THE SCHINZEL HYPOTHESIS FOR POLYNOMIALS

ARNAUD BODIN, PIERRE DÈBES, AND SALAH NAJIB

Abstract. The Schinzel hypothesis is a famous conjectural statement about primes in value sets of polynomials, which generalizes the Dirichlet theorem about primes in an arithmetic progression. We consider the situation that the ring of integers is replaced by a polynomial ring and prove the Schinzel hypothesis for a wide class of them: polynomials in at least one variable over the integers, polynomials in several variables over an arbitrary field, etc. We achieve this goal by developing a version over rings of the Hilbert specialization property. A polynomial Goldbach conjecture is deduced, along with a result on spectra of rational functions.

1. Introduction

The so-called Schinzel Hypothesis (H), which builds on an earlier conjecture of Bunyakovsky, was stated in [SS58]. Consider a set $\underline{P} = \{P_1, \ldots, P_s\}$ of s polynomials, irreducible in $\mathbb{Z}[y]$, of degree $\geqslant 1$ and such that

(*) there is no prime $p \in \mathbb{Z}$ dividing all values $\prod_{i=1}^{s} P_i(m)$, $m \in \mathbb{Z}$.

Hypothesis (H) concludes that there are infinitely many $m \in \mathbb{Z}$ such that $P_1(m), \ldots, P_s(m)$ are prime numbers. If true, the Schinzel hypothesis would solve many classical problems in number theory: the twin prime problem (take $\underline{P} = \{y, y+2\}$), the infiniteness of primes of the form y^2+1 (take $\underline{P} = \{y^2+1\}$), the Sophie Germain prime problem ($\underline{P} = \{y, 2y+1\}$), etc. However it is wide open except for one polynomial P_1 of degree one, in which case it is the Dirichlet theorem about primes in an arithmetic progression.

We consider the situation that the ring $\mathbb{Z}$ is replaced by a polynomial ring $R[\underline{x}]$ in $n \geqslant 1$ variables over some ring R, and "prime" is understood as "irreducible". We prove the Schinzel Hypothesis in this situation for a wide class of rings R, for example $\mathbb{Z}$, or $k[u]$ with k an arbitrary field. The infiniteness of integers m is replaced by a degree condition.

1.1. **Main result.** Specifically, let R be a Unique Factorization Domain (UFD) with fraction field K. Our assumptions include K being a field with the product formula. Definition is recalled in §4. The basic example is $K = \mathbb{Q}$. The product formula is: $\prod_p |a|_p \cdot |a| = 1$ for every $a \in \mathbb{Q}^*$, where

---

Date: February 21, 2019.

2010 *Mathematics Subject Classification.* Primary 12E05, 12E25, 12E30; Sec. 11C08, 11N80, 13Fxx.

Key words and phrases. Polynomials, Irreducibility, Specialization, Hilbertian Fields.

Acknowledgment. This work was supported in part by the Labex CEMPI (ANR-11-LABX-0007-01) and by the ANR project "LISA" (ANR-17-CE40–0023-01).

p ranges over all prime numbers, $|\cdot|_p$ is the p-adic absolute value and $|\cdot|$ is the standard absolute value. The rational function field $k(u_1,\dots,u_r)$ in $r \geqslant 1$ variables over an arbitrary field k is another example.

Given n indeterminates $x_1,\dots,x_n$, set $R[\underline{x}] = R[x_1,\dots,x_n]$ $(n \geqslant 0)$[1]. Consider $s \geqslant 1$ polynomials $P_1,\dots,P_s$, irreducible in $R[\underline{x},y]$, of degree $\geqslant 1$ in y. Set $\underline{P} = \{P_1,\dots,P_s\}$ and let $\mathcal{I}rr_n(R,\underline{P})$ be the set of polynomials $M \in R[\underline{x}]$ such that $P_1(\underline{x},M(\underline{x})),\dots,P_s(\underline{x},M(\underline{x}))$ are irreducible in $R[\underline{x}]$.

For every n-tuple $\underline{d} = (d_1,\dots,d_n)$ of integers $d_i \geqslant 0$, denote the set of polynomials $M \in R[\underline{x}]$ such that $\deg_{x_i}(M) \leqslant d_i$, $i = 1,\dots,n$, by $\mathcal{P}ol_{R,n,\underline{d}}$. It is an affine space over R: the coordinates correspond to the coefficients.

Theorem 1.1. *Assume that $n \geqslant 1$ and R is a UFD with fraction field a field K with the product formula, imperfect if K is of characteristic $p > 0$ (i.e. $K^p \neq K$). For every $\underline{d} \in (\mathbb{N}^*)^n$ such that $d_1 + \cdots + d_n \geqslant \max_{1\leqslant i\leqslant s} \deg_{\underline{x}}(P_i) + 2$, the set $\mathcal{I}rr_n(R,\underline{P})$ is Zariski-dense in $\mathcal{P}ol_{R,n,\underline{d}}$.*

In particular, the following *Schinzel hypothesis for $R[\underline{x}]$* holds true:

(**) *there exist polynomials $M \in R[\underline{x}]$ with partial degrees any suitably large integers such that $P_1(\underline{x},M(\underline{x})),\dots,P_s(\underline{x},M(\underline{x}))$ are irreducible in $R[\underline{x}]$* [2].

Irreducibility over R is a main point. As a comparison, the Hilbert specialization property provides elements $m \in K$ such that $P_1(\underline{x},m),\dots,P_s(\underline{x},m)$ are irreducible over K (provided that all $\deg_{\underline{x}}(P_i)$ are $\geqslant 1$). Developing a *Hilbert property over rings* will in fact be the core of our approach; we say more about this in §1.6.

Rings R satisfying the assumptions of Theorem 1.1 include:
(a) the ring $\mathbb{Z}$ of integers, and more generally, every ring $\mathcal{O}_k$ of integers of a number field k of class number 1,
(b) every polynomial ring $k[u_1,\dots,u_r]$ with $r \geqslant 1$ and k an arbitrary field.
(c) fields (so $R = K$) with the product formula, imperfect if of characteristic $p > 0$ e.g. $\mathbb{Q}$, $k(u_1,\dots,u_r)$ ($r \geqslant 1$, k arbitrary), their finite extensions.

As to the analog of assumption (*), it is automatically satisfied under our hypotheses (Lemma 2.1). Our approach also allows the situation that the polynomials P_i have several variables $y_1,\dots,y_m$, which leads to a multivariable Schinzel hypothesis for polynomials (Theorem 5.3).

1.2. **Examples.** Take $R[\underline{x}]$ as above and $P_i = b_i(\underline{x})y^{\rho_i} + a_i(\underline{x})$ with $\rho_i \in \mathbb{N}^*$, a_i, b_i relatively prime in $R[\underline{x}]$ (possibly in R) and such that $-a_i/b_i$ satisfies the Capelli condition that makes $b_i y^{\rho_i} + a_i$ irreducible in $K(\underline{x})[y]$, i.e. $-a_i/b_i \notin K(\underline{x})^\ell$ for every prime divisor ℓ of ρ_i and $-a_i/b_i \notin -4K(\underline{x})^4$ if $4 \mid \rho_i$. Then

(***) *there exist polynomials $M \in R[\underline{x}]$ with partial degrees any suitably large integers such that $b_1 M^{\rho_1} + a_1,\dots,b_s M^{\rho_s} + a_s$ are irreducible in $R[\underline{x}]$.*

This solves the polynomial analogs of all famous number-theoretic problems mentioned above (twin prime, etc.), and proves the Dirichlet theorem as well.

[1]For $n = 0$, we mean $R[\underline{x}] = R$, which is the original context of Schinzel's hypothesis.

[2]Up to adding $P_0 = y$ to the set $\underline{P}$, one may also require that M be irreducible in $R[\underline{x}]$.

On the other hand, Schinzel's hypothesis for $R[\underline{x}]$ obviously fails (hence Theorem 1.1 too) for $n = 1$ if $R = K$ is algebraically closed. It also fails for the finite field $R = \mathbb{F}_2$ and $\underline{P} = \{y^8 + x^3\}$: from an example of Swan [Swa62, pp.1102-1103], $M(x)^8 + x^3$ is reducible in $\mathbb{F}_2[x]$ for every $M \in \mathbb{F}_2[x]$. Interestingly enough, results of Kornblum-Landau [KL19] show that it does hold for $\mathbb{F}_q[x]$ in the degree one case and for one polynomial, i.e., in the situation of the Dirichlet theorem; see also [Ros02, Theorem 4.7]. The situation that $R = K$ is a finite field, and the related one that $R = K$ is a PAC field[3], and $n = 1$, have led to valuable variants; see [BS09], [BS12], [BW05].

1.3. **Special rings.** The special situation that $R = K$ is a field is easier, and is dealt with in §2. In the addendum to Theorem 1.1 (in §2), K is assumed to be a Hilbertian field, more exactly a *totally Hilbertian* field (definitions are in §4.1). This provides more fields than those in §1.1(c) for which Theorem 1.1 holds (with $R = K$): every abelian extension of $\mathbb{Q}$, the field $k((u_1, \dots, u_r))$ of formal power series over a field k in at least two variables, etc.

For $R = k[u]$ with k a field, we have this version of Theorem 1.1 in which the partial degrees of M are prescribed, including the degree in u.

Theorem 1.2. *With $\underline{P}$ as above and $n \geqslant 1$, assume $R = k[u]$ with k an arbitrary field. For every $\underline{d} \in (\mathbb{N}^*)^n$ satisfying $d_1 + \cdots + d_n \geqslant \max_{1 \leqslant i \leqslant s} \deg_{\underline{x}}(P_i) + 2$, there is an integer $d_0 \geqslant 1$ such that for every integer $\delta \geqslant d_0$, there is a polynomial $M \in \mathcal{I}rr_n(R, \underline{P})$ satisfying*

$$\begin{cases} \deg_{x_j}(M) = \ d_j & j = 1, \dots, n \\ \deg_u(M) = \begin{cases} \delta & \textit{if } \operatorname{char}(k) = 0 \\ p\delta & \textit{if } \operatorname{char}(k) = p > 0. \end{cases} \end{cases}$$

Identifying $k[u][x_1, \dots, x_n]$ with a polynomial ring in $n + 1$ variables, it follows that Schinzel's hypothesis holds for polynomial rings in at least 2 variables over a field of characteristic 0. In characteristic $p > 0$, a weak version holds where one degree is allowed to be any suitably large multiple of p.

In the degree one case of the Schinzel hypothesis, i.e. in the Dirichlet situation, one can get rid of this last restriction.

Theorem 1.3. *Assume that $n \geqslant 2$ and k is an arbitrary field. Let (A_1, B_1), $\dots$, (A_s, B_s) be s pairs of nonzero relatively prime polynomials in $k[\underline{x}]$. There is an integer $d_0 \geqslant 1$ with this property: for all integers $d_1, \dots, d_n$ larger than d_0, there exists an irreducible polynomial $M \in k[\underline{x}]$ such that $A_i + B_i M$ is irreducible in $k[\underline{x}]$, $i = 1, \dots, s$, and $\deg_{x_j}(M) = d_j$, $j = 1, \dots, n$.*

To our knowledge, this was unknown, even for $s = 1$. When k is infinite, we have a stronger version, not covered either by Theorems 1.1 and 1.2. Let $\overline{k}$ denote an algebraic closure of k.

[3]A field K is PAC if every curve over K has infinitely many K-rational points. The first examples of PAC fields were ultraproducts of finite fields.

Theorem 1.4. *Assume $n \geqslant 2$ and k is an infinite field. Let $A, B \in k[\underline{x}]$ be two nonzero relatively prime polynomials and $\mathcal{I}rr_n(k, A, B)$ the set of polynomials $M \in k[\underline{x}]$ such that $A+BM$ is irreducible in $k[\underline{x}]$. For every $\underline{d} \in (\mathbb{N}^*)^n$, $\mathcal{I}rr_n(\overline{k}, A, B)$ contains a nonempty Zariski open subset of $\mathcal{P}ol_{k,n,\underline{d}}(k)$.*

1.4. **The Goldbach problem.** The analog of the Goldbach conjecture for a polynomial ring $R[\underline{x}]$ is that every nonconstant polynomial $\mathcal{Q} \in R[\underline{x}]$ is the sum of two irreducible polynomials $F, G \in R[\underline{x}]$ with $\deg(F) \leqslant \deg(\mathcal{Q})$ (and so $\deg(G) \leqslant \deg(\mathcal{Q})$ too). Pollack [Pol11] showed it in the 1-variable case when R is a Noetherian integral domain with infinitely many maximal ideals, or, if $R = S[u]$ with S an integral domain. His method relies on a clever use of the Eisenstein criterion.

Finding Goldbach decompositions for $\mathcal{Q} \in R[\underline{x}]$ ($n \geqslant 1$) corresponds to the special situation of the degree 1 case of the Schinzel hypothesis for which $\underline{P} = \{P_1, P_2\}$ with $P_1 = -y$ and $P_2 = y + \mathcal{Q}$. We obtain this result.

Corollary 1.5. *Let R be a ring as in Theorem 1.1. Every nonconstant polynomial $\mathcal{Q} \in R[\underline{x}]$ is the sum of two irreducible polynomials $F, G \in R[\underline{x}]$ with $F = a + bx_1^{d_1} \cdots x_n^{d_n}$ $(a, b \in R)$ a binomial of degree $d_1 + \cdots + d_n \leqslant \deg(\mathcal{Q})$.*

One can even take $d_1 + \cdots + d_n = 1$ when $R = K$ is a Hilbertian field, or when $n \geqslant 2$ and $R = K$ is an infinite field (the latter was already known from [BDN09, Corollary 4.3(2)]). On the other hand, the Goldbach conjecture fails for $\mathbb{F}_2[x]$ and $\mathcal{Q}(x) = x^2 + x$ (note that $x^2 + x + 1$ is the only irreducible polynomial in $\mathbb{F}_2[x]$ of degree 2). From Corollary 1.5 however, it holds true for $\mathbb{F}_q[x, y]$ if condition $\deg(F) \leqslant \deg(\mathcal{Q})$ is replaced by $\deg_x(F) \leqslant \deg_x(\mathcal{Q})$.

1.5. **Spectra.** The following result uses Theorem 1.3 as a main ingredient.

Corollary 1.6. *Assume that $n \geqslant 2$ and k is an arbitrary field. Let $\mathcal{S} \subset k$ be a finite subset, $a_0 \in \overline{k} \setminus \mathcal{S}$, separable over k and $V \in k[\underline{x}]$ a nonzero polynomial. Then, for all suitably large integers $d_1, \ldots, d_n$ (larger than some d_0 depending on $\mathcal{S}$, a_0, V), there is a polynomial $U \in k[\underline{x}]$ such that:*
(a) *$U(\underline{x}) - aV(\underline{x})$ is reducible in $k[\underline{x}]$ for every $a \in \mathcal{S}$,*
(b) *$U(\underline{x}) - a_0V(\underline{x})$ is irreducible in $k(a_0)[\underline{x}]$ of degree* $\max(\deg(U), \deg(V))$,
(c) $\deg_{x_i}(U) = d_i$, *$i = 1, \ldots, n$.*

If $\mathcal{S} \neq k$, e.g. if k is infinite, a_0 can be chosen in k itself.

A more precise version of Corollary 1.6, given in §5.5, shows that one can even prescribe all irreducible factors but one of each polynomial $U(\underline{x}) - aV(\underline{x})$, $a \in \mathcal{S}$, provided that these factors satisfy some standard condition.

If k is algebraically closed, the irreducibility condition (b) implies that the rational function U/V is *indecomposable* [Bod08, Theorem 2.2]; "indecomposable" means that U/V cannot be written $h \circ H$ with $h \in k(u)$ and $H \in k(\underline{x})$ with $\deg(h) \geqslant 2$. The set of all $a \in k$ such that $U(\underline{x}) - aV(\underline{x})$ is reducible in $k[\underline{x}]$ is called the *spectrum* of U/V and the indecomposability condition equivalent to the spectrum being finite. Corollary 1.6 rephrases to conclude that given $\mathcal{S}$ and V as above, indecomposable rational functions $U/V \in k(\underline{x})$ exist with a spectrum containing $\mathcal{S}$ and satisfying (c). See [Naj04] [Naj05] for the special case $V = 1$ and [BDN17, §3.1.1] for further results.

1.6. **Hilbertian rings.** Except for Theorem 1.4 for which we use geometrical tools (§3), we follow a Hilbert like specialization approach.

Given an irreducible polynomial $F(\underline{\lambda}, \underline{x}) \in R[\underline{\lambda}, \underline{x}]$ with $\deg_{\underline{x}}(F) \geqslant 1$, the Hilbert property provides specializations $\lambda_1^*, \ldots, \lambda_r^* \in K$ of the indeterminates from $\underline{\lambda}$ such that $F(\lambda_1^*, \ldots, \lambda_r^*, \underline{x})$ is irreducible in $K[\underline{x}]$ (§4.1).

As suggested above and detailed in §2, the challenge for our purpose is to make it work *over the ring* R, i.e., to be able to find $\lambda_1^*, \ldots, \lambda_r^*$ in R such that $F(\lambda_1^*, \ldots, \lambda_r^*, \underline{x})$ is irreducible in $R[\underline{x}]$. A problem however is that this is false in general, even with $R = \mathbb{Z}$. Take $F = (\lambda^2 - \lambda)\, x + (\lambda^2 - \lambda + 2)$ in $\mathbb{Z}[\lambda, x]$; for every $\lambda^* \in \mathbb{Z}$, $F(\lambda^*, \underline{x})$ is divisible by 2, hence reducible in $\mathbb{Z}[x]$.

To remedy this problem, we develop the notion of *Hilbertian ring* introduced in [FJ08, §13.4]. The defining property is that, for separable polynomials $F(\underline{\lambda}, x)$ in the one variable x, tuples $(\lambda_1^*, \ldots, \lambda_r^*)$ can be found with coordinates in the ring R and satisfying the specialization property over K.

Our approach to reach irreducibility over R can be summarized as follows. It may be of interest for the sole sake of the Hilbertian field theory.

(*Hilbert sections 4 and 5*) Assume that K is of characteristic 0, or K is of characteristic $p > 0$ and imperfect (the *imperfectness assumption*).

(a) We extend the property of Hilbertian rings to all irreducible polynomials $F(\underline{\lambda}, \underline{x})$ (not just the separable ones $F(\underline{\lambda}, x)$), and show in fact a stronger version: $\lambda_1^*, \ldots, \lambda_r^*$ can be chosen pairwise relatively prime (Prop.4.2); and for $R = k[u]$, their degrees in u can be prescribed off a finite range (Theorem 4.8).

(b) We show that if K is a field with the product formula, then R is a Hilbertian ring (Theorem 4.6); this improves on [FJ08, Prop.13.4.1] where the assumption is that R is finitely generated over $\mathbb{Z}$, or over $k[u]$ for some field k.

(c) For R both a UFD and a Hilbertian ring, we show that our polynomials $F(\underline{\lambda}, \underline{x})$, due to their structure, satisfy the specialization property *over the ring* R, and we prove Theorem 1.1 in this situation (§5).

The imperfectness assumption relates to a classical subtlety in positive characteristic. There are two notions of *Hilbertian fields*, depending on whether the specialization property is requested for all irreducible polynomials or only for the separable ones. We follow [FJ08] and use the name *Hilbertian* for the weaker (the latter), and we say *totally Hilbertian* for the stronger (precise definitions are in §4.1). They are equivalent under the imperfectness assumption [Uch80] [FJ08, Proposition 12.4.3].

Final note. The original Schinzel hypothesis has also appeared in Arithmetic Geometry, notably around the question of whether, for appropriate varieties over a number field k, the Brauer-Manin obstruction is the only obstruction to the Hasse principle: if rational points exist locally (over all completions of k), they should exist globally (over k). In 1979, Colliot-Thélène and Sansuc

[CTS82] noticed that this is true for a large family of conic bundle surfaces over $\mathbb{P}^1_{\mathbb{Q}}$ if one assumes Schinzel's hypothesis. This conjectural statement has become since a working hypothesis of the area. See for example [HW16] for some last developments. Although the number field environment seems closely tied to the question, it could be interesting to investigate the potential use of our polynomial version of the Schinzel hypothesis to some similar questions over appropriate fields like rational function fields.

The paper is organized as follows. The strategy is detailed in §2. §3 is devoted to the geometric case that $R = k[\underline{x}]$ with $n \geqslant 2$ and k is an infinite field; Theorem 1.4 is proved. §4 is the Hilbert part. The main results from §1 (other than Theorem 1.4) are finally proved in §5.

2. General strategy

Throughout the paper, R is a UFD with fraction field K. Recall that a polynomial with coefficients in R is said to be *primitive w.r.t.* R if its coefficients are relatively prime in R.

All indeterminates are algebraically independent over $\overline{K}$.

Let $\underline{x} = (x_1, \dots, x_n)$ $(n \geqslant 1)$ and $\underline{\lambda} = (\lambda_0, \lambda_1, \dots, \lambda_\ell)$ $(\ell \geqslant 1)$ be two tuples of indeterminates and let $\underline{Q} = (Q_0, Q_1, \dots, Q_\ell)$ with $Q_0 = 1$ be a $(\ell+1)$-tuple of nonzero polynomials in $R[\underline{x}]$, distinct up to multiplicative constants in $K^\times$. Set

$$M(\underline{\lambda}, \underline{x}) = \textstyle\sum_{i=0}^{\ell} \lambda_i Q_i(\underline{x}).$$

Consider a set $\underline{P} = \{P_1, \dots, P_s\}$ of s polynomials

$$P_i(\underline{x}, y) = P_{i\rho_i}(\underline{x})\, y^{\rho_i} + \cdots + P_{i1}(\underline{x}) y + P_{i0}(\underline{x}),$$

irreducible in $R[\underline{x}, y]$ and of degree $\rho_i \geqslant 1$ in y, $i = 1, \dots, s$. Each polynomial $P_i(\underline{x}, y)$ is irreducible in $K(\underline{x})[y]$ and is primitive w.r.t. $R[\underline{x}]$.

Finally set, for $i = 1, \dots, s$,

$$F_i(\underline{\lambda}, \underline{x}) = P_i(\underline{x}, M(\underline{\lambda}, \underline{x})) = P_i(\underline{x}, \textstyle\sum_{j=0}^{\ell} \lambda_j Q_j(\underline{x})).$$

In the case $\rho_i = 1$, i.e., $P_i = A_i(\underline{x}) + B_i(\underline{x}) y$, the polynomial F_i rewrites

$$F_i(\underline{\lambda}, \underline{x}) = A_i(\underline{x}) + B_i(\underline{x}) \left(\textstyle\sum_{j=0}^{\ell} \lambda_j Q_j(\underline{x}))\right).$$

Lemma 2.1. (a) *Each polynomial $F_i(\underline{\lambda}, \underline{x})$ is irreducible in $R[\underline{\lambda}, \underline{x}]$ and of degree $\geqslant 1$ in $\underline{x}$. Furthermore, if $\deg_y(P_i) = 1$, $F_i(\underline{\lambda}, \underline{x})$ is irreducible in $\overline{K}[\underline{\lambda}, \underline{x}]$.*
(b) *If R is infinite and $\Pi = \prod_{i=1}^{s} P_i$, there is no irreducible polynomial $p \in R[\underline{x}]$ dividing all polynomials $\Pi(\underline{x}, M(\underline{x}))$ with $M \in R[\underline{x}]$.*

Note that (b) fails if R is finite: with $R = \mathbb{F}_2$ and $\underline{P} = \{x, x+1\}$, the polynomial x divides all polynomials $M(x)(M(x)+1)$ $(M \in \mathbb{F}_2[x])$.

Proof. (a) Fix an integer $i \in \{1, \dots, s\}$. By assumption, the polynomial $P_i(\underline{x}, \lambda_0)$ is irreducible in $R[\underline{x}, \lambda_0]$. It is also irreducible in the bigger ring $R[\underline{x}, \underline{\lambda}]$. Consider the ring automorphism $R[\underline{x}, \underline{\lambda}] \to R[\underline{x}, \underline{\lambda}]$ that is the identity on $R[\underline{x}, \lambda_1, \dots, \lambda_\ell]$ and maps λ_0 to the polynomial $\lambda_0 + \sum_{i=1}^{\ell} \lambda_i Q_i(\underline{x})$.

The polynomial $F_i(\underline{\lambda}, \underline{x})$ is the image of $P_i(\underline{x}, \lambda_0)$ by this isomorphism. Hence it is irreducible in $R[\underline{x}, \underline{\lambda}]$.

To see that $\deg_{\underline{x}}(F_i) \geqslant 1$, write F_i as a polynomial in λ_1. The leading coefficient is $P_{i\rho_i}(\underline{x})Q_1(\underline{x})^{\rho_i}$; it is of positive degree in $\underline{x}$ since Q_1 is by assumption. This proves that $\deg_{\underline{x}}(F_i) \geqslant 1$.

In the case $\rho_i = 1$, irreducibility of $F_i(\underline{\lambda}, \underline{x})$ in $\overline{K}[\underline{x}, \underline{\lambda}]$ follows from the above case, applied with R taken to be $\overline{K}$, and the fact that the polynomial $P_i(\underline{x}, y) = A_i(\underline{x}) + B_i(\underline{x})y$ is irreducible in $\overline{K}[\underline{x}, y]$. Namely $P_i(\underline{x}, y)$ is of degree 1 in y and is primitive w.r.t. $\overline{K}[\underline{x}]$. Primitivity follows from the fact that, as A_i and B_i are relatively prime in $R[\underline{x}]$, then
- they are relatively prime in $K[\underline{x}]$ (an application of Gauss's lemma), and,
- they are relatively prime in $\overline{K}[\underline{x}]$. For lack of reference for this last point, we provide below a quick argument.

Prove by induction on n that for every field K, for every nonzero $A, B \in K[\underline{x}]$, if A and B have a common divisor $D \in \overline{K}[\underline{x}]$ with $\deg(D) > 0$, they have a common divisor $C \in K[\underline{x}]$ with $\deg(C) > 0$. The case $n = 1$ follows from the Bézout theorem. Then, for $n \geqslant 2$, if D is as in the claim, we may assume that $\deg_{(x_2,\dots,x_n)}(D) > 0$. Observe then that D divides A and B in $\overline{K(x_1)}[x_2, \dots, x_n]$. By induction A and B have a common divisor $C \in K(x_1)[x_2, \dots, x_n]$ with $\deg_{(x_2,\dots,x_n)}(C) > 0$. Using Gauss's lemma, one easily constructs a polynomial $C_0 = c(x_1)C \in K[x_1][x_2, \dots, x_n]$ (with $c(x_1) \in K[x_1]$) dividing both A and B in $K[x_1][x_2, \dots, x_n]$.

(b) If the claim is false, there is an irreducible polynomial $p \in R[\underline{x}]$ such that $\Pi(\underline{x}, M(\underline{x})) = 0$ in the quotient ring $R[\underline{x}]/(p(\underline{x}))$ for all $M \in R[\underline{x}]$. But $R[\underline{x}]/(p(\underline{x}))$ is an integral domain, and it is infinite. Indeed, if p is nonconstant, say $d = \deg_{x_1}(p) \geqslant 1$, the elements $\sum_{i=0}^{d-1} r_i x_1^i$ with $r_0, \dots, r_{d-1} \in R$ are infinitely many different elements in $R[\underline{x}]/(p(\underline{x}))$; and if $p \in R$, then the quotient ring is $R/(p)[\underline{x}]$, which is infinite too. Conclude that the polynomial $\Pi(\underline{x}, y)$ which has infinitely many roots in $R[\underline{x}]/(p(\underline{x}))$ is zero in the ring $(R[\underline{x}]/(p(\underline{x}))[y]$. As this ring is an integral domain, there is an index $i \in \{1, \dots, s\}$ such that $P_i(\underline{x}, y)$ is zero in $(R[\underline{x}]/(p(\underline{x}))[y]$. This contradicts $P_i(\underline{x}, y)$ being primitive w.r.t. $R[\underline{x}]$. □

Denote the set of polynomials $F_1, \dots, F_s$ by $\underline{F}$ and consider the subset

$$H_R(\underline{F}) \subset R^{\ell+1},$$

of all $(\ell+1)$-tuples $\underline{\lambda}^* = (\lambda_0^*, \dots, \lambda_\ell^*)$ such that $F_i(\underline{\lambda}^*, \underline{x})$ is irreducible in $R[\underline{x}]$, for each $i = 1, \dots, s$. It can be equivalently viewed as the set of all polynomials of the form $m(\underline{x}) = \sum_{j=0}^{\ell} m_j Q_j(\underline{x})$ $(m_0, \dots, m_\ell \in R)$ such that $P_i(\underline{x}, m(\underline{x}))$ is irreducible in $R[\underline{x}]$, $i = 1, \dots, s$.

Theorems 1.1 – 1.3 will be obtained *via* the following special case of our situation: for a given $\underline{d} = (d_1, \dots, d_n) \in (\mathbb{N}^*)^n$, the polynomials Q_i are all the monic monomials $Q_0, Q_1, \dots, Q_{N_{\underline{d}}}$ in $\mathcal{P}ol_{R,n,\underline{d}}$. The polynomial

$$M_{\underline{d}}(\underline{\lambda}, \underline{x}) = \sum_{i=0}^{N_{\underline{d}}} \lambda_i Q_i(\underline{x})$$

is then the *generic polynomial in n variables of i-th partial degree d_i*, $i = 1, \ldots, n$, and Theorems 1.2 and 1.3 are about the set

$$H_R(\underline{F}) = \mathcal{I}rr_n(R, \underline{P}) \cap \mathcal{P}ol_{R,n,\underline{d}}$$

For example, anticipating on the reminder on Hilbertian fields in §4.1, we can immediately prove this statement, already alluded to in §1.

Addendum to Theorem 1.1. *The set $\mathcal{I}rr_n(R, \underline{P})$ is Zariski-dense in $\mathcal{P}ol_{R,n,\underline{d}}$ for every $\underline{d} \in (\mathbb{N}^*)^n$, in each of these two situations:*
(a) *$R = K$ is a totally Hilbertian field,*
(b) *$R = K$ is a Hilbertian field and $\deg_y(P_1) = \ldots = \deg_y(P_s) = 1$.*

Proof. By definition, $H_K(\underline{F})$ is a *Hilbert subset*. Furthermore, from Remark 5.5, it contains a *separable Hilbert subset* if $\deg_y(P_1) = \ldots = \deg_y(P_s) = 1$. It follows from the definitions that $H_K(\underline{F})$ is Zariski-dense in $K^{N_{\underline{d}}+1} = \mathcal{P}ol_{K,n,\underline{d}}$ in both situations. One does not even need to assume that $d_1 + \cdots + d_n \geqslant \max_{1 \leqslant i \leqslant s} \deg_{\underline{x}}(P_i) + 2$; the statement holds for example for $d_1 = \ldots = d_n = 1$. $\square$

When R is more generally a ring, we have to further guarantee that:
- the Hilbert subset $H_K(\underline{F})$ contains $(\ell + 1)$-tuples with coordinates in R,
- for some of these $(\ell+1)$-tuples $\underline{\lambda}^*$, the corresponding polynomials $F_i(\underline{\lambda}^*, \underline{x})$ are primitive w.r.t. R, and so irreducible in $R[\underline{x}]$.

For $R = k[u_1, \ldots, u_r]$, polynomials in $R[\underline{x}]$ can be viewed as polynomials in at least two variables over the field k. We explain in §3 how geometric specialization techniques can be used, if k is also infinite. For more general rings R, more arithmetic specialization tools are needed, which we develop in §4. The specific argument for the primitivity point is given in §5.1; it takes advantage of the special form of the polynomial F_i and, as mentioned before, cannot extend to arbitrary polynomials $F \in R[\underline{\lambda}, \underline{x}]$.

3. The geometric part

Lemma 3.1 is our specialization tool here. Based on results of Bertini, Krull and Noether, it is in the same vein as those from [BDN09], [BDN17]. We prove it in §3.1, then deduce Theorem 1.4 in §3.2.

3.1. **The specialization lemma.**

Notation is as in §2. Consider the special case of the general situation from §2 for which $s = 1 = \rho_1$. One degree 1 polynomial $P(\underline{x}, y)$ is given: $P(\underline{x}, y) = A(\underline{x}) + B(\underline{x})y$ with $A, B \in R[\underline{x}]$ two nonzero relatively prime polynomials, or $P(\underline{x}, y) = y$. We then have:

$$\begin{aligned} F(\underline{\lambda}, \underline{x}) &= A(\underline{x}) + B(\underline{x}) \left(\textstyle\sum_{j=0}^{\ell} \lambda_j Q_j(\underline{x}) \right) \\ &= A(\underline{x}) + \lambda_0 B(\underline{x}) + \lambda_1 B(\underline{x}) Q_1(\underline{x}) + \cdots + \lambda_\ell B(\underline{x}) Q_\ell(\underline{x}) \end{aligned}$$

Lemma 3.1. *Assume that $n \geqslant 2$, $R = K$ is an algebraically closed field and the following holds (which implies $\ell \geqslant 1$):*

(a) *there is an index $i_0 \in \{1, \ldots, \ell\}$ such that*
- $\deg(Q_{i_0}) \not\equiv 0$ *modulo p if* $\mathrm{char}(K) = p > 0$,

- $\deg(Q_{i_0}) \neq 0$ *if* $\mathrm{char}(K) = 0$.

(b) *there is* <u>no</u> *polynomial* $\chi \in K[\underline{x}]$ *such that* $A, B, Q_1, \ldots, Q_\ell \in K[\chi]$.

Then the set $H_K(F)$ *of all* $(\ell+1)$*-tuples* $\underline{\lambda}^* = (\lambda_0^*, \ldots, \lambda_\ell^*)$ *such that* $F(\underline{\lambda}^*, \underline{x})$ *is irreducible in* $K[\underline{x}]$ *contains a nonempty Zariski open subset of* $K^{\ell+1}$.

Remark 3.2. Assumptions (a) and (b) can probably be improved but the following examples show they cannot be totally removed. In each of them, $F(\underline{\lambda}, \underline{x})$ is reducible in $\overline{K(\underline{\lambda})}[\underline{x}]$ and every non-trivial factorization yields a Zariski dense subset of $\underline{\lambda}^* \in K^{\ell+1}$ such that $F(\underline{\lambda}^*, \underline{x})$ is reducible in $K[\underline{x}]$.

- If $A, B, Q_1, \ldots, Q_\ell \in K[\chi]$ for some $\chi \in K[\underline{x}]$, one can write $F(\underline{\lambda}, \underline{x}) = h(\chi)$ with $h \in \overline{K(\underline{\lambda})}[u]$. If $\deg(h) \geqslant 2$, h is reducible and so is $F(\underline{\lambda}, \underline{x})$ in $\overline{K(\underline{\lambda})}[\underline{x}]$.
- For $A = x_1^2$, $B = -x_2^2$, $\ell = 1$ and $Q_0 = Q_1 = 1$, we have
$$F(\underline{\lambda}, \underline{x}) = x_1^2 - \lambda_0 x_2^2 - \lambda_1 x_2^2 = (x_1 - \sqrt{\lambda_0 + \lambda_1}\, x_2)(x_1 + \sqrt{\lambda_0 + \lambda_1}\, x_2).$$
- If $\mathrm{char}(K) = p > 0$, for $A = x_1^p$, $B = x_2^p$, $\ell = 1$, $Q_0 = 1$, $Q_1 = x_2^p$, we have
$$F(\underline{\lambda}, \underline{x}) = x_1^p + \lambda_0 x_2^p + \lambda_1 x_2^{2p} = (x_1 + \lambda_0^{1/p} x_2 + \lambda_1^{1/p} x_2^2)^p.$$

Proof. Assume that the conclusion of Lemma 3.1 is false. From the Bertini-Noether theorem [FJ08, Prop. 9.4.3], $F(\underline{\lambda}, \underline{x})$ is reducible in $\overline{K(\underline{\lambda})}[\underline{x}]$. Clearly then polynomials $F(\underline{x}, \underline{\lambda}^*)$ are reducible in $K[\underline{x}]$ for all $\underline{\lambda}^* \in K^{\ell+1}$ such that $\deg(F(\underline{x}, \underline{\lambda}^*)) = \deg_{\underline{x}}(F)$. The Bertini-Krull theorem [Sch00, Theorem 37] then yields that one of the following conditions holds:

1. $\mathrm{char}(K) = p > 0$ and $F(\underline{\lambda}, \underline{x}) \in K[\underline{\lambda}, \underline{x}^p]$ with $\underline{x}^p = (x_1^p, \ldots, x_n^p)$,
2. there exist $\phi, \psi \in K[\underline{x}]$ with $\deg_{\underline{x}}(F) > \max(\deg(\phi), \deg(\psi))$ satisfying the following: there is an integer $\delta \geqslant 1$ and $\ell + 2$ polynomials $H, H_0, H_1, \ldots, H_\ell \in K[u, v]$ homogeneous of degree δ such that

$$\begin{cases} A(\underline{x}) = H(\phi(\underline{x}), \psi(\underline{x})) = \sum_{i=0}^{\delta} h_i\, \phi(\underline{x})^i \psi(\underline{x})^{\delta-i} \\ B(\underline{x}) = H_0(\phi(\underline{x}), \psi(\underline{x})) = \sum_{i=0}^{\delta} h_{0i}\, \phi(\underline{x})^i \psi(\underline{x})^{\delta-i} \\ BQ_1(\underline{x}) = H_1(\phi(\underline{x}), \psi(\underline{x})) = \sum_{i=0}^{\delta} h_{1i}\, \phi(\underline{x})^i \psi(\underline{x})^{\delta-i} \\ \qquad\vdots \\ BQ_\ell(\underline{x}) = H_\ell(\phi(\underline{x}), \psi(\underline{x})) = \sum_{i=0}^{\delta} h_{\ell i}\, \phi(\underline{x})^i \psi(\underline{x})^{\delta-i} \end{cases}$$

The rest of the proof consists in ruling out both conditions (1) and (2).

For condition (1), this readily follows from the assumption on $\deg(Q_{i_0})$: if $\mathrm{char}(k) = p > 0$, the polynomials B and BQ_{i_0} cannot be both in $K[\underline{x}^p]$.

Assume condition (2) holds. Note that the polynomials ϕ and ψ are relatively prime in $K[\underline{x}]$ as a consequence of A, B being relatively prime in $K[\underline{x}]$. We claim that the two conditions

$$\begin{cases} B(\underline{x}) = H_0(\phi(\underline{x}), \psi(\underline{x})) \\ BQ_{i_0}(\underline{x}) = H_{i_0}(\phi(\underline{x}), \psi(\underline{x})) \end{cases}$$

lead to this conclusion: there is $(\beta, \gamma) \in K^2$ such that $\beta\phi(\underline{x}) + \gamma\psi(\underline{x}) = 1$. We show it by induction on the common degree δ of H_0 and H_{i_0}.

For $\delta = 1$, write $B = a\phi + b\psi$ and $BQ_{i_0} = a'\phi + b'\psi$ with $a, b, a', b' \in K$. If $\deg(B) = 0$, then $a\phi + b\psi \in K \setminus \{0\}$ and the claim is established. Assume

$\deg(B) > 0$. If $ab' - a'b \neq 0$, any irreducible factor π of B divides $a\phi + b\psi$ and $a'\phi + b'\psi$, hence divides both ϕ and ψ in $K[\underline{x}]$, which contradicts ϕ and ψ being relatively prime. As there is at least one such factor π, we have $(a, b) = \kappa(a', b')$ for some nonzero $\kappa \in K$. It follows that $B = \kappa BQ_{i_0}$ and $\deg(Q_{i_0}) = 0$. This contradicts our assumption. Hence the claim is established for $\delta = 1$.

Assume the claim is proved for $\delta \geqslant 1$ and that

$$\begin{cases} B = \prod_{j=1}^{\delta+1}(a_j\phi + b_j\psi) \\ BQ_{i_0} = \prod_{j=1}^{\delta+1}(a'_j\phi + b'_j\psi) \end{cases}$$

for some $(\delta+1)$-tuples $((a_1, b_1), \ldots, (a_{\delta+1}, b_{\delta+1}))$ and $((a'_1, b'_1), \ldots, (a'_{\delta+1}, b'_{\delta+1}))$ with components in K^2.

If $\deg(B) = 0$, all polynomials $a_j\phi + b_j\psi$, $j = 1, \ldots, \delta+1$, are of degree 0. Hence there exists $(\beta, \gamma) \in K^2$ such that $\beta\phi + \gamma\psi = 1$. Assume $\deg(B) > 0$. As above in the case $\delta = 1$, use an irreducible factor of B in $K[\underline{x}]$ to conclude that there exist two indices j, j' such that this irreducible factor divides both $a_j\phi + b_j\psi$ and $a'_{j'}\phi + b'_{j'}\psi$. We may assume that $j = j' = \delta + 1$. As above in the case $\delta = 1$, it follows from ϕ, ψ relatively prime in $K[\underline{x}]$ that

$$a_{\delta+1}\phi + b_{\delta+1}\psi = \kappa(a'_{\delta+1}\phi + b'_{\delta+1}\psi)$$

for some nonzero $\kappa \in K$. Consider the polynomial $B_1 = B/(a_{\delta+1}\phi + b_{\delta+1}\psi)$. It is nonzero and we have

$$\begin{cases} B_1 = \prod_{j=1}^{\delta}(a_j\phi + b_j\psi) \\ \kappa B_1 Q_{i_0} = \prod_{j=1}^{\delta}(a'_j\phi + b'_j\psi) \end{cases}$$

From the induction hypothesis, applied to B_1 and $\kappa B_1 Q_{i_0}$, there is $(\beta, \gamma) \in K^2$ such that $\beta\phi + \gamma\psi = 1$. This completes the proof of our claim.

Fix $(\beta, \gamma) \in K^2$ such that $\beta\phi + \gamma\psi = 1$. Pick $(a, b) \in K^2$ such that $a\gamma - \beta b \neq 0$ and set $\chi = a\phi + b\psi$. We have $\deg(\chi) > 0$. Then $K\phi + K\psi = K\chi + K$ and so $A, B, BQ_1, \ldots, BQ_\ell$ are in $K[\chi]$. It follows that $A, B, Q_1, \ldots, Q_\ell$ are in $K[\chi]$ too. Here is an argument. Fix $i \in \{1, \ldots, \ell\}$. Since $B, BQ_i \in K[\chi]$, Q_i writes $Q_i = (p/q)(\chi)$ for some $p, q \in K[t]$ relatively prime. But then there exists $u, v \in K[t]$ such that $u(\chi)p(\chi) + v(\chi)q(\chi) = 1$. Since $q(\chi)$ divides $p(\chi)$ in $K[\underline{x}]$, we have $\deg(q) = 0$. Hence $Q_i \in K[\chi]$. □

3.2. **Proof of Theorem 1.4.** Assume $n \geqslant 2$, fix an infinite field k, two nonzero relatively prime polynomials A, B in $k[\underline{x}]$ and a n-tuple $\underline{d} \in (\mathbb{N}^*)^n$. As explained in §2, consider the special case of Lemma 3.1 for which the polynomials Q_i are all the monomials $Q_0, \ldots, Q_{N_{\underline{d}}}$ in $\mathcal{P}ol_{k,n,\underline{d}}$ (with $Q_0 = 1$). We then have $F(\underline{\lambda}, \underline{x}) = A(\underline{x}) + B(\underline{x})M_{\underline{d}}(\underline{\lambda}, \underline{x})$ with $M_{\underline{d}} = \sum_{i=0}^{N_{\underline{d}}} \lambda_i Q_i$ the generic polynomial in n variables of partial degree d_i in x_i, $i = 1, \ldots, n$.

Lemma 3.1 concludes that $H_k(F) = \mathcal{I}rr_n(\overline{k}, A, B) \cap \mathcal{P}ol_{k,n,\underline{d}}(\overline{k})$ contains a nonempty Zariski open subset of $\mathcal{P}ol_{k,n,\underline{d}}(\overline{k})$. As k is infinite, the set $\mathcal{I}rr_n(\overline{k}, A, B) \cap \mathcal{P}ol_{k,n,\underline{d}}(k)$ also contains a nonempty Zariski open subset of $\mathcal{P}ol_{k,n,\underline{d}}(k)$. This proves Theorem 1.4.

Remark 3.3. (a) If k is finite however, non emptyness of $\mathcal{I}rr_n(k,A,B)$ cannot be guaranteed at this stage: each finite set $\mathcal{I}rr_n(k,A,B)\cap \mathcal{P}ol_{k,n,\underline{d}}(k)$ ($\underline{d}\in (\mathbb{N}^*)^n$) could be covered by an hypersurface. For infinite fields, Theorem 1.4 clearly covers Theorem 1.3. We will use a different method, in §4, to prove Theorem 1.3 for finite fields (which will also reprove the infinite case).
(b) Lemma 3.1 can be used in other situations. For example, let $A,B,C\in K[\underline{x}]$ be nonzero polynomials, with A, B relatively prime and $C\in K[\underline{x}]$ distinct from A, B, up to multiplicative constants in $K^\times$. Assume hypotheses (a) and (b) of Lemma 3.1 respectively hold for $Q_{i_0}=C$ and for A,B,C. Lemma 3.1 shows that the set of $(\lambda,\mu)\in K^2$ such that $A+B(\lambda C+\mu)$ is irreducible in $K[\underline{x}]$ contains a nonempty Zariski open subset of $\mathbb{A}^2_K$.

4. The Hilbert side

This section introduces the notion of Hilbertian ring and establishes some corresponding specialization tools, which will be important ingredients of the proofs of the main theorems in §5.

4.1. **Basics from the Hilbertian field theory.** We recall the basic definitions and refer to chapters 12 and 13 of [FJ08] for more. Other classical references include [Sch82], [Sch00], [Lan83].

Consider a field K and two tuples $\underline{\lambda}=(\lambda_1,\ldots,\lambda_r)$ and $\underline{x}=(x_1,\ldots,x_n)$ ($r\geqslant 1$, $n\geqslant 1$) of indeterminates. Given m polynomials $f_1(\underline{\lambda},\underline{x}),\ldots,f_m(\underline{\lambda},\underline{x})$ ($m\geqslant 1$) in $\underline{x}$ with coefficients in $K(\underline{\lambda})$, irreducible in the ring $K(\underline{\lambda})[\underline{x}]$ and a polynomial $g\in K[\underline{\lambda}]$, $g\neq 0$, consider the set

$$H_K(f_1,\ldots,f_m;g)=\left\{\underline{\lambda}^*\in K^r \;\middle|\; \begin{array}{l} f_i(\underline{\lambda}^*,\underline{x}) \text{ irreducible in } K[\underline{x}]\\ \text{for each } i=1,\ldots,m,\\ \text{and } g(\underline{\lambda}^*)\neq 0.\end{array}\right\}$$

Call $H_K(f_1,\ldots,f_m;g)$ a *Hilbert subset of* K^r. If in addition $n=1$ and each f_i is separable in x (i.e., f_i has no multiple root in $\overline{K(\underline{\lambda})}$), call $H_K(f_1,\ldots,f_m;g)$ a *separable Hilbert subset of* K^r. The field K is called *Hilbertian* if every separable Hilbert subset of K^r is nonempty and *totally Hilbertian* if every Hilbert subset of K^r is nonempty ($r\geqslant 1$). Equivalently, "nonempty" can be replaced by "Zariski-dense in K^r" in the definitions. As recalled earlier, a field K is totally Hilbertian if and only if it is Hilbertian and the imperfectness condition holds: K is imperfect if of characteristic $p>0$.

Classical Hilbertian fields include the field $\mathbb{Q}$, the rational function fields $\mathbb{F}_q(u)$ (with u some indeterminate) and all of their finitely generated extensions [FJ08, Theorem 13.4.2], every abelian extension of $\mathbb{Q}$ [FJ08, Theorem 16.11.3], fields $k((u_1,\ldots,u_r))$ of formal power series in $r\geqslant 2$ variables over a field k [FJ08, Theorem 15.4.6]; all of them are also totally Hilbertian. Algebraically closed fields, the fields $\mathbb{R}$, $\mathbb{Q}_p$ of real, of p-adic numbers, more generally Henselian fields are non-Hilbertian. The fraction field of a UFD R need not be Hilbertian (take $R=\mathbb{Z}_p$), even if R has infinitely many distinct prime ideals: a counter-example is given in [FJ08, Example 15.5.8].

Fields with the product formula provide other examples of Hilbertian fields. Recall from [FJ08, §15.3] that a nonempty set S of primes $\mathfrak{p}$ of K, with associated absolute value $|\ |_{\mathfrak{p}}$, is said to satisfy the product formula if for each $\mathfrak{p} \in S$, there exists $\beta_{\mathfrak{p}} > 0$ such that:

(1) *For each* $a \in K^{\times}$*, the set* $\{\mathfrak{p} \in S \,|\, |a|_{\mathfrak{p}} \neq 1\}$ *is finite and* $\prod_{\mathfrak{p}\in S} |a|_{\mathfrak{p}}^{\beta_{\mathfrak{p}}} = 1$.

In this case call K a field with the product formula. From a result of Weissauer, such fields are Hilbertian [FJ08, Theorem 15.3.3]. The fields $\mathbb{Q}$, $k(\lambda_1, \ldots, \lambda_r)$ with k any field and $r \geqslant 1$, and their finite extensions, are fields with the product formula.

4.2. **Hilbertian ring.** The following definition is given in [FJ08, §13.4].

Definition 4.1. An integral domain R with fraction field K is said to be a *Hilbertian ring* if every separable Hilbert subset of K^r ($r \geqslant 1$) contains r-tuples $\underline{\lambda}^* = (\lambda_1^*, \ldots, \lambda_r^*)$ with coordinates in R.

Since Zariski open subsets of Hilbert subsets remain Hilbert subsets, it is equivalent to require that a Zariski dense subset of tuples $\underline{\lambda}^*$ exist in Definition 4.1. Under the imperfectness assumption, a better property holds for Hilbertian rings, and extends to arbitrary Hilberts sets.

Proposition 4.2. *Let R be an integral domain such that the fraction field K is imperfect if of characteristic $p > 0$. The following are equivalent.*
(i) *R is a Hilbertian ring.*
(ii) *Every separable Hilbert subset of K contains elements $\lambda^* \in R$.*
(iii) *For every nonzero $\lambda_0^* \in R$ and every $\underline{a} = (a_1, \ldots, a_r) \in R^r$, every Hilbert subset of K^r ($r \geqslant 1$) contains r-tuples $\underline{\lambda}^* = (\lambda_1^*, \ldots, \lambda_r^*)$ with nonzero coordinates in R and such that $\lambda_i^* \equiv a_i\ [\mathrm{mod}\ \lambda_0^* \cdots \lambda_{i-1}^*]$, $i = 1, \ldots, r$.*

Clearly, it suffices to prove (ii) ⇒ (iii). This is done in §4.4 by reducing the number of variables to reach the separable situation $r = n = 1$ of Definition 4.1. We recall a classical tool.

4.3. **The Kronecker substitution.** Given an arbitrary field K, an irreducible polynomial $f \in K[\underline{\lambda}, \underline{y}]$, of degree $\geqslant 1$ in $\underline{y} = (y_1, \ldots, y_m)$ and an integer $D > \max_{1\leqslant i\leqslant m} \deg_{y_i}(f)$, the Kronecker substitution is the map

$$S_D : \mathcal{P}ol_{K(\underline{\lambda}),m,\underline{D}} \to \mathcal{P}ol_{K(\underline{\lambda}),1,D^m}, \quad \text{with } \underline{D} = (D, \ldots, D),$$

deriving from the substitution of $y^{D^{i-1}}$ for y_i, $i = 1, \ldots, m$, and leaving the coefficients in the field $K(\underline{\lambda})$ unchanged.

Proposition 4.3. *There exist a finite set $\mathcal{S}(f)$ of irreducible polynomials $g \in K[\underline{\lambda}][y]$ of degree $\geqslant 1$ in y and a nonzero polynomial $\varphi \in K[\underline{\lambda}]$ such that the Hilbert subset $H_K(f) \subset K^r$ contains the Hilbert subset*

$$H_K(\mathcal{S}(f); \varphi)$$

Furthermore, the finite set $\mathcal{S}(f)$ can be taken to be the set of irreducible divisors of $S_D(f)$ in $K[\underline{\lambda}][y]$.

Proof. See [FJ08, Lemma 12.1.3]. The statement is only stated for $r = 1$ but the proof carries over to the situation $r \geqslant 1$ by merely changing the single variable for an r-tuple $\underline{\lambda} = (\lambda_1, \dots, \lambda_r)$ of variables. □

We will also use several times the following observation.

Lemma 4.4. *Let R be a Hilbertian ring with a fraction field K of characteristic $p > 0$ and imperfect. There are infinitely many $a \in R$ that are different modulo K^p.*

Proof. Let R be a Hilbertian ring. Clearly K is Hilbertian, in particular it is infinite. Assume further that K is of characteristic $p > 0$ and imperfect. Then $K \neq K^p$ and K/K^p is a nonzero vector space over the infinite field K^p. Thus K/K^p is infinite. It follows that if $h \in \mathbb{N}$ is an integer, one can find $h+1$ elements $k_1, \dots, k_{h+1}$ of K that are different modulo K^p. If $\delta \in R$ is a common denominator of $k_1, \dots, k_{h+1}$, then $\delta k_1, \dots, \delta k_{h+1}$ are elements of R that are distinct modulo K^p. The conclusion follows. □

4.4. **Proof of Proposition 4.2.** Fix an integral domain R satisfying the imperfectness assumption and assume that condition (ii) holds. Let $\lambda_0^* \in R \setminus \{0\}$, $\underline{a} = (a_1, \dots, a_r) \in R^r$ and $\mathcal{H} \subset K^r$ be a Hilbert subset.

4.4.1. *First reductions.* Consider the Hilbert subset $\mathcal{H}_{\lambda_0^*, a_1}$ deduced from $\mathcal{H}$ by substituting $\lambda_0^* \lambda_1 + a_1$ to λ_1 in the polynomials involved in $\mathcal{H}$. This first reduction is used at the end of the proof in §4.4.4.

From the standard reduction Lemma 12.1.1 from [FJ08], the Hilbert subset $\mathcal{H}_{\lambda_0^*, a_1}$ contains a Hilbert subset of the form

$$H_K(f_1, \dots, f_m; g) = \left\{ \underline{\lambda}^* \in K^r \;\middle|\; \begin{array}{l} f_i(\underline{\lambda}^*, \underline{x}) \text{ irreducible in } K[\underline{x}] \\ \text{for each } i = 1, \dots, m, \\ \qquad\qquad g(\underline{\lambda}^*) \neq 0 \end{array} \right\}$$

with $f_1, \dots, f_m$ irreducible polynomials in $K[\underline{\lambda}, \underline{x}]$, of degree at least 1 in $\underline{x}$ and $g \in K[\underline{\lambda}]$, $g \neq 0$.

For $i = 1, \dots, m$, view f_i as a polynomial in $\underline{y} = (\lambda_2, \dots, \lambda_r, x_1, \dots, x_n)$ with coefficients in $K[\lambda_1]$. From Proposition 4.3, there is a finite set $\mathcal{S}(f_i)$ of irreducible polynomials $g \in K[\lambda_1][y]$ of degree $\geqslant 1$ in y and a nonzero polynomial $\varphi_i \in K[\lambda_1]$ such that the Hilbert subset $H_K(f_i) \subset K$ contains the Hilbert subset $H_K(\mathcal{S}(f_i); \varphi_i) \subset K$.

Consider the Hilbert subset

$$H_K(\mathcal{S}(f_1) \cup \dots \cup \mathcal{S}(f_m); \varphi_1 \cdots \varphi_m) \subset K.$$

From the standard reduction Lemma 12.1.4 from [FJ08], this Hilbert subset contains a Hilbert subset of the form

$$H_K(g_1, \dots, g_\nu) = \left\{ \lambda_1^* \in K \;\middle|\; \begin{array}{l} g_i(\lambda_1^*, y) \text{ irreducible in } K[y] \\ \text{for each } i = 1, \dots, \nu, \end{array} \right\}$$

with $g_1, \dots, g_\nu$ irreducible polynomials in $K[\lambda_1, y]$, monic and of degree at least 2 in y.

4.4.2. **1st case:** *$g_1, \dots, g_\nu$ are separable in y.* From assumption (ii), there is an element $\lambda_1^* \in R \setminus \{-a_1/\lambda_0^*\}$ such that, for each $i = 1, \dots, \nu$, $g_i(\lambda_1^*, y)$ is irreducible in $K[y]$ and $\deg_{\underline{x}}(f_i(\lambda_1^*, \lambda_2, \dots, \lambda_r, \underline{x})) \geqslant 1$. We refer to §4.4.4 for the end of the proof which is common to 1st and 2nd cases.

4.4.3. **2nd case:** *$g_1, \dots, g_\nu$ are not all separable in y.* Necessarily K is of characteristic $p > 0$. The following lemma (which we will use a second time) adjusts arguments from [FJ08, Prop. 12.4.3]. For simplicity, set $\lambda = \lambda_1$.

Lemma 4.5. *Under the 2nd case assumption, for every nonzero $\lambda_0^* \in R$, there is a nonzero $b \in \lambda_0^* R$ with this property: there exist irreducible polynomials $\widetilde{Q}_1, \dots, \widetilde{Q}_\nu$ in $K[\lambda, y]$, separable, monic of degree $\geqslant 1$ in y such that for all but finitely many $\tau \in H_K(\widetilde{Q}_1, \dots, \widetilde{Q}_\nu)$, $\tau^p + b$ is in $H_K(g_1, \dots, g_\nu)$.*

Proof of Lemma 4.5. Assume $g_1, \dots, g_\ell$ are not separable in y (with $\ell \geqslant 1$) and $g_{\ell+1}, \dots, g_\nu$ are separable in y. For each $i = 1, \dots, \ell$, there exists $Q_i \in K[\lambda, y]$ irreducible, separable, monic and of degree $\geqslant 1$ in y and q_i a power of p different from 1 such that $g_i(\lambda, y) = Q_i(\lambda, y^{q_i})$. Since $g_i(\lambda, y)$ is irreducible in $K[\lambda, y]$, Q_i has a coefficient $h_i \in K[\lambda]$ which is not a pth power. Choose $a_i \in R$ with $h_i(\lambda + a_i) \in K^p[\lambda]$ if there exists any, otherwise let $a_i = 0$. Also set $Q_i = g_i$ for $i = \ell + 1, \dots, \nu$.

Consider the elements $a \in R$ from Lemma 4.4. Among the corresponding elements $a\lambda_0^* \in R$, which are also different modulo K^p, there is at least one, say $b = a\lambda_0^*$, such that $b \in R \setminus \bigcup_{i=1}^{\ell}(a_i + K^p)$. By [FJ08, Lemma 12.4.2(b)], $h_i(\lambda + b) \notin K^p[\lambda]$, $i = 1, \dots, \ell$.

Consider the polynomials $\widetilde{Q}_i(\lambda, y) = Q_i(\lambda^p + b, y)$, $i = 1, \dots, \nu$. They are monic and separable in y. Furthermore, as detailed in §12.4 from [FJ08] (and [FJ] which clarifies the argument), they are irreducible in $K[\lambda, y]$.

Let $\tau \in H_K(\widetilde{Q}_1, \dots, \widetilde{Q}_\nu)$ but not in the set C, finite by [FJ08, Lemma 12.4.2(c)], of all elements $c \in R$ with $h_i(c^p + b) \in K^p$ for some $i = 1, \dots, \ell$. For $i = \ell + 1, \dots, \nu$, we have $\widetilde{Q}_i(\tau, y) = g_i(\tau^p + b, y)$ and so $g_i(\tau^p + b, y)$ is irreducible in $K[y]$. Let $i \in \{1, \dots, \ell\}$. Since $\tau \notin C$, we have $h_i(\tau^p + b) \notin K^p$. Hence $Q_i(\tau^p + b, y) = \widetilde{Q}_i(\tau, y) \notin K^p[y]$. From the choice of τ, this polynomial is irreducible in $K[y]$. By [FJ08, Lemma 12.4.1], we obtain that

$$\widetilde{Q}_i(\tau, y^{q_i}) = Q_i(\tau^p + b, y^{q_i}) = g_i(\tau^p + b, y)$$

is irreducible in $K[y]$. Whence finally: $\tau^p + b \in H_K(g_1, \dots, g_\nu)$. □

Use then the assumption (ii) of Proposition 4.2 to conclude that for the element b and the polynomials $\widetilde{Q}_1, \dots, \widetilde{Q}_\nu$ given by Lemma 4.5, the Hilbert subset $H_K(\widetilde{Q}_1, \dots, \widetilde{Q}_\nu)$ contains infinitely many elements $\tau \in R$. Fix one off the finite list of exceptions in the final sentence of Lemma 4.5 and such that $\lambda_1^* = \tau^p + b$ is different from $-a_1/\lambda_0^*$. The element $\lambda_1^* \in R$ is then in $H_K(g_1, \dots, g_\nu)$ and $\lambda_0^*\lambda_1^* + a_1 \neq 0$. Up to excluding finitely many more τ above, we may also assure that $\deg_{\underline{x}}(f_i(\lambda_1^*, \lambda_2, \dots, \lambda_r, \underline{x})) \geqslant 1$ $(i = 1, \dots, \nu)$. (We have only used here that $b \in R$. The possible choice of b in $\lambda_0^* R$ will be used later (§4.6.1)).

4.4.4. *End of proof of Proposition 4.2.* Applying Prop.4.3 and taking into account the first reduction changing $\mathcal{H}$ to $\mathcal{H}_{\lambda_0^*,a_1}$ yields in both cases that

(2) there is $\lambda_1^* \in R\setminus\{0\}$ such that $\lambda_1^* \equiv a_1$ [mod λ_0^*], $f_i(\lambda_1^*,\lambda_2,\ldots,\lambda_r,\underline{x})$ is irreducible in $K[\lambda_2,\ldots,\lambda_r,\underline{x}]$ and is of degree at least 1 in $\underline{x}$, $i=1,\ldots,m$.

Repeating this argument provides a r-tuple $\underline{\lambda}^* = (\lambda_1^*,\ldots,\lambda_r^*)$ in $(R\setminus\{0\})^r$ such that $f_1(\underline{\lambda}^*,\underline{x}),\ldots,f_m(\underline{\lambda}^*,\underline{x})$ are irreducible in $K[\underline{x}]$ (so $\underline{\lambda}^*$ is in the original Hilbert subset $\mathcal{H}$) and such that $\lambda_i^* \equiv a_i$ [mod $\lambda_0^*\cdots\lambda_{i-1}^*$], $i=1,\ldots,r$.

4.5. **UFD with fraction field with the product formula.**

Theorem 4.6. *If R is an integral domain such that the fraction field K has the product formula and is imperfect if of characteristic $p>0$, then R is a Hilbertian ring.*

Fix a ring R as in the statement. Theorem 4.6 relies on the following lemma, whose main ingredient is a result for fields with the product formula. Recall a useful tool in a field K with a set S of primes $\mathfrak{p}$ satisfying the product formula. For every $a\in K$, the (*logarithmic*) *height* $h(a)$ of a is defined by:

$$h(a) = \textstyle\sum_{\mathfrak{p}\in S}\log(\max(1,|a|_{\mathfrak{p}})).$$

Clearly $h(a^n) = nh(a)$ ($n\in\mathbb{N}$) and $h(1/a) = h(a)$ if $a\neq 0$.

Lemma 4.7. *Let $f_1,\ldots,f_m$ be m irreducible polynomials in $K(\lambda)[y]$. For all but finitely many $t_0\in R$, there is a nonzero element $a\in R$ with the following property: if $b\in R$ is of height $h(b)>0$, the Hilbert subset $H_K(f_1,\ldots,f_m)$ contains infinitely many elements of R of the form t_0+ab^ℓ ($\ell>0$).*

Proof. [Dèb99, Theorem 3.3] proves the weaker version for which the element a is only asserted to lie in K. However the proof can be adjusted so that $a\in R$. Specifically, the same argument there leads to the stronger conclusion provided that, if K is of characteristic $p>0$, infinitely many $a\in R$ can be found that are different modulo K^p. This is the conclusion of Lemma 4.4. □

Proof of Theorem 4.6. We prove condition (ii) from Proposition 4.2. Let $\mathcal{H}\subset K$ be a separable Hilbert subset. From Lemmas 12.1.1 and 12.1.4 of [FJ08], the Hilbert subset $\mathcal{H}$ contains a separable Hilbert subset of the form

$$H_K(f_1,\ldots,f_m) = \left\{\lambda^*\in K \;\middle|\; \begin{array}{l} f_i(\lambda^*,y) \text{ irreducible in } K[y] \\ \text{for each } i=1,\ldots,m, \end{array}\right\}$$

with $f_1,\ldots,f_m$ irreducible polynomials in $K[\lambda,y]$, monic, separable and of degree at least 2 in y.

Pick an element $t_0\in R$ that avoids the finite set of exceptions in Lemma 4.7. Consider an element $a\in R$ associated to this t_0 in Lemma 4.7. Choose an element $b\in R$ of height $h(b)>0$.

Here is an argument showing that such b exist. Fix a prime $\mathfrak{p}\in S$. Recall that by definition, the corresponding absolute value is nontrivial [FJ08, §13.3]: there exists $b\in K$ such that $|b|_{\mathfrak{p}}\neq 1$. One may assume that $b\in R$.

From the product formula, there is a prime $\mathfrak{p}_0 \in S$ such that $|b|_{\mathfrak{p}_0} > 1$. We have $h(b) \geqslant \log(\max(1, |b|_{\mathfrak{p}_0})) > 0$.

From Lemma 4.7, $\lambda_1^* = t_0 + ab^\ell \in R$ is in the Hilbert subset $H_K(f_1, \ldots, f_m)$, hence in the Hilbert subset $\mathcal{H}$, for infinitely many integers $\ell > 0$. □

4.6. **Polynomial rings in one variable.**

Theorem 4.8. *Assume that $R = k[u]$ with k an arbitrary field. Let $\mathcal{H}$ be a Hilbert subset of K^r ($r \geqslant 1$), $\lambda_0^* \in R$ a nonzero element of R and $d_1 \geqslant 1$ an integer. Define $\widetilde{p}$ by*

$$\widetilde{p} = \begin{cases} 1 & \text{if } \mathrm{char}(k) = 0 \text{ or } \mathcal{H} \text{ is a separable Hilbert subset} \\ p & \text{otherwise.} \end{cases}$$

Denote the subset of $\mathcal{H}$ of r-tuples $\underline{\lambda}^* = (\lambda_1^*, \ldots, \lambda_r^*) \in R^r$ such that λ_1^* and $\lambda_0^* \lambda_2^* \cdots \lambda_r^*$ are relatively prime in R and $\max_{1 \leqslant i \leqslant r} \deg(\lambda_i^*) = \widetilde{p} d_1$ by $\mathcal{H}_{\lambda_0^*, \widetilde{p} d_1}$. There is an integer d_0 such that if $d_1 \geqslant d_0$, the set $\mathcal{H}_{\lambda_0^*, \widetilde{p} d_1}$ is nonempty.

When $R = k[u]$, statement (iii) from Proposition 4.2 also holds for the Hilbert subset $\mathcal{H}$: there the congruence conditions are stronger but no control is given on the degree in u of $\lambda_1^*, \ldots, \lambda_r^*$ as in Theorem 4.8.

We divide the proof of Theorem 4.8 into two parts. The situation: one parameter, one variable, is considered in §4.6.1, the general one in §4.6.2.

4.6.1. *Proof of Theorem 4.8* – situation $r = n = 1$ –. We are given a Hilbert subset $\mathcal{H} \subset K = k(u)$, a nonzero element $\lambda_0^* \in k[u]$, an integer $d_1 \geqslant 1$ and we need to find an element $\lambda_1^* \in k[u]$ such that $\lambda_1^* \in \mathcal{H}$, λ_1^* and λ_0^* are relatively prime and $\deg(\lambda_1^*) = \widetilde{p} d_1$.

From Lemmas 12.1.1 and 12.1.4 from [FJ08], the Hilbert subset $\mathcal{H}$ contains a Hilbert subset of the form

$$H_K(f_1, \ldots, f_m) = \left\{ \lambda^* \in K \;\middle|\; \begin{array}{l} f_i(\lambda^*, y) \text{ irreducible in } K[y] \\ \text{for each } i = 1, \ldots, m. \end{array} \right\}$$

with $f_1, \ldots, f_m$ irreducible polynomials in $K[\lambda, y]$,
monic and of degree at least 2 in y.

We distinguish the two cases corresponding to the definition of $\widetilde{p}$.

Separable case: $\mathrm{char}(k) = 0$ or $\mathcal{H}$ is a separable Hilbert subset. As $n = 1$, the Hilbert subset $\mathcal{H}$ is also separable under the assumption $\mathrm{char}(k) = 0$. So we may assume that the polynomials $f_1, \ldots, f_m$ above are separable in y. We distinguish two sub-cases.

- *1st sub-case*: k is infinite. Use [Lan83, Prop.4.1 p.236] to assert that there exists a nonempty Zariski open subset $V \subset \mathbb{A}_k^2$ such that for all but finitely many $\gamma \in k$,

$$\{\tau + \gamma(u - \beta)^{d_1} \in k[u] \mid (\tau, \beta) \in V\} \subset H_K(f_1, \ldots, f_m).$$

Fix a nonzero $\gamma \in k$ off the finite exceptional list. There are infinitely many different $(\tau, \beta) \in V$ such that no root in $\overline{k}$ of the polynomial $\lambda_0^* \in k[u]$ is a root of $\tau + \gamma(u - \beta)^{d_1}$, and so $\tau + \gamma(u - \beta)^{d_1}$ and λ_0^* are relatively prime.

The corresponding elements $\lambda_1^* = \tau + \gamma(u-\beta)^{d_1}$ are infinitely many different elements of the set $\mathcal{H}_{\lambda_0^*,d_1}$. In this case, one can take $d_0 = 1$.

- *2nd sub-case*: k is finite. Start with another classical reduction, namely [FJ08, Lemma 13.1.2], to conclude that there exist polynomials $Q_1, \dots, Q_\nu$ in $K[\lambda, y]$, irreducible in $\overline{K}[\lambda, y]$, monic and separable in y, of degree $\geqslant 2$ in y and such that the Hilbert subset $H_K(f_1, \dots, f_m)$ contains the set

$$H'_K(Q_1, \dots, Q_\nu) = \left\{ \lambda^* \in K \;\middle|\; \begin{array}{c} Q_i(\lambda^*, y) \text{ has no root in } K \\ \text{for each } i = 1, \dots, \nu \end{array} \right\}$$

Consider the set $\{\mathfrak{p}_i \mid i \in I\}$ of irreducible factors of the given polynomial $\lambda_0^* \in k[u]$; view them as primes of K. Apply [FJ08, Lemma 13.3.4] to assert that, for each $j = 1, \dots, \nu$, there are infinitely primes $\mathfrak{p}_j$ of K such that there is an $a_{\mathfrak{p}_j} \in R$ with this property: if $a \in R$ satisfies $a \equiv a_{\mathfrak{p}_j} \mod \mathfrak{p}_j$, then $Q_j(a, v) \neq 0$ for every $v \in K$. For each $j = 1, \dots, \nu$, pick one such prime $\mathfrak{p}_j$ that is different from all primes $\mathfrak{p}_i$ with $i \in I$.

Denote the ideal $(\prod_{j=1}^{\nu} \mathfrak{p}_j)(\prod_{i \in I} \mathfrak{p}_i) \subset R$ by $\mathcal{I}$. From the Chinese Remainder Theorem, there exists $a_0 \in R$ such that every $a \in a_0 + \mathcal{I}$ satisfies

$$\begin{cases} a \equiv a_{\mathfrak{p}_j} \mod \mathfrak{p}_j \text{ for } j = 1, \dots, \nu, \\ a \equiv 1 \mod \mathfrak{p}_i \text{ for } i \in I. \end{cases}$$

Consider such an a and rename it λ_1^*. It follows from the first condition that $\lambda_1^* \in H'_K(Q_1, \dots, Q_\nu)$ and so $\lambda_1^* \in H_K(f_1, \dots, f_m) \subset \mathcal{H}$. It follows from the second condition that $\lambda_1^* \not\equiv 0 \mod \mathfrak{p}_i$ for every $i \in I$. Hence λ_1^* and λ_0^* are relatively prime. Finally when $\lambda_1^* = a$ ranges over $a_0 + \mathcal{I}$, $\deg(\lambda_1^*)$ assumes all but finitely many values in $\mathbb{N}$. Therefore there is an integer d_0 such that $\mathcal{H}_{\lambda_0^*,d_1} \neq \emptyset$ for every $d_1 \geqslant d_0$.

2nd case: $\mathrm{char}(k) = p > 0$ *and* $\mathcal{H}$ *is not a separable Hilbert subset.* Not all the polynomials $f_1, \dots, f_m$ are separable in y. Proceed as in §4.4.3. From Lemma 4.5, there is a nonzero $b \in \lambda_0^* R$ and some irreducible polynomials $\widetilde{Q}_1, \dots, \widetilde{Q}_m$ in $K[\lambda, y]$, separable, monic of degree $\geqslant 1$ in y such that for all but finitely many $\tau \in H_K(\widetilde{Q}_1, \dots, \widetilde{Q}_m)$, $\tau^p + b$ is in $H_K(f_1, \dots, f_m)$.

From the separable case of the current proof, there is an integer $d_0 \geqslant 1$ with the following property: the Hilbert subset $H_K(\widetilde{Q}_1, \dots, \widetilde{Q}_\nu)$ contains infinitely many elements $\tau \in R$ such that τ and λ_0^* are relatively prime and $\deg(\tau) = d_1$. Fix one off the finite list of exceptions in the final sentence of Lemma 4.5 and set $\lambda_1^* = \tau^p + b$. We then have $\lambda_1^* \in H_K(f_1, \dots, f_m)$. Furthermore λ_1^* and λ_0^* are relatively prime in R. Finally assuming that d_0 is also larger than $\deg(b)$, we have $\deg(\lambda_1^*) = pd_1$ if $d_1 \geqslant d_0$, thus finally proving that $\lambda_1^* \in \mathcal{H}_{\lambda_0^*,pd_1}$.

4.6.2. *Proof of Theorem 4.8* – situation $r \geqslant 1$, $n \geqslant 1$ –. As in §4.6.1 we distinguish two cases according to the definition of $\widetilde{p}$.

Separable case: $\mathcal{H}$ is a separable Hilbert subset (in particular $n = 1$). From Lemma 12.1.1 and Lemma 12.1.4 from [FJ08], the separable Hilbert subset $\mathcal{H} \subset K^r$ contains a Hilbert subset of the form

$$H_K(f_1,\ldots,f_m)=\left\{\underline{\lambda}^*\in K^r\ \middle|\ \begin{array}{l} f_i(\underline{\lambda}^*,x) \text{ irreducible in } K[x] \\ \text{for each } i=1,\ldots,m, \end{array}\right\}$$

with $f_1,\ldots,f_m$ irreducible polynomials in $K[\underline{\lambda},x]$, separable, monic and of degree at least 2 in x.

Set $\mathcal{K}=K(\lambda_3,\ldots,\lambda_r)$ (with $\mathcal{K}=K$ if $r=2$) and regard $f_1,\ldots,f_m$ as polynomials in the ring $\mathcal{K}(\lambda_1)[\lambda_2,x]$. By [FJ08, Proposition 13.2.1], there exists a nonempty Zariski open subset $U\subset\mathbb{A}^2_{\mathcal{K}}$ such that

$$\{a+b\lambda_1\,|\,(a,b)\in U\}\subset H_{\mathcal{K}(\lambda_1)}(f_1,\ldots,f_m).$$

Furthermore, up to shrinking U, one may require that the polynomials

$$f_i(\lambda_1,a\lambda_1+b,\lambda_3,\ldots,\lambda_r,x),\ i=1,\ldots,m \tag{4}$$

are separable and of degree at least 2 in x, and that $b\neq 0$. As $R=k[u]\subset\mathcal{K}$ is infinite, the open subset U contains elements $(a,b)\in R^2$. For such (a,b), the polynomials above in (4) are in $K[\lambda_1,\lambda_3,\ldots,\lambda_r,x]$ and are irreducible in $K(\lambda_1,\lambda_3,\ldots,\lambda_r)[x]$. Repeating this procedure provides an $(r-1)$-tuple $((a_2,b_2),\ldots,(a_r,b_r))\in(R^2)^{r-1}$ with $b_2\cdots b_r\neq 0$ such that the polynomials

$$g_i(\lambda_1,x)=f_i(\lambda_1,a_2\lambda_1+b_2,\ldots,a_r\lambda_1+b_r,x),\ i=1,\ldots,m$$

are in $K[\lambda_1,x]$, irreducible in $K(\lambda_1)[x]$, separable and of degree $\geqslant 2$ in x.

From the proof in situation $r=n=1$ and in the separable case (in §4.6.1), there is an integer $\delta_0\geqslant 1$ with this property: the Hilbert subset $H_K(g_1,\ldots,g_m)$ contains an element $\lambda_1^*\in R$ relatively prime to $\lambda_0^*\cdot b_2\cdots b_r$ and such that $\deg(\lambda_1^*)=\delta_1$ if $\delta_1\geqslant\delta_0$. Request further to δ_0 to satisfy:

$$\delta_0>\max\nolimits_{2\leqslant i\leqslant r}\deg(b_i). \tag{5}$$

Set $d_0=\delta_0+\max_{2\leqslant i\leqslant r}\deg(a_i)$ and fix an integer $d_1\geqslant d_0$. It follows from $d_1-\max_{2\leqslant i\leqslant r}\deg(a_i)\geqslant\delta_0$ that the Hilbert subset $H_K(g_1,\ldots,g_m)$ contains an element $\lambda_1^*\in R$ such that $\deg(\lambda_1^*)=d_1-\max_{2\leqslant i\leqslant r}\deg(a_i)$.

Consequently we have the following:
- the r-tuple $\underline{\lambda}^*=(\lambda_1^*,a_2\lambda_1^*+b_2,\ldots,a_{r-1}\lambda_1^*+b_{r-1},a_r\lambda_1^*+b_r)\in R^r$ is in the original Hilbert subset $\mathcal{H}$, and, denoting the i-th component of $\underline{\lambda}^*$ by λ_i^*,
- λ_1^* is relatively prime to $\lambda_0^*\lambda_2^*\cdots\lambda_r^*$,
- the largest degree of $\lambda_1^*,\ldots,\lambda_r^*$ is d_1 (due to condition (5), this largest degree is $\max_{2\leqslant i\leqslant r}\deg(a_i\lambda_1^*)$).

This proves that $\underline{\lambda}^*\in\mathcal{H}_{\lambda_0^*,d_1}$.

General case: We will use the Kronecker substitution. The Hilbert subset $\mathcal{H}$ contains a Hilbert subset

$$H_K(f_1,\ldots,f_m;g)=\left\{\underline{\lambda}^*\in K^r\ \middle|\ \begin{array}{l} f_i(\underline{\lambda}^*,\underline{x}) \text{ irreducible in } K[\underline{x}] \\ \text{for each } i=1,\ldots,m, \\ \qquad g(\underline{\lambda}^*)\neq 0 \end{array}\right\}$$

with $f_1,\ldots,f_m$ irreducible polynomials in $K[\underline{\lambda},\underline{x}]$, of degree at least 1 in $\underline{x}$ and $g\in K[\underline{\lambda}]$, $g\neq 0$.

As in §4.4, Proposition 4.3, followed by [FJ08, Lemma 12.1.4], provides polynomials $g_1, \dots, g_\nu$, irreducible in $K[\lambda_1, y]$, monic and of degree $\geqslant 2$ in y with this property. For every $\lambda_1^* \in H_K(g_1, \dots, g_\nu)$, each of the polynomials

$$f_i(\lambda_1^*, \lambda_2, \dots, \lambda_r, \underline{x}),\ i = 1, \dots, m,$$

is irreducible in $K[\lambda_2, \dots, \lambda_r, \underline{x}]$. From the proof in situation $r = n = 1$ (§4.6.1), the Hilbert subset $H_K(g_1, \dots, g_\nu)$ contains infinitely many $\lambda_1^* \in R$ relatively prime to λ_0^*. Repeating this argument $(r-2)$ times provides $\lambda_1^*, \dots, \lambda_{r-1}^* \in R$ such that $f_i(\lambda_1^*, \dots, \lambda_{r-1}^*, \lambda_r, \underline{x})$ is irreducible in $K[\lambda_r, \underline{x}]$ $(i = 1, \dots, m)$ and λ_i^* and $\lambda_0^* \lambda_1^* \cdots \lambda_{i-1}^*$ are relatively prime $(i = 1, \dots, r-1)$.

Repeating the argument once more but applying this time the full conclusion of the case $r = n = 1$ of the proof including the degree condition, we obtain that there is an integer d_0, which we may also choose to be larger than $\max_{1 \leqslant i \leqslant r-1} \deg(\lambda_i^*)$, with the following property: if $d_1 \geqslant d_0$, there exists an element $\lambda_r^* \in R$ such that
- $f_i(\lambda_1^*, \dots, \lambda_{r-1}^*, \lambda_r^*, \underline{x})$ is irreducible in $K[\underline{x}]$, $i = 1, \dots, m$,
- λ_r^* and $\lambda_0^* \lambda_1^* \cdots \lambda_{r-1}^*$ are relatively prime,
- $\deg(\lambda_r^*) = \widetilde{p} d_1$.

Finally the r-tuple $\underline{\lambda}^*$ is in the original Hilbert subset $\mathcal{H}$, λ_i^* and $\lambda_0^* \lambda_1^* \cdots \lambda_{i-1}^*$ are relatively prime $(i = 1, \dots, r)$, and consequently, λ_1^* is relatively prime to $\lambda_0^* \lambda_2^* \cdots \lambda_r^*$, and $\max_{1 \leqslant i \leqslant r} \deg(\lambda_i^*) = \widetilde{p} d_1$. Thus the set $\mathcal{H}_{\lambda_0^*, d_1}$ is nonempty.

5. Proofs of the main results

5.1. **Proof of Theorem 1.1 and Theorem 1.2.** Recall the notation from §2: R is a UFD with fraction field K, $\underline{x} = (x_1, \dots, x_n)$, $\underline{\lambda} = (\lambda_0, \lambda_1, \dots, \lambda_\ell)$ $(n \geqslant 1,\ \ell \geqslant 1)$ are two tuples of indeterminates, $\underline{Q} = (Q_0, Q_1, \dots, Q_\ell)$, with $Q_0 = 1$, is a $(\ell+1)$-tuple of nonzero polynomials in $R[\underline{x}]$, distinct up to multiplicative constants in $K^\times$, $\underline{P} = \{P_1, \dots, P_s\}$ is a set of s polynomials

$$P_i(\underline{x}, y) = P_{i\rho_i}(\underline{x})\, y^{\rho_i} + \cdots + P_{i1}(\underline{x}) y + P_{i0}(\underline{x}),$$

irreducible in $R[\underline{x}, y]$ and of degree $\rho_i \geqslant 1$ in y, $i = 1, \dots, s$. We also set

$$M(\underline{\lambda}, \underline{x}) = \textstyle\sum_{j=0}^{\ell} \lambda_j Q_j(\underline{x})$$

and, for $i = 1, \dots, s$,

$$F_i(\underline{\lambda}, \underline{x}) = P_i(\underline{x}, M(\underline{\lambda}, \underline{x})) = P_i(\underline{x}, \textstyle\sum_{j=0}^{\ell} \lambda_j Q_j(\underline{x}))$$

The polynomials $F_1, \dots, F_s$ are irreducible in $R[\underline{\lambda}, \underline{x}]$ (Lemma 2.1). Finally, for $\underline{F} = \{F_1, \dots, F_s\}$, we introduced the subset

$$H_R(\underline{F}) \subset R^{\ell+1}$$

of all $(\ell+1)$-tuples $\underline{\lambda}^*$ (or equivalently, of polynomials $\Lambda(\underline{x}) = \sum_{j=0}^{\ell} \lambda_i^* Q_j(\underline{x})$) such that $F_i(\underline{\lambda}^*, \underline{x}) = P_i(\underline{x}, \Lambda(\underline{x}))$ is irreducible in $R[\underline{x}]$, $i = 1, \dots, s$.

Given a nonzero element $\lambda_{-1}^* \in R$ and a tuple $\underline{a} = (a_0, \dots, a_\ell) \in R^{\ell+1}$, consider the subset

$$H_{R, \lambda_{-1}^*, \underline{a}}(\underline{F}) \subset H_R(\underline{F})$$

of those $(\ell+1)$-tuples $\underline{\lambda}^* = (\lambda_0^*, \dots, \lambda_\ell^*) \in H_R(\underline{F})$ which further satisfy the congruences $\lambda_i^* \equiv a_i\ [\bmod\ \lambda_{-1}^* \lambda_0^* \cdots \lambda_{i-1}^*]$, $i = 0, \dots, \ell$.

Make this additional assumption on $Q_0, \ldots, Q_\ell$ (which implies $\ell \geqslant 2$):

(1) *$Q_0, \ldots, Q_\ell$ are monomials with coefficient 1, $Q_0 = 1$ and*

$$\min(\deg(Q_1), \deg(Q_2)) > \max_{1 \leqslant i \leqslant s} \deg_{\underline{x}}(P_i).$$

Theorem 5.1. *Let λ_{-1} be a nonzero element of R and $\underline{a} = (1, \ldots, 1) \in R^{\ell+1}$.*
(a) *Assume that R is a UFD and a Hilbertian ring and K is imperfect if it is of characteristic $p > 0$. The subset $H_{R,\lambda^*_{-1},\underline{a}}(\underline{F})$ is Zariski-dense in $R^{\ell+1}$.*
(b) *If $R = k[u]$ with k an arbitrary field and d_1 is a suitably large integer, then $H_R(\underline{F})$ contains a polynomial $\Lambda = \sum_{j=0}^{\ell} \lambda^*_i\, Q_j(\underline{x})$ with $\underline{\lambda}^* = (\lambda^*_0, \ldots, \lambda^*_\ell) \in R^{\ell+1}$ such that λ^*_1 and $\lambda^*_{-1}\lambda^*_0\lambda^*_2 \cdots \lambda^*_\ell$ are relatively prime and $\deg_u(\Lambda) = \widetilde{p} d_1$.*

Proof. The number of monomials Q_i is $\ell + 1 \geqslant 3$. Each F_i is of degree $\geqslant 1$ in $\underline{x}$ and is irreducible in $K(\underline{\lambda})[\underline{x}]$, $i = 1, \ldots, s$ (Lemma 2.1). Let $g \in K[\underline{\lambda}]$ be a nonzero polynomial and consider the Hilbert subset

$$H_K(\underline{F}; g) \subset K^{\ell+1}.$$

In situation (a), it follows from Proposition 4.2 that the Hilbert subset $H_K(\underline{F}; g)$ contains an $(\ell+1)$-tuple $\underline{\lambda}^* = (\lambda^*_0, \ldots, \lambda^*_\ell) \in R^{\ell+1}$ satisfying the congruences $\lambda^*_i \equiv 1$ [mod $\lambda^*_{-1}\lambda^*_0 \cdots \lambda^*_{i-1}$], $i = 0, \ldots, \ell$.

In situation (b), from Theorem 4.8, the Hilbert subset $H_K(\underline{F}; g)$ contains an $(\ell+1)$-tuple $\underline{\lambda}^*$ such that λ^*_1 and $\lambda^*_{-1}\lambda^*_0\lambda^*_2 \cdots \lambda^*_\ell$ are relatively prime and $\max_{0 \leqslant i \leqslant \ell} \deg(\lambda^*_i) = \widetilde{p} d_1$, i.e, $\deg_u(\Lambda) = \widetilde{p} d_1$ for $\Lambda = \sum_{j=0}^{\ell} \lambda^*_i\, Q_j(\underline{x})$.

Each $F_i(\underline{\lambda}^*, \underline{x})$ being irreducible in $K[\underline{x}]$, to finish the proof, it suffices to show that $F_i(\underline{\lambda}^*, \underline{x})$ is primitive w.r.t. R ($i = 1, \ldots, s$).

Assume otherwise, i.e., for some $i = 1, \ldots, s$, there is an irreducible element $\pi \in R$ dividing all the coefficients of $F_i(\underline{\lambda}^*, \underline{x})$. The quotient ring $\overline{R} = R/(\pi)$ is an integral domain. Use the notation $\overline{U}$ to denote the class modulo (π) of polynomials U with coefficients in R. We have:

(2) $$\overline{P}_{i\rho_i}(\underline{x})\, \overline{M}(\underline{\lambda}^*, \underline{x})^{\rho_i} + \cdots + \overline{P}_{i1}(\underline{x})\, \overline{M}(\underline{\lambda}^*, \underline{x}) = -\overline{P}_{i0}(\underline{x}).$$

We distinguish two cases.

1st case: π divides all polynomials $P_{ij}(\underline{x})$, $j = 1, \ldots, \rho_i$. From (2), π also divides $P_{i0}(\underline{x})$. This contradicts $P_i(\underline{x}, y)$ being primitive w.r.t. R.

2nd case: there is an index $j \in \{1, \ldots, \rho_i\}$ such that π does not divides $P_{ij}(\underline{x})$. As λ^*_1 and λ^*_2 are relatively prime (in both situations (a) and (b)), one of the two is not divisible by π. Conjoin this with our monomials Q_i being of coefficient 1 to conclude that $\overline{M}(\underline{\lambda}^*, \underline{x}) \neq 0$ in $R/(\pi)[\underline{x}]$ and that there is at least one nonzero term $\overline{P}_{ij}(\underline{x})\, \overline{M}(\underline{\lambda}^*, \underline{x})^j$ with $j \in \{1, \ldots, \rho_i\}$. Furthermore we have:

$$\deg(\overline{M}(\underline{\lambda}^*, \underline{x})) \geqslant \min(\deg(Q_1), \deg(Q_2)).$$

Using next the following inequality (coming from assumption (1)):

$$\min(\deg(Q_1), \deg(Q_2)) > \max_{\substack{1 \leqslant i \leqslant s \\ 1 \leqslant j \leqslant \rho_i}} \deg(P_{ij}),$$

we obtain that all nonzero terms $\overline{P}_{ij}(\underline{x})\,\overline{M}(\underline{\lambda}^*,\underline{x})^j$ with $j\in\{1,\dots,\rho_i\}$ are of different degrees: otherwise, for two integers $j,k\in\{1,\dots,\rho_i\}$ with $k>j$, we would have the following, where $\delta=\deg(\overline{M}(\underline{\lambda}^*,\underline{x}))$:

$$\max_{\substack{1\leqslant i\leqslant s\\ 1\leqslant h\leqslant\rho_i}}\deg(P_{ih})\geqslant\deg(\overline{P}_{ij})-\deg(\overline{P}_{ik})=(k-j)\delta\geqslant\delta,$$

which contradicts the preceding inequalities. It follows that the left-hand side of (2) is of degree $\geqslant\deg(\overline{M}(\underline{\lambda}^*,\underline{x}))$. But then the following inequality (using again assumption (1)):

$$\deg(\overline{M}(\underline{\lambda}^*,\underline{x}))\geqslant\min(\deg(Q_1),\deg(Q_2))>\max_{1\leqslant i\leqslant s}\deg(P_{i0}(\underline{x})).$$

contradicts identity (2). □

Proof of Theorem 1.1 and Theorem 1.2. From Theorem 4.6, the assumption on R in Theorem 1.1 implies that of Theorem 5.1(a), and $R=k[u]$ in both Theorem 1.2 and Theorem 5.1(b). Theorems 1.1 and 1.2 then correspond to the special case of Theorem 5.1 for which, for a given $\underline{d}\in(\mathbb{N}^*)^n$, the Q_i are all the monomials $Q_0,Q_1,\dots,Q_{N_{\underline{d}}}$ in $\mathcal{P}ol_{k,n,\underline{d}}$ and Q_1, Q_2 are monomials of degree $d_1+\cdots+d_n$ and $d_1+\cdots+d_n-1$. Assumption on $d_1,\dots,d_n$ in Theorems 1.1 and 1.2 guarantees assumption (1) of Theorem 5.1. □

Remark 5.2. The proof shows that Theorem 1.1 holds under the more general assumption that R is a UFD, a Hilbertian ring and K is imperfect if of characteristic $p>0$. We note that there exist UFD with a Hilbertian fraction field satisfying the imperfectness assumption but not Hilbertian as a ring, e.g. the ring $\mathbb{C}[[u_1,\dots,u_n]]$ of formal power series with $n\geqslant 2$ [FJ08, Example 15.5]. It is unclear whether Theorem 1.1 holds for these rings.

5.2. **The multivariable Schinzel hypothesis.** Theorem 5.1 offers more flexibility than Theorem 1.1 and Theorem 1.2. Instead of taking for $Q_0,\dots,Q_\ell$ all the monomials in $\mathcal{P}ol_{k,n,\underline{d}}$, one may want to work with a proper subset of them and construct irreducible polynomials of the form $P_i(\underline{x},M(\underline{x}))$ with some of the coefficients in $M(\underline{x})$ equal to 0.

In this manner one can extend Theorems 1.1 and 1.2 to the situation that $P_1,\dots,P_s$ are polynomials in m variables $y_1,\dots,y_m$.

Let R be a UFD with fraction field a field K with the product formula, imperfect if K is of characteristic $p>0$. Let $\underline{x}=(x_1,\dots,x_n)$ $(n\geqslant 1)$ and $\underline{y}=(y_1,\dots,y_m)$ $(m\geqslant 1)$ be two tuples of indeterminates.

Theorem 5.3. *Let $\underline{P}=\{P_1,\dots,P_s\}$ be a set of polynomials, irreducible in $R[\underline{x},\underline{y}]$ and of degree $\geqslant 1$ in $\underline{y}$. Let $\mathcal{I}rr_n(R,\underline{P})$ be the set of all m-tuples $\underline{M}=(M_1,\dots,M_m)\in R[\underline{x}]^m$ such that $P_i(\underline{x},\underline{M}(\underline{x}))$ is irreducible in $R[\underline{x}]$, $i=1,\dots,s$. For every $\underline{d}\in(\mathbb{N}^*)^n$ such that*

$$D:=d_1+\cdots+d_n\geqslant\max_{1\leqslant i\leqslant s}(\deg(P_i)+2),$$

the set $\mathcal{I}rr_n(R,\underline{P})$ is Zariski-dense in $\mathcal{P}ol_{R,n,\underline{d}}\times\cdots\times\mathcal{P}ol_{R,n,D^{m-1}\underline{d}}$.

The proof is an easy induction left to the reader: use Theorem 5.1 to successively specialize in $R[\underline{x}]$ the indeterminates $y_1,\dots,y_m$.

5.3. **Proof of Corollary 1.5 (Goldbach).** Fix an integral domain R as in Theorem 1.1, an integer $n \geqslant 1$ and a nonconstant polynomial $\mathcal{Q} \in R[\underline{x}]$.

Let $\underline{P} = \{P_1, P_2\}$ with $P_1 = -y$ and $P_2 = y + \mathcal{Q}$. We will proceed as in Theorem 5.1 but with only two monomials Q_0, Q_1 (so $\ell = 1$) and without assuming condition (1) from §5.1.

Assume that we are not in the case $n = 1 = \deg(\mathcal{Q})$; this case is dealt with separately. Let Q_∞ be a monic nonconstant monomial appearing in $\mathcal{Q}$ with a nonzero coefficient. Denote this coefficient by q_∞. Let Q_1 be a nonconstant monomial distinct from Q_∞ and of degree $\deg(Q_1) \leqslant \deg(\mathcal{Q})$. Denote the coefficient of $Q_0 = 1$ in $\mathcal{Q}$ by q_0 (the constant coefficient).

As in the proof of Theorem 5.1, Proposition 4.2 provides nonzero λ_0^*, λ_1^* in R satisfying the following: for $M = \lambda_0^* + \lambda_1^* Q_1$, both M and $M + \mathcal{Q}$ are irreducible in $K[\underline{x}]$, $\lambda_0^* \equiv 1 - q_0$ [mod q_∞] and $\lambda_1^* \equiv 1$ [mod λ_0^*] (the elements $q_\infty, \lambda_0^*, \lambda_1^*$ play the respective roles of $\lambda_0^*, \lambda_1^*, \lambda_2^*$ from Proposition 4.2).

To conclude, it suffices to show that M and $M + \mathcal{Q}$ are primitive. As λ_0^* and λ_1^* are relatively prime, M is primitive. As for $M + \mathcal{Q}$, it follows from this: the coefficients of Q_∞ and Q_0 in $M + \mathcal{Q}$ are relatively prime. Indeed the former is q_∞ and the latter is $\lambda_0^* + q_0$ which is congruent to 1 modulo q_∞.

Finally, in the case $n = 1 = \deg(\mathcal{Q})$, write $\mathcal{Q} = q_1 x + q_0$. We can take:

$$\begin{cases} \text{if } q_1 \neq 1 & \mathcal{Q} = [x + (q_0 - 1)] + [(q_1 - 1)x + 1] \\ \text{if } q_1 \neq -1 & \mathcal{Q} = [-x + (q_0 - 1)] + [(q_1 + 1)x + 1] \\ \text{if } q_1 = 1 = -1 & \mathcal{Q} = [rx + (rq_0 + 1)] + [(r + 1)x + (rq_0 + q_0 + 1)] \\ & \text{with } r \in R \setminus \{0, 1\}. \end{cases}$$

The more specific conclusion, alluded to in §1.4, that one can further take $\deg(Q_1) = 1$ if $R = K$ is a Hilbertian field, or if $R = K$ is an infinite field and $n \geqslant 2$, can be obtained from similar arguments but using the Addendum to Theorem 1.1 (in §2) and Theorem 1.4 instead of Theorem 5.1.

5.4. **Proof of Theorem 1.3.** Retain the notation from §5.1 but consider the degree 1 case. That is, we have, for $i = 1, \ldots, s$:

$$\begin{cases} P_i = A_i(\underline{x}) + B_i(\underline{x})y \\ F_i(\underline{\lambda}, \underline{x}) = A_i(\underline{x}) + B_i(\underline{x}) \left(\sum_{j=0}^{\ell} \lambda_j Q_j(\underline{x})\right). \end{cases}$$

Assume further that the polynomials Q_i are the monomials $Q_0, Q_1, \ldots, Q_{N_{\underline{d}}}$ in $\mathcal{P}ol_{k,n,\underline{d}}$ for some $\underline{d} \in (\mathbb{N}^*)^n$, with as before $Q_0 = 1$ and Q_1 and Q_2 monomials of degree $d_1 + \cdots + d_n$ and $d_1 + \cdots + d_n - 1$.

Lemma 5.4. *If as above* $\deg_y(P_1) = \ldots = \deg_y(P_s) = 1$*, then the Hilbert subset* $H_K(F_1, \ldots, F_s) \subset K^{N_{\underline{d}}+1}$ *contains a separable Hilbert subset.*

Proof of Lemma 5.4. Fix $D > \max_{\substack{1 \leqslant j \leqslant n \\ 1 \leqslant i \leqslant s}} \deg_{x_j}(F_i)$ and consider the Kronecker substitution:

$$S_D : \mathcal{P}ol_{K(\underline{\lambda}),n,\underline{D}} \to \mathcal{P}ol_{K(\underline{\lambda}),1,D^n}, \quad \text{with } \underline{D} = (D, \ldots, D),$$

mapping x_j to $x^{D^{j-1}}$, $j = 1, \dots, n$ (introduced in §4.2). Fix $i \in \{1, \dots, s\}$. From Proposition 4.3, there exist a finite set $\mathcal{S}(F_i)$ of irreducible polynomials in $K[\underline{\lambda}][x]$ of degree $\geqslant 1$ in x and a nonzero polynomial $\varphi_i \in K[\underline{\lambda}]$ such that the Hilbert subset $H_K(F_i) \subset K^{N_{\underline{d}}+1}$ contains the Hilbert subset $H_K(\mathcal{S}(F_i); \varphi_i)$. Furthermore, one can take for $\mathcal{S}(F_i)$ the set of irreducible divisors in $K[\underline{\lambda}][x]$ of the following polynomial (in which $M_{\underline{d}} = \sum_{h=0}^{N_{\underline{d}}} \lambda_h Q_h$):

$$S_D(A_i + B_i M_{\underline{d}}) = S_D(A_i) + S_D(B_i) \sum_{h=0}^{N_{\underline{d}}} \lambda_h S_D(Q_h).$$

The polynomials $S_D(Q_h)$ are distinct monomials in x (up to multiplicative constants in $K^\times$): this indeed follows from the fact that two different integers between 0 and $D^{n-1} - 1$ have different D-adic expansions $a_1 + a_2 D + \cdots + a_{n-1} D^{n-2}$ with $0 \leqslant a_j \leqslant D - 1$, $j = 1, \dots, n-1$.

Note that $S_D(A_i)$ and $S_D(B_i)$ may not be relatively prime (take for example $A_i = x_2 - 1$ and $B_i = x_3 - 1$) and so Lemma 2.1 cannot be used directly. Denote the gcd of $S_D(A_i)$ and $S_D(B_i)$ by $\Delta \in K[x]$. Conclude from Lemma 2.1 that the polynomial

$$f_i := \frac{S_D(A_i + B_i M_{\underline{d}})}{\Delta} = \frac{S_D(A_i)}{\Delta} + \frac{S_D(B_i)}{\Delta} \sum_{h=0}^{N_{\underline{d}}} \lambda_h S_D(Q_h)$$

is irreducible in $\overline{K}[\underline{\lambda}, x]$. Since $\Delta \in K[x]$, its irreducible factors f in $K[\underline{\lambda}, x]$ are in fact in $K[x]$, and so satisfy $H_K(f) = K^{N_{\underline{d}}+1}$. Conclude that one can take $\mathcal{S}(F_i) = \{f_i\}$ where f_i is the polynomial displayed above.

The polynomial f_i has an additional property: it is separable in x. Indeed, if $p > 0$, not all exponents of x in f_i are divisible by p (note that $\sum_{h=0}^{N_{\underline{d}}} \lambda_h S_D(Q_h)$ is the generic polynomial in one variable of degree $D^n - 1$).

We have thus proved that the Hilbert subset $H_K(F_1, \dots, F_s) \subset K^{N_{\underline{d}}+1}$ contains the separable Hilbert subset $H_K(f_1, \dots, f_s; \varphi_1 \cdots \varphi_s)$. □

Proof of Theorem 1.3. The statement is about polynomials in at least 2 variables that are denoted $x_1, \dots, x_n$ there. For consistency with the previous notation, we relabel them here $u, x_1, \dots, x_n$, with $n \geqslant 1$. Set $R = k[u]$ and view $k[u, x_1, \dots, x_n]$ as $R[\underline{x}]$.

Up to adding it to the given list $(A_1, B_1), \dots, (A_s, B_s)$ of couples of relatively prime polynomials in $R[\underline{x}]$, one may assume that the couple $(1, 0)$ is in this list; this will guarantee that the desired polynomial M is itself irreducible in $R[\underline{x}]$ as requested.

With the notation from this subsection, Lemma 5.4 gives that the Hilbert subset $H_K(F_1, \dots, F_s) \subset K^{N_{\underline{d}}+1}$ contains a separable Hilbert subset, say $H_K(f_1, \dots, f_s; \varphi)$. From the separable case of Theorem 4.8, there is an integer d_0 such that for every integer $\delta \geqslant d_0$, $H_K(f_1, \dots, f_s; \varphi)$ contains a tuple $\underline{\lambda}^* \in R^{N_{\underline{d}}+1}$ such that λ_1^* and λ_2^* are relatively prime in R and $\deg_u(M_{\underline{d}}(\underline{\lambda}^*, \underline{x})) = \delta$. We have *a fortiori* $\underline{\lambda}^* \in H_K(F_1, \dots, F_s) \subset K^{N_{\underline{d}}+1}$:

$$F_i(\underline{\lambda}^*, \underline{x}) = A_i(\underline{x}) + B_i(\underline{x}) M_{\underline{d}}(\underline{\lambda}^*, \underline{x}) \text{ is irreducible in } K[\underline{x}],\ i = 1, \dots, s.$$

Assume d_0 large enough so that, if $d_i \geqslant d_0$, $i = 1, \dots, n$, then

$$d_1 + \cdots + d_n - 1 > \max_{i=1,\ldots,s} \max(\deg(A_i), \deg(B_i)).$$

Irreduciblility of each $A_i(\underline{x})+B_i(\underline{x})M_{\underline{d}}(\underline{\lambda}^*, \underline{x})$ in $R[\underline{x}]$ is deduced by proving it is primitive from λ_1^*, λ_2^* being relatively prime as in the proof of Theorem 5.1.

Finally, up to multiplying φ by the coordinate λ_h corresponding to the monomial $x_1^{d_1} \cdots x_n^{d_n}$, one guarantees $\deg_{x_i}(M_{\underline{d}}(\underline{\lambda}^*, \underline{x})) = d_i$, $i = 1, \ldots, n$. This completes the proof: $M_{\underline{d}}(\underline{\lambda}^*, \underline{x})$ is the requested polynomial. □

Remark 5.5. Lemma 5.4 also shows that the degree 1 case of the Schinzel hypothesis holds when R is a Hilbertian field (totally Hilbertian is not needed), thus completing the proof of the addendum to Theorem 1.1 in situation (b).

5.5. **Proof of Corollary 1.6.** Assume $n \geqslant 2$, fix an arbitrary field k, a subset $\mathcal{S} = \{a_1, \ldots, a_t\} \subset k$, $a_0 \in \overline{k} \setminus \mathcal{S}$, separable over k, and $V \in k[\underline{x}]$, $V \neq 0$. We will show this more precise version of Corollary 1.6.

Corollary 1.6 (explicit form)**.** *Let $w_0, \ldots, w_t \in k[\underline{x}]$ be $t+1$ nonzero polynomials with $w_0 = 1$. Assume that $(w_i) + (w_j) = k[\underline{x}]$ for $i \neq j$ and each w_i is relatively prime to V. For all suitably large integers $d_1, \ldots, d_n$ (larger than some d_0 depending on $\mathcal{S}, a_0, V, w_1, \ldots, w_t$), there is a polynomial $U \in k[\underline{x}]$ such that these three conclusions hold:*

(a) $U - a_iV = w_iH_i$ *with* $H_i \in k[\underline{x}]$ *irreducible in* $k(a_0)[\underline{x}]$ *and not dividing* w_i, $i = 1, \ldots, t$,

(b) $\deg(U - a_0V) = \max(\deg(U), \deg(V))$,

(c) $\deg_{x_i}(U) = d_i$, $i = 1, \ldots, n$.

In order to obtain the version of Corollary 1.6 from §1, it suffices to choose $w_1, \ldots, w_t$ as in the statement but not in k and

$$d_1 > \max(\deg(V), \deg(w_1), \ldots, \deg(w_t)).$$

It then follows from $\deg(U) \geqslant \deg_{x_1}(U) = d_1$ (using (c)) that $\deg(U-a_iV) = \deg(U)$, and next from (a) that $U - a_iV$ is reducible, $i = 1, \ldots, t$.

Remark 5.6. The assumption $(w_i) + (w_j) = k[\underline{x}]$ is necessary when $V = 1$: if we have $U - a_iV = w_iH_i$ and $U - a_jV = w_jH_j$ for two distinct indices i, j, then $w_iH_i - w_jH_j = (a_j - a_i)V$.

Proof. As $(w_i) + (w_j) = k[\underline{x}]$, $i \neq j$, the Chinese Remainder Theorem may be used to conclude that there is a polynomial $U_0 \in k[\underline{x}]$ such that

$$U_0 - a_iV = w_ip_i \text{ with } p_i \in k[\underline{x}],\ i = 1, \ldots, t.$$

As $w_0 = 1$, we also have $U_0 - a_0V = w_0p_0$ for some p_0, but here p_0 is in $k(a_0)[\underline{x}]$. Furthermore the polynomials $U \in k(a_0)[\underline{x}]$ satisfying the same $(t+1)$ conditions are of the form

$$U(\underline{x}) = U_0(\underline{x}) + M(\underline{x}) \prod_{i=0}^{t} w_i(\underline{x})$$

for some $M \in k(a_0)[\underline{x}]$. For such a polynomial U, we have

$$U - a_iV = w_i \left(p_i + M \textstyle\prod_{j\neq i} w_i(\underline{x})\right),\ \ i = 0, \ldots, t.$$

Up to changing U_0, we may assume that $p_0, \ldots, p_t$ are nonzero.

For each $i = 0, \dots, t$, the polynomials $A_i = p_i$ and $B_i = \prod_{j \neq i} w_i(\underline{x})$ are relatively prime in $k(a_0)[\underline{x}]$. Namely if $\pi \in k(a_0)[\underline{x}]$ is a common irreducible divisor in $k(a_0)[\underline{x}]$ of these two polynomials, then π divides p_i and π divides w_j for some $j \neq i$ and hence, π is a common divisor of $U_0 - a_i V$ and $U_0 - a_j V$. Therefore π divides V and w_j, which contradicts the assumption $(V, w_j) = 1$.

Set $R = k(a_0)[x_n]$, $K = k(a_0)(x_n)$, $\underline{x} = (x_1, \dots, x_{n-1})$ and, for $\underline{d} \in (\mathbb{N}^*)^{n-1}$ and $i = 0, \dots, t$,

$$\begin{cases} P_i = A_i(\underline{x}) + B_i(\underline{x})y \\ F_i(\underline{\lambda}, \underline{x}) = A_i(\underline{x}) + B_i(\underline{x}) \left(\sum_{j=0}^{N_{\underline{d}}} \lambda_j Q_j(\underline{x}) \right). \end{cases}$$

As in the proof of Theorem 1.3, the Hilbert subset $H_K(F_0, \dots, F_t)$ contains a separable Hilbert subset $H_K(f_0, \dots, f_t, \varphi)$ with $f_0, \dots, f_t \in K[\underline{\lambda}, x]$ of degree $\geqslant 1$ in x and $\varphi \in K[\underline{\lambda}]$, $\varphi \neq 0$.

The field extension $k(a_0)/k$ is finite and separable. Setting $R_0 = k[x_n]$ and $K_0 = k(x_n)$, so is the extension K/K_0. From [FJ08, Corollary 12.2.3], $H_K(f_0, \dots, f_t, \varphi)$ contains a separable Hilbert subset $\mathcal{H}_{K_0}$ of $K_0^{N_{\underline{d}}+1}$.

Proceed as in the proof of Theorem 1.3 to conclude that there is an integer d_0 with the following property: if $\delta_1, \delta_2, \dots, \delta_n$ are integers $\geqslant d_0$, the Hilbert subset $\mathcal{H}_{K_0}$, and so the Hilbert subset $H_K(F_0, \dots, F_t)$ too, contains a tuple $\underline{\lambda}^* = (\lambda_0^*, \dots, \lambda_{N_{\underline{d}}}^*) \in R_0^{N_{\underline{d}}+1}$ such that λ_1^* and λ_2^* are irreducible in R_0, and $\deg_{x_i}(M_{\underline{d}}(\underline{\lambda}^*, \underline{x})) = \delta_i$, $i = 1, \dots, n$. Choosing again for Q_1, Q_2 monomials of respective degrees $d_1 + \cdots + d_{n-1}$ and $d_1 + \cdots + d_{n-1} - 1$ and assuming d_0 suitably large, we obtain as for Theorem 1.3 that each of the polynomials

$$F_i(\underline{x}) = A_i(\underline{x}) + B_i(\underline{x}) M_{\underline{d}}(\underline{\lambda}^*, \underline{x})$$

is irreducible in $k(a_0)[x_n][x_1, \dots, x_{n-1}]$, $i = 0, \dots, t$.

Up to increasing d_0, one can further guarantee that $\delta_1, \dots, \delta_n$ are large enough so that $\deg(M_{\underline{d}}(\underline{\lambda}^*, \underline{x})) > \deg(U_0)$ and F_i does not divide w_i, $i = 1, \dots, s$. The polynomial

$$U(\underline{x}) = U_0(\underline{x}) + M_{\underline{d}}(\underline{\lambda}^*, \underline{x}) \prod_{i=0}^{t} w_i(\underline{x})$$

is in $k[\underline{x}]$ and satisfies the required condition $U - a_i V = w_i H_i$, with $H_i = F_i$ irreducible in $k(a_0)[\underline{x}]$, $i = 0, \dots, t$. Up to replacing the Hilbert subset $H_K(f_0, \dots, f_t, \varphi)$ by a Zariski open subset of it, one can also request that $\deg(U - a_0 V) = \max(\deg(U), \deg(V))$. Finally $\deg_{x_i}(U) = \delta_i + \sum_{j=1}^{t} \deg_{x_i}(w_j)$ can be taken to be any given suitably large integer d_i, $i = 1, \dots, n$. □

References

[BDN09] Arnaud Bodin, Pierre Dèbes, and Salah Najib. Irreducibility of hypersurfaces. *Comm. Algebra*, 37(6):1884–1900, 2009.

[BDN17] Arnaud Bodin, Pierre Dèbes, and Salah Najib. Families of polynomials and their specializations. *J. Number Theory*, 170:390–408, 2017.

[Bod08] Arnaud Bodin. Reducibility of rational functions in several variables. *Israel J. Math.*, 164:333–347, 2008.

[BS09] Lior Bary-Soroker. Dirichlet's theorem for polynomial rings. *Proc. Amer. Math. Soc.*, 137:73–83, 2009.

[BS12] Lior Bary-Soroker. Irreducible values of polynomials. *Adv. Math.*, 229(2):854–874, 2012.

[BW05] Andreas O. Bender and Olivier Wittenberg. A potential analogue of Schinzel's hypothesis for polynomials with coefficients in $\mathbb{F}_q[t]$. *Int. Math. Res. Not.*, (36):2237–2248, 2005.

[CTS82] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc. Sur le principe de Hasse et l'approximation faible, et sur une hypothèse de Schinzel. *Acta Arith.*, 41:33–53, 1982.

[Dèb99] Pierre Dèbes. Density results for Hilbert subsets. *Indian J. Pure Appl. Math.*, 30(1):109–127, 1999.

[FJ] Michael D. Fried and Moshe Jarden. *Field arithmetic.* next edition.

[FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic.* Ergebnisse der Mathematik und ihrer Grenzgebiete. A Series of Modern Surveys in Mathematics, 11. Springer-Verlag, Berlin, 3rd edition, 2008. Revised by Jarden. xxiv+792 pp.

[HW16] Yonatan Harpaz and Olivier Wittenberg. On the fibration method for zero-cycles and rational points. *Ann. of Math.*, 183:229–295, 2016.

[KL19] Heinrich Kornblum and Edmund Landau. Über die Primfunktionen in einer arithmetischen Progression. *Math. Z.*, 5(1-2):100–111, 1919.

[Lan83] Serge Lang. *Fundamentals of Diophantine geometry.* Springer-Verlag, New York, 1983.

[Naj04] Salah Najib. Sur le spectre d'un polynôme à plusieurs variables. *Acta Arith.*, 114(2):169–181, 2004.

[Naj05] Salah Najib. Une généralisation de l'inégalité de Stein-Lorenzini. *J. Algebra*, 292(2):566–573, 2005.

[Pol11] Paul Pollack. On polynomial rings with a Goldbach property. *Amer. Math. Monthly*, 118(1):71–77, 2011.

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[Sch82] Andrzej Schinzel. *Selected topics on polynomials.* University of Michigan Press, Ann Arbor, Mich., 1982.

[Sch00] Andrzej Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier.

[SS58] Andrzej Schinzel and Waclaw Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith.*, 4:185–208; erratum 5 (1958), 259, 1958.

[Swa62] Richard G. Swan. Factorization of polynomials over finite fields. *Pacific J. Math.*, 12:1099–1106, 1962.

[Uch80] Kôji Uchida. Separably Hilbertian fields. *Kodai Math. J.*, 3(1):83–95, 1980.

Email address: `arnaud.bodin@univ-lille.fr`
Email address: `pierre.debes@univ-lille.fr`
Email address: `slhnajib@gmail.com`

Laboratoire Paul Painlevé, Mathématiques, Cité Scientifique, Université de Lille, 59655 Villeneuve d'Ascq Cedex, France

Laboratoire Paul Painlevé, Mathématiques, Cité Scientifique, Université de Lille, 59655 Villeneuve d'Ascq Cedex, France

Laboratoire ATRES, Faculté Polydisciplinaire de Khouribga, Université Sultan Moulay Slimane, BP 145, Hay Ezzaytoune, 25000 Khouribga, Maroc.