IRREDUCIBLE VALUES OF POLYNOMIALS

LIOR BARY-SOROKER

ABSTRACT. Schinzel’s Hypothesis H is a general conjecture in number theory on prime values of polynomials that generalizes, e.g., the twin prime conjecture and Dirichlet’s theorem on primes in arithmetic progression. We prove an arithmetic analog of this conjecture for polynomial rings over pseudo algebraically closed fields. This implies results over large finite fields. A main tool in the proof is an irreducibility theorems à la Hilbert.

1. Introduction

A necessary condition for a finite family of irreducible polynomials $f_1(X), \ldots, f_r(X) \in \mathbb{Z}[X]$ with positive leading coefficients to admit infinitely many simultaneous prime values in $\mathbb{Z}$ is that there are no local obstructions, i.e., the function $x \mapsto f_1(x) \cdots f_r(x) \mod p$ is not the zero function, for all primes $p \in \mathbb{Z}$. Schinzel’s Hypothesis H predicts that this condition is also necessary. Special cases of this conjecture are Dirichlet’s theorem on primes in arithmetic progressions (taking $f_1 = aX + b$) and the twin prime conjecture (taking $f_1 = X - 1$ and $f_2 = X + 1$). Dirichlet’s theorem is the only proven case of the conjecture, sieve methods are used to obtain near-misses of the conjecture (e.g., Brun’s sieve and Chen’s theorem).

The analogy between the rings $\mathbb{Z}$ and $\mathbb{F}_q[t]$, where $\mathbb{F}_q$ is the field of $q$ elements, suggests a naïve Hypothesis H analog for the ring $\mathbb{F}_q[t]$; for every finite family of irreducible polynomials $f_1(t, X), \ldots, f_r(t, X) \in \mathbb{F}_q[t, X]$ having no local obstructions there exist infinitely many simultaneous prime values in $\mathbb{F}_q[t]$. It is quite surprising that this conjecture fails, e.g., all the values of $X^8 + t^3$ in $\mathbb{F}_2[t]$ are composite [?]. In [?] Conrad, Conrad, and Gross study global obstructions coming from values of the Möbius function.

Nevertheless there are some general results for large finite fields. In [?] Bender and Wittenberg find linear irreducible substitutions under the assumption that the Zariski closure of each of the plane curves $f_i(T, X)$ in $\mathbb{P}^2$ is smooth, a technical assumption on the characteristic (in particular the characteristic is odd) and of course, that the cardinality of the field is sufficiently large comparable to the degrees of the polynomials.

In [?] Pollack proves an arithmetic type result.

**Theorem 1.1** (Pollack). Let $n, B$ be positive integers, $p$ a prime such that $p \nmid 2n$, $q$ a power of $p$, $f_1(X), \ldots, f_r(X) \in \mathbb{F}_q[X]$ non-associate irreducible polynomials such that $\sum \deg(f_i) \leq B$. Then the number of degree $n$ monic $g(t) = t^n + \cdots \in \mathbb{F}_q[t]$ for which all of the $f_i(g(t))$ are irreducible in $\mathbb{F}_q[t]$ is

$$q^n - O_{n, B}(q^{n-\frac{3}{2}}).$$

The asserted constant in Pollack’s theorem is of order of magnitude $(n!)^B$, hence the asymptotic is useless when $n \to \infty$, but it works when $n$ is fixed and $q \to \infty$. A conjectural formula for $q^n \to \infty$ is given in [?], there the main term depends on local data.

In this work we prove an arithmetic type theorem for PAC fields satisfying an obvious necessary condition. A field $K$ is called PAC (short for pseudo algebraically closed field) if $V(K) \neq \emptyset$, for every absolutely irreducible non-void $K$-variety $V$. For example, Pop shows that the field $\mathbb{Q}[\sqrt{-1}]$ we get by taking all totally real numbers and $\sqrt{-1}$ is PAC. Let $\sigma_1, \ldots, \sigma_e \in \text{Gal}(\mathbb{Q})$ and let $\mathbb{Q}(\sigma_1, \ldots, \sigma_e)$ be the field fixed by all $\sigma_1, \ldots, \sigma_e$. Then Jarden proves that the probability that $\mathbb{Q}(\sigma_1, \ldots, \sigma_e)$ is PAC is 1, w.r.t. the probability Haar measure of the profinite, hence compact,
group $\text{Gal}(\mathbb{Q})$. (Here $\mathbb{Q}$ is the field of all algebraic numbers, and $\text{Gal}(\mathbb{Q}) = \text{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q})$ is the absolute Galois group of $\mathbb{Q}$.)

**Theorem 1.2.** Let $K$ be a PAC field of characteristic $p \geq 0$, let $f_1, \ldots , f_r \in K[X]$ be non-associate irreducible separable polynomials with respective roots $\omega_1, \ldots , \omega_r$, and let $n$ be a positive integer, odd if $p = 2$. Suppose that

\begin{itemize}
  \item (*) $K(\omega_i)$ has a separable extension of degree $n$, for $i = 1, \ldots , r$.
\end{itemize}

Then there exists a Zariski dense set of $(a_1, \ldots , a_n) \in K^n$ such that, for $g(t) = t^n + a_1 t^{n-1} + \cdots + a_n$, all of the $f_i(g(t))$ are separable and irreducible in $K[t]$.

Note that (\textit{\textbf{a}}) is necessary. Indeed, assume $f_i(g(t))$ to be separable and irreducible. Choose a root $\eta_i$ of $g(t) - \omega_i$. Then $f_i(g(\eta_i)) = f_i(\omega_i) = 0$, hence $\eta_i$ is a root of $f_i(g(t))$. Moreover $K(\omega_i) \subseteq K(\eta_i)$ and

$$\deg(f_i \circ g) = [K(\eta_i) : K] = [K(\eta_i) : K(\omega_i)][K(\omega_i) : K] \leq n \cdot \deg(f_i) = \deg(f_i \circ g),$$

so $[K(\eta_i) : K] = n \cdot \deg f$ and $[K(\eta_i) : K(\omega_i)] = \deg(g(t)) = n$, as needed.

Theorem 1.2 is more than an analog of Theorem 1.1, it actually implies it, as explained below. Moreover, Theorem 1.2 contains the ‘wild’ case in odd characteristic, i.e., when $2 \nmid p \mid n$, and the ‘tame’ case is characteristic 2, i.e., when $p = 2$ and $n$ is odd. Therefore it strengthens Theorem 1.1 to these important cases.

A pseudo finite field $K$ is defined to be a perfect PAC field with $\text{Gal}(K) \cong \tilde{\mathbb{Z}}$. The latter condition implies in particular (\textit{\textbf{a}}) for any $\omega_i$. So we get the following

**Corollary 1.3.** Let $n, B > 0$ be fixed. Then any pseudo finite field $K$ of characteristic $p \geq 0$ satisfies the following elementary statement. For every irreducible polynomials $f_1(X), \ldots , f_r(X) \in K[X]$ satisfying $\sum \deg(f_i) \leq B$ there exists a Zariski dense set of $(a_1, \ldots , a_n) \in K^n$ such that, for $g(t) = t^n + a_1 t^{n-1} + \cdots + a_n$, all of the $f_i(g)$ are irreducible, provided $n$ is odd if $p = 2$.

In [?], Ax proves that an elementary statement is true for almost all finite fields if and only if it is true for all pseudo finite fields (see also [?], [20.10]). Therefore, an immediate consequence is that Corollary 1.3 implies Theorem 1.1 in a weak sense, namely, it gives existence of $g$’s, but not the mentioned asymptotic. But in fact, while proving the theorem, a more technical statement is proved, from it Theorem 1.1 follows in its full strength using the Lang-Weil estimates, including the case $p = 2$ and $n$ is odd, and the case $2 \nmid p \mid n$.

**Theorem 1.4.** Let $n, B$ be positive integers, $p$ a prime, $q$ a power of $p$, $f_1(X), \ldots , f_r(X) \in \mathbb{F}_q[X]$ non-associate irreducible polynomials such that $\sum \deg(f_i) \leq B$. Assume $n$ is odd if $p = 2$. Then the number of degree $n$ monic $g(t) \in \mathbb{F}_q[t]$ for which all of the $f_i(g(t))$ are irreducible in $\mathbb{F}_q[t]$ is

$$\frac{q^n}{n^r} + O_{n,B}(q^{n-\frac{1}{2}}).$$

An interesting special case is when $f_i = X^2 + 1$:

**Corollary 1.5.** Assume $q \gg r, n$ and that $n$ is odd if $q$ is even. Then there exists a monic polynomial $g(t) \in \mathbb{F}_q[t]$ of degree $n$ such that $g, g+1, \ldots , g+r-1$ are irreducible.

When $r = 1$, Pollack proves a result over small finite fields: Over a finite field $\mathbb{F}_q$ there are infinitely many $g$ such that $g, g+1$ are irreducible [?, Theorem 4].

Another interesting case is $f_i = X^2 + 1$, which can be considered as an analog of Landau’s problem. Recall that $X^2 + 1$ is irreducible in $\mathbb{F}_q$ if and only if $q \equiv 1 \mod 4$.

**Corollary 1.6.** Assume $q \gg n$ and that $n$ is odd if $q$ is even. Then there exists a monic polynomial $g(t) \in \mathbb{F}_q[t]$ of degree $n$ such that $g(t)^2 + 1$ is irreducible.

A natural way to try to prove Theorem 1.2 is the following. (For simplicity assume $r = 1$ and $f = f_1$.) Let $G(A(t)) = t^n + A_1 t^{n-1} + A_2 t^{n-2} + \cdots + A_n$ be a generic polynomial, i.e., $A = (A_1, \ldots , A_n)$ is an $n$-tuple of algebraically independent variables. Consider the polynomial $F(A, t) = f(G(A, t))$. It is easy to show that this polynomial is irreducible. So the proof reduces to the following question: Can we specialize $A \mapsto a \in K^n$ so that irreducibility is preserved?
If $K$ is a number field (more generally, Hilbertian field), then Hilbert’s irreducibility theorem gives the desired irreducible specialization. On the other contrast, if $K$ is algebraically closed, it is obvious that no irreducible specialization exists, if the $t$-degree of $F$ is greater than 1.

We prove here a weak Hilbert’s irreducibility theorem for PAC fields, that gives a necessary and sufficient condition for a polynomial over a PAC field to have a Zariski dense set of irreducible specializations (in fact we prove a more general result, see Theorem 2.4). The condition is given in terms of embedding problems.

In order to apply the weak Hilbert’s irreducibility theorem in our situation we have to calculate the Galois group of $F(A,t)$. We show that for a positive integer $n$, odd if $p = 2$, we have

$$\operatorname{Gal}(F, K(A)) \cong S_n \wr_{t \Omega} \operatorname{Gal}(f, K).$$

Here $\Omega$ is the set of roots of $f$, $\operatorname{Gal}(f, K)$ acts on $\Omega$ in a natural way, and $S_n \wr_{t \Omega} \operatorname{Gal}(f, K)$ is the permutational wreath product. It is a little bit technical to show that this calculation is equivalent to the following result, which may be of interest by itself:

**Proposition 1.7.** Let $\tilde{K}$ be an algebraically closed field of characteristic $p \geq 0$, let $n$ be a positive integer, odd if $p = 2$, let $\Omega \subseteq \tilde{K}$ be a finite set, let $G(A,t) = t^n + A_1 t^{n-1} + A_2 t^{n-2} + \cdots + A_n$ be a generic polynomial. Then the splitting fields $F_\omega$ of $G - \omega$, $\omega \in \Omega$ are linearly disjoint over $\tilde{K}(A)$ and

$$\operatorname{Gal}\left( \prod_{\omega \in \Omega} (G - \omega) \right) \cong S_n^\Omega.$$

It surprised the author to find out that these results fails when $p = n = 2$. In this case the assertion holds true if and only if $\sum_{i=1}^{2\ell} \omega_i \neq 0$ for every even number of distinct elements $\omega_1, \ldots, \omega_{2\ell} \in \Omega$. If $n = 2k > 2$, we suspect this result to fail, but we do not know to prove it, or to give an exact condition for it to hold, as we had for $n = 2$. From this it follows that Theorem 1.2 and hence Theorem 1.3 holds true when $p = n = 2$.

We conclude the introduction with a remark. It is interesting to consider Schinzel’s Hypothesis H for polynomial rings over other fields. This can be done for fields having a PAC extension that satisfies (\textit{a}). Examples of such interesting families of fields can be found in [\textit{a}, ?]. This will be dealt somewhere else.

**Acknowledgments.** I thanks Moshe Jarden for pointing out several mistakes in an earlier version, for many remarks and suggestions that contributed to the presentation of paper, Peter Müller for letting me know about Pollack’s work, and Wulf-Dieter Geyer, Dan Haran, Ehud Hrushovski, Christian Kappen, Zeev Rudnick, and Tomer Schlank for helpful discussions.

Part of this work was done while the author was a Lady Davis postdoc fellow in the Hebrew University of Jerusalem. The author is an Alexander von Humboldt postdoc fellow in The Instituts für Experimentelle Mathematik in Duisburg-Essen University. This research is partially supported by a grant from the ERC.

2. Weak Hilbert’s irreducibility theorem

2.1. Geometric embedding problems. Let $K$ be a field, $V,W$ irreducible smooth affine $K$-varieties, and $\rho: W \to V$ a finite separable morphism. Let $R,S$ be the respective rings of regular functions of $V,W$, consider $R$ as a subring of $S$, and let $F/E$ be the corresponding function field extension.

Assume that $V$ is absolutely irreducible and that $F/E$ is Galois. Then the field of constants of $V$ is $K$ and the field of constants $L = F \cap \tilde{K}$ of $W$ is Galois over $K$. (Here $\tilde{K}$ is a fixed algebraic closure of $K$.) We have the restriction of automorphisms map $\alpha: \operatorname{Gal}(F/E) \to \operatorname{Gal}(L/K)$. This data defines an embedding problem for $K$ that we call a geometric embedding problem:

$$\mathcal{E}(W/V) := \begin{array}{ccc}
\operatorname{Gal}(K) \\
\Rightarrow \\
\pi \\
\alpha \\
\downarrow \\
\operatorname{Gal}(L/K).
\end{array}$$
We note that a geometric embedding problem is a birational object, hence it depends only on the function field extension $F/E$. Therefore it coincides with the geometric embedding problem as defined in [?] in terms of function fields. In this work it is more natural to work with varieties since we are interested in irreducible specialization of polynomials.

A weak solution of $\mathcal{E}(W/V)$ is a homomorphism $\theta : \text{Gal}(K) \rightarrow \text{Gal}(F/E)$ in the category of profinite groups, i.e. continuous. A weak solution is proper if it is surjective. In this paper we will mainly have weak solutions, hence we decided to abbreviate the term ‘weak solution’ and write in short ‘solution’.

Rational points on $V$ induce solutions in the following way. Let $p \in V(K)$ be a $K$-rational point of $V$ that is étale in $W$ and let $\mathfrak{P} \in \rho^{-1}(p)$. By abuse of notation we also denote by $\mathfrak{P}$ the corresponding maximal ideal of the local ring $R_p$ at $p$, and we use similar notation for $\mathfrak{P}$. Then we have a homomorphism $\mathfrak{P}^* : \text{Gal}(K) \rightarrow \text{Gal}(F/E)$ defined by

\[
\mathfrak{P}^*(\sigma)(x) \mod \mathfrak{P} = \sigma(x \mod \mathfrak{P}), \quad \text{for all } x \in S_{\mathfrak{P}}.
\]

The map $x \mapsto x \mod \mathfrak{P}$ bijectively maps $L \subseteq S$ to $L \subseteq S_{\mathfrak{P}}/\mathfrak{P}$, hence for $x \in L$ we have $\mathfrak{P}^*(\sigma)(x) = \sigma(x)$, so $\pi = \alpha \circ \mathfrak{P}^*$. In other words, $\mathfrak{P}^*$ is a solution of the embedding problem $\mathcal{E}(W/V)$. This solution is continuous since it factors through $\text{Gal}(K(\mathfrak{P})/K)$, where $K(\mathfrak{P}) = S_{\mathfrak{P}}/\mathfrak{P}$ is the residue field at $\mathfrak{P}$. A solution that equals $\mathfrak{P}^*$ for some $\mathfrak{P}$ as above is said to be geometric.

The question whether a given solution is geometric is difficult, and can be considered as a finite version of Grothendieck’s section conjecture.

We note that if $\Phi$ is a place of $F$ that extends the map $S \rightarrow S/\mathfrak{P}$ and such that the residue field of $E$ is $K$, then the geometric solution $\Phi^*$ that is defined in [?] coincides with $\mathfrak{P}^*$, since both are defined by the same formula. Therefore, here we present a different formulation of the same notion.

If $\Omega \in \rho^{-1}(p)$, then there exists $\tau \in \text{Gal}(F/EL) = \ker \alpha$ such that $\Omega = \tau \mathfrak{P}$. We thus get by [1] that $\Omega^* = \tau \mathfrak{P}^* \tau^{-1}$. Vice-versa, every $\tau \mathfrak{P}^* \tau^{-1}$ comes from $\Omega \in \rho^{-1}(p)$. Therefore it makes sense to define $p^*$ to be the ker $\alpha$-inner-automorphism class $\{\mathfrak{P}^* | \mathfrak{P} \in \rho^{-1}(p)\}$. We call this class the Artin class of geometric solutions, this name is derived from the special case where $K$ is finite.

Assume that $K$ is a finite field consisting of $q$ elements. Then the absolute Galois group of $K$ is generated by a distinguish element, namely the Frobenius automorphism $\text{Frob} : x \mapsto x^q$. For each étale $\mathfrak{P} \in \rho^{-1}(p)$ we set $[W/V, \mathfrak{P}/p] = \mathfrak{P}^*(\text{Frob})$ and call $[W/V, \mathfrak{P}/p]$ the Frobenius element at $\mathfrak{P}$. Then we define the Artin symbol $(W/V, p)$ as the conjugacy class of all Frobenius elements of $\mathfrak{P} \in \rho^{-1}(p)$. Then the map $\mathfrak{P}^* \mapsto (W/V, p)$ is a bijection, when the base field is finite.

Next we describe special kind of geometric embedding problems that are associated to polynomials. Let $V$ be a polynomial of degree $n$ defined over $E$. In general the roots are not defined over $E$, but we can define them by taking $E^n$ is the splitting field of $f$. For each $a G(f)$ we set $V_a = \text{Spec}(S)$, where $S$ is the integral closure of $R$ in $F$. Let $\rho : V_f \rightarrow V$ be the corresponding map. Then $\rho$ is a finite separable morphism and $F/E$ is Galois. We call $\mathcal{E}(f,V) := \mathcal{E}(V_f/V)$ the geometric embedding problem associated to $f$. Note that the Galois group $\text{Gal}(F/K(V))$ naturally acts on $\Omega$, so there is a degree $n := \deg f$ group.

A rational point, $p \in V(K)$, is étale in $V_f$ if and only if the discriminant of $f$ is invertible at $p$ [?, Corollary 3.16]. Hence if and only if $f \mod p$ is a separable polynomial.

2.2. Factorizations of polynomials under a specialization map. The orbit type of a solution $\theta : \text{Gal}(K) \rightarrow \text{Gal}(F/E)$ of $\mathcal{E}(f,V)$ is the partition of $n$ defined by the length of the $\theta(\text{Gal}(K))$-orbits of the roots of $f$. If there is only one orbit, we say that the solution is transitive. Since the orbit type is invariant under inner-automorphisms, it makes sense to define the orbit type of a class of ker $\alpha$-inner-automorphisms of solutions to be the orbit type of one solution in the class.

The factorization type of a separable polynomial of degree $n$ is the partition of $n$ defined by the degrees of its irreducible factors. A basic fact in Galois theory is that the factorization type of a separable polynomial equals the orbit type of its Galois group.
The next lemma connects the factorization type of a specialized polynomial with the orbit type of the image of a geometric solution of the associated embedding problem.

**Lemma 2.1.** Let \( V = \text{Spec}(R) \) be an absolutely irreducible smooth affine \( K \)-variety, let \( f(X) \in R[X] \) be a monic separable polynomial, and let \( p \in V(K) \) be étale in \( V_f \). Then the factorization type of \( f \mod p \) equals the orbit type of \( p^* \).

In particular, \( f \mod p \) is irreducible if and only if \( p^* \) is transitive.

**Proof.** Choose some \( \mathfrak{P} \in \rho^{-1}(p) \). Since \( p \) is étale in \( V_f \), the discriminant of \( f \) is invertible at \( p \), so the map \( S_p \to S_p/\mathfrak{P} \) induces a bijection between the roots of \( f \) and the roots of \( f \mod p \). By [1], the action of \( \text{Gal}(K) \) on the roots of \( f \mod p \) coincides with the action of \( \mathfrak{P}^*(\text{Gal}(K)) \) on the roots of \( f \). Hence the assertion. \( \square \)

In the following result given a geometric embedding problem \( \mathcal{E}(W/V) \) and a solution \( \theta \) we give a form \( \hat{W} \) of \( W \) with a correspondence between rational points on \( \hat{W} \) and points on \( W \) inducing \( \theta \).

**Proposition 2.2.** Consider a geometric embedding problem \( \mathcal{E}(W/V) \) as defined at the beginning of this section. Let \( \theta : \text{Gal}(K) \to \text{Gal}(F/E) \) be a solution of \( \mathcal{E}(W/V) \) and let \( M = K_{\ker \theta} \) be the solution field. Then

(a) \( W \times_K M \) factors to a disjoint union of absolutely irreducible components, let \( W_M \) denote one of them.

(b) There exists an absolutely irreducible smooth variety \( \hat{W} \) with a diagram of finite separable morphisms

\[
\begin{align*}
W \ar{p}{
\hat{W} \ar{\pi}{\hat{W} \times_K M} \ar{\rho}{V} \ar{\nu}{W_M}
}
\end{align*}
\]

such that \( \deg \pi = |\ker \alpha|, \nu \) is an isomorphism, and for any \( \Omega \in W_M(\hat{K}) \) the following holds:

\[
\mathfrak{P}^* = \theta, \text{ for } \mathfrak{P} = p(\nu(\Omega)) \text{ if and only if } \hat{\mathfrak{P}} \in \hat{W}(K), \text{ for } \hat{\mathfrak{P}} = \hat{p}(\nu(\Omega)),
\]

provided \( \hat{\mathfrak{P}} \) is étale over \( V \) (equivalently, \( \Omega \) étale over \( V \)).

(c) Let \( \Theta \) be the \( \ker \alpha \)-inner-automorphism class of \( \theta \), and let \( U \subseteq V(K) \) be the set of all \( p \in V(K) \) that are étale in \( W \) and \( p^* = \Theta \). Then \( \pi(W(K)) = U \) and, for every \( p \in U \),

\[
|\pi^{-1}(p) \cap \hat{W}(K)| = \frac{|\ker \alpha|}{|\Theta|}.
\]

**Proof.** The kernel \( \text{Gal}(M) \) of \( \theta \) contains the kernel \( \text{Gal}(L) \) of \( \alpha \), so \( L \subseteq M \). Therefore \( W \times_K M \) factors to absolutely irreducible components. These components are disjoint because \( W \) is smooth and isomorphic because the function field extension \( F/E \) of \( W \to V \) is Galois. Since \( W \times_K M = \text{Spec}(S \otimes_K M) \) and \( SM \) is regular over \( M \), the canonical map \( S \otimes_K M \to SM \) defined by \( s \otimes m \mapsto sm \) defines an embedding of the absolutely irreducible smooth variety \( W_M = \text{Spec}(SM) \) into \( W \otimes_K M \).

So \( \iota(W_M) \) is an absolutely irreducible factor of \( W \otimes_K M \).

We prove [1] using [?, Proposition 3.2], where the assertion is proved in the language of function fields: Let \( \bar{F} = FM \). In the proof of [?, Proposition 3.2] a separable extension \( \bar{E} \subseteq \bar{F} \) of \( E \) is constructed with the following properties:

(1) \( \bar{E} \) is regular over \( K \).
(2) \( \text{Gal}(\bar{F}/E) \cong G \times_G \bar{H} \), where \( G = \text{Gal}(F/E), \bar{G} = \text{Gal}(L/K), \) and \( H = \text{Gal}(EM/E) \cong \text{Gal}(M/K) \cong \theta(\text{Gal}(K)). \) So \( \theta \) induces an embedding \( \theta : H \to G \).
(3) \( \text{Gal}(\bar{F}/\bar{E}) \cong \Delta = \{(\bar{\theta}(h), h) \mid h \in H\} \).
(4) A \( K \)-rational place \( \varphi \) of \( E \) extends to a place of \( \Phi \) of \( F \) with \( \Phi^* = \theta \) if and only if \( \varphi \) extends to a \( K \)-rational place \( \hat{\Phi} \) of \( \bar{E} \). In fact, something slightly stronger appears in the proof:
(5) For a place \( \Psi \) of \( FM \) that is trivial on \( M \) we have \( \Phi^* = \theta \), for \( \Phi = \Psi|_F \), if and only if, \( \hat{\Phi} = \Psi|_{\bar{E}} \) is \( K \)-rational.
From (2) and (3) we have
\[ (6) \quad \hat{E} : E = \frac{|G \times \hat{G} H|}{|\Delta|} = \frac{|G \times \hat{G} H|}{|H|} = |\ker \alpha|. \]
Since \( \Delta \cap (\ker(G \times \hat{G} H \to H)) = 1 \) and \( \ker(G \times \hat{G} H \to H) \cong \text{Gal}(\hat{F}/EM) \), Galois correspondence implies that
\[ (7) \quad \hat{E}(EM) = \hat{E}M = \hat{F}. \]
Recall that \( R \) (resp. \( S \)) is the ring of regular functions on \( V \) (resp. \( W \)), and since \( V, W \) are smooth, \( S \) is the integral closure of \( R \) in \( F \). Let \( \hat{S} \) be the integral closure of \( R \) in \( \hat{E} \). By (1) we have that \( \hat{S} \otimes_k M \cong \hat{S}M \), and by (4) we get that \( \hat{S}M = SM \). So we have the following ring extension diagram.

\[
\begin{array}{ccc}
S & \xrightarrow{\pi'} & S \otimes_k M & \xrightarrow{\iota'} & SM \\
\downarrow & & \downarrow & & \downarrow \\
R & \xrightarrow{\pi''} & \hat{S} & \xrightarrow{\hat{\iota}'} & \hat{S}M
\end{array}
\]

Taking spectra we get the diagram of varieties given in (13) (where \( \hat{W} = \text{Spec}(\hat{S}) \)). Then \( \hat{W} \) is absolutely irreducible by (1) and deg \( \Delta \) implies that \( \hat{W} \) is geometrically irreducible by (1) and deg \( \Delta \).

Let \( \Omega \in W_M(\hat{K}) \) be étale over \( V \) and denote by \( \hat{\Omega} \) and \( \hat{\Psi} \) the respective images of \( \Omega \) in \( W \) and \( \hat{W} \). First assume that \( \hat{\Psi} \in \hat{W}(K) \). Then \( \hat{\Psi} \otimes \hat{K} = \hat{K} \) (by abuse of notation \( \hat{\Psi} \) also denotes the ideal of \( \hat{S} \) associated to the point). Extend the map \( \hat{\Psi} : \hat{S} \to \hat{S}/\hat{\Psi} \) to a \( K \)-rational place \( \hat{\Phi} \) of \( \hat{S} \). Extend \( \hat{\Phi} \) linearly to a place \( \hat{\Psi} \) of \( \hat{F} \). Then \( \hat{\Phi} = \hat{\Psi}|_F \) extends the map \( S \to \hat{S}/\hat{\Psi} \). As explained in the definition of geometric solutions, \( \hat{\Phi}^* \) and \( \hat{\Psi}^* \) coincides, so \( \hat{\Phi}^* = \hat{\Psi}^* = \hat{\Theta} \) by (5).

Conversely, assume that \( \hat{\Phi}^* = \hat{\Theta} \). Extend \( SM \to SM/\Omega \) to a place \( \hat{\Psi} \) of \( \hat{F} \), and let \( \hat{\Phi} \) and \( \hat{\Phi} \) the restrictions to \( \hat{E} \) and \( F \), respectively. This can be done such that the residue field of \( \hat{\Phi} \) is \( S/\hat{\Psi} \). Then \( \hat{\Phi}^* = \hat{\Psi}^* = \hat{\Theta} \) by (5), \( \hat{\Phi} \) is \( K \)-rational, and in particular, \( \hat{S}/\hat{\Psi} = K \), so \( \hat{\Psi} \in \hat{W}(K) \). This finishes the proof of (12).

Finally we prove (13). Let \( p \in V(K) \) be étale in \( W \), and assume \( p = \pi(\hat{\Psi}) \), for \( \hat{\Psi} \in \hat{W}(K) \). Choose \( \Omega \in W_M \) lying above \( \hat{\Psi} \) and let \( \Psi = p(\iota(\Omega)) \). Then \( \Psi^* = \Theta \) by (12), so \( \Psi^* = \Theta \), and thus \( p \in U \). Thus \( \pi(\hat{W}(K)) \subseteq U \).

Note that since \( W_M \) is an irreducible factor of \( W \times_K M \), every point of \( W \) can be uniquely lifted to \( W_M \). Similarly for \( \hat{W} \), since \( W_M \cong \hat{W} \times_K M \). Let \( p \in U \), so \( \Psi^* = \Theta \). Note that \( \ker \alpha \) acts on \( \rho^{-1}(p) \), and \( \sigma(\Psi)^* = \sigma(\Psi)^\sigma \). So, since there are \( |\Theta| \) such solutions, the set \( P \) of \( \Psi \) with \( \Psi^* = \theta \) is of size \( d = |\ker \alpha|/|\Theta| \). Then \( P_M = (p \circ \iota)^{-1}(P) \) is also of size \( d \), and hence \( \hat{P} = p(\iota(P_M)) \) is of size \( d \).

By (14), \( \hat{P} \subseteq \pi^{-1}(p) \cap \hat{W}(K) \). Assume \( \Psi \notin \hat{P} \). Take \( \Omega \in W_M \) lying above it and take \( \Psi = p(\Omega) \). Then \( \Psi^* \neq \Theta \). So \( \Psi \notin \hat{W}(K) \).

2.3. Irreducibility theorem for PAC fields. In this section we study conditions for a polynomial \( f(X) \in R[X] \) that is irreducible and separable to admit irreducible specializations. First we need the following consequence of Proposition 2.23.

**Proposition 2.3.** A field \( K \) is PAC if and only if every solution \( \theta \) of every geometric embedding problem \( E(W/V) \) is geometric. Moreover, for each \( \theta \) there exists a Zariski dense set of \( p \in V(K) \), étale in \( W \), such that \( p^* = \Theta \), where \( \Theta \) is the \( \ker \alpha \)-inner-automorphism class of \( \theta \).

**Proof.** Let \( E(W/V) \) be a geometric embedding problem, and let \( \theta \) be a solution. Every open subvariety of \( \hat{W} \) given in Proposition 2.23 has \( K \)-rational points, hence \( \hat{W}(K) \) is Zariski dense. The assertion follows, since for every \( p \in \pi(\hat{W}(K)) \subseteq V(K) \) that is étale in \( W \) we have \( p^* = \Theta \).

Vice-versa, let \( V \) be an absolutely irreducible \( K \)-variety, we can assume that \( V \) is smooth, otherwise we replace \( V \) by an open subvariety. Consider the geometric embedding problem \( E(V/V) \). It has a solution, the trivial one, say \( \Theta \colon \text{Gal}(K) \to 1 \). By assumption \( \theta = p^* \), for some \( p \in V(K) \). In particular, \( V(K) \) is not empty, and \( K \) is PAC. 

\( \square \)
Let $V$ be an absolutely irreducible smooth $K$-variety, $R$ the ring of regular functions, and $f(X) \in R[X]$ a monic separable polynomial. By Lemma 2.1 to have $p \in V(K)$ such that $f \mod p$ is of a given factorization type, say $P$, it is necessary that $E(f, V)$ has a solution with orbit type $P$. Over PAC fields this condition also suffices.

**Theorem 2.4.** Let $K$ be a PAC field, $V$ an absolutely irreducible smooth $K$-variety with ring of regular function $R$, $f(X) \in R[X]$ a separable monic polynomial, and $P$ a partition of $\text{deg } f$. Assume that the induced embedding problem has a solution whose orbit type is $P$. Then there exists a Zariski dense set of $p \in V(K)$ such that $f \mod p$ is a separable polynomial of factorization type $P$.

**Proof.** Let $\theta$ be a solution of factorization type $P$. By Proposition 2.3 we have $\Theta = p^*$, for a Zariski dense set of $p \in V(K)$ that are étale in $V_f$. For each such $p$, the action of $\text{Gal}(K)$ on the roots of $f \mod p$ coincides (up to labeling of the roots) with the action on the image of $\theta$ on the roots of $f$. The latter has orbit type $P$, so the factorization type of $f \mod p$ is $P$. $\square$

**Remark 2.5.** From the proof follows a stronger statement. Namely, under the notation of the theorem, there exists a Zariski dense set of $p \in V(K)$ such that the splitting field of $f \mod p$ is the solution field $\overline{K}_{\ker \theta}$ of $\theta$.

**Remark 2.6.** The theorem holds true even if $f$ is not monic, and $V$ is not smooth. Indeed, in that case we replace $V$ with a smooth open subvariety, such that, the leading coefficient of $f$ is invertible in the ring of regular functions.

To connect Theorem 2.4 to Hilbertian fields, one needs to take $V = \mathbb{A}^n$, and take $P$ the partition to a single part.

**Corollary 2.7.** Let $K$ be a PAC field, $f(A_1, \ldots, A_n, X) \in K[A_1, \ldots, A_n, X]$ a monic polynomial in $n + 1$ variables, $n \geq 1$, that is separable in $X$, and let $g(A_1, \ldots, A_n)$ nonzero polynomial. Assume that the associated embedding problem $E(f, \mathbb{A}^n)$ has a transitive solution. Then there exists $a_1, \ldots, a_n \in K^n$ such that

$$f(a_1, \ldots, a_n, X) \text{ is irreducible and } g(a_1, \ldots, a_n) \neq 0.$$  

An interesting special case, that appears in [?], is when $f(A_1, \ldots, A_n, X)$ is the ‘most’ irreducible, i.e., when $\text{Gal}(f, \overline{K}(A_1, \ldots, A_n))$ is the full symmetric group. Then $E(f, \mathbb{A}^n)$ is

$$\begin{array}{c}
\text{Gal}(K) \\
\downarrow \\
S_n \\
\downarrow \\
1
\end{array}$$

so a transitive solution exists if and only if $K$ has a separable extension of degree $n$.

### 3. Calculating a Galois group of compositum of polynomials

#### 3.1. Galois groups of shifted generic polynomials

Let us start by fixing the notation that will be used throughout this section:

- $K$ an algebraically closed field of characteristic $p \geq 0$,
- $S_n$ the symmetric group on $n$ letters,
- $A_1, \ldots, A_n$ $n$ algebraically independent variables,
- $\Omega = \{\omega_1, \ldots, \omega_m\} \subseteq K$ subset of $K$ of $m$ elements,
- $g(A, X) = X^n + A_1 X^{n-1} + \cdots + A_n$ a general polynomial,
- $g_i(A, X) = g(A, X) - \omega_i$ shifted general polynomials, $i = 1, \ldots, m$,
- $F_i$ the splitting field of $g_i$ over $K(A)$, $i = 1, \ldots, m$. 


Indeed, the proper normal subgroups of \( S_n \) (e.g., \([?, \text{Example 4, VI, §2}])
Hence, \( \text{Gal}(g, K(A)) \cong S_n \). The objective of the section is to prove Proposition [17] i.e., that \( F_1, \ldots, F_r \) are linearly disjoint. Equivalently,
\[
\text{Gal}\left( \prod_{i=1}^{m} g_i, K(A) \right) \cong S_n^m
\]
(since \( \text{Gal}(F_i/K(A)) = S_n \)).

This will be proved in a series of lemmas.

Assume for a short while that \( p = n = 2 \). As mentioned in the introduction, the above assertion
fails to hold. Nevertheless, one can characterize \( \Omega \)'s for which the assertion holds: \( F_1, \ldots, F_m \) are linearly disjoint if and only if the sum of any even number of \( \omega_i \)'s does not vanish. We leave this
as an exercise for the reader. We do not know what happen when \( p = 2 \) and \( n > 2 \) is even. A
naive possibility is suggested in the following question.

**Question 3.1.** Assume \( p = 2 \), \( n \) even. Does the following assertion hold true? \( F_1, \ldots, F_m \) are linearly disjoint if and only if every even sum of distinct elements of \( \Omega \) does not vanish.

In the answer is no, characterize the finite subsets \( \Omega \subseteq K \) for which \( F_1, \ldots, F_m \) are linearly disjoint.

We note that the assertion of Theorems [141] and [142] holds for polynomials \( f_1, \ldots, f_r \) such that
the set \( \Omega \) of all their roots satisfies the assertion of the proposition, as will be shown in the sequel.

Now we start proving Proposition [142]. We denote by \( A_n \) the alternating group.

**Lemma 3.2.** Let \( r, n \geq 1 \), for each \( i = 1, \ldots, r \) let \( \alpha_i : G \to S_n \) be an epimorphism, and let
\( \alpha = \prod \alpha_i : G \to n^r \). Assume \( \beta : G \to (\mathbb{Z}/2\mathbb{Z})^r \) induced by the natural map \( S_n^r \to S_n^r/A_n^r \) is surjective. Then \( \alpha \) is surjective.

**Proof.** The case \( r = 1 \) is trivial; we proceed by induction on \( r \). Let \( S = S_n \) and \( S' = S_n^{-1} \). By
induction we have that \( \alpha' = \prod_{i=1}^{r-1} \alpha_i : G \to S' \) is surjective. Let \( M' = \ker \alpha', M = \ker \alpha \), and \( A = G/M'M \). Let \( S' \to A \) and \( S \to A \) be the projections induced by \( \alpha', \alpha \), respectively. Then the image of \( \alpha = \alpha' \times \alpha_r \) in \( S' \times S \) is \( S' \times A S \).

Since \( G/M = S \cong S_n \), there exists \( M \leq E \leq G \) such that \( E/M \cong A_n \). Similarly, there exists \( M' \leq E' \leq G \) such that \( E'/M' \cong A_n^{-1} \).

![Diagram](https://example.com/diagram.png)

We have

(a) \( E/M \) contains all proper normal subgroups of \( G/M \),
(b) \( E'/M \) is contained in every subgroup of \( G/M' \) of index 2, and
(c) \( E'E = G \).

Indeed, the proper normal subgroups of \( S_n \) are \( A_n, 1 \), and if \( n = 4 \), the the Klein group \( V_4 \). Thus \( A_n \) contains all proper normal subgroups, and [14] follows.

For a group \( H \) we let \( H^{(2)} \) be the subgroup generated by squares. Then every index 2 subgroup
contains \( H^{(2)} \). Since \( (h_1, h_2)^2 = (h_1^2, h_2^2) \) we have \( (H_1 \times H_2)^{(2)} = H_1^{(2)} \times H_2^{(2)} \). Note that \( S_n^{(2)} = A_n \), since \( S_n^{(2)} \subseteq A_n \), \( (i \ j \ k)^2 = (i \ j \ k) \), and \( A_n \) is generated by 3-cycles. Thus \( (S_n^{r-1})^{(2)} = A_r^{-1} \), so \( (G/M')^{(2)} = E'/M' \), and [15] follows.


We have \( \ker(\beta) = E' \cap E \), so by assumption \( G/E' \cap E \cong (\mathbb{Z}/2\mathbb{Z})^r \). Since \( G/E' \cong (\mathbb{Z}/2\mathbb{Z})^{r-1} \) we have \( E'/E \cong E'/E' \cap E \cong \mathbb{Z}/2\mathbb{Z} \), so \( G : E' = (G : E)/E' : E) = 2/2 = 1 \), and \( E \) has trivial Galois group.

We continue with the proof. If \( A = 1 \), then \( G = S' \times S \cong S_n' \), and we are done. Assume \( A \neq 1 \).

Then \( M' \) is a proper normal subgroup of \( G/M' \), hence \( M' \) is a quotient of \( G/M' \), so \( E' \leq E \) trivially follows.

In particular \( M' \leq E \). Then \( G/E \cong \mathbb{Z}/2\mathbb{Z} \) is a quotient of \( G/M' \), so \( E \) implies \( E' \leq E \). But then \( E' = E \neq G \), which contradicts \( E \).

For each \( i \), let \( E_i \) be the fixed field of \( A_i \) in \( E \). Then \( E_i/K(\mathbf{A}) \) is a quadratic extension. Clearly if \( E_1, \ldots, E_m \) are linearly disjoint, then \( E_1, \ldots, E_m \) are linearly disjoint. The next lemma shows that the converse holds.

**Lemma 3.3.** If \( E_1, \ldots, E_m \) are linearly disjoint over \( K(\mathbf{A}) \), then \( F_1, \ldots, F_m \) are linearly disjoint over \( K(\mathbf{A}) \).

**Proof.** Let \( \alpha_i : \text{Gal}(K(\mathbf{A})) \to \text{Gal}(E_i/K(\mathbf{A})) \), let \( \alpha = \prod_i \alpha_i : \text{Gal}(K) \to \prod_i \text{Gal}(E_i/K) \cong S_n^m \), and let \( \beta : \text{Gal}(K) \to \prod_i \text{Gal}(E_i/K) \cong (\mathbb{Z}/2\mathbb{Z})^m \). By the assumption of the lemma, \( \beta \) is surjective, so by Lemma 3.2 \( \alpha \) is surjective. Thus \( F_1, \ldots, F_m \) are linearly disjoint.

Let \( h(X) \) be a separable polynomial of degree \( n \) defined over a field \( L \) and let \( x_1, \ldots, x_n \) be its roots. We consider the Galois group of \( h \) over \( L \) as a permutation group on the roots of \( h \). We let \( E_h \subseteq L(x_1, \ldots, x_n) \) be the extension of degree at most \( 2 \) which is the fixed field of all even elements in the Galois group of \( h \).

If \( p \neq 2 \), then \( E_h \) is generated by a root of \( X^2 - \Delta(h) \), where \( \Delta(h) = \prod_{i \neq j} (x_i - x_j) \) is the discriminant of the polynomial. Let \( \delta(h) \) be the square class of \( \Delta(h) \), i.e., \( \delta(h) = [\Delta(h)] \in L'/(L')^2 = H^1(L, \mathbb{Z}/2\mathbb{Z}) \). The last equality follows from Kummer theory. This group is abelian of exponent 2, hence we regard it as a vector space over \( \mathbb{F}_2 \).

If \( p = 2 \), then \( E_h \) is generated by a root of the Artin-Schreier extension \( X^2 + X + A(h) \), where \( A(h) = \sum_{i \neq j} \frac{x_i x_j}{x_i + x_j} \) (see, e.g., [1]). Then we let \( \delta(h) \) be the Artin-Schreier coset of \( A(h) \), i.e., \( \delta(h) = A(h) + \varphi(L) \in L'/\varphi(L) = H^1(L, \mathbb{Z}/2\mathbb{Z}) \), where \( \varphi(x) = x^2 + x \). The last equality follows from Artin-Schreier theory. This group, as for \( p \neq 2 \), is abelian of exponent 2, hence a vector space over \( \mathbb{F}_2 \).

We call \( \delta(h) \) the discriminant class of \( h \).

For each \( i = 1, \ldots, m \), \( E_i = E_{g_i} \). Therefore \( E_1, \ldots, E_m \) are linearly disjoint if and only if \( \delta(g_i) \) are linearly independent. So Lemma 3.3 can be reformulated in terms of the discriminant classes.

**Lemma 3.4.** If \( \delta(g_1), \ldots, \delta(g_m) \) are linearly independent, then \( F_1, \ldots, F_m \) are linearly disjoint over \( K(\mathbf{A}) \).

General polynomials are complicated for calculations. Hence in the last lemma before the proof of the proposition, we shall reduced to specialized polynomials.

**Lemma 3.5.** Let \( a = (a_1, \ldots, a_n) \) be an \( n \)-tuple in a field containing \( K \), let \( h(a, X) = g(a, X) \in K(\mathbf{A})[X] \). For each \( i = 1, \ldots, m \) let \( h_i = h - \omega_i \). Assume \( h_1, \ldots, h_m \) are separable and \( \delta(h_1), \ldots, \delta(h_m) \) are linearly disjoint. Then \( \delta(g_1), \ldots, \delta(g_m) \) are linearly disjoint.

We shall use this lemma only when \( p \neq 2 \), but for the sake of completeness, we proof it for arbitrary characteristic.

**Proof.** We start with \( p \neq 2 \). Let \( V = K(\mathbf{A})^*/(K(\mathbf{A})^*)^2 \). For each \( v \in V \), there exists a unique square-free polynomial \( f_v(\mathbf{A}) \) such that \( v = [f_v] \). For \( u, v \in V \) we have \( f_{u+v} = f_u f_v / d^2 \), where \( d = \gcd(f_u, f_v) \). Let \( U = \{ v \in V \mid f_v(\mathbf{A}) \neq 0 \} \).

Then \( U \) is a subspace. Indeed, \( f_{v+w}(\mathbf{a}) = f_w(\mathbf{a}) f_v(\mathbf{a}) / d^2(\mathbf{a}) \neq 0 \).

Let \( W = K(\mathbf{A})^*/(K(\mathbf{A})^*)^2 \). Let \( T : U \to W \) be the map induced by \( \mathbf{A} \to \mathbf{a} \), i.e., \( T(u) = [f_u(\mathbf{a})] \).

It is a linear map, because, by the above

\[
T(v + u) = [f_v(\mathbf{a}) f_u(\mathbf{a}) / d^2(\mathbf{a})] = [f_v(\mathbf{a})] [f_u(\mathbf{a})] = [f_v(\mathbf{a})] + [f_u(\mathbf{a})] = T(v) + T(u).
\]

For each \( i \), let \( E_i \) be the fixed field of \( A_i \) in \( E \). Then \( E_i/K(\mathbf{A}) \) is a quadratic extension. Clearly if \( E_1, \ldots, E_m \) are linearly disjoint, then \( E_1, \ldots, E_m \) are linearly disjoint. The next lemma shows that the converse holds.
Since there is a polynomial formula for the discriminant in term of the coefficients, it follows that \( \Delta(h_i) = \Delta(g_i)(a) \) (recall that \( \Delta(g_i) \in K[A] \)). Let \( f_i \) be the square-free part of \( \Delta(g_i) \), so \( \Delta(g_i) = f_i a^d \), and so \( \Delta(h_i) = f_i(a) a^d(a) \). The assumption that \( h_i \) is separable implies that \( \Delta(h_i) \neq 0 \). So we get \( T(\delta(g_i)) = [f_i(a)] = \delta(h_i) \). This finishes the proof for \( p \neq 2 \).

Assume \( p = 2 \). Let \( R = K[A, \Delta(g_1)^{-1}, \ldots, \Delta(g_m)^{-1}] \). Let \( u = f(A, A) \in K(A) \) with \( \gcd(f, k) = 1 \). Then the denominator of \( u^2 + u \) is \( k^2(A) \). In particular, if \( u^2 + u \in R \), then \( u \in R \). Thus \( R \) maps to \( R/\varphi(R) \) under the map \( K(A) \to \varphi(K(A)) \). In particular \( A \to a \) induces a map \( T : R/\varphi(R) \to K(a)/\varphi(K(a)) \).

As mentioned above, \( \delta(g_i) \) is the class generated by \( \prod_{l \neq l'} \frac{x_l x_{l'}}{x_l + x_{l'}} \), where \( x_1, \ldots, x_n \) are the roots of \( g_i \). The common denominator of this expression is

\[
\prod_{l \neq l'} (x_l + x_{l'}) = \prod_{l \neq l'} (x_l - x_{l'}) = \Delta(g_i).
\]

Therefore, \( \delta(g_i) \in R \) and \( \delta(h_i) \in T(R/\varphi(R)) \). This finishes the proof for \( p = 2 \). \( \square \)

**Proof of Proposition 1.7.** From the series of lemmas, it suffices to find \( A \to a \) such that \( \delta(h_i) \in H^1(K(a), \Bbb{Z}/2\Bbb{Z}) \) are linearly independent, where \( h_i(X) = g_i(a, X) \). It will be more convenient to specify the coefficients of \( h(X) = X^n + a_1 X^{n-1} + \cdots + a_n \) instead of the sequence \( (a_1, \ldots, a_n) \).

We divide the proof into several cases.

**The case when \( p \nmid n \) and \( n \) is even.** Consider \( h(T, X) = X^n - T \), where \( T \) is a variable over \( K \). Then \( \text{Gal}(h, K(T)) = C_n \) and the splitting field is \( K(\sqrt{2T}) \). Thus \( K(\sqrt{2T}) \) is the unique quadratic subextension, and \( \text{Gal}(K(\sqrt{2T})/K(\sqrt{T})) = C_{n/2} = C_n \cap A_n \). So \( \delta(h) = [T] \), hence \( \delta(h_i) = [T - \alpha_i] \), which are obviously linearly independent in \( K(T)^*/(K(T)^*)^2 \).

**The case when \( p \nmid n(n-1) \).** We shall use basic facts on ramification theory, one reference that includes all we use is [?]. Let \( S, T \) be two algebraically independent variables, let \( h_0(X) = X^n - SX^{n-1} \) and \( h(T, X) = h_0(X) - T \). Let \( K = K(S) \), \( R = K'[T] \), let \( U = K'(T)[X]/(h) \cong K'(x) \), where \( h(T, x) = 0 \). Since \( T = h(x) \) we have \( R[x] = K'[x] \), so \( R[x] \) is the integral closure of \( R \) in \( U \). We then have that the different of the extension \( U/K'(T) \) is the ideal generated by the derivative \( h_0'(x) = nx^{n-2} - \frac{n-1}{n} S \). So all the ramified primes are \( (x)/(T) \), \( (x - s_1)/(T - t_1) \), where \( s_1 = \frac{n-1}{n} S \) and \( t_1 = h_0(s_1) = S^n \beta \), \( \beta \in K^* \). The ramification indices are \( n - 1 \) and \( 2 \), respectively. Thus the corresponding inertia groups \( I_0, I_1 \) are generated by \( (n-1)- \) and by a transposition, respectively.

This implies that (1) \( I_1 \) is not contained in \( A_n \), and (2) \( I_0 \) is contained in \( A_n \) if and only if \( n \) is even. Thus the extension corresponding to the fixed field of the odd permutations is ramified at \( (T - t_1) \) and if \( n \) is odd also at \( (T) \). Therefore, \( \delta(h) = [(T - t_1)] \) if \( n \) is even, and \( = [(T)/(T - t_1)] \) if \( n \) is odd. In both cases, \( \delta(h_i) \) are linearly independent in \( K(S,T)^*/(K(S,T)^*)^2 \).

**The case when \( n \) is odd and \( p \mid n - 1 \).** Similar argument as in the previous case shows that the discriminant classes \( \delta(h_i) \) are linearly independent, where \( h = X^n - SX^{n-2} - T \).

**The case \( p = 2 \) and \( n \) is odd.** Here we use a different argument: Let \( L = K(A_1, \ldots, A_{n-1}) \), and let \( U_i = L(A_n)[x_i] \), where \( x_i \in F_i \) is a root of \( g_i(A, X) \), \( i = 1, \ldots, m \). As the ramification at infinity is tame, it suffices to show that the \( A_n \)-finite ramification loci of the \( U_i/L(A_n) \) are distinct. (Indeed, then the finite ramification loci of the \( F_i \) will be distinct, and hence, the \( F_i \) will be linearly disjoint.)

The different of \( U_i/L(A_n) \) is contained in the ideal generated by \( \frac{\partial q}{\partial x}(x_i) \). Thus the ramification points of \( U_i/L(A_n) \) are \( A_n = g_i(u_1), \ldots, g_i(u_r) \), where \( u_1, \ldots, u_r \) are the distinct roots of \( \frac{\partial q}{\partial x} = \frac{\partial q}{\partial x} \) in a fixed algebraic closure of \( L \). We have

\[
\frac{\partial q}{\partial X}(X) = X^{n-1} + \sum_{j=1}^{n-1} A_{2j} X^{n-2j-1} = \left(X^{\frac{n-1}{2}} + \sum_{j=1}^{n-1} \sqrt{A_{2j}} X^{\frac{n-2j-1}{2}} \right)^2 = \prod_{j=1}^{r} (X - u_j)^2,
\]

so \( r = \frac{n-1}{2} \). Note that \( u_1, \ldots, u_r \) are distinct, and furthermore, are algebraically independent variables because they are roots of a polynomial with variable coefficients. Since the coefficients of \( \frac{\partial q}{\partial x} \) depend only on even indexed \( A_i, u_1, \ldots, u_r \) are algebraically independent of \( A_1, A_3, \ldots, A_n \).
Substituting \( u_j \) in the above equation, and multiplying by \( u_j \) gives that

\[
u_j^n + A_2 u_j^{n-2} + \cdots + A_{n-1} u_j = 0.
\]

Thus, for \( j \neq j' \),

\[
g_i(A, u_j) + g_i(A, u_{j'}) = A_1(u_j^{n-1} + u_{j'}^{n-1}) + A_3(u_j^{n-3} + u_{j'}^{n-3}) + \cdots + (A_n + \alpha_i) + (A_n + \alpha_{i'}),
\]

But \( A_n = g_i(A, u_1), \ldots, g_i(A, u_r) \) are the ramification points of \( U_i/L(A_n) \), so these are disjoint when \( i \) varies. (Note that we used several times that \(-1 = 1 \) in \( K \)).

The case when \( p \neq 2 \) and \( p \mid n \). Take \( h(T, X) = X^n + \frac{1}{2}X^2 + T \). We shall use that \( \Delta(h) \) equals the resultant of \( h \) and \( h' \) and then we apply the formula for the resultant given by the determinant of the corresponding Sylvester matrix. We note that \( h' = X \). Then we have

\[
\Delta(h) = \begin{vmatrix} 1 & \cdots & \frac{1}{T} & 0 & T & 0 & \cdots & 0 \\ 1 & \cdots & \frac{1}{T} & 0 & T & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & 1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & \cdots & 1 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{vmatrix} = \pm T.
\]

(We developed the determinant by the last column, then we got an upper triangular matrix with 1’s on the diagonal.) Hence \( \delta(h_i) = |T - \alpha_i| \), so the \( \delta(h_i) \) are linearly disjoint.

\[
3.2. \textbf{Galois group of composition of polynomials.} \quad \text{The symmetric group } \text{Sym}(\Psi) \text{ is maximal in the family of all permutation groups on } \Psi, \text{ in the sense the every permutation group on } \Psi \text{ embeds (by definition) into Sym}(\Psi). \text{ We will show that the permutational wreath product plays a similar role, when considering permutation groups on } \Psi \times \Omega \text{ that respect the projection map } \Psi \times \Omega \to \Omega.
\]

The Galois group of the composition of polynomials \( \text{Gal}(f \circ g) \) maps onto the Galois group of the outer polynomial \( \text{Gal}(f) \). We shall prove that if the inner polynomial is generic, then \( \text{Gal}(f \circ g) \) is the maximal possible, namely the wreath product, namely the wreath product, provided \( \text{deg } g \) is odd of the characteristic is 2.

**Proposition 3.6.** Let \( K \) be a field of characteristic \( p \geq 0 \), \( n \) a positive integer, odd if \( p = 2 \), \( f(X) \in K[X] \) a separable polynomial, \( g(A, X) = X^n + A_1X^{n-1} + \cdots + A_n \) a polynomial whose coefficients are variables, \( \Omega, \Phi \) the sets of roots of \( f, f \circ g \). Then, the splitting field of \( f \circ g \) over \( K(A) \) is regular over the splitting field of \( f \) and

\[
\text{Gal}(f \circ g, K(A)) \cong S_n \wr \Omega \text{ Gal}(f, K).
\]

This isomorphism respects the actions of the LHS on \( \Phi \) and RHS on \( \{1, \ldots, n\} \times \Omega \).

Before proving this result we bring the formal definition of the permutational wreath product and two auxiliary results in Galois theory.

Let \( H, G \) be finite groups acting on finite sets \( \Psi, \Omega \), respectively. Then \( H^\Omega = \{\zeta: \Omega \to H\} \) acts “independently on each row” of \( \Phi := \Psi \times \Omega \), that is, \( \zeta.(\psi, \omega) = (\zeta(\omega), \psi, \omega) \). We let \( G \) act on the second coordinate of \( \Phi \), namely, \( g.(\psi, \omega) = (\psi, g.\omega) \), so \( G \) permutes the “columns”. The group generated by these permutations is the **permutational wreath product**, the group structure is

\[
H \wr \Omega G = H^\Omega \rtimes G,
\]

where \( \zeta^{-1}(\omega) := (g.\zeta)(\omega) = \zeta(g.\omega) \), for \( \zeta \in H^\Omega, \omega \in \Omega \), and \( g \in G \).
Each element of $H \wr_\Omega G$ has a unique representation as a product $\zeta g$, where $\zeta \in H^\Omega$ and $g \in G$. The multiplication is then given by $\zeta g k = \zeta \xi^{-1} g k, \zeta, \xi \in H^\Omega$ and $g, k \in G$. Hence $\zeta g = g^{-1} \zeta g$.

The action of $H \wr_\Omega G$ on $\Phi$ is given by:

$$(\zeta g)(\psi, \omega) := (\zeta(g, \psi), g, \omega).$$

The action is well defined because

$$(g \zeta g^{-1})(\psi, \omega) = g(\zeta^{-1}(\omega), \psi) = (\zeta(g, \psi), g, \omega) = (\zeta g)(\omega, \psi).$$

The morphism $\zeta g \mapsto g: H \wr_\Omega G \to G$ respects the corresponding actions because the projection on the second coordinate of $\zeta g(\psi, \omega)$ equals $g, \omega$.

The following lemma is an exercise in basic Galois theory which we prove for the sake of completeness.

**Lemma 3.7.** Let $r$ and $n$ be positive integers, $[n] = \{1, \ldots, n\}$, and $K \subseteq L_i \subseteq M_i$ a tower of finite separable extensions with $[M_i : L_i] \leq n$, for $i = 1, \ldots, r$. Let $N$ be the Galois closure of the compositum of $M_1, \ldots, M_r$ over $K$,

$H = \text{Gal}(N/K)$,

$\hat{L}_i$ the Galois closure of $L_i/K$,

$\hat{L}$ the compositum of $\hat{L}_1, \ldots, \hat{L}_r$,

$G = \text{Gal}(\hat{L}/K)$, and

$\Omega = \bigsqcup_{i=1}^r \Omega_i$, where $\Omega_i$ is the set of all embeddings of $L_i$ to $N$ that fix $K$.

Then:

(a) $G$ is a permutation group on $\Omega$ and there exists an embedding $\rho: H \to S_n \wr_\Omega G$ such that $\rho(\sigma) = \zeta_\sigma \sigma |_{\hat{L}_i}$, for some $\zeta_\sigma: \Omega \to S_n$ and every $\sigma \in H$.

(b) $[M_i : L_i] = n$ (for some $i \in [r]$) if and only if $H' = \rho(H)$ acts transitively on $[n] \times \Omega_i$.

**Proof.** The Galois group $\text{Gal}(\hat{L}/K)$ acts naturally on $\Omega_i$, namely $\sigma \cdot \omega_i = \sigma_i \cdot \omega_i$. This action is faithful. By Galois correspondence, the assumption that $\hat{L}$ is the compositum of $\hat{L}_1, \ldots, \hat{L}_r$ is equivalent to $\bigcap_{i=1}^r \text{Gal}(\hat{L}/\hat{L}_i) = 1$. The restriction maps $G \to \text{Gal}(\hat{L}_i/K)$ induce an action of $G$ on each $\Omega_i$, and thus on $\Omega$. An element $\sigma \in G$ fixes all elements $\omega \in \Omega_i$ if and only if $\sigma \in \text{Gal}(\hat{L}/\hat{L}_i)$. Therefore if $\sigma$ fixes all $\omega \in \Omega$, then $\sigma \in \bigcap_{i=1}^r \text{Gal}(\hat{L}/\hat{L}_i) = 1$. This implies that $G$ is a permutation group on $\Omega$.

For each $i$, let $\Phi_i$ be the set of all embeddings of $M_i$ to $N$ that fix $K$. Then the same argument as above gives that $H$ is a permutation group on $\Phi = \prod_{i=1}^r \Phi_i$.

Let $\Psi_i \subseteq \Phi_i$ be the set of all embeddings of $M_i$ to $N$ that fix $L_i$. Then $n \geq [M_i : L_i] = [\Psi_i]$. Let us enumerate the elements of $\Psi_i = \{\psi_{i1}, \ldots, \psi_{ik_i}\}$ ($k_i \leq n$). Let $T_i: \Omega_i \to H$ be a section of the restriction map, i.e., $T(\omega)|_{L_i} = \omega$, for all $\omega \in \Omega_i, i = 1, \ldots, r$, and let $T = \prod_{i=1}^r T_i: \Omega \to H$.

(Note that, if $L_i = L_j$ for some $i \neq j$, we understand $\sigma|_{L_i} \in \Omega_i$ and $\sigma|_{L_j} \in \Omega_j$ as distinct elements of $\Omega$, although they induce the same function on $L_i$)

Then

(i) for every $\psi_{ij} \in \Psi_i$, we have $\psi_{ij}|_{L_i} = \text{id}_{L_i}$ (by definition), thus

(ii) $(\sigma T(\omega))|_{L_i} = \sigma|_\omega$, for every $\sigma \in H$.

(iii) If $\varphi \in \Phi_i$, then $T(\varphi|_{L_i})^{-1} \varphi \in \Psi_i$, hence it equals $\psi_{i,j} T(\varphi)$ for some $J(\varphi) \in [k_i]$.

(iv) If $\omega \in \Omega_i$, $\psi_{ij} \in \Psi_i$, and $\sigma \in H$, then $u := \sigma T(\omega)\psi_{ij} \in \Phi_i$. Hence, by (ii) $u|_{L_i} = \sigma|_\omega$ and by (iii) $(T(u)|_{L_i})^{-1} u = \psi_{i,j}(u)$. So $J(u)$ depends only on $j, \sigma$, and $\omega$ and for fixed $\sigma, \omega$ this dependency is injective. Therefore $J(u) = \zeta_{\sigma}(\omega), j$, for some $\zeta_{\sigma}(\omega) \in \text{Sym}(k_i) \leq S_n$. 

Consider the map $\rho^*: \Phi \to [n] \times \Omega$ defined by $\varphi \in \Phi \mapsto (J(\varphi), \varphi|_{\Omega_i}) \in [n] \times \Omega_i$. By (iii), the map $(j, \omega) \mapsto T(\omega)\psi_{ij}$, for $\omega \in \Omega_i$ and $j \in [n]$ is the inverse of $\rho^*$, so $\rho^*$ is a bijection, and thus induces an embedding

$$\rho: H \to \text{Sym}([n] \times \Omega)$$

that respects the actions of the former on $\Phi$ and the latter on $[n] \times \Omega$. For (a) it suffices to show that the image $H'$ of $\rho$ is contained in the wreath product $S_n \wr \Omega$ (considered as a subgroup of $\text{Sym}([n] \times \Omega)$). And indeed, for $\sigma \in H$, if we write $\bar{\sigma} = \sigma|_L$, then we have (using (i)-(iv))

$$\rho(\sigma)(j, \omega) = \rho^*(\sigma(T(\omega)\psi_{ij})) = (J(\sigma T(\omega)\psi_{ij}),(\sigma T(\omega)\psi_{ij}|_{\Omega_i}))$$

for $j \in [k]$ and $\omega \in \Omega_i$. So $\rho(\sigma) = ((\zeta_\sigma)^{\bar{\sigma}}, \bar{\sigma}) \in S_n \wr \Omega$, as needed for (a).

If $[M_i : L_i] = n$, then $|\Psi_i| = n$, so $|\Psi_i| = n\cdot|\Omega_i|$. Then, since $\rho^*$ is injective and $\rho^*(\Phi_i) \subseteq [n] \times \Omega_i$, we get that $\rho^*(\Phi_i) = [n] \times \Omega_i$. Now since $H$ acts transitively on $\Phi_i$, its image $H'$ acts transitively on $[n] \times \Omega_i$.

\[ \square \]

**Corollary 3.8.** Let $f, g \in K[X]$ be such that $f \circ g$ is separable, let $\Omega_f, \Omega_{f \circ g}$ be the sets of roots of $f$ and $f \circ g$, respectively, and let $n = \deg g$. Then there exists an embedding

$$\rho: \text{Gal}(f \circ g, K) \to S_n \wr \Omega_f \text{ Gal}(f, K)$$

that respects the action of the LHS on $\Omega_{f \circ g}$ and of the RHS on $[n] \times \Omega_f$. Moreover, if $\tilde{f}(X)$ is an irreducible factor of $f$ with set of roots $\tilde{\Omega} \subseteq \Omega_f$, then $\tilde{f}(g(X))$ is irreducible over $K$ if and only if the image of $\rho$ acts transitively on $[n] \times \tilde{\Omega}$.

**Proof.** Let $f = \prod_{i=1}^m f_i$ be the factorization of $f$ into a product of irreducible polynomials. Let $\omega_i$ be a root of $f_i$, for $i = 1, \ldots, r$. Let $L_i = K(\omega_i)$ and let $M_i = K(\nu_i)$, where $\nu_i$ is a root of $g(X) - \omega_i$. Since $\omega_i = g(\nu_i)$ we have $K \subseteq L_i \subseteq M_i$ and $[M_i : L_i] \leq n$. These extension are separable because $f(g(X)) = \prod_{\omega \in \Omega_f} (g(X) - \omega)$ is separable. Now Proposition 3.7 implies the assertion. \[ \square \]

**Proof of Proposition 3.4** Let $G = \text{Gal}(f(X), K) \cong \text{Gal}(f(X), K(A))$. Let $g_i(\mathbf{A}, X) = g(\mathbf{A}, X) - \omega_i$, where $\Omega = \{\omega_1, \ldots, \omega_m\}$ are the roots of $f$. Then, since $f$ is separable, and since $f(g_i(\mathbf{A}, X)) = \prod_{i=1}^m g_i$, we get that $f \circ g$ is separable. Let $F$ be the splitting field of $f \circ g$ over $K(A)$ and $L$ the splitting field of $f$ over $K$. By Corollary 3.3 we can consider $H = \text{Gal}(F/K(A))$ as a subgroup of $S_n \wr \Omega_f$. The kernel $\text{Gal}(F/L(A))$ of the restriction map $H \to G$ coincides with $H \cap S_n^\Omega$. Proposition 3.7 implies that $\text{Gal}(F\tilde{K}/\tilde{K}(A)) = S_n^\Omega$, because it is the Galois group of the product of the $g_i$’s. (Here $\tilde{K}$ is an algebraic closure of $K$.) We have

$$S_n^\Omega \supseteq H \cap S_n^\Omega = \text{Gal}(F/L(A)) \supseteq \text{Gal}(F\tilde{K}/\tilde{K}(A)) = S_n^\Omega,$$

hence $\text{Gal}(F/L(A)) = S_n^\Omega$, $F$ is regular over $L$, and $\text{Gal}(F/K(A)) = S_n \wr \Omega_f \cap G$. \[ \square \]

4. **Proof of Theorem 1.3**

Let $K$ be a PAC field of characteristic $p \geq 0$, $f_1, \ldots, f_r$ irreducible non-associate polynomials, and $f = f_1 \cdots f_r$. Let $g(\mathbf{A}, t) = t^n + A_1 t^{n-1} + \cdots + A_n$ be a polynomial with variable coefficients. Let $F$ (resp. $L$) be the splitting field of $f \circ g$ (resp. $f$) over $K(A)$ (resp. $K$). Then, by Proposition 3.3 $F$ is regular over $L$ and $\text{Gal}(F/K(A)) = S_n \wr \Omega_f \text{ Gal}(L/K)$, where $\Omega = \prod_{i=1}^r \Omega_i$ is the set of the roots of $f_i$, and $\Omega_i$ is the set of the roots of $f_i$, $i = 1, \ldots, r$. Moreover, the restriction map $\alpha: \text{Gal}(F/K(A)) \to \text{Gal}(L/K)$ coincides with the wreath product projection $S_n \wr \Omega_f \text{ Gal}(L/K) \to \text{Gal}(L/K)$. So

$$\mathcal{E}(f \circ g, K^n_K) = (r_{L}: \text{Gal}(K) \to \text{Gal}(L/K), \alpha: S_n \wr \Omega_f \text{ Gal}(L/K) \to \text{Gal}(L/K)).$$

(Here $r_{L}: \text{Gal}(K) \to \text{Gal}(L/K)$ is the restriction map.)

By assumption, each $K(\omega_i)$ has a degree $n$ separable extension, for some $\omega_i \in \Omega_i$, $i = 1, \ldots, r$. Thus Lemma 3.7 (applied to $L_i = K(\omega_i)$ and $M_i$ the degree $n$ separable extension of $K(\omega_i)$) gives a homomorphism $\theta: \text{Gal}(K) \to S_n \wr \Omega_f \text{ Gal}(L/K)$ such that $\beta \circ \theta = r_{L}$. So $\theta$ is a solution
of $E(f \circ g, K_n^\omega)$. Moreover, Lemma 3.7 gives that $\theta(\text{Gal}(K(\omega))) = \theta(\text{Gal}(K))$ acts transitively on $[n] \times \Omega$, hence acts transitively on the roots of $f_i(g(A, t))$.

By Proposition 2.3 there exists a Zariski dense set of $p \in \mathbb{A}^n(K)$ such that $p^* = \theta$. By Lemma 2.1, $f_i(g(A, t))$ mod $p = f_i(g(a, t))$ is irreducible over $K$.

\section{5. Proof of Theorem 1.4}

\subsection{5.1. Weak version.} Let $K$ be a pseudo finite field, i.e., a perfect PAC field with $\text{Gal}(K) = \hat{\mathbb{Z}}$. Fix $n, B$. Theorem 1.2 asserts that $K$ satisfies the elementary statement $\epsilon(K)$:

If $(1+1 = 0 \Rightarrow n \text{ odd})$ and (for every $f_1, \ldots, f_r \in K[X]$ irreducible, non-assoc., and such that $\sum \deg f_i \leq B$), then there exists $(a_1, \ldots, a_n) \in K^n$ such that for $g(t) = t^n + a_1 t^{n-1} + \cdots + a_n$ and for every $i = 1, \ldots, r$ we have $f_i(g(t))$ is irreducible.

By Ax’s theorem [2, Proposition 20.10.4] this implies that for every $q = p^r$ sufficiently large $\mathbb{F}_q$ satisfies $\epsilon(\mathbb{F}_q)$. Hence we immediately get a weak form of Theorem 1.4.

In order to prove the full theorem basing on pseudo finite fields, we proof a more technical theorem than Theorem 1.2 for pseudo finite fields, and then apply Ax’s theorem.

\subsection{5.2. Strong version.} We need an auxiliary lemma.

\begin{lemma}
Let $n$ be a positive integer, let $\Omega$ be a set of cardinality $\nu$, let $G = \langle \sigma \rangle$, for some $\sigma \in \text{Sym}(\Omega)$, let $\hat{\Omega} = \prod_{i=1}^n \hat{\Omega}_i$ be the factorization of $\Omega$ to $G$-orbits, and let $H = S_n \wr_0 G$. Then

(a) For each $\eta \in S_n^\Omega$, $\eta \in H$ acts of $[n] \times \Omega_i$.

(b) Let $T = \{ \eta \in H | \eta \text{ acts transitively on } [n] \times \Omega_i, \forall i \}$. Then $S_n^\Omega$ acts transitively on $T$, and $|T| = \frac{(n!)^\nu}{\nu!}$.
\end{lemma}

\begin{proof}
Since $\eta \sigma, (k, \omega) = (\eta \sigma, k, \sigma \omega)$, we get $[3]$

Assume $\eta \sigma \in T$ and let $I = \langle \eta \sigma \rangle$. Then $I \cdot (k, \omega) = [n] \times \Omega_i$, for each $(k, \omega) \in [n] \times \Omega_i$. Let $\zeta \in S_n^\Omega$. Then $\zeta^{-1} I \zeta \cdot (k, \omega) = \zeta^{-1} I \cdot (k', \omega) = \zeta^{-1} [n] \times \Omega_i = [n] \times \Omega_i$. So $(\eta \sigma)^\zeta \in T$, and $S_n^\Omega$ acts on $T$.

It remains to prove that this action is transitive and to calculate $|T|$. We first prove it under the assumption that $G$ is transitive, i.e., that $r = 1$.

Let $\eta \in S_n^\Omega$ and $g = \eta \sigma \in S_n \wr_0 G$. We have

$$g^k = (\eta \sigma)^k = \eta \cdots \eta^{\sigma^{(k-1)}} \sigma^k.$$ 

Since the order of $\sigma$ is $\nu$, it follows that $g^\nu$ is the stabilizer of $[n] \times \{ \omega \}$, for some fixed $\omega \in \Omega$. Hence $g$ acts transitively on $[n] \times \Omega$ if and only if $g^\nu$ acts transitively on $[n] \times \{ \omega \}$. We have

$$g^\nu \cdot (i, \omega) = \eta \cdots \eta^{\sigma^{(\nu-1)}} \cdot (i, \omega) = (\eta(\omega) \cdots \eta(\sigma^{(\nu-1)}(\omega)))^i.$$ 

So $g^\nu$ acts transitively on $[n] \times \{ \omega \}$ if and only if $(\eta(\omega) \cdots \eta(\sigma^{(\nu-1)}(\omega)))$ is an $n$-cycle. We can choose $\eta(\omega), \cdots, \eta(\sigma^{(\nu-2)}(\omega)) \in S_n$ to be arbitrary and $\eta(\sigma^{n-1})$ to be $\eta(\omega) \cdots \eta(\sigma^{(\nu-1)}(\omega)))^{-1}$, where $\tau$ is an $n$-cycle. Since there are $(n-1)!$ $n$-cycles in $S_n$, we have $(n!)^{\nu-1}(n-1)! = \frac{(n!)^\nu}{\nu!}$ such choices.

Let $g = \eta \sigma \in T$. Then by the latter paragraph, $\tau = \eta(\omega) \eta(\sigma(\omega)) \cdots \eta(\sigma^{(\nu-1)}(\omega))$ is an $n$-cycle. Let $\zeta \in S_n^\Omega$; then we have

$$g = g^\zeta \iff \eta \sigma = \zeta^{-1} \eta \sigma^{\zeta^{-1}} \sigma \iff \zeta = \eta \sigma^{\zeta^{-1}} \eta^{-1}$$

$$\Rightarrow \zeta(\omega) = \zeta(\sigma(\omega))^{\sigma^{-1}(\omega)} = \zeta(\sigma(\omega))^{\eta^{-1}(\sigma(\omega))\eta^{-1}(\omega)} = \cdots = \zeta(\sigma^{(\nu-1)}(\omega))^{\eta^{-1}(\sigma^{(\nu-1)}(\omega)) \cdots \eta^{-1}(\sigma(\omega))\eta^{-1}(\omega)} = \zeta(\omega)^{\tau^{-1}}.$$ 

The latter condition is satisfied if and only if $\zeta(\omega)$ commutes with $\tau$ and $\zeta(\sigma^{(\nu)}(\omega))$ are determined by the equations. Since the centralizer of $\tau$ in $S_n$ is $\langle \tau \rangle$ (\cite{7, Satz 6.5}) in we get that there are $n$ such $\zeta$. Then the size of the orbit of $\eta \sigma$ is $\frac{(n!)^\nu}{\nu!} = |T|$, so the action is transitive.
Next we consider the general case. Let $\sigma_i$ (resp. $G_i$) be the image of $\sigma$ (resp. $G$) under the map $\text{Sym}(\Omega) \to \text{Sym}(\Omega_i)$. The map $\eta \sigma \mapsto (\eta |_{\Omega_i})_i$ defines an isomorphism

$$\varphi: S_n \ltimes G \to \prod_{i=1}^r S_n \ltimes G_i,$$

that respects actions. Let $T^{(i)} = \{\eta \sigma_i \in S_n \ltimes G_i \mid \eta \sigma_i \text{ acts transitively on } [n] \times \Omega_i\}$. Then $\rho$ induces a bijection $\rho^{(i)}: T \to \prod_{i=1}^r T^{(i)}$, and it follows that $|T| = \prod_{i=1}^r |T^{(i)}| = \prod_{i=1}^r n!^{|\Omega_i|}$.

A $S_n^\Omega$-orbit $U$ of $T$ is mapped under $\varphi$ to a product $\prod_i U_i$, where $U_i$ is an $S_n^\Omega$ orbit of $T^{(i)}$. Thus $U_i = T^{(i)}$, for every $i = 1, \ldots, r$, and $U = T$.

**Theorem 5.2.** Let $n, B$ be fixed and let $K$ be a pseudo finite field of characteristic $p \geq 0$. If $(1 + 1 = 0 \Rightarrow n \text{ odd})$ and (for every $f_1, \ldots, f_r \in K[X]$ irreducible, non-associate, and such that $\nu = \sum \deg f_i \leq B$), then there exists an absolutely irreducible smooth $K$-variety $\hat{W}$ and a finite separable map $\pi: \hat{W} \to \hat{A}^n$ of degree $n!^\nu$ such that for every $a = (a_1, \ldots, a_n) \in \hat{A}^n$ for which all $f_i(t^n + a_1 t^{n-1} + \cdots + a_n)$ are separable we have

1. $\pi^{-1}(a) = 0$ or $n!^\nu$.
2. $a \in (\pi(\hat{W}(K)))$ if and only if all $f_i(t^n + a_1 t^{n-1} + \cdots + a_n)$ are irreducible.

**Proof.** Let $g(A, t) = t^n + A_1 t^{n-1} + \cdots + A_n$ be a generic polynomial, let $f = f_1 \cdots f_r$. Then, by Proposition 3.3, the associated embedding problem $\mathcal{E}(f \circ g, \hat{A}^n)$ is

$$\mathcal{E} = \mathcal{E}(f \circ g, \hat{A}^n) = (r_L: \text{Gal}(K) \to \text{Gal}(L/K), \alpha: S_n \ltimes \text{Gal}(L/K) \to \text{Gal}(L/K)).$$

(Here $r_L: \text{Gal}(K) \to \text{Gal}(L/K)$ is the restriction map.) Let $\Sigma$ be a (topological) generator of $\text{Gal}(K) \cong \hat{Z}$; then $\sigma = |\Sigma|_L$ is a generator of $\text{Gal}(L/K)$. A homomorphism $\theta: \text{Gal}(K) \to S_n \ltimes \text{Gal}(L/K)$ is a solution of $\mathcal{E}$ if and only if $\theta(\Sigma) = \eta \sigma$, for some $\eta \in S_n^\Omega$. The image of $\theta$ acts transitively on $[n] \times \Omega_i$, if and only if $\eta \sigma$ acts transitively on $[n] \times \Omega_i$, $i = 1, \ldots, r$. Thus by Lemma 5.1, there exists a unique $\ker \alpha$-inner-automorphism class of solutions, say $\Theta$, of cardinality $n!^\nu$.

Let $V = \hat{A}^n$ and $W = V_{f_{\nu} g}$. For $p = a = (a_1, \ldots, a_n) \in \hat{A}^n$ we have $f \circ g \mod p = f(g(a, t))$ and $p$ is etale in $W$ if and only if $f(g(a, t))$ is separable, if and only if all $f_i(g(a, t))$ are separable.

The action of $\text{Gal}(K)$ on the roots of $f_i(g(a, t))$ is the same as the action of $\mathcal{P}^*$ on the roots of $f_i(g(a, t))$, up to labeling of the roots, where $\mathcal{P}^* \in \mathcal{P}^*$ (by Eq. 1.1 that defines geometric solutions).

Therefore, $f_i(g(a, t))$ is irreducible if and only if the image of $\mathcal{P}^* \in \mathcal{P}^*$ acts transitively on the roots of $f_i(g(a, t))$. By Lemma 5.1 the latter holds true if and only if the action of $[n] \times \Omega_i$ is transitive. Equivalently, all $f_i(g(a, t))$ are irreducible if and only if $\mathcal{P}^* = \Theta$.

By Proposition 2.2 there exists an absolutely irreducible smooth $K$-variety $\hat{W}$ and a finite separable map $\pi: \hat{W} \to \hat{A}^n$ of degree $\ker \alpha = (n!)^\nu$ such that for $p = a = (a_1, \ldots, a_n)$ that is etale in $W$ we have $\mathcal{P}^* = \Theta$ if and only if $p \in \pi(\hat{W}(K))$ and $\pi^{-1}(a) = 0$ or $\frac{|\ker \alpha|}{n!} = n!^\nu$. This proves that $f_i(g(a, t))$ is irreducible for every $i$ if and only if $\mathcal{P}^* = \Theta$ for $p = a$ if and only if $p \in \pi(\hat{W}(K))$, and the proof is done.

We are now ready to prove Theorem 1.4.

**Proof of Theorem 1.4.** Since the assertion of Theorem 5.2 is elementary, it holds for large finite fields. In particular, there is a variety as stated.

$h(t) = f(t^n + a_1 t^{n-1} + \cdots + a_n)$ has a double root if and only if $\gcd(h, h') \neq 1$, which is a is a closed condition on the coefficients $a_1, \ldots, a_n$. Thus it contributes to the error term $O_B(q^{n-1})$.

By the Lang-Weil estimates, we have $|\hat{W}(F_q)| = q^n + O_{n,B}(q^{n-\frac{1}{2}})$ (the error term depends on the degree of $\pi$ which equals $|\ker \alpha| = (n!)^\nu$, hence depends on $n$ and $\nu \leq B$). Thus, by Theorem 5.2 there are exactly

$$\frac{|\hat{W}(K)|}{n!^\nu} + O_B(q^{n-1}) = \frac{1}{n!} q^n + O_{n,B}(q^{n-\frac{1}{2}})$$

$a \in F_q^n$ for which all $f_i(t^n + a_1 t^{n-1} + \cdots + a_n)$ are irreducible. 

□
6. Concluding remarks

The results of this paper can be generalized in few ways.

(a) In Theorem 1.4 one can consider specializing $X \mapsto g(t)$ in $f_i(X)$ such that the $f_i(g(t))$ will have a given factorization type, not only irreducible, as is done in [3]. Clearly not every factorization type of $f_i(g(t))$ can occur, since the irreducible factors are conjugated, so they have the same degree. Under this restriction one can get asymptotic for the number of such monic $g$’s of degree $n$. The only extra thing is to extend Lemma 5.1 to other partitions. For brevity, the author decided to omit the exact formulation and proof.

(b) As mentioned in the introduction, Theorem 1.2 can be extended to the family of fields that have a PAC extension satisfying (⋆). The extra ingredient needed are double embedding problems and the lifting property appearing in [3]. However since it is outside of the scope of this paper, this will be dealt in details somewhere else.

Institut für Experimentelle Mathematik, Universität Duisburg-Essen, Ellernstrasse 29, D-45326 Essen, Germany

E-mail address: barylior@math.huji.ac.il