September 16, 2013

Dear Bjorn,

In the Field Arithmetic workshop in Oberwolfach you asked a question on Bertini's theorem over finite fields. Let $\mathcal{H}(d,N)$ be the set of hypersurfaces in $\mathbb{P}^N_{\mathbb{F}_q}$ of degree d. The conjecture you made was:

Conjecture 1. *Let $X \subseteq \mathbb{P}^N_{\mathbb{F}_q}$ be locally closed and geometrically irreducible of dimension ≥ 2. Then*

$$\lim_{d\to\infty} \frac{\#\{H \in \mathcal{H}(d,N) : H \cap X \text{ is geometrically irreducible}\}}{\#\mathcal{H}(d,N)} = 1.$$

You also sketched a proof for X smooth projective of dimension ≥ 3 that I won't repeat here.

Here I want to present a way to attack this problem using the theory of Hilbertian fields. This approach will give the conjecture with a restricted set of hypersurfaces replacing $\mathcal{H}(d,N)$. To do so I will use an explicit Hilbert irreducibility theorem, that seems to be new although an analog result over $\mathbb{Q}$ is known.

Before starting with the actual mathematics I want to stress out that this letter contains many but not all details. I tried to skip details that seems technical to write, and that I have the feeling that you can easily fill up.

I plan to apply for a grant of the German-Israeli Foundation for Scientific R&D together with Arno Fehm and to include this topic as one of the proposed research projects. Do you think it is suitable for such a purpose?

1. The connection between Hilbert's irreducibility theorem and Bertini theorem over finite fields

Recall that a subset H of a field K is called **Hilbert set** if there exists a polynomial $f(y,z) \in K[y,z]$ that is separable and irreducible as a polynomial over $K(y)$ and a nonzero $g(y) \in K[y]$ such that

$$H = \{a \in K \mid f(a,z) \text{ is irreducible and } g(a) \neq 0\}.$$

We denote by $\mathcal{P}_{d,r}$ the subset of $\mathbb{F}_q[x_1,\dots,x_r]$ of degree d polynomials.

Theorem 2. *[Explicit Hilbert's Irreducibility Theorem] Let $K = \mathbb{F}_q(x_1,\dots,x_r)$ be a rational function field over a finite field $\mathbb{F}_q$ and let $H \subseteq K$ be a Hilbert set. Then*

$$\lim_{d\to\infty} \frac{\#(H \cap \mathcal{P}_{d,r})}{\#\mathcal{P}_{d,r}} = 1.$$

We note that $\mathcal{P}_{d,r}$ may be replaced by other subsets of K that behaves sufficiently nice, e.g. by the set of polynomials of degree at most d, see below.

A complete proof of Theorem 2 appears in §2.

Let me now show what Theorem 2 gives toward Conjecture 1 (skipping many of the details). Given $X \subseteq \mathbb{P}^N_{\mathbb{F}_q}$ of dimension $r+1 \geq 2$, we find an open affine subscheme $U \subseteq \mathbb{P}^N_{\mathbb{F}_q}$ such that $X \cap U = \operatorname{Spec}(A)$, for a reduced finitely generated $\mathbb{F}_q$-algebra $A = \mathbb{F}_q[T_1, \ldots, T_N, g^{-1}]/I$ and such that $\dim X \cap U = \dim X = r+1$. Using Noether's normalization lemma [2, Cor. 16.8], we get a dominant separable map $\pi\colon U \to \mathbb{A}^{r+1}_{\mathbb{F}_q}$ such that $\pi|_{X\cap U}\colon X \cap U \to V$ is a finite map onto an open subscheme $V = \operatorname{Spec}(B)$, of $\mathbb{A}^{r+1}_{\mathbb{F}_q}$, where $B = \mathbb{F}_q[x_1, \ldots, x_r, y, (g')^{-1}]$. Taking U and V even smaller, equivalently, localizing the corresponding rings, we may assume without loss of generality that A is generated by one element over B, that is that $A = B[z]/(f(x_1, \ldots, x_r, y, z))$ with $\deg_z(f) \geq 1$.

We have that $X \cap U$ is absolutely irreducible, which amounts to f being absolutely irreducible. Since the absolute Galois group of $\mathbb{F}_q$ is pro-cyclic, and in particular small in the sense that there are finitely many (in fact exactly one) extension of any given degree, the set H of all $h \in \mathbb{F}_q(x_1, \ldots, x_r)$ such that $f(x_1, \ldots, x_r, h(x_1, \ldots, x_r), z)$ is absolutely irreducible contains a Hilbert set [3, Proposition 16.11.1]. Hence, by Theorem 2,

$$\lim_{d\to\infty} \frac{\#(H \cap \mathcal{P}_{d,r})}{\#\mathcal{P}_{d,r}} = 1. \tag{1}$$

For each $h \in \mathcal{P}_{d,r}$, let F_h be the hypersurface which is the completion of $\pi^{-1}(\{y = h(x_1, \ldots, x_r)\})$ in $\mathbb{P}^N_{\mathbb{F}_q}$. Then $\deg F_h \leq Cd$, where C is a fixed number depending only on π. Since the coordinate ring of $F_h \cap X \cap U$ is $\mathbb{F}_q[x_1, \ldots, x_r, y, z, (g')^{-1}]/(y - h, f) = \mathbb{F}_q[x_1, \ldots, x_r, z, (g')^{-1}]/(f(x_1, \ldots, x_r, h, z))$, $F_h \cap X \cap U$ is absolutely irreducible if and only if $f(x_1, \ldots, x_r, h, z)$ is absolutely irreducible. Hence (1) may be reformulated as

$$\lim_{d\to\infty} \frac{\#\{h \in \mathcal{P}_{d,r} \mid F_h \cap X \cap U \text{ is absolutely irreducible}\}}{\#\mathcal{P}_{d,r}} = 1. \tag{2}$$

To get rid of the U one needs to notice that if $F_h \cap X \cap U$ is absolutely irreducible, then either $F_h \cap X$ is absolutely irreducible or $F_h \cap (\mathbb{P}^N \smallsetminus U)$ contains one of the irreducible components of $X \cap (\mathbb{P}^N \smallsetminus U)$. It seems that the number of such hypersurfaces is of smaller order of magnitude than $\#\mathcal{P}_{d,r}$.

To conclude, I sketched a proof of:

Theorem 3. *Let $X \subseteq \mathbb{P}^N_{\mathbb{F}_q}$ be locally closed and geometrically irreducible of dimension $r+1 \geq 2$. Then there exist an open subset $U \subseteq \mathbb{P}^N_{\mathbb{F}_q}$ and a dominant separable morphism $\pi\colon U \to \mathbb{P}^{r+1}_{\mathbb{F}_q}$ such that*

$$\lim_{d\to\infty} \frac{\#\{H \in \mathcal{H}_\pi(d) : H \cap X \text{ is geometrically irreducible}\}}{\#\mathcal{H}_\pi(d)} = 1,$$

where $\mathcal{H}_\pi(d)$ consists on the completions F_h of $\pi^{-1}(\{y = h(x_1, \ldots, x_r)\})$, $h \in \mathcal{P}_{d,r}$.

Note that this theorem in particular gives an existence result: There exists an hypersurface H of arbitrary large degree such that $X \cap H$ is absolutely irreducible.

2. Explicit Hilbert's irreducibility theorem

In this section we prove Theorem 2.

Let $\mathbf{x} = (x_1, \dots x_r)$ be a tuple of variables. A family $\{\mathcal{F}_d \mid d \geq 1\}$ of *finite* subsets of $\mathbb{F}_q[\mathbf{x}]$ is called **nicely distributed** if for every epimorphism $\Phi\colon \mathbb{F}_q[\mathbf{x}] \to A$ onto a *finite* $\mathbb{F}_q$-algebra A there exists $d_0 > 0$ such that for every $d > d_0$ the fibers of the restriction $\Phi|_{\mathcal{F}_d}\colon \mathcal{F}_d \to A$ are all of the same cardinality. Clearly the family $\mathcal{P}_{\leq d} = \{h \in \mathbb{F}_q[\mathbf{x}] \mid \deg h \leq d\}$ is nicely distributed. Thus also $\mathcal{P}_d = \mathcal{P}_{\leq d} \smallsetminus \mathcal{P}_{\leq d-1}$ is nicely distributed.

For a field K, a subset T of $\mathbb{A}^1(K) = K$ is called **thin of type** 1 if T is Zariski closed, i.e. finite. A subset T is called **thin of type** 2 is $T \subseteq \pi(C(K))$, where C is an absolutely irreducible K-curve, and $\pi\colon C \to \mathbb{A}^1$ is a dominant separable K-map of degree at least 2. In general T is called **thin** if it is contained in a finite union of thin sets of types 1 and 2.

We prove below the following result.

Theorem 4. *Let $\mathbf{x} = (x_1, \dots x_r)$ be a tuple of variables, $K = \mathbb{F}_q(\mathbf{x})$, and $\mathcal{F}_d$ a nicely distributed family of subsets of $\mathbb{F}_q[\mathbf{x}]$. Then for every thin set T in $\mathbb{A}^1(K)$ we have*
$$\lim_{d\to\infty} \frac{\#(T \cap \mathcal{F}_d)}{\#\mathcal{F}_d} = 0.$$

There is a classical connection between Hilbert sets and thin sets:

> A subset T of K is thin if and only if there exists a Hilbert set $H \subseteq K$ such that $H \cap T = \emptyset$ and vice versa, $H \subseteq K$ is Hilbert if there is a thin set T such that $H \cap T = \emptyset$.

Thus Theorem 4 may be reformulated in terms of Hilbert sets:

Theorem 5. *Let $\mathbf{x} = (x_1, \dots x_r)$ be a tuple of variables, $K = \mathbb{F}_q(\mathbf{x})$, and $\mathcal{F}_d$ a nicely distributed family of subsets of $\mathbb{F}_q[\mathbf{x}]$. For every Hilbert set H of K we have*
$$\lim_{d\to\infty} \frac{\#(H \cap \mathcal{F}_d)}{\#\mathcal{F}_d} = 1.$$

Clearly Theorem 2 is a special case of Theorem 5 with $\mathcal{F}_d = \mathcal{P}_d$.

We start with some auxiliary lemmas.

Let R be an integral domain and $f \in R[y,z]$ a polynomial. We say that f is **absolutely irreducible** if it is irreducible in $F[y,z]$, where F is an algebraic closure of the fraction field of R.

Let $\mathbb{F}_q$ be a finite field with algebraic closure $\mathbb{F}$. The **degree** of $\mathbf{a} \in \mathbb{A}^r(\mathbb{F}) = \mathbb{F}^r$ is d if d is minimal such that $\mathbf{a} \in \mathbb{F}_{q^d}^r$, i.e. $[\mathbb{F}_q(\mathbf{a}) : \mathbb{F}_q]$, where $\mathbb{F}_q(\mathbf{a})$ is the field generated by the coordinates of $\mathbf{a}$.

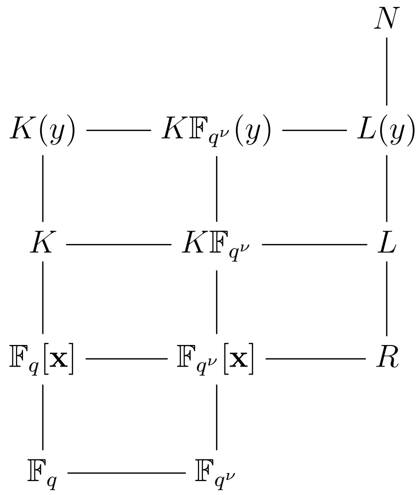
Lemma 6. *Let $\mathbf{x} = (x_1, \dots, x_r)$, let $f(\mathbf{x}, y, z) \in \mathbb{F}_q[\mathbf{x}][y,z]$ be an absolutely irreducible polynomial of positive degree in z and let $\mathbb{F}_{q^\nu}$ be the algebraic closure of $\mathbb{F}_q$ in the splitting field N of f over $\mathbb{F}_q(\mathbf{x})(y)$. For a multiple of d of ν let $\mathcal{S}_d$ be* *the subset of all degree d points $\mathbf{a} \in \mathbb{A}^r(\mathbb{F})$ such that $f(\mathbf{a}, y, z) \in \mathbb{F}_{q^d}[y, z]$ is absolutely irreducible and such that $\mathbb{F}_{q^d}$ is algebraically closed in the splitting field $N_{\mathbf{a}}$ of $f(\mathbf{a}, y, z)$ over $\mathbb{F}_{q^d}(y)$. Then there exists a positive constant $c = c(\deg(f)) > 0$, depending only on $\deg(f)$, such that*

$$\#\mathcal{S}_d \geq cq^{dr}$$

for every sufficiently large $d \in \nu\mathbb{Z}$.

Proof. We first note that $f(\mathbf{a}, y, z) \in \mathbb{F}_q(\mathbf{a})[y, z]$ is absolutely irreducible for all but finitely many $\mathbf{a} \in \mathbb{F}^r$ (see e.g. [3, Proposition 9.4.3]). So if d is sufficiently large and $\mathbf{a} \in \mathbb{F}^r$ is of degree d, then $f(\mathbf{a}, y, z)$ is absolutely irreducible.

Let $K = \mathbb{F}_p(\mathbf{x})$, let L be the algebraic closure of K in N, let R be the integral closure of $\mathbb{F}_{q^\nu}[\mathbf{x}]$ in L, and choose a monic irreducible $f_1 \in R[y, z]$ whose root generates $N/L(y)$.



Since N/L is regular, f_1 is absolutely irreducible. By [3, Proposition 9.4.3], for all but finitely many homomorphisms $\phi\colon R \to \mathbb{F}$ the polynomial $\phi(f_1)$ is absolutely irreducible. Hence if we choose d sufficiently large and $\mathbf{a} \in \mathbb{F}^r$ of degree d then $\phi(\mathbf{x}) = \mathbf{a}$ implies that $\phi(f_1)$ is absolutely irreducible.

Let $\mathcal{T}_d$ be the subset of all $\mathbf{a} \in \mathbb{F}^r$ of degree d such that $\phi(R) = \mathbb{F}_{q^d}$ for any $\phi\colon R \to \mathbb{F}$ with $\phi(\mathbf{x}) = \mathbf{a}$. By [1, Proposition 2.2][1] with $V = \mathbb{A}^r_{\mathbb{F}_{q^d}}$ and W the normalization of $\mathbb{A}^r_{\mathbb{F}_{q^d}}$ in the Galois closure N' of $L\mathbb{F}_{q^d}/K\mathbb{F}_{q^d}$ we get that up to a closed set (of degree independent of d) $\mathcal{T}_d = \pi(\hat{W}(\mathbb{F}_{q^d}))$, where $\hat{W}$ is a form of W (hence its degree in some fixed embedding into a projective space is independent

[1] In fact we need here an explicit Chebotarev theorem for varieties of arbitrary dimension. For dimension 1 it is due to Jarden. The proposition we quote implies quite forwardly the Chebotarev theorem in arbitrary dimension using similar methods, but the Chebotarev theorem itself in arbitrary dimension appears nowhere in the literature, to the best of my knowledge.

of d) and $\deg \pi = [N' : K\mathbb{F}_{q^d}]$. By Lang-Weil estimates $\#\hat{W}(\mathbb{F}_q^d) \sim q^{dr}$, as $d \to \infty$, hence $\#\mathcal{T}_d \sim c' q^{dr}$, where $c' = \frac{1}{\deg \pi}$.

If $\mathbf{a} \in \mathcal{T}_d$, then $N_{\mathbf{a}}$ is generated by a root of $\phi(f_1) \in \mathbb{F}_{q^d}[y, z]$ over $\mathbb{F}_{q^d}(y)$ (the residue field of $L(y)$). Since $\phi(f_q)$ is absolutely irreducible, $N_{\mathbf{a}}/\mathbb{F}_{q^d}$ is regular. Hence $\mathbf{a} \in \mathcal{S}_d$, so $\mathcal{T}_d \subseteq \mathcal{S}_d$. In particular, if $0 < c < c'$ is fixed, then for every sufficiently large d we have $\#\mathcal{S}_d \geq \#\mathcal{T}_d \geq cq^{dr}$. □

The following is a consequence of the effective Cheobotarev theorem for function fields.

Lemma 7. *Let $B > 0$, q a prime power, and $f \in \mathbb{F}_q[y, z]$ a polynomial that is separable and of degree at least $n := \deg_z f \geq 2$ in z. Assume that $\deg f \leq B$ and that $\mathbb{F}_q$ is algebraically closed in the splitting field N of f over $\mathbb{F}_q(y)$. Let Y be the set of $\alpha \in \mathbb{F}_q$ such that $f(\alpha, z)$ has a root in $\mathbb{F}_q$. Then there exist constants $1 > c_1 = c_1(n)$ and $c_2 = c_2(B)$, the former depending only on n the latter depending only on B, such that*

$$\frac{\#Y}{q} \leq c_1 + c_2 q^{-1/2}.$$

In particular if n and B are fixed and q is sufficiently large, then $\frac{\#Y}{q} \leq c_3$, for some $1 > c_3$.

Proof. Let $G = \mathrm{Gal}(N/\mathbb{F}_q(y))$ be the Galois group of f over $\mathbb{F}_q(y)$ considered as a permutation group on the roots of f. Let $C \subseteq G$ be the subset of elements with at least one fixed point. Clearly C is a union of conjugacy classes, and $C \neq G$ since G is transitive and nontrivial[2]. Then for every $\alpha \in \mathbb{F}_q$ such that $f(\alpha, z)$ is separable and of degree n we have that $f(\alpha, z)$ has a root if and only if the Frobenius conjugacy class of the prime $(y - \alpha)$ of $\mathbb{F}_q(y)$ in N is contained in C. Clearly the number of α such that $f(\alpha, z)$ is not separable or of degree $< n$ is less then a constant depending only on B. Hence by [3, Proposition 6.4.8] we get the assertion. □

Proof of Theorem 4. It suffices to prove the assertion for T thin of type 2. A thin set of type 2 is contained, up to finitely many elements, in a set of the form

$$\tilde{T} = \{h \in K \mid f(\mathbf{x}, h(\mathbf{x}), z) \text{ has a root in } K\},$$

where $f(\mathbf{x}, y, z) \in \mathbb{F}_q[\mathbf{x}][y, z]$ is an absolutely irreducible polynomial that is separable and of degree at least 2 in z. We may replace T by $\tilde{T}$ without loss of generality.

---

[2]Let μ be the number of pairs (g, i) such that $g \in G$ fixes i. Then if G_i is the stabilizer of i, then since G is transitive $[G : G_i] = n$, and so $\mu = \sum_i \#G_i = \sum_i |G|/n = |G|$. So on average the number of fixed points of $g \in G$ is 1. Since G is not trivial, the identity element has more fixed points than the average, thus there must be $g \in G$ with less fixed points, i.e. with no fixed points.

Let N be the splitting field of of $f(\mathbf{x},y,z)$ over $K(y)$ and $\mathbb{F}_{q^\nu}$ the algebraic closure of $\mathbb{F}_q$ in N. Let d_0 be a sufficiently large multiple of ν, put $q' = q^{d_0}$, and let $\mathcal{S}_{d_0}$ be as in Lemma 6, i.e. the set of $\mathbf{a} \in \mathbb{A}^r(\mathbb{F})$ of degree d_0 such that $f(\mathbf{a},y,z) \in \mathbb{F}_{q_0^d}[y,z]$ is absolutely irreducible and such that $\mathbb{F}_{q'}$ is algebraically closed in the splitting field $N_\mathbf{a}$ of $f(\mathbf{a},y,z)$ over $\mathbb{F}_{q'}(y)$. Then

$$\#\mathcal{S}_{d_0} \geq cq^{d_0 r}, \tag{3}$$

for some $c > 0$ that depends only on $\deg(f)$.

Let $\phi_\mathbf{a} \colon \mathbb{F}_q[\mathbf{x}] \to \mathbb{F}_{q'}$ be the epimorphism defined by $\phi(\mathbf{x}) = \mathbf{a}$ and let

$$\Phi \colon \mathbb{F}_q[\mathbf{x}] \to \prod_{\mathbf{a}\in\mathcal{S}_{d_0}} \mathbb{F}_{q'}$$

given by $\Phi(\mathbf{x}) = (\mathbf{a} \mid \mathbf{a} \in \mathcal{S}_{d_0})$ (that is to say $\Phi = \prod_{\mathbf{a}\in\mathcal{S}_d} \phi_\mathbf{a}$). Since the kernels of $\phi_\mathbf{a}$ are distinct maximal ideals and the kernel of Φ is the intersection of $\ker \phi_\mathbf{a}$, the Chinese Remainder Theorem gives that Φ is surjective.

For a finite set A we denote by μ_A the the uniform probability measure on A. If, for $h \in \mathcal{F}_d$, the polynomial $f(\mathbf{x}, h(\mathbf{x}), z)$ has a root in K, say $k(\mathbf{x})$, then for all $\mathbf{a} \in \mathcal{S}_{d_0}$ the polynomial $f(\mathbf{a}, h(\mathbf{a}), z)$ has a root in $\mathbb{F}_{q'}$, namely $k(\mathbf{a})$[3]. Choose d to be sufficiently large with respect to d_0. Then, by definition, the fibers of $\Phi|_{\mathcal{F}_d} \colon \mathcal{F}_d \to \prod_{\mathbf{a}\in\mathcal{S}_{d_0}} \mathbb{F}_{q'}$ all have the same cardinality. Let

$$\begin{aligned} X &= T \cap \mathcal{F}_d = \{h \in \mathcal{F}_d \mid f(\mathbf{x}, h(\mathbf{x}), z) \text{ has a root in } K\} \\ X_\mathbf{a} &= \{h \in \mathcal{F}_d \mid f(\mathbf{a}, h(\mathbf{a}), z) \text{ has a root in } \mathbb{F}_q'\} \\ Y_\mathbf{a} &= \{b \in \mathbb{F}_{q'} \mid f(\mathbf{a}, b, z) \text{ has a root in } \mathbb{F}_q'\}, \end{aligned}$$

where $\mathbf{a} \in \mathcal{S}_d$. Then $X \subseteq \bigcap_{\mathbf{a}\in\mathcal{S}_d} X_\mathbf{a} = \Phi|_{\mathcal{F}_d}^{-1}(\prod_{\mathbf{a}\in\mathcal{S}_d} Y_\mathbf{a})$. So, since the fibers of $\Phi|_{\mathcal{F}_d}$ are of the same size, we get that

$$\mu_{\mathcal{F}_d}(X) \leq \mu_{\mathcal{F}_d}\left(\bigcap_{\mathbf{a}\in\mathcal{S}_{d_0}} X_\mathbf{a}\right) = \mu_{\prod_{\mathbf{a}\in\mathcal{S}_{d_0}}\mathbb{F}_{q'}}\left(\prod_{\mathbf{a}\in\mathcal{S}_d} Y_\mathbf{a}\right) = \prod_{\mathbf{a}\in\mathcal{S}_{d_0}} \mu_{\mathbb{F}_{q'}}(Y_\mathbf{a}). \tag{4}$$

It remains to estimate $\mu_{\mathbb{F}_{q'}}(Y_\mathbf{a})$; so fix $\mathbf{a} \in \mathcal{S}_{d_0}$. We are in the setting of Lemma 7 with $\deg(f)$, q', $N_\mathbf{a}$, $f(\mathbf{a},y,z)$, and $Y_\mathbf{a}$ replacing B, q, N, f, and Y respectively. Since d_0 is sufficiently large, so is $q' = q^{d_0}$, and so Lemma 7 gives that $\mu_{\mathbb{F}_{q'}}(Y_\mathbf{a}) = \frac{\#Y}{q'} \leq c_3$ for some fixed constant $c_3 < 1$ depending only on $\deg(f)$. Plug this and (3) into (4) to conclude that for every $\epsilon > 0$ if d_0 is sufficiently large and d is

[3]There is a subtle point here of why $\mathbf{a}$ does not annihilates the denominator of $k(\mathbf{x})$: The denominator of $k(\mathbf{x})$ is bounded in terms of f, hence if d_0 is sufficiently large, $k(\mathbf{a})$ is well defined and finite. Another solution for this problem is to note that we may, without loss of generality, assume that f is monic in z, and hence roots of it are polynomials, by Gauss' lemma.

sufficiently large with respect to d_0, then

$$\mu_{\mathbb{F}_q}(X) \leq \prod_{\mathbf{a}} \mu_{\mathbb{F}_{q'}}(Y_{\mathbf{a}}) \leq c_3^{\#\mathcal{S}_{d_0}} \leq c_3^{cq^{d_0 r}} < \epsilon,$$

as needed. □

Best regards,
Lior

References

[1] Lior Bary-Soroker. Irreducible values of polynomials. *Advances in Mathematics*, 229(2):854–874, January 2012.

[2] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[3] M D Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008.