut and T. Zink, Modular curves, Shimura curves and Goppa codes better than Warshamov-Gilbert bound, Math. Nach. 109(1982), 21-28.

[ZS] O. Zariski and P. Samuel, Commutative Algebra II, Springer, New York 1960.