ON THE BATEMAN-HORN CONJECTURE ABOUT POLYNOMIAL RINGS

by

Lior Bary-Soroker*

Institut für Experimentelle Mathematik, Universität Duisburg-Essen

Ellernstr. 29, 45326 Essen, Germany

e-mail: barylior@post.tau.ac.il

and

Moshe Jarden**

School of Mathematics, Tel Aviv University

Ramat Aviv, Tel Aviv 69978, Israel

e-mail: jarden@post.tau.ac.il

Abstract:

Given a power q of a prime number p and "nice" polynomials $f_1, \dots, f_r \in \mathbb{F}_q[T, X]$ with $r = 1$ if $p = 2$, we establish an asymptotic formula for the number of pairs $(a_1, a_2) \in \mathbb{F}_q^2$ such that $f_1(T, a_1T + a_2), \dots, f_r(T, a_1T + a_2)$ are irreducible in $\mathbb{F}_q[T]$. In particular that number tends to infinity with q.

MR Classification: 12E30

Directory: \Jarden\Diary\BSJ

23 December, 2011

---

* Alexander von Humboldt postdoc fellow.

** Research supported by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation, and by an ISF grant.

Introduction

Let $f_1, \dots, f_r \in \mathbb{Z}[X]$ be non-associate irreducible polynomials with positive leading coefficients. A conjecture of Bateman and Horn [BaH62, (1)] predicts for $x > 1$ that the number $N(f_1, \dots, f_r; x)$ of positive integers $1 \leq n \leq x$ such that $f_1(n), \dots, f_r(n)$ are prime numbers satisfies

$$N(f_1, \dots, f_r; x) \sim \frac{s(f_1, \dots, f_r)}{\prod_{i=1}^{r} \deg(f_i)} \frac{x}{\log^r x},$$

where

$$s(f_1, \dots, f_r) = \prod_p \frac{1 - \frac{\omega(p)}{p}}{\left(1 - \frac{1}{p}\right)^r} \text{ and } \omega(p) = \#\{0 \leq n \leq p-1 \mid f_1(n) \cdots f_r(n) \equiv 0 \mod p\}.$$

If $\omega(p) = p$ for some p, then $s(f_1, \dots, f_r) = 0$. Also, for each $n \in \mathbb{Z}$ there exists $1 \leq i \leq r$ such that $p | f_i(n)$, thus $N(f_1, \dots, f_r)$ is finite. If $\omega(p) < p$ for all p, then $s(f_1, \dots, f_r)$ converges to a positive real number [BaH62, p. 364], hence the conjecture predicts the existence of infinitely many n's such that $f_1(n), \dots, f_r(n)$ are all prime numbers. This is a conjecture of Schinzel. The special case where $r = 1$, $f_1(X) = X$, and $s(f_1) = 1$ reduces to the prime number theorem. When $r = 1$ and $f_1(X) = aX + b$ with $\gcd(a, b) = 1$, and $s(f_1) = \frac{a}{\varphi(a)}$, we get Dirichlet's theorem. Likewise, in the case where $f_1(X) = X$ and $f_2(X) = X + 2$, the Bateman-Horn Conjecture generalizes the Hardy-Littlewood conjecture about the density of the twin primes. Calculations made by Littlewood show that in this case $s(f_1, f_2) \approx 1.32$ [BaT04, p. 335].

It is customary in number theory to replace $\mathbb{Z}$ by the ring $\mathbb{F}_q[T]$, where q is a power of a prime number p. In our case we would like to consider irreducible non-associate polynomials $f_1, \dots, f_r \in \mathbb{F}_q[T, X]$ and ask for the number of $g \in \mathbb{F}_q[T]$ such that $f_1(T, g(T)), \dots, f_r(T, g(T))$ are irreducible in $\mathbb{F}_q[T]$.

It turns out that the naive analog of Schinzel's conjecture may fail when one of the f_i's is a polynomial in X^p. For example, Swan proves in [Swa62] that $g(T)^8 + T^3$ is reducible for each $g \in \mathbb{F}_2[T]$. Thus, more restrictions are needed to restore Schinzel's and the Bateman-Horn conjectures [CCG08].

In a conference in the American Institute of Mathematics [Gao03], S. Gao posed the following question:

PROBLEM A: *Let $f \in \mathbb{F}_q[T, X]$ be an irreducible polynomial. Count (or estimate) the number of pairs $(a_1, a_2) \in \mathbb{F}_q \times \mathbb{F}_q$ such that the polynomial $f(T, a_1T + a_2)$ is irreducible in $\mathbb{F}_q[T]$.*

Bender and Wittenberg [BeW05, Thm. 1.1 and Prop. 4.1] prove the first result in this direction:

PROPOSITION B: *Let q be a power of a prime number and $f_1, \ldots, f_r$ polynomials of total degrees $d_1, \ldots, d_r$, respectively. Suppose each $1 \leq i \leq r$ satisfies*

(1a) *$p \nmid d_i(d_i - 1)$ and*

(1b) *the Zariski closure C_i in $\mathbb{P}^2_{\mathbb{F}_q}$ of the affine plane curve defined by $f_i(T, X) = 0$ is smooth.*

Then for each large k there exists $(a_1, a_2) \in \mathbb{F}^2_{q^k}$ such that each of the polynomials $f_1(T, a_1T + a_2), \ldots, f_r(T, a_1T + a_2)$ is irreducible in $\mathbb{F}_{q^k}[T]$.

Moreover, for $r = 1$ and $q > 9(d(d-1)d + 2)^2$ the number of pairs $(a_1, a_2) \in \mathbb{F}^2_q$ such that $f_1(T, a_1T + a_2)$ is irreducible in $\mathbb{F}_q[T]$ is at least $\frac{1}{d!}q^2 + c_1q^{3/2} + c_2q + c_3q^{\frac{1}{2}} + c_4$, where c_1, c_2, c_3, c_4 are explicitely given constants depending only on d.

Note that Condition (1a) implies that $p \neq 2$. Our main result improves Proposition B in three ways. First, it includes the case $p = 2$, albeit with the restriction that $r = 1$ in this case. Second, we replace the condition that the C_i's be smooth by a less restrictive condition of being "characteristic-0-like" (see Section 1 for definition) and **nodal** (i.e. having only nodes as singularities). Finally, our result is quantitative for arbitrary r, that is, we give an asymptotic formula for the number of pairs (a_1, a_2) for which the polynomials $f_i(T, a_1T + a_2)$ are irreducible, when $q \to \infty$. Thus, our result solves Problem A for "nice" polynomials.

THEOREM C: *Let $f_1, \ldots, f_r \in \mathbb{F}_q[T, X]$ be non-associate absolutely irreducible characteristic-0-like nodal polynomials, where q is a power of a prime p such that $r = 1$ if $p = 2$. For each $1 \leq i \leq r$ let $d_i = \deg_T(f_i(T, X))$ and set $d = \prod_{i=1}^r d_i$. Then,*

$$\#\{(a_1, a_2) \in \mathbb{F}_q^2 \mid f_i(T, a_1T + a_2) \text{ is irreducible in } \mathbb{F}_q[T],\ i = 1, \ldots, r\} = \frac{q^2}{d} + O(q^{3/2}),$$

where the constant of the O is a computable function in $\sum_{i=1}^r d_i$.

Note that the leading terrm in our approximation formula is $\frac{q^2}{d}$. For large q and for $d > 2$, this improves the lower bound given in Theorem B for $r = 1$ that has the leading term $\frac{q^2}{d!}$.

Apart from standard combinatorial arguments, the proof of Theorem C is based on three ingredients: geometrical arguments used in the proof of the theorem about the stability of fields [FrJ08, Section 18.9], the field crossing argument [FrJ08, Section 24.1], and the Lang-Weil estimates.

Proposition 4.1 proves that Proposition B is a special case of Theorem C.

Finally we mention that Pollack [Pol08] and the first author [BaS10] treat the case of the analog of the Bateman–Horn Conjecture when T does not occur in the f_i's.

1. Direct Product of Symmetric Groups

Let Γ be a projective plane curve defined over a field K by an absolutely irreducible homogeneous equation $f(X_0, X_1, X_2) = 0$ with a generic point $\mathbf{x} = (x_0{:}x_1{:}x_2)$. Then the point

$$\mathbf{x}^* = (x_0^*{:}x_1^*{:}x_2^*) = \Big(\frac{\partial f}{\partial X_0}(\mathbf{x}) : \frac{\partial f}{\partial X_1}(\mathbf{x}) : \frac{\partial f}{\partial X_2}(\mathbf{x})\Big) \tag{1}$$

is a generic point of an absolutely irreducible projective plane K-curve Γ^*, known as the **dual curve** of Γ. The points of Γ^* parametrize the tangents of Γ at simple points. The map $\mathbf{x} \mapsto \mathbf{x}^*$ extends to a rational map $\Gamma \to \Gamma^*$.

LEMMA 1.1: *Let K be an algebraically closed field with* $\mathrm{char}(K) \neq 2$. *Let Γ and Δ be distinct absolutely irreducible projective plane K-curves. Suppose both Γ and Δ have only finitely many inflection points. Then Γ and Δ have only finitely many common tangents.*

Proof: Assume Γ and Δ have infinitely many common tangents. Then $\Gamma^*(K) \cap \Delta^*(K)$ is infinite, hence $\Gamma^* = \Delta^*$, so $\Gamma^{**} = \Delta^{**}$. Since both Γ and Δ has only finitely many inflection points, $\Gamma^{**} = \Gamma$ and $\Delta^{**} = \Delta$ [GeJ89, Prop. 4.5]. Therefore, $\Gamma = \Delta$, in contrast to our assumption. ∎

Given an absolutely irreducible projective plane K-curve Γ, we write $\Gamma_{\tilde{K}}$ for the $\tilde{K}$-curve obtained by base change from K to its algebraic closure $\tilde{K}$. It is well known, that if Γ is not a line and $\mathrm{char}(K) = 0$, then

(2a) $\Gamma_{\tilde{K}}$ has only finitely many inflection points,

(2b) $\Gamma_{\tilde{K}}$ has only finitely many double tangents, and

(2c) $\Gamma_{\tilde{K}}$ is not strange,

[FrJ76, Lemma 3.2]. In general we say that Γ is a **characteristic-0-like curve** if it satisfies Condition (2).

We say that Γ is a **nodal curve**, if all of the singular points of $\Gamma_{\tilde{K}}$ are nodes [Ful89, p. 66].

We say that an absolutely irreducible polynomial $f \in K[T, X]$ is **characteristic-0-like nodal** if the Zariski closure Γ in $\mathbb{P}^2_K$ of the affine plane curve defined by the equation $f(T, X) = 0$ is a characteristic-0-like nodal curve.

Finally we say that polynomials $f, g \in K[T, X]$ are **non-associate** if $f \neq \lambda g$ for all $\lambda \in K^\times$.

LEMMA 1.2: *Let K be an infinite field and $f_1, \ldots, f_r \in K[T, X]$ be absolutely irreducible non-associate characteristic-0-like nodal polynomials of degrees $d_1, \ldots, d_r$, respectively. Then:*

(a) *There exist $\alpha, \beta \in K$ such that for each $1 \leq i \leq r$ we have*

$$\mathrm{Gal}\Big(f_i\big(T, \frac{\alpha + T + \beta U}{U}\big), \tilde{K}(U)\Big) \cong S_{d_i}.$$

(b) *If, in addition, $\mathrm{char}(K) \neq 2$ and we set $f = f_1 \cdots f_r$, then α, β can be chosen such that*

$$\mathrm{Gal}\Big(f\big(T, \frac{\alpha + T + \beta U}{U}\big), \tilde{K}(U)\Big) \cong \prod_{i=1}^{r} S_{d_i}.$$

Proof of (a): For each $1 \leq i \leq r$ let Γ_i be the Zariski closure in $\mathbb{P}^2_K$ of the absolutely irreducible affine plane K-curve defined over K by the equation $f_i(T, X) = 0$. By our assumption on the f_i's, the absolutely irreducible projective plane K-curves $\Gamma_1, \ldots, \Gamma_r$ are distinct. Since the Γ_i's are characteristic-0-like curves, there are finitely many lines

$L_1, \dots, L_m$ in $\mathbb{P}_{\tilde{K}}$ such that if

$$\mathbf{o} \in \mathbb{P}^2(\tilde{K}) \smallsetminus \bigcup_{i=1}^{r} \Gamma_i(\tilde{K}) \cup \bigcup_{j=1}^{m} L_j(\tilde{K}), \tag{3}$$

then for each $1 \le i \le r$ we have [FrJ76, proof of Lemma 3.2]:

(4a) $\mathbf{o}$ lies on no tangent to Γ_i at an inflection point;

(4b) no double tangent to Γ_i goes through $\mathbf{o}$;

(4c) $\mathbf{o}$ lies on no line that goes through two singular points of Γ_i;

(4d) $\mathbf{o}$ lies on no tangent to Γ_i that goes through a singular point of Γ_i; and

(4e) only finitely many lines through $\mathbf{o}$ are tangents to Γ_i.

Since K is infinite, we may choose a point $\mathbf{o} = (1{:}{-}\alpha{:}\beta) \in \mathbb{P}^2(K)$ that satisfies (3), hence also (4). Then $\mathbf{o}$ is the intersection of the lines Λ_α and Λ_β respectively defined by the homogeneous equations $-\alpha X_0 - X_1 = 0$ and $\beta X_0 - X_2 = 0$ with coefficients in K.

We consider $1 \le i \le r$. Then $\deg(\Gamma_i) = \deg(f_i) = d_i$. We choose a transcendental element t over K and a root x_i of the equation $f_i(t, X)$ in $\widetilde{K(t)}$, and set $F_i = K(t, x_i)$. The projection $\lambda\colon \mathbb{P}^2_{\tilde{K}} \smallsetminus \{\mathbf{o}\} \to \mathbb{P}^1_K$ from $\mathbf{o}$ is defined over K by

$$\lambda(X_0{:}X_1{:}X_2) = (-\alpha X_0 - X_1 : \beta X_0 - X_2).$$

In particular, $\lambda(1{:}t{:}x_i) = (-\alpha - t : \beta - x_i)$ is a generic point of $\mathbb{P}^1_K$ and

$$u_i = \frac{-\alpha - t}{\beta - x_i} \tag{5}$$

is transcendental over K (because $\deg(f_i) \ge 2$).

A central argument in the proof of [FrJ76, Lemma 3.3] states that every line in $\mathbb{P}^2_{\tilde{K}}$ that passes through $\mathbf{o}$ cuts $\Gamma_{i,\tilde{K}}$ in at least $d_i - 1$ points and almost every such line cuts $\Gamma_{i,\tilde{K}}$ in d_i points. Then, by [FrJ76, Lemma 2.1], u_i is a separating transcendental element for F_i/K and the Galois closure $\hat{F}_i$ of $F_i/K(u_i)$ satisfies

$$\mathrm{Gal}(\hat{F}_i/K(u_i)) \cong \mathrm{Gal}(\hat{F}_i\tilde{K}/\tilde{K}(u_i)) \cong S_{d_i}.$$

By (5), $x_i = \frac{\alpha+t+\beta u_i}{u_i}$, so $F_i = K(t, u_i)$. Since $f_i(t, x_i) = 0$, we have $f_i\big(t, \frac{\alpha+t+\beta u_i}{u_i}\big) = 0$. Hence, the rational function $f_i\big(T, \frac{\alpha+T+\beta U}{U}\big)$ in the variables T, U is absolutely irreducible, separable in T, and with Galois group over $\tilde{K}(U)$ isomorphic to S_{d_i}, as claimed.

Proof of (b): Now we assume that $\mathrm{char}(K) \neq 2$. Then, by Lemma 1.1 only finitely many lines in $\mathbb{P}^2_{\tilde{K}}$ are tangents to two of the curves $\Gamma_1, \ldots, \Gamma_r$. Using the notation of the proof of (a), we may assume that these lines belong to the set $\{L_1, \ldots, L_m\}$. Then the point $\mathbf{o}$ satisfies, in addition to (4) also the following condition:

(6) Each line through $\mathbf{o}$ is a tangent to at most one of the curves $\Gamma_1, \ldots, \Gamma_r$.

Let $1 \leq i \leq r$ and consider a prime divisor $\mathfrak{p}$ of $\tilde{K}(u_i)/\tilde{K}$ that ramifies in $\hat{F}_i\tilde{K}$. Then $\mathfrak{p}$ may be identified with the intersection point of $\mathbb{P}^1_{\tilde{K}}$ with a tangent L to Γ_i at a point P that goes through $\mathbf{o}$. Indeed, in this case, the intersection multiplicity of L with Γ_i at P is 2 and is 1 at all other intersection points (by (4)). Thus, by Bezout's theorem, L has $d_i - 1$ intersection points with Γ_i, so $\mathfrak{p}$ decomposes in $F_i\tilde{K}$ as $\mathfrak{p} = 2\mathfrak{p}_1 + \mathfrak{p}_2 + \cdots + \mathfrak{p}_{d-1}$ with distinct prime divisors $\mathfrak{p}_1, \cdots, \mathfrak{p}_{d-1}$. We also identify u_i with the variable U. It follows from (6) that for all $i \neq j$, the set of the prime divisors of $\tilde{K}(U)/\tilde{K}$ that ramify in $\hat{F}_i\tilde{K}$ is disjoint from the set of prime divisors of $\tilde{K}(U)/\tilde{K}$ that ramify in $\hat{F}_j\tilde{K}$. Therefore, by Riemann-Hurwitz, we have for each $1 \leq j \leq r$ that $(\hat{F}_j\tilde{K}) \cap (\prod_{i\neq j} \hat{F}_j\tilde{K}) = \tilde{K}(U)$ [FrJ08, Rem. 16.2(b)]. Consequently, by (a),

$$\mathrm{Gal}\Big(f\big(T, \frac{\alpha+T+\beta U}{U}\big), \tilde{K}(U)\Big) \cong \prod_{i=1}^{r} \mathrm{Gal}(\hat{F}_i/\tilde{K}(U)) \cong \prod_{i=1}^{r} S_{d_i},$$

as claimed. ∎

The following corollary does not assume K to be infinite.

COROLLARY 1.3: *Let K be a field and let $f_1, \ldots, f_r \in K[T, X]$ be non-associate characteristic-0-like nodal absolutely irreducible polynomials of degrees $d_1, \ldots, d_r$, respectively. Let A and B be variables. We set $f = f_1 \cdots f_r$ and assume that $r = 1$ if* $\mathrm{char}(K) = 2$. *Then,* $\mathrm{Gal}(f(T, AT + B), K(A, B)) \cong \prod_{i=1}^{r} S_{d_i}$.

Proof: First we prove the corollary for $\tilde{K}$ rather than for K. To this end we use the fact that $\tilde{K}$ is infinite to choose $\alpha, \beta \in \tilde{K}$ such that (a) of Lemma 1.2 holds, and also

(b) of that Lemma holds if $\mathrm{char}(K) \neq 2$. Then we extend the specialization $(A, B) \to \left(\frac{1}{U}, \frac{\alpha+\beta U}{U}\right)$ to a $\tilde{K}$-place φ of the splitting field of $f(T, AT + B)$ over $K(A, B)$. Then $\mathrm{Gal}\big(f\big(T, \frac{\alpha+T+\beta U}{U}\big), \tilde{K}(U)\big)$ is a quotient of a subgroup of $\mathrm{Gal}(f(T, AT + B), \tilde{K}(A, B))$, namely the quotient of the decomposition group by the inertia group of φ. Since, $\mathrm{Gal}(f(T, AT + B), \tilde{K}(A, B)) \leq \prod_{i=1}^{r} S_{d_i}$ and $\mathrm{Gal}\big(f(T, \frac{\alpha+T+\beta U}{U}), \tilde{K}(U)\big) \cong \prod_{i=1}^{r} S_{d_i}$, we conclude that $\mathrm{Gal}(f(T, AT + B), \tilde{K}(A, B)) \cong \prod_{i=1}^{r} S_{d_i}$.

The truth of the corollary for K now follows from its truth for $\tilde{K}$ and from the following inclusion of groups: $\prod S_{d_i} \cong \mathrm{Gal}(f(T, AT + B), \tilde{K}(A, B)) \leq \mathrm{Gal}(f(T, AT + B), K(A, B)) \leq \prod_{i=1}^{r} S_{d_i}$. ∎

2. The Field Crossing Argument

The field crossing argument has already been used in the original proofs of the Chebotarev density theorem for number fields. It has been used again in the proof of the Chebotarev density theorem for function fields of one variable over finite fields, of the arithmetic proof of the Hilbert irreducibility theorem, in the theory of Frobenius fields, and on many more occasions. See also [Deb99, Prop. 22.2]. Here we use it to replace the counting of points with a given Artin class by the counting of rational points of an absolutely irreducible variety over a finite field (Theorem 3.1). The argument itself appears in the proof of Lemma 2.8.

Definition 2.1: Ring-cover. Let S/R be an extension of integral domains whose corresponding extension of quotient fields F/E is finite and separable. We say that S/R is a **ring-cover** if R is integrally closed, $S = R[z]$, z is integral over R, and the discriminant of $\mathrm{irr}(z, E)$ is a unit of R. In this case S is the integral closure of R in F [FrJ08, Def. 1.6.3] and S/R is an étale extension of rings [Ray70, p. 19]. Thus, the corresponding map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ of affine K-schemes is finite and étale. If F/E is in addition Galois, we say that S/R is a **Galois ring-cover**. ∎

For the rest of this section we fix a field K, variables $A_1, \ldots, A_n, T$, let $\mathbf{A} = (A_1, \ldots, A_n)$, and set $E = K(\mathbf{A})$.

Definition 2.2: We define the **total degree** of a polynomial $h = \sum_{i=1}^{m} c_i T^i \in E[T]$ to be

$$\text{total.deg}(h) = \max_{1 \le i \le m} \big(\max(\deg(f_i), \deg(g_i)) + i \big),$$

where $c_i = \frac{f_i(\mathbf{A})}{g_i(\mathbf{A})}$ is a reduced presentation of c_i with $f_i, g_i \in K[\mathbf{A}]$ and $\deg(f_i), \deg(g_i)$ are the degrees of f_i, g_i, respectively. Under this definition, the total degree of h coincides with the degree of h as a polynomial in $A_1, \ldots, A_n, T$ if $h \in K[\mathbf{A}, T]$. ∎

Definition 2.3: Bound. In the following results we apply several algorithms to polynomials $f_1, \ldots, f_k \in E[T]$ whose output are polynomials $h_1, \ldots, h_{k'} \in E[T]$. We say that the total degrees of $h_1, \ldots, h_{k'}$ are **bounded** if we can compute a function $p\colon \mathbb{Z} \to \mathbb{R}$ that depends only on the algorithms (but not on K neither on $f_1, \ldots, f_k$) such that $\sum_{i=1}^{k'} \text{total.deg}(h_i) \le p(m)$, where $m = \sum_{i=1}^{k} \text{total.deg}(f_i)$. Note that iteration of algorithms with output of bounded total degree have again an output of bounded total degrees. ∎

Notation 2.4: Left conjugation. Given a map θ from a set G to a group S and an element $\tau \in S$, we write ${}^{\tau}\theta$ for the map from G to S defined for all $\sigma \in G$ by the rule ${}^{\tau}\theta(\sigma) = \tau\theta(\sigma)\tau^{-1}$. Note that ${}^{\tau\tau'}\theta = {}^{\tau}({}^{\tau'}\theta)$ for $\tau, \tau' \in S$ and ${}^{1}\theta = \theta$ for the unit element 1 of S. ∎

Definition 2.5: Points and homomorphisms. Let A be an integrally closed integral domain which is finitely generated over a field K and such that $E = \text{Quot}(A)$ is regular over K. Let F be a finite Galois extension of E and write B for the integral closure of A in F. Suppose B/A is a ring cover. Let $X = \text{Spec}(A)$ and $Y = \text{Spec}(B)$, and let $\lambda\colon Y \to X$ be the finite étale morphism associated with the inclusion $A \subseteq B$. The points $\mathbf{a} \in X(K)$ bijectively corresponds to K-homomorphisms $\varphi_{\mathbf{a}}\colon A \to K$. The points $\mathbf{b} \in Y(K_s)$ with $\lambda(\mathbf{b}) = \mathbf{a}$ bijectively correspond to epimorphisms $\varphi_{\mathbf{b}}\colon B \to K(\mathbf{b})$ that extend $\varphi_{\mathbf{a}}$. Since B/A is étale and Galois, for each $\mathbf{b}$ as above the extension $K(\mathbf{b})/K$ is Galois that depends only on $\mathbf{a}$, and $\varphi_{\mathbf{b}}$ defines an embedding $\varphi^*\colon \text{Gal}(K(\mathbf{b})/K) \to \text{Gal}(F/E)$ such that $\varphi_{\mathbf{b}}(\varphi^*(\sigma)x) = \sigma(\varphi_{\mathbf{b}}(x))$ for all $\sigma \in \text{Gal}(K(\mathbf{b})/K)$ and $x \in B$ [FrJ08, Lemma 6.1.4]. Let $\text{Gal}(K) = \text{Gal}(K_s/K)$ be the absolute Galois group of K. Composing φ^* with res: $\text{Gal}(K) \to \text{Gal}(K(\mathbf{b})/K)$, we get a homomorphism $\varphi^*_{\mathbf{b}}\colon \text{Gal}(K) \to \text{Gal}(F/E)$

with $\mathrm{Ker}(\varphi_{\mathbf{b}}^*) = \mathrm{Gal}(K(\mathbf{b}))$ such that $\varphi_{\mathbf{b}}(\varphi_{\mathbf{b}}^*(\sigma)x) = \sigma(\varphi_{\mathbf{b}}(x))$ for all $\sigma \in \mathrm{Gal}(K)$ and $x \in B$. The image $\varphi_{\mathbf{b}}^*(\mathrm{Gal}(K))$ of $\varphi_{\mathbf{b}}^*$ is the **decomposition group** $D_{\mathbf{b/a}}$ of $\mathbf{b}$ over $\mathbf{a}$. In particular, if F' is the fixed field of $D_{\mathbf{b/a}}$ in F and $x \in B \cap F'$, then $\varphi_{\mathbf{b}}(x) \in K$. Finally we note that for each $\mathbf{a} \in X(K)$, the action of $\mathrm{Gal}(F/E)$ on the set of prime ideals of B lying over $\mathrm{Ker}(\varphi_{\mathbf{a}})$ defines an action of $\mathrm{Gal}(F/E)$ on $\lambda^{-1}(\mathbf{a}) \cap Y(K_s)$ such that for all $\mathbf{b} \in Y(K_s)$ with $\lambda(\mathbf{b}) = \mathbf{a}$ and each $\tau \in \mathrm{Gal}(F/E)$ we have $K(\tau\mathbf{b}) = K(\mathbf{b})$, $\lambda(\tau\mathbf{b}) = \mathbf{a}$, $\varphi_{\tau\mathbf{b}} = \varphi_{\mathbf{b}} \circ \tau^{-1}$, and $\varphi_{\tau\mathbf{b}}^* = {}^{\tau}(\varphi_{\mathbf{b}}^*)$.

In order to prove the latter equality we consider $\sigma \in \mathrm{Gal}(K)$ and $x \in B$. By definition

$$\varphi_{\mathbf{b}}(\tau^{-1}(\varphi_{\tau\mathbf{b}}^*(\sigma)x)) = \varphi_{\tau b}(\varphi_{\tau\mathbf{b}}^*(\sigma)x) = \sigma(\varphi_{\tau\mathbf{b}}(x)) = \sigma(\varphi_{\mathbf{b}}(\tau^{-1}x)) = \varphi_{\mathbf{b}}(\varphi_{\mathbf{b}}^*(\sigma)(\tau^{-1}x)).$$

If x is a primitive element of the cover B/A, then $\varphi_{\mathbf{b}}$ map the set of K-conjugates of x injectively into K_s (because the discriminant of $\mathrm{irr}(x, E)$ is a unit of B). It follows in this case that $\tau^{-1}(\varphi_{\tau\mathbf{b}}^*(\sigma)x) = \varphi_{\mathbf{b}}^*(\sigma)(\tau^{-1}x)$. Thus, $\varphi_{\tau\mathbf{b}}(\sigma)x = (\tau \circ \varphi_{\mathbf{b}}^*(\sigma) \circ \tau^{-1})x$. Therefore, $\varphi_{\tau\mathbf{b}}(\sigma)x = \tau \circ \varphi_{\mathbf{b}}^*(\sigma) \circ \tau^{-1}$ for all $\sigma \in \mathrm{Gal}(K)$. This means that $\varphi_{\tau\mathbf{b}}(\sigma) = {}^{\tau}(\varphi_{\mathbf{b}}^*)$, as claimed.

The star operation is functorial in B: Let F' be a finite Galois extension of E that contains F, let B' be the integral closure of A in F', and let $Y' = \mathrm{Spec}(B')$. Suppose B'/A is a ring-cover and let $\mathbf{b}' \in Y'(K_s)$ lie over $\mathbf{b} \in Y(K_s)$. Then $\varphi_{\mathbf{b}'}^*|_F = \varphi_{\mathbf{b}}^*$. ∎

LEMMA 2.6: *Let $t_1, \ldots, t_r$ elements of E_s and let $f_1, \ldots, f_r \in E[T]$ be separable polynomials that satisfy $f_i(\mathbf{A}, t_i) = 0$, $i = 1, \ldots, r$. Then there exist polynomials $h \in K[\mathbf{A}, T]$ and $0 \neq g \in K[\mathbf{A}]$ of bounded total degrees and an element $t \in E_s$ such that $h(\mathbf{A}, t) = 0$, $E(t) = E(t_1, \ldots, t_r)$, and $K[\mathbf{A}, g(\mathbf{A})^{-1}, t]/K[\mathbf{A}, g(\mathbf{A})^{-1}]$ is a cover of rings. Moreover, the discriminant of $f_i(\mathbf{A}, T)$ as a polynomial in $\mathbf{A}$ is invertible in $K[\mathbf{A}, g(\mathbf{A})^{-1}]$, $i = 1, \ldots, r$.*

Proof: The proof of the primitive element theorem [Lan93, Thm. V.4.6] assures that if C is a subset of $K[\mathbf{A}]$ of a large bounded cardinality, then there exist $c_1, \ldots, c_r \in C$ such that $t = c_1t_1 + \cdots + c_rt_r$ satisfies $K(t) = K(t_1, \ldots, t_r)$. In particular, there exist such $c_1, \ldots, c_r \in K[\mathbf{A}]$ with bounded degrees. Dividing each f_i by its leading coefficient, we

may assume that f_i is monic (as a polynomial in T). Let

$$h(\mathbf{A}, T) = \prod_{(t'_1,\ldots,t'_r)} (T - \sum_{i=1}^{r} c_i t'_i),$$

where for each $1 \leq i \leq r$ the index t'_i ranges over all roots of f_i in E_s. Then $h(\mathbf{A}, T) \in E[T]$ and the coefficients of h are polynomials in the coefficients of f_i with bounded degrees. Moreover, $h(\mathbf{A}, t) = 0$.

Let $g(\mathbf{A})$ be the product of the numerators and the denominators of the discriminants of $f_1, \ldots, f_r, h$. Then $g \in K[\mathbf{A}]$ and has a bounded degree. By Definition 2.1, h and g satisfy all of the requirements of the lemma. ∎

LEMMA 2.7: *Let G be a group of order d, let θ be the regular embedding of G in S_d, and let $H = \{\tau \in S_d \mid {}^{\tau}\theta = \theta\}$. Then $|H| = d$.*

Proof: We identify S_d with the group S_G of all permutations of G. Then $\theta(\sigma)(x) = \sigma x$ for all $\sigma, x \in G$. It follows that $\tau^{-1} \in H$ if and only if $\sigma \cdot \tau(x) = \tau(\sigma x)$ (where the left hand side is the product of the elements σ and $\tau(x)$ of G) for all $\sigma, x \in G$. In particular, for $\sigma = x^{-1}$ we get $x^{-1} \cdot \tau(x) = \tau(1)$, so $\tau(x) = x \cdot \tau(1)$. Conversely, if $\tau(x) = x \cdot \tau(1)$, then the former condition holds, so $\tau \in H$. Since $\tau(1)$ can take d values, i.e. the elements of G, there are exactly d possibilities for τ. ∎

The following central result is built on [BaS10, Lemma 2.2].

LEMMA 2.8: *Let K be a field and $A_1, \ldots, A_n, T$ variables. For each $1 \leq i \leq r$ let $f_i \in K[\mathbf{A}, T]$ be an absolutely irreducible polynomial which is separable and of degree d_i in T. Let L_i be a Galois extension of K of degree d_i.*

We denote the splitting field of $f = f_1 \cdots f_r$, considered as a polynomial in T, over $E = K(\mathbf{A})$ by F and assume that $\mathrm{Gal}(F/E) \cong \prod_{i=1}^{r} S_{d_i}$.

Then there exist a proper algebraic subset V of $\mathbb{A}^n_K$, a absolutely irreducible normal affine K-variety W', and a finite étale map $\rho' \colon W' \to U$ with $U = \mathbb{A}^n_K \setminus V$ such that the following conditions hold:

(a) *V and W' are defined in $\mathbb{A}^n_K$ and $\mathbb{A}^{n+3}_K$, respectively, by polynomials with coefficients in K of bounded total degrees.*

(b) $\deg(f_i(\mathbf{a},T)) = d_i$ *for each* $\mathbf{a} \in U(K)$ *and for* $i = 1,\dots,r$.

(c) $\rho'(W'(K))$ *is the set of all* $\mathbf{a} \in U(K)$ *such that* L_i *is generated by a root of* $f_i(\mathbf{a},T)$, $i = 1,\dots,r$. *In particular,* $f_i(\mathbf{a},T)$ *is irreducible of degree* d_i *for all* $\mathbf{a} \in \rho'(W'(K))$ *and* $1 \le i \le r$.

(d) $|(\rho')^{-1}(\mathbf{a}) \cap W'(K)| = \prod_{i=1}^{r} d_i$ *for all* $\mathbf{a} \in \rho'(W'(K))$.

Proof: For each $1 \le i \le r$ let F_i be the splitting field of f_i over E. Then $F = \prod_{i=1}^{r} F_i$ and since $\mathrm{Gal}(F/E) \cong \prod_{i=1}^{r} S_{d_i}$, we have $\mathrm{Gal}(F_i/E) \cong S_{d_i}$ for $i = 1,\dots,r$. For each $1 \le i \le r$ we define a homomorphism θ_i: $\mathrm{Gal}(K) \to S_{d_i}$ in the following way: First we identify the symmetric group S_{d_i} with the group of all permutations of $\mathrm{Gal}(L_i/K)$ (which we consider as a set of d_i elements). Then, for each $\sigma \in \mathrm{Gal}(K)$ we define $\theta_i(\sigma)$ as a permutation of $\mathrm{Gal}(L_i/K)$ by the rule $\theta_i(\sigma)(\lambda) = \sigma|_{L_i} \cdot \lambda$ for all $\lambda \in \mathrm{Gal}(L_i/K)$. Identifying $\mathrm{Gal}(F_i/E)$ with S_{d_i}, this defines a homomorphism θ_i: $\mathrm{Gal}(K) \to \mathrm{Gal}(F_i/E)$ with $\mathrm{Ker}(\theta_i) = \mathrm{Gal}(L_i)$. Since $\mathrm{Gal}(F/E) \cong \prod_{i=1}^{r} \mathrm{Gal}(F_i/E)$, the map θ: $\mathrm{Gal}(K) \to \mathrm{Gal}(F/E)$ defined by $\theta(\sigma)|_{F_i} = \theta_i(\sigma)$ for all $\sigma \in \mathrm{Gal}(K)$ and $1 \le i \le r$ is a well defined homomorphism with $\mathrm{Ker}(\theta) = \mathrm{Gal}(L)$, where $L = L_1 \cdots L_r$. It induces an embedding $\bar{\theta}$: $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/E)$ satisfying $\bar{\theta}(\sigma|_L) = \theta(\sigma)$ for each $\sigma \in \mathrm{Gal}(K)$. We denote the fixed field of $\theta(\mathrm{Gal}(K))$ in F by E'.

Now we break up the rest of the proof into several parts.

PART A: *Field crossing argument.* We consider the Galois extension $\hat{F} = FL$ of E and note that since F/K is a regular extension,

$$\mathrm{Gal}(\hat{F}/E') = \mathrm{Gal}(\hat{F}/F) \times \mathrm{Gal}(\hat{F}/E'L) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(F/E'), \tag{1}$$

where the latter isomorphism is induced by the corresponding restriction maps. Next we consider the subgroup

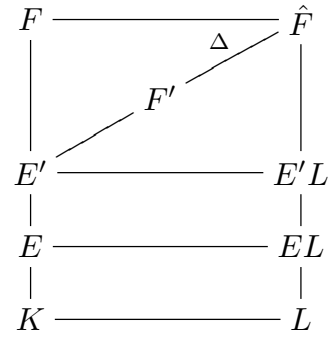
$$\Delta = \{\delta \in \mathrm{Gal}(\hat{F}/E) \mid \bar{\theta}(\delta|_L) = \delta|_F\}$$

of $\mathrm{Gal}(\hat{F}/E')$. Using (1) and the injectivity of $\bar{\theta}$, one sees that $\Delta \cap \mathrm{Gal}(\hat{F}/F) = 1$ and $\Delta \cap \mathrm{Gal}(\hat{F}/E'L) = 1$. Moreover, $\Delta \cdot \mathrm{Gal}(\hat{F}/F) = \mathrm{Gal}(\hat{F}/E)$ and $\Delta \cdot \mathrm{Gal}(\hat{F}/E'L) = \mathrm{Gal}(\hat{F}/E')$.

Indeed, by (1), for each $\varepsilon \in \mathrm{Gal}(\hat{F}/E')$ there exists $\delta \in \mathrm{Gal}(\hat{F}/E')$ such that $\delta|_F = \varepsilon|_F$ and $\delta|_L = (\bar{\theta})^{-1}(\varepsilon|_F)$. Then, $\varepsilon = \delta \cdot \delta^{-1}\varepsilon$, $\delta \in \Delta$, and $(\delta^{-1}\varepsilon)|_F = 1$, so $\delta^{-1}\varepsilon \in \mathrm{Gal}(\hat{F}/F)$. Similarly, there exists $\delta' \in \mathrm{Gal}(\hat{F}/E')$ such that $\delta'|_L = \varepsilon|_L$ and $\delta'|_F = \bar{\theta}(\varepsilon|_L)$. Thus, $\varepsilon = \delta' \cdot (\delta')^{-1}\varepsilon$, $\delta' \in \Delta$ and $((\delta')^{-1}\varepsilon)|_L = 1$, so $(\delta')^{-1}\varepsilon \in \mathrm{Gal}(\hat{F}/E'L)$. It follows that the fixed field F' of Δ in $\hat{F}$ satisfies

$$FF' = F'L = \hat{F} \qquad \text{and} \qquad F \cap F' = F' \cap E'L = E' \tag{2}$$

and fits into the following diagram of fields:



Part B: *Integral étale extensions of rings.* By Lemma 2.6 applied to the roots of f, there exist a polynomial $h \in K[\mathbf{A}, T]$, separable in T, and a nonzero polynomial $g \in K[\mathbf{A}]$ of bounded total degrees, and there exists an element $t \in F$ such that $h(\mathbf{A}, t) = 0$, $F = E(t)$, and $K[\mathbf{A}, g(\mathbf{A})^{-1}, t]/K[\mathbf{A}, g(\mathbf{A})^{-1}]$ is a ring-cover. Moreover, the discriminant of each $f_i(\mathbf{A}, T)$ considered as a polynomial in T is invertible in $K[\mathbf{A}, g(\mathbf{A})^{-1}]$.

Applying Lemma 2.6 to t and to a primitive element of L/K, we find a polynomial $\hat{h} \in K[\mathbf{A}, T]$, separable in T, a nonzero polynomial $\hat{g} \in K[\mathbf{A}]$, and an element $\hat{t} \in \hat{F}$ such that $\hat{h}, \hat{g}$ have bounded degrees, $\hat{h}(\mathbf{A}, \hat{t}) = 0$, $\hat{F} = E(\hat{t})$, and $K[\mathbf{A}, \hat{g}(\mathbf{A})^{-1}, \hat{t}]/K[\mathbf{A}, \hat{g}(\mathbf{A})^{-1}]$ is a ring-cover. Moreover, $\hat{g}$ may be taken as a multiple of g.

Let $\hat{t}_1, \ldots, \hat{t}_k$ be a Δ-orbit starting with $\hat{t}_1 = \hat{t}$ and write $\prod_{j=1}^{k}(T - \hat{t}_j) = T^k + t'_1 T^{k-1} + \cdots + t'_k$. Then $F' = E(t'_1, \ldots, t'_k)$ [FrJ08, End of the proof of Lemma 19.3.2]. Moreover, each of the coefficients of $\mathrm{irr}(t'_j, E)$, $j = 1, \ldots, k$, is a symmetric polynomial in the E-conjugates of $\hat{t}$ of a bounded total degree. Hence, those coefficients are polynomials in the coefficients of $\hat{h}$ of bounded degrees having integral coefficients. Applying

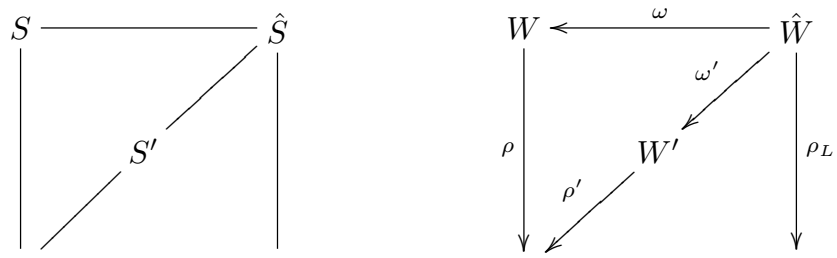
Lemma 2.6 now to $\mathrm{irr}(t_1', E), \ldots, \mathrm{irr}(t_k', E)$, we can compute polynomials $h' \in K[\mathbf{A}, T]$ and $g' \in K[\mathbf{A}]$ of bounded total degrees and an element $t' \in F'$ such that $h'(\mathbf{A}, t') = 0$, $g'(\mathbf{A}) \neq 0$, $S' = K[\mathbf{A}, g'(\mathbf{A})^{-1}, t']$ is a ring cover of $R = K[\mathbf{A}, g'(\mathbf{A})^{-1}]$, and $F' = E(t')$. Moreover, g' may be taken as a multiple of $\hat{g}$, hence of g. Also,

(3) the discriminant of $f_i(\mathbf{A}, T)$ is invertible in R, $i = 1, \ldots, r$.

Let $S = R[t]$ and $\hat{S} = R[\hat{t}]$. Then S is the integral closure of R in F, S' is the integral closure of R in F', and $\hat{S}$ is the integral closure of R, S, and S' in $\hat{F}$. It follows from (2) that $SL = \hat{S}$ and $S'L = \hat{S}$. Moreover, S/R, S'/R, $\hat{S}/S$, $\hat{S}/S'$, and $\hat{S}/R$ are ring covers in the sense of Definition 2.1.

Part C: *Fiber products.* Let V be the Zariski closed subset of $\mathbb{A}_K^n$ defined by the equation $g'(\mathbf{A}) = 0$. Then $U = \mathbb{A}_K^n \smallsetminus V$ is a non-empty Zariski open subset of $\mathbb{A}_K^n$. We set $W = \mathrm{Spec}(S)$, $W' = \mathrm{Spec}(S')$, and $\hat{W} = \mathrm{Spec}(\hat{S})$. By Part B, V, W, and W' are closed subsets of $\mathbb{A}_K^n$, $\mathbb{A}_K^{n+3}$, and $\mathbb{A}_K^{n+3}$, respectively, defined by polynomials with coefficients in K of bounded degrees. Moreover, the ring-covers in the left diagram of inclusions of rings in (4) define finite étale morphisms as in the right diagram of (4):

(4)



Here $U_L = U \times_{\mathrm{Spec}(K)} \mathrm{Spec}(L) = \mathrm{Spec}(RL)$ and each of the three rectangles in the right diagram of (4) is cartesian, i.e. $\hat{W} = W \times_U W'$, $\hat{W} = W \times_U U_L$, and $\hat{W} = W' \times_U U_L$. This concludes the proof of (a).

Part D: *Geometric points.* For each $\mathbf{a} \in U(K)$ and each $\mathbf{b} \in W(K_s)$ with $\rho(\mathbf{b}) = \mathbf{a}$ we consider the homomorphisms $\varphi_{\mathbf{b}}\colon S \to K_s$ and $\varphi_{\mathbf{b}}^*\colon \mathrm{Gal}(K) \to \mathrm{Gal}(F/E)$ introduced in Definition 2.5. By Diagram (4), $\varphi_{\mathbf{b}}\colon S \to K_s$ uniquely extends to an L-homomorphism $\hat{\varphi}\colon \hat{S} \to K_s$. Let $\hat{b}$ be the unique point of $\hat{W}(K_s)$ with $\omega(\hat{\mathbf{b}}) = \mathbf{b}$ and $\varphi_{\hat{b}} = \hat{\varphi}$. Then let $\mathbf{b}'$ be the unique point of $W'(K_s)$ with $\omega'(\hat{\mathbf{b}}) = \mathbf{b}'$ and $\varphi_{\mathbf{b}'} = \varphi_{\hat{\mathbf{b}}}|_{S'}$. Again, the map $\hat{\mathbf{b}} \mapsto \mathbf{b}'$ is bijective.

CLAIM: $\mathbf{b}' \in W'(K)$ if and only if $\varphi^*_{\mathbf{b}} = \theta$.

First we note that by (2), there exists for each $\sigma \in \mathrm{Gal}(K)$ a unique element $\hat{\theta}(\sigma) \in \Delta = \mathrm{Gal}(\hat{F}/F')$ such that

$$\hat{\theta}(\sigma)|_F = \theta(\sigma) \text{ and } \hat{\theta}(\sigma)|_L = \sigma|_L. \tag{5}$$

Since $\theta(\mathrm{Gal}(K)) = \mathrm{Gal}(F/F')$, this implies that $\hat{\theta}$: $\mathrm{Gal}(K) \to \mathrm{Gal}(\hat{F}/F')$ is an epimorphism with $\mathrm{Ker}(\hat{\theta}) = \mathrm{Gal}(L)$.

Suppose $\mathbf{b}' \in W'(K)$. Then $\hat{\mathbf{b}} \in \hat{W}(L)$, so $\varphi_{\hat{\mathbf{b}}}$ fixes the elements of L. Hence, for each $\sigma \in \mathrm{Gal}(K)$ and $x \in L$ we have $\varphi^*_{\mathbf{b}}(\sigma)x = \varphi_{\hat{\mathbf{b}}}(\varphi^*_{\mathbf{b}}(\sigma)x) = \varphi_{\hat{\mathbf{b}}}(\sigma x) = \sigma x$. Therefore, $\varphi^*_{\hat{\mathbf{b}}}(\sigma)|_L = \sigma|_L = \hat{\theta}(\sigma)|_L$. Also, $\varphi^*_{\hat{b}}(\mathrm{Gal}(K)) \leq \mathrm{Gal}(F/F')$, so that $\varphi^*_{\hat{\mathbf{b}}}(\sigma)x = x = \hat{\theta}(\sigma)x$ for each $x \in F'$. It follows from (1) that $\varphi^*_{\hat{\mathbf{b}}} = \hat{\theta}$. Applying $\mathrm{res}_{\hat{F}/F}$ to the latter equality, we get $\varphi^*_{\mathbf{b}} = \theta$.

Conversely, suppose $\varphi^*_{\mathbf{b}} = \theta$. Then $\mathrm{Ker}(\varphi^*_{\mathbf{b}}) = \mathrm{Ker}(\theta) = \mathrm{Gal}(L)$, so $\mathbf{b} \in W(L)$, hence $\hat{\mathbf{b}} \in \hat{W}(L)$. It follows that for each $\sigma \in \mathrm{Gal}(K)$ we have $\varphi^*_{\hat{b}}(\sigma)|_F = \varphi^*_{\mathbf{b}}(\sigma) = \theta(\sigma) = \hat{\theta}(\sigma)|_F$ and $\varphi^*_{\hat{b}}(\sigma)|_L = \sigma|_L = \hat{\theta}(\sigma)|_L$. By Part A, $\varphi^*_{\hat{b}}(\sigma) = \hat{\theta}(\sigma) \in \mathrm{Gal}(\hat{F}/F')$. Therefore, $\varphi_{\hat{b}}(S') = K$. Consequently, $\mathbf{b}' = \omega'(\hat{\mathbf{b}})$ satisfies $\mathbf{b}' \in W'(K)$. This concludes the proof of the Claim.

PART E: *The orbit of* θ. Following Notation 2.4, the group $\mathrm{Gal}(F/E)$ acts on the set of all homomorphisms from $\mathrm{Gal}(K)$ into $\mathrm{Gal}(F/E)$ by left conjugation. Let $\Theta = \{{}^\tau\theta \mid \tau \in \mathrm{Gal}(F/E)\}$ be the $\mathrm{Gal}(F/E)$-orbit of θ.

For each $\mathbf{a} \in U(K)$ we consider the conjugacy class of homomorphisms $\Phi^*_{\mathbf{a}} = \{\varphi^*_{\mathbf{b}} \mid \mathbf{b} \in W(K_s) \text{ and } \rho(\mathbf{b}) = \mathbf{a}\}$. By Part D

$$\rho'(W'(K)) = \{\mathbf{a} \in U(K) \mid \Phi^*_{\mathbf{a}} = \Theta\}. \tag{6}$$

CLAIM: *A point* $\mathbf{a} \in U(K)$ *satisfies* $\Phi^*_{\mathbf{a}} = \Theta$ *if and only if each root of* $f_i(\mathbf{a}, T)$ *generates* L_i *over* K, $i = 1, \ldots, r$.

First suppose $\Phi^*_{\mathbf{a}} = \Theta$. Then there exists $\mathbf{b} \in W(K_s)$ such that $\rho(\mathbf{b}) = \mathbf{a}$ and $\varphi^*_{\mathbf{b}} = \theta$. Since the discriminant of $f_i(\mathbf{A}, T)$ is a unit of R, $\varphi_{\mathbf{b}}$ maps the set of roots of $f_i(\mathbf{A}, T)$ in F bijectively on the set of roots of $f_i(\mathbf{a}, T)$ in K_s. Let x be a root of $f_i(\mathbf{A}, T)$

in F and let $\sigma \in \mathrm{Gal}(K)$. If $\sigma(\varphi_{\mathbf{b}}(x)) = \varphi_{\mathbf{b}}(x)$, then $\varphi_{\mathbf{b}}(\varphi^*_{\mathbf{b}}(\sigma)x) = \varphi_{\mathbf{b}}(x)$, hence, by the injectivity property of $\varphi_{\mathbf{b}}$, we have $\varphi^*_{\mathbf{b}}(\sigma)x = x$, so $\theta(\sigma)x = x$. By the definition of θ, there exists $\lambda \in \mathrm{Gal}(L_i/K)$ such that $\sigma|_{L_i}\lambda = \lambda$. Therefore, $\sigma \in \mathrm{Gal}(L_i)$. Conversely, if $\sigma \in \mathrm{Gal}(L_i)$, then $\sigma(\varphi_{\mathbf{b}}(x)) = \varphi_{\mathbf{b}}(\varphi^*_{\mathbf{b}}(\sigma)x) = \varphi_{\mathbf{b}}(\theta(\sigma)x) = \varphi_{\mathbf{b}}(\theta_i(\sigma)x) = \varphi_{\mathbf{b}}(x)$. Consequently, $L_i = K(\varphi_{\mathbf{b}}(x))$.

Conversely, suppose for each $1 \leq i \leq r$ there exists a root $\bar{x}_i$ of $f_i(\mathbf{a}, T)$ with $L_i = K(\bar{x}_i)$. Then, by (b) and by the assumption on L_i, $\deg(f_i(\mathbf{a}, T) = d_i = [L_i : K] = [K(\bar{x}_i) : K]$. Hence, $\mathrm{Gal}(L_i/K)$ acts freely on the roots of $f_i(\mathbf{a}, T)$. Choosing $\mathbf{b} \in W(K_s)$ with $\rho(\mathbf{b}) = \mathbf{a}$, this implies that the group $\varphi^*_{\mathbf{b}}(\mathrm{Gal}(K))|_{F_i}$ acts freely on the roots of $f_i(\mathbf{A}, T)$. By definition, this is also the case for the group $\theta(\mathrm{Gal}(K))|_{F_i}$. Since $\mathrm{Gal}(f_i(\mathbf{A}, T), K(\mathbf{A})) = S_{d_i}$, there exists $\tau_i \in \mathrm{Gal}(F_i)$ such that ${}^{\tau_i}(\mathrm{res}_{F/F_i} \circ \theta) = \mathrm{res}_{F_i/F} \circ \varphi^*_{\mathbf{b}}$. Since $\mathrm{Gal}(F/E) = \prod_{i=1}^{r} \mathrm{Gal}(F_i/E)$, there exists $\tau \in \mathrm{Gal}(F/E)$ such that $\tau|_{F_i} = \tau_i$ for $i = 1, \ldots, r$. Hence, ${}^{\tau}\theta = \varphi^*_{\mathbf{b}}$. Therefore, $\Theta = \Phi^*_{\mathbf{a}}$, as claimed.

The first statement of (c) of our Lemma follows now from (6) and from the Claim. The second one follows from the first and from (b).

PART F: *Let $\mathbf{a} \in U(K)$. We prove that $|(\rho')^{-1}(\mathbf{a}) \cap W'(K)| = \frac{[F:E]}{|\Theta|}$.*

The stabilizer $H = \{\tau \in \mathrm{Gal}(F/E) \mid {}^{\tau}\theta = \theta\}$ of θ satisfies

$$|H| = \frac{[F : E]}{|\Theta|} \tag{7}$$

Let $B = \{\mathbf{b} \in \rho^{-1}(\mathbf{a}) \mid \varphi^*_{\mathbf{b}} = \theta\}$. We prove that H acts regularly on B. Indeed, if $\tau \in H$ and $\mathbf{b} \in B$, then by Definition 2.5, $\varphi^*_{\tau\mathbf{b}} = {}^{\tau}(\varphi^*_{\mathbf{b}}) = {}^{\tau}\theta = \theta$, so $\tau\mathbf{b} \in B$. Thus, H acts on B. Next we prove that the action is transitive. To this end let $\mathbf{b}, \mathbf{b}' \in B$. Then there exists $\tau \in \mathrm{Gal}(F/E)$ with $\mathbf{b}' = \tau\mathbf{b}$. Hence, $\theta = \varphi^*_{\mathbf{b}'} = \varphi^*_{\tau\mathbf{b}} = {}^{\tau}(\varphi^*_{\mathbf{b}}) = {}^{\tau}\theta$, so $\tau \in H$, as desired. Finally the action of H is free. Indeed, if $\mathbf{b} \in B$ and $\tau\mathbf{b} = \mathbf{b}$, then by Definition 2.5, $\varphi_{\mathbf{b}} \circ \tau^{-1} = \varphi_{\tau\mathbf{b}} = \varphi_{\mathbf{b}}$. Since $\varphi_{\mathbf{b}}$ is injective on the roots of $h(\mathbf{A}, T)$, this implies that $\tau = 1$, which proves our assertion.

It follows that $|B| = |H|$. As in Part D let B' be the set of all points $\mathbf{b}' \in W'(K_s)$ corresponding to the points $\mathbf{b} \in B$. Since the map $\mathbf{b} \mapsto \mathbf{b}'$ is injective, we have $|B'| = |B| = |H|$. Moreover, by the Claim of Part D, $B' = \rho^{-1}(\mathbf{a}) \cap W'(K)$. Hence, by (7), $|\rho^{-1}(\mathbf{a}) \cap W'(K)| = \frac{[F:E]}{|\Theta|}$, as claimed.

PART G: *We prove:* $|\Theta| = \prod_{i=1}^{r}(d_i - 1)!$.

By (7), $|\Theta| = \frac{|\mathrm{Gal}(F/E)|}{|H|}$. Since $|\mathrm{Gal}(F/E)| = |\prod_{i=1}^{r} S_{d_i}| = \prod_{i=1}^{r} d_i!$, it suffices to prove that $|H| = \prod_{i=1}^{r} d_i$. Since $\mathrm{Gal}(F/E) \cong \prod_{i=1}^{r} \mathrm{Gal}(F_i/E)$ and $\theta = \prod_{i=1}^{r} \theta_i$, we have ${}^{\tau}\theta = \theta$ if and only if ${}^{\tau_i}\theta_i = \theta_i$, where $\tau_i = \tau|_{F_i}$ for $i = 1, \ldots, r$. Hence, it suffices to prove that $\#\{\tau \in \mathrm{Gal}(F_i/E) \mid {}^{\tau}\theta_i = \theta_i\} = d_i$. But this follows from Lemma 2.7.

The combination of Part F and Part G implies Statement (d) of our lemma. ∎

3. Finite Fields and PAC Fields

We combine Corollary 1.3 with Lemma 2.8 to the case when $K = \mathbb{F}_q$ and establish an asymptotic formula for the number of pairs $(a_1, a_2) \in \mathbb{F}_q^2$ such that $f_i(T, a_1T + a_2)$ is irreducible in $\mathbb{F}_q[T]$ when $f_1, \ldots, f_r \in \mathbb{F}_q[T, X]$ are characteristic-0-like nodal non-associate polynomials.

THEOREM 3.1: *Let $f_1, \ldots, f_r \in \mathbb{F}_q[T, X]$ be characteristic-0-like nodal non-associate polynomials, where q is a power of a prime p such that $r = 1$ if $p = 2$. For each $1 \le i \le r$ let $d_i = \deg(f_i(T, X))$ and set $d = \prod_{i=1}^{r} d_i$. Then,*

$$\#\{(a_1, a_2) \in \mathbb{F}_q^2 \mid f_i(T, a_1T + a_2) \text{ is irreducible in } \mathbb{F}_q[T],\ i = 1, \ldots, r\} = \frac{q^2}{d} + O(q^{3/2}),$$

where the constant of the O is a computable function in $\sum_{i=1}^{r} \deg(f_i(T, X))$.

Proof: Let $K = \mathbb{F}_q$ and let A_1, A_2 be additional variables. For each $1 \le i \le r$ let $f_i'(A_1, A_2, T) = f_i(T, A_1T + A_2)$, let F_i be the the splitting field of $f_i'(A_1, A_2, T)$ over $E = K(A_1, A_2)$, and let $F = F_1 \cdots F_r$. By Corollary 1.3, $\mathrm{Gal}(F/E) = \prod_{i=1}^{r} S_{d_i}$. For each $1 \le i \le r$ let $L_i = \mathbb{F}_{q^{d_i}}$ be the unique Galois extension of $\mathbb{F}_q$ of degree d_i and note that $d_i = \deg_T(f_i'(A_1, A_2, T))$.

Let $m = \sum_{i=1}^{r} \deg(f_i'(A_1, A_2, T)) = \sum_{i=1}^{r} \deg(f_i(T, X))$ and consider the objects V, $U = \mathbb{A}_K^2 \setminus V$, and $\rho'\colon W' \to U$ supplied by Lemma 2.8 with respect to $K = \mathbb{F}_q$, to $f_1', \ldots, f_r'$, and to $L_1, \ldots, L_r$. In particular, V is a Zariski closed subset of $\mathbb{A}_K^2$ defined by a nonzero polynomial of an m-bounded degree. Thus, there exists an m-bounded constant c_1 such that

$$\#V(K) \le c_1 q. \tag{1}$$

Moreover, W' is an absolutely irreducible affine K-subvariety of $\mathbb{A}^5_K$ defined by polynomials of m-bounded degrees. In addition, $\dim(W') = 2$, because $\rho'\colon W' \to U$ is a finite morphism. The Lang-Weil estimates give an explicit m-bounded constant c_2 such that

$$|\#W'(K) - q^2| \le c_2 q^{\frac{3}{2}}. \tag{2}$$

(See [LaW54, Thm. 1], [FHJ94, (1) and (2) of Section 3], or [Zyw10, Thm. 2.1]. Note that the estimates given in [Zyw10] are exponential in the degrees of the polynomials that define W'.)

Let I be the set of all $(a_1, a_2) \in \mathbb{F}_q^2$ such that $f_i(T, a_1T + a_2)$ is irreducible in $\mathbb{F}_q[T]$ for $i = 1, \ldots, r$. By Lemma 2.8(c), $\rho'(W'(K))$ is the set of all $(a_1, a_2) \in U(K)$ such that for each $1 \le i \le r$ the field L_i is generated over K by a root of $f_i(T, a_1T + a_2)$. Moreover, by Lemma 2.8(b), $\deg(f_i(T, a_1T + a_2)) = d_i$ for $i = 1, \ldots, r$. Since L_i is the unique extension of K of degree d_i, this implies that $\rho'(W'(K)) = I \cap U(K)$, so $|\rho(W'(K))| = d \cdot |(I \cap U(K))|$.

By Lemma 2.8(d), $|(\rho')^{-1}(\mathbf{a}) \cap W'(K)| = d$ for each $\mathbf{a} \in \rho(W'(K))$. Hence, by (2), $|\#(I \cap U(K)) - \frac{q^2}{d}| \le \frac{c_2}{d} q^{\frac{3}{2}}$. It follows from (1) that $|\#I - \frac{q^2}{d}| \le \frac{c_2}{d} q^{\frac{3}{2}} + c_1 q$, as desired. ∎

Almost the same proof can be applied to PAC fields.

THEOREM 3.2: *Let K be a PAC field and let $f_1, \ldots, f_r \in K[T, X]$ be characteristic-0-like nodal polynomials. Suppose for each i the field K has a Galois extension L_i of degree $\deg(f_i(T, X))$. Then $\mathbb{A}^2_K$ has a Zariski-dense subset B such that $f_i(T, a_1T + a_2)$ is irreducible for $i = 1, \ldots, r$.*

Proof: if one of two associated polynomial is irreducible, so is the other. Thus, after possible dropping some of the f_i's, we may assume that $f_1, \ldots, f_r$ are non-associate. Let A_1, A_2 be additional variable and set $E = K(A_1, A_2)$. For each $1 \le i \le r$ let $f_i'(A_1, A_2, T) = f_i(T, A_1T + A_2)$, let F_i be the splitting field of $f_i'(A_1, A_2, T)$ over $E = K(A_1, A_2)$ and set $F = F_1 \cdots F_r$. By Corollary 1.3, $\mathrm{Gal}(F/E) = \prod_{i=1}^r S_{d_i}$ and note that $d_i = \deg_T(f_i'(A_1, A_2, T))$.

Consider the objects U and $\rho'\colon W' \to U$ supplied by Lemma 2.8 with respect to $f_i', \ldots, f_r'$. Since K is PAC and W' is an absolutely irreducible K-variety, the set

$W'(K)$ is non-empty, so there exists $\mathbf{a} \in \rho'(W'(K))$. By Lemma 2.8, $f_i(T, a_1T + a_2)$ is irreducible for each $1 \leq i \leq r$. ∎

4. Concluding Remarks

The following proposition proves that Theorem 1.1 of [BeW05] is a special case of our main result.

PROPOSITION 4.1: *Let K be a field of characteristic p and $f \in K[T, X]$ an irreducible polynomial of degree d such that*

(1a) *$p \nmid d(d-1)$, and*

(1b) *the Zariski closure $\Gamma_{\tilde{K}}$ in $\mathbb{P}^2_{\tilde{K}}$ of the affine plane curve defined by $f(T, X) = 0$ is smooth.*

Then Γ is characteristic-0-like and nodal.

Proof: By assumption, Γ is irreducible and by (1b), Γ is absolutely irreducible. In the proof of [BeW05, Prop. 3.1], Bender and Wittenberg show for $K = \mathbb{F}_q$ that assumption (1) implies that the map of $\Gamma_{\tilde{K}}$ into its dual curve is separable. The proof is however valid for every field K. It follows from [Kat73, Cor. 3.5.0 and Cor. 3.2.1] that the intersection multiplicities of all but finitely many lines L in $\mathbb{P}^2_{\tilde{K}}$ with Γ are at most 2. In particular, for only finitely many points $\mathbf{p} \in \Gamma_{\tilde{K}}$, the intersection number of the tangent to Γ at $\mathbf{p}$ is greater than 2. This means that Γ has only finitely many inflection points.

By (1a), $p \neq 2$. Hence, by [GeJ89, Prop. 4.5], $\Gamma_{\tilde{K}}$ has only finitely many double tangents. Again, by (1a), $\Gamma_{\tilde{K}}$ is not a line and not a conic in characteristic 2. Hence, by Samuel [Har77, Thm. IV.3.9], $\Gamma_{\tilde{K}}$ is not strange. Finally, $\Gamma_{\tilde{K}}$ is nodal because it is smooth. Consequently, Γ is characteristic-0-like and nodal. ∎

One of the ingredients of the proof of Lemma 1.1 (on which eventually our proof of Theorem 3.1 in case $r \geq 2$ relies) is that the dual curves of distinct absolutely irreducible projective plane K-curves are distinct, if $\mathrm{char}(K) \neq 2$. The following example shows that this is not the case if $\mathrm{char}(K) = 2$. Thus, our proof of Theorem 3.1 fails if $\mathrm{char}(K) = 2$ and $r \geq 2$. We do not know if the theorem itself holds in that case.

Example 4.2 (Bjorn Poonen): Let K be an algebraically closed field of characteristic 2. We consider the homogeneous polynomial

$$f(X_0, X_1, X_2) = X_1^5 + X_1^2 X_0^3 + X_0^4 X_2$$

and the projective plane curve Γ defined by the equation $f(X_0, X_1, X_2) = 0$. The finite part of Γ is defined by the equation $X^5 + X^2 = Y$. This may be used to prove that Γ is absolutely irreducible. Moreover, Γ has only finitely many inflection points (e.g. $(0, 0)$ is a simple non-inflection point, now use [GeJ89, Cor. 3.2]), only finitely many double tangents (see next paragraph), and Γ is not strange (the latter assertion is also a special case of a theorem of Samuel [Har77, Thm. IV.3.9]).

Let $(x_0{:}x_1{:}x_2)$ be a generic homogeneous point of Γ. Applying (1) of Section 1, we find that $(x_0^*{:}x_1^*{:}x_2^*) = (x_0^2 x_1^2 : x_1^4 : x_0^4)$ is a generic point of Γ^*. In particular the map $\Gamma \to \Gamma^*$ is purely inseparable, so Γ has only finitely many double tangents [GeJ89, Lemma 4.2]. The point $(x_0^*{:}x_1^*{:}x_2^*)$ lies on the irreducible homogeneous plane curve defined by the equation $X_1 X_2 = X_0^2$. Hence, the latter equation defines Γ^*.

Next we define an additional projective pland curve Δ by exchanging the variables X_1 and X_2. In other words, the equation that defines Δ is $X_2^5 + X_2^2 X_0^3 + X_0^4 X_1 = 0$. The equation that defines Δ^* will therefore be $X_2 X_1 = X_0^2$. It follows that $\Gamma^* = \Delta^*$ although $\Gamma \neq \Delta$. ∎

References

[BaH62] P. T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers,* Mathematics of Computation **16** (1962), 363–367.

[BaS10] L. Bary-Soroker, *Irreducible values of polynomials,* manuscript 2010.

[BaD04] P. T. Bateman and H. G. Diamond, *Analytic Number Theory - An Introductory Course,* World Scientific Publishing Co., Denver 2004

[BeW05] A. O. Bender and O. Wittenberg *A Potential analogue of Schinzel's hypothesis for polynomials with coefficients in* $\mathbb{F}_q[t]$, International Mathematics Research Notices **36** (2005), 2238–2248.

[CCG08] B. Conrad, K. Conrad, and R. Gross, Prime specialization in genus 0, Transactions of the AMS **360** (2008), 2867-2908.

[Deb99] P. Dèbes, *Galois Covers with Prescribed Fibers: The Beckmann-Black Problem,* Annale Scuola Normale Superiore Pisa **28** (1999), 273–286.

[FHJ94] M. Fried, D. Haran, M. Jarden, *Effective counting of the points of definable sets over finite fields,* Israel Journal of Mathematics **85** (1994), 103–133.

[FrJ76] M. Fried and M. Jarden, *Diophantine properties of subfields of* $\tilde{\mathbb{Q}}$, American Journal of Mathematics **100** (1978), 653–666.

[FrJ08] M. D. Fried and M. Jarden, *Field Arithmetic, Third Edition, revised by Moshe Jarden,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2008.

[Gau03] S. Gao, *Problem 6, AIM Workshop on "Future Directions in Algorithmic Number Theory,"* American Institute of Mathematics, California, 2003, http://www.aimath.org/ARCC/workshops/primesinp.html

[GeJ89] W.-D. Geyer and M. Jarden, *On stable fields in positive characteristic,* Geometriae Dedicata **29** (1989), 335–375.

[Ful89] W. Fulton, *Algebraic Curves,* Addison Weseley, Redwood City, 1989.

[Har77] R. Hartshorne, *Algebraic Geometry,* Graduate Texts in Mathematics **52**, Springer, New York, 1977.

[Kat73] N. Katz, *Pinceaux de Lefschetz: théorème d'existence, Groups de monodromies en Géométrie Algébrique II,* Springer Lecture Notes in Mathematics **340** (1973), 212-353.

[Lan93] S. Lang, *Algebra, Third Edition,* Eddison-Wesley, Reading, 1993.

[LaW54] S. Lang and A. Weil, *Number of points of varieties in finite fields,* American Journal of Mathematics **76** (1954), 819–827.

[Pol08] P. Pollack, *Simultaneous prime specializations of polynomials over finite fields,* Proceedings of the London Mathematical Society **97** (2008), 545–567.

[Ray70] M. Raynaud, *Anneaux Locaux Henséliens,* Lecture Notes in Mathematics **169**, Springer, Berlin, 1970.

[Swa62] R. G. Swan, *Factorization of polynomials over finite fields,* Pacific Journal of Mathematics **12** (1962), 1099–1106.