# The Hilbert–Schinzel specialization property

Arnaud Bodin, Pierre Dèbes, Joachim König, Salah Najib

# THE HILBERT-SCHINZEL SPECIALIZATION PROPERTY

ARNAUD BODIN, PIERRE DÈBES, JOACHIM KÖNIG, AND SALAH NAJIB

Abstract. We establish a version "over the ring" of the celebrated Hilbert Irreducibility Theorem. Given finitely many polynomials in $k+n$ variables, with coefficients in $\mathbb{Z}$, of positive degree in the last $n$ variables, we show that if they are irreducible over $\mathbb{Z}$ and satisfy a necessary "Schinzel condition", then the first $k$ variables can be specialized in a Zariski-dense subset of $\mathbb{Z}^k$ in such a way that irreducibility over $\mathbb{Z}$ is preserved for the polynomials in the remaining $n$ variables. The Schinzel condition, which comes from the Schinzel Hypothesis, is that, when specializing the first $k$ variables in $\mathbb{Z}^k$, the product of the polynomials should not always be divisible by some common prime number. Our result also improves on a "coprime" version of the Schinzel Hypothesis: under some Schinzel condition, coprime polynomials assume coprime values. We prove our results over many other rings than $\mathbb{Z}$, e.g. UFDs and Dedekind domains.

## 1. Introduction

This paper is about specialization properties of polynomials $P(\underline{t},\underline{y})$ with coefficients in an integral domain $Z$. The $k+n$ variables from the two tuples $\underline{t}=(t_1,\dots,t_k)$ and $\underline{y}=(y_1,\dots,y_n)$ $(k,n\geqslant 1)$ are of two types; the $t_i$ are those to be specialized, unlike the $y_i$. The next statement introduces both a central property and a main result of the paper.

Say that a non-unit $a\in Z$, $a\neq 0$, is *a fixed divisor of $P$ w.r.t. $\underline{t}$* if $P(\underline{m},\underline{y})\equiv 0 \pmod a$ for every $\underline{m}\in Z^k$, and denote the set of all fixed divisors by $\mathcal{F}_{\underline{t}}(P)$.

**Theorem 1.1.** *Let $Z$ be the ring of integers of a number field of class number 1 or any polynomial ring $R[x_1,\dots,x_r]$ $(r\geqslant 1)$ over a UFD $R$* [1]*. Then the ring $Z$ has the* Hilbert-Schinzel specialization property*, for any integers $k,n,s\geqslant 1$; i.e. the following holds:*
*Let $P_1(\underline{t},\underline{y}),\dots,P_s(\underline{t},\underline{y})$ be $s$ polynomials, irreducible in $Z[\underline{t},\underline{y}]$, of degree $\geqslant 1$ in $\underline{y}$. Assume that the product $P_1\cdots P_s$ has no fixed divisor in $Z$ w.r.t. $\underline{t}$. Then there is a Zariski-dense subset $H\subset Z^k$ such that $P_1(\underline{m},\underline{y}),\dots,P_s(\underline{m},\underline{y})$ are irreducible in $Z[\underline{y}]$ for every $\underline{m}\in H$.*

*Remark* 1.2. The fixed divisor assumption $\mathcal{F}_{\underline{t}}(P_1\cdots P_s)=\emptyset$ is necessary, and may fail. For example, the polynomial $P=(t^p-t)y+(t^p-t+p)$, with $p$ a prime number, is irreducible in $\mathbb{Z}[t,y]$; and $p\in\mathcal{F}_t(P)$, since $p$ divides $(m^p-m)$ for every $m\in\mathbb{Z}$. A similar example occurs with $Z=\mathbb{F}_q[u]$. Take $P=(t^q-t+u)y+(t^q-t)^2+u$. For every $m(u)\in\mathbb{F}_q[u]$, the constant term of $m(u)^q-m(u)$ is zero, so $P(m(u),y)$ is divisible by $u$.

The name "Schinzel" in our specialization property refers to the Schinzel Hypothesis [SS58], which corresponds to the case $(k=1,\ n=0,\ Z=\mathbb{Z})$: if $P_1(t),\dots,P_s(t)$ are irreducible in $\mathbb{Z}[t]$ and the product has no fixed prime divisor, then $P_1(m),\dots,P_s(m)$ are

*Date*: November 29, 2021.
2010 *Mathematics Subject Classification.* Primary 12E05, 12E30; Sec. 13Fxx, 11A05, 11A41.
*Key words and phrases.* Primes, Polynomials, Schinzel Hypothesis, Hilbert's Irreducibility Theorem.
*Acknowledgment.* The first and second authors were supported by the Labex CEMPI (ANR-11-LABX-0007-01). The first author was also supported by the ANR project "LISA" (ANR-17-CE40–0023-01), and thanks the University of British Columbia for his visit at PIMS.

[1] As usual, UFD stands for Unique Factorization Domain and PID for Principal Ideal Domain.

prime numbers for infinitely many $m \in \mathbb{Z}$. This statement implies many famous conjectures in number theory, like the Twin Prime conjecture (for $P_1(t) = t$ and $P_2(t) = t + 2$). It is however still out of reach; the case $n = 0$ is excluded in Theorem 1.1.

Another special case of interest is when $Z = \mathbb{Z}$ and each polynomial $P_i$ is of the form $P_i = P_{i1}(\underline{t})y_1 + \cdots + P_{i\ell}(\underline{t})y_\ell$. Theorem 1.1 then concludes, under the corresponding assumptions, that for every $\underline{m}$ in some Zariski-dense subset of $\mathbb{Z}^k$, the values $P_{i1}(\underline{m}), \ldots, P_{i\ell}(\underline{m})$ are *coprime*[2], for each $i = 1, \ldots, s$. This was proved by Schinzel [Sch02]; see also [Eke91] and [Poo03] for the special case $s = 1$, $\ell = 2$ but with a positive density result for the good $\underline{m}$.

This coprime conclusion is interesting for its own sake. Theorem 1.1 already carries it over to more general rings than $\mathbb{Z}$. We show that it holds on even more rings. For simplicity, we restrict below to the situation that *one* set of polynomials $P_j(t)$ in *one* variable is given, and refer to Theorem 3.7 for the general version.

**Theorem 1.3.** *Assume that $Z$ is a UFD or a Dedekind domain. Let $Q$ be the fraction field of $Z$. Then the* coprime Schinzel Hypothesis *holds for $Z$, i.e. the following is true: Let $P_1(t), \ldots, P_\ell(t) \in Z[t]$ be $\ell \geqslant 2$ nonzero polynomials, coprime in $Q[t]$ and such that:*

(AV) *no non-unit of $Z$ divides all values $P_1(z), \ldots, P_\ell(z)$ with $z \in Z$.*

*Then there exists an element $m \in Z$ such that $P_1(m), \ldots, P_\ell(m)$ are coprime in $Z$.*

Assumption on Values (AV) is the exact translation of the fixed divisor assumption $\mathcal{F}_t(P) = \emptyset$ for the polynomial $P = P_1(t)y_1 + \cdots + P_\ell(t)y_\ell$ considered above.

*Remark* 1.4. (a) The situation that $Z$ is a UFD is the natural context for the coprime Schinzel Hypothesis: primes are the irreducible elements, Gauss's lemma is available, etc. We will however not use the full UFD property and prove Theorem 1.3 for domains that we call *near UFD*. These play a central role in the paper and are defined by this sole property: *every non-zero element has finitely many prime divisors, and every non-unit has at least one*; we say more on near UFDs in §2.3. Theorem 1.3 also holds for some non near UFDs, starting with Dedekind domains; the ring of entire functions is another type of example (Proposition 2.6); on the other hand, the coprime Schinzel Hypothesis may fail, e.g. for $Z = \mathbb{Z}[\sqrt{5}]$ (Proposition 2.10).

(b) If $Z$ is infinite, then infinitely many $m$ in fact satisfy the conclusion of Theorem 1.3 (see Remark 2.2). If $Z$ is finite, it is a field, and for fields, "coprime" means "not all zero". This makes the coprime Schinzel Hypothesis obviously true, with the difference for finite fields that the infiniteness of good $m$ is of course not true. [3]

(c) Theorem 1.3 with $Z = \mathbb{Z}$, contained as we said in [Sch02, Thm.1], is also a corollary of [BDN20a, Thm.1.1], which shows this stronger property for $Z$ a PID:

(**) *for $P_1(t), \ldots, P_\ell(t)$ as in Theorem 1.3, but not necessarily satisfying assumption* (AV)*, the set $\mathcal{D} = \{\gcd(P_1(m), \ldots, P_\ell(m)) \mid m \in \mathbb{Z}\}$ is finite and stable under gcd.*

We show in §2.5 that this property is false in general when $Z$ is only a UFD.

In addition to the original Schinzel Hypothesis and its coprime version, Theorem 1.1 relates to Hilbert's Irreducibility Theorem (HIT). In the setup of Theorem 1.1 and with

[2]Elements from an integral domain are *coprime* if they have no common divisor other than units.

[3]Passing from "at least one" to "infinitely many" prime values is not nearly as convenient for the original Schinzel Hypothesis. Indeed, [SS20] establishes asymptotic results showing that "most" irreducible integer polynomials without fixed prime divisors take at least one prime value, whereas the infiniteness assertion is not known for a single non-linear polynomial.

$Q$ the fraction field of $Z$, the classical Hilbert result concludes that for every $\underline{m}$ in some Zariski-dense subset $H \subset Q^k$, the polynomials $P_1(\underline{m}, \underline{y}), \dots, P_s(\underline{m}, \underline{y})$ are irreducible *in* $Q[\underline{y}]$ [FJ08, Theorem 13.14.2]. In Theorem 1.1, we insist that $H \subset Z^k$ and the irreducibility of $P_1(\underline{m}, \underline{y}), \dots, P_s(\underline{m}, \underline{y})$ be *over the ring* $Z$, i.e. in $Z[\underline{y}]$. As $Z$ is a UFD, this is equivalent to $P_1(\underline{m}, \underline{y}), \dots, P_s(\underline{m}, \underline{y})$ being irreducible in $Q[\underline{y}]$ and *primitive w.r.t.* $Z$ [4].

For an integral domain that is not necessarily a UFD, we generalize the Hilbert-Schinzel property as follows. Assume that $Z$ is of characteristic 0 or imperfect[5].

*Definition* 1.5. The ring $Z$ has the *Hilbert-Schinzel specialization property* for integers $k, n, s \geqslant 1$ if the following holds. Let $P_1(\underline{t}, \underline{y}), \dots, P_s(\underline{t}, \underline{y})$ be $s$ polynomials, irreducible in $Q[\underline{t}, \underline{y}]$, primitive w.r.t. $Z$, of degree $\geqslant 1$ in $\underline{y}$. Assume that $P_1 \cdots P_s$ has no fixed divisor in $Z$ w.r.t. $\underline{t}$. Then there is a Zariski-dense subset $H \subset Z^k$ such that for every $\underline{m} \in H$, the polynomials $P_1(\underline{m}, \underline{y}), \dots, P_s(\underline{m}, \underline{y})$ are irreducible in $Q[\underline{y}]$ and primitive w.r.t. $Z$.

It follows from the conclusion that for $\underline{m} \in H$, the polynomials $P_1(\underline{m}, \underline{y}), \dots, P_s(\underline{m}, \underline{y})$ are irreducible in $Z[\underline{y}]$; this implication holds without the UFD assumption.

More classical definitions (recalled in Definition 4.1) disregard the primitivity part. For a *Hilbertian ring*, only the irreduciblity in $Q[\underline{y}]$ is requested in the conclusion, and the fixed divisor condition $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s) = \emptyset$ is not assumed. If $Z$ is a field (and so conditions on primitivity and fixed divisors automatically hold and may be omitted), Definition 1.5 is that of a *Hilbertian field*.

The following result generalizes Theorem 1.1.

**Theorem 1.6.** *Assume that $Z$ is a Hilbertian ring. Then we have the following.*
(a) *If $Z$ is a near UFD[6], the Hilbert-Schinzel property holds for any $k, n, s \geqslant 1$.*
(b) *If $Z$ is a Dedekind domain, the Hilbert-Schinzel property holds with $k = 1$ and $n, s \geqslant 1$.*

Hilbert's Irreducibility Theorem is one of the few general and powerful tools in Arithmetic Geometry. Typically it is used when one needs to find irreducible fibers of some morphism above closed points, defined over some field. The flagship example, Hilbert's motivation in fact, was the realization of the symmetric group $S_k$ as a Galois group over $\mathbb{Q}$, via the consideration of the morphism $\mathbb{A}^k \to \mathbb{A}^k/S_k$, or equivalently, of the generic polynomial $P(\underline{t}, y) = y^k + t_1 y^{k-1} + \cdots + t_k$ of degree $k$ (e.g. [Ser92, §3]). More geometric situations *à la* Bertini are numerous too, starting with that of an irreducible family of hypersurfaces $(P(\underline{t}, \underline{y}) = 0) \subset \mathbb{A}^n$ parametrized by $\underline{t} \in \mathbb{A}^k$ (see [FJ08, §10.4] for a specific statement of the Bertini-Noether theorem). Theorem 1.6 extends the scope of HIT and its applications to allow working over *rings*. It is for example a good tool when investigating the arithmetic of families of number rings $\mathbb{Z}[\underline{t}, y]/\langle P(\underline{t}, y)\rangle$ with $\underline{t} \in \mathbb{Z}^k$, or, in a geometric context, to deal with Bertini irreducibility conclusions over rings.

*Remark* 1.7. (a) [BDN20b, Theorem 4.6] provides a large class of Hilbertian rings: those domains $Z$ such that the fraction field $Q$ has *a product formula* (and is of characteristic 0 or imperfect). We refer to [FJ08, §15.3] or [BDN20b, §4.1] for a full definition. The basic example is $Q = \mathbb{Q}$. The product formula is: $\prod_p |a|_p \cdot |a| = 1$ for every $a \in \mathbb{Q}^\star$, where $p$

[4] A polynomial over an integral domain $Z$ is *primitive w.r.t. $Z$* if its coefficients are coprime in $Z$. A monomial is primitive iff its leading coefficient is a unit of $Z$. The zero polynomial is not primitive.

[5] *Imperfect* means that $Z^p \neq Z$ if $p = \mathrm{char}(Z)$. This "imperfectness assumption" is made to avoid some subtelty from the Hilbertian field theory (e.g. explained in [BDN20b, §4.1]) that otherwise leads to distinguish between Hilbertian fields and strongly Hilbertian fields and is irrelevant in this paper.

[6] as defined in Remark 1.4(a).

ranges over all prime numbers, $|\cdot|_p$ is the $p$-adic absolute value and $|\cdot|$ is the standard absolute value. Rational function fields $k(x_1,\dots,x_r)$ in $r \geqslant 1$ variables over a field $k$, and finite extensions of fields with the product formula are other examples [FJ08, §15.3].

(b) The more concrete product formula condition on $Q$ may thus replace the Hilbertian ring assumption in Theorem 1.6. This shows Theorem 1.1 as a special case of Theorem 1.6(a). This also provides a large class of rings to which Theorem 1.6(b) applies: *all rings of integers of number fields*. On the other hand, as mentioned earlier, the coprime Schinzel Hypothesis fails for $Z = \mathbb{Z}[\sqrt{5}]$, and so, so does the Hilbert-Schinzel property. Yet, $\mathbb{Z}[\sqrt{5}]$ is a Hilbertian ring; it is however neither a near UFD nor a Dedekind domain.

(c) It is unclear whether Theorem 1.6(b) extends to the situation $k \geqslant 1$. We refer to Theorem 4.4 for a version of Theorem 1.6 for Dedekind domains with $k \geqslant 1$ and $s = 1$.

(d) We show further, in Lemma 3.1, that for a near UFD $Z$, assumption $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s) = \emptyset$ always holds in Definition 1.5 (and so can be omitted) if $Z$ has this *infinite residue property*: every principal prime ideal $pZ$ is of infinite norm $|Z/pZ|$. Furthermore this property automatically holds in these cases: (a) $Z = R[u_1,\dots,u_r]$ is any polynomial ring over an integral domain $R$ unless $Z = \mathbb{F}_q[u]$, (b) if $Z$ contains an infinite field. The infinite residue property fails if $Z$ is $\mathbb{Z}$ or, more generally, the ring of integers of a number field. Other ways to get rid of the assumption $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s) = \emptyset$ are explained in §4.3.1.

The paper is organized as follows. The coprime Schinzel Hypothesis (from Theorem 1.3) will be defined in its general form for $s \geqslant 1$ sets of polynomials $\{P_{i1}(\underline{t}),\dots,P_{i\ell_i}(\underline{t})\}$ in $k \geqslant 1$ variables $t_1,\dots,t_k$ (see Definition 3.2). Section 2 is devoted to the special case $k = s = 1$, i.e. the case considered in Theorem 1.3, and Section 3 to the general case $k, s \geqslant 1$. The Hilbert-Schinzel specialization property (from Definition 1.5) is discussed in Section 4; in particular, Theorem 1.6 is proved there.

## 2. The coprime Schinzel Hypothesis - case $k = s = 1$

For simplicity, and to avoid confusion, we denote by $\mathcal{C}opSch(1,1)$ the coprime Schinzel Hypothesis in the form given in Theorem 1.3 (which corresponds to the case $k = s = 1$ of Definition 3.2 given later).

In §2.1, we introduce a basic parameter of the problem. We then prove Theorem 1.3 for Dedekind domains in §2.2. The other case of Theorem 1.3 will be proved in the more general situation $k, s \geqslant 1$ in §3 for *near UFDs*. We introduce them and briefly discuss some basic properties in §2.3. In §2.4, we consider property $\mathcal{C}opSch(1,1)$ over rings that are neither near UFDs nor Dedekind domains. Finally §2.5 discusses the gcd stability property mentioned in Remark 1.4(c) and displays the counter-example announced there.

Let $Z$ be an integral domain. Denote the fraction field of $Z$ by $Q$ and the group of invertible elements, also called units, by $Z^\times$.

### 2.1. **A preliminary lemma.**

Let $t$ be a variable and $P_1,\dots,P_\ell \in Z[t]$ be $\ell$ nonzero polynomials ($\ell \geqslant 2$), assumed to be coprime in $Q[t]$; equivalently, they have no common root in an algebraic closure of $Q$. As $Q[t]$ is a PID, we have $\sum_{i=1}^{\ell} P_i\, Q[t] = Q[t]$. It follows that $(\sum_{i=1}^{\ell} P_i\, Z[t]) \cap Z$ is a nonzero ideal of $Z$. Fix a nonzero element $\delta \in Z$ in this ideal. For example, if $\ell = 2$, one can take $\delta$ to be the resultant $\rho = \mathrm{Res}(P_1, P_2)$ [Lan65, V §10].

**Lemma 2.1.** *For every $m \in Z$, denote the set of common divisors of $P_1(m),\dots,P_\ell(m)$ by $\mathcal{D}_m$. Then for every $m \in Z$, the set $\mathcal{D}_m$ is a subset of the set of divisors of $\delta$. Furthermore, for every $z \in Z$, we have $\mathcal{D}_m = \mathcal{D}_{m+z\delta}$.*

*Proof.* From the coprimality assumption in $Q[t]$ of $P_1, \dots, P_\ell$, there exist some polynomials $V_1, \dots, V_\ell \in Z[t]$ satisfying a Bézout condition

$$V_1(t)P_1(t) + \cdots + V_\ell(t)P_\ell(t) = \delta.$$

The same holds with any $m \in Z$ substituted for $t$. The first claim follows. For the second claim, we adjust an argument of Frenkel and Pelikán [FP17] who observed this periodicity property in the special case ($\ell = 2$, $Z = \mathbb{Z}$) with $\delta$ equal to the resultant $\rho = \mathrm{Res}(P_1, P_2)$.

For every $m, z \in Z$, we have $P_i(m + z\delta) \equiv P_i(m) \pmod{\delta}$, $i = 1, \dots, \ell$. It follows that the common divisors of $P_1(m), \dots, P_\ell(m), \delta$ are the same as those of $P_1(m + z\delta), \dots, P_\ell(m + z\delta), \delta$. As both the common divisors of $P_1(m), \dots, P_\ell(m)$ and those of $P_1(m + z\delta), \dots, P_\ell(m + z\delta)$ divide $\delta$, the conclusion $\mathcal{D}_m = \mathcal{D}_{m+z\delta}$ follows. □

*Remark* 2.2 (on the set of "good" $m$). It follows from the periodicity property that, if $Z$ is infinite, then the set, say $\mathcal{S}$, of all $m \in Z$ such that $P_1(m), \dots, P_\ell(m)$ are coprime in $Z$, is infinite if it is nonempty. The set $\mathcal{S}$ can nevertheless be of arbitrarily small density. Take $Z = \mathbb{Z}$, $P_1(t) = t$, $P_2(t) = t + \Pi_h$, with $\Pi_h$ ($h \in \mathbb{N}$) the product of primes in $[1, h]$. The set $\mathcal{S}$ consists of the integers which are prime to $\Pi_h$. Its density is:

$$\frac{\varphi(\Pi_h)}{\Pi_h} = \left(1 - \frac{1}{2}\right) \cdots \left(1 - \frac{1}{p_h}\right)$$

where $p_h$ is the $h$-th prime number and $\varphi$ is the Euler function. The sequence $\varphi(\Pi_h)/\Pi_h$ tends to 0 when $h \to \infty$ (since the series $\sum_{h=0}^{\infty} 1/p_h$ diverges).

2.2. **Proof of Theorem 1.3 for Dedekind domains.** The assumptions and notation of this paragraph, including Proposition 2.3 below are as follows. The ring $Z$ is a Dedekind domain. As in the coprime Schinzel Hypothesis, $P_1(t), \dots, P_\ell(t)$ are $\ell \geqslant 2$ nonzero polynomials in $Z[t]$, coprime in $Q[t]$ and satisfying Assumption (AV); $\delta$ is the associated parameter from §2.1 and $\delta Z = \prod_{i=1}^{r} \mathcal{Q}_i^{e_i}$ is the factorization of the principal ideal $\delta Z$ into prime ideals of $Z$. We also define $\mathfrak{I}$ as the ideal generated by all values $P_1(z), \dots, P_\ell(z)$ with $z \in Z$, and factor $\mathfrak{I}$ into prime ideals: $\mathfrak{I} = \prod_{i=1}^{q} \mathcal{Q}_i^{g_i}$; we may assume that each of the prime ideals $\mathcal{Q}_1, \dots, \mathcal{Q}_r$ dividing $\delta Z$ indeed occurs in the product by allowing exponents $g_i$ to be 0.

Consider then the ideals $\mathcal{Q}_i^{g_i+1}$, $i = 1, \dots, r$. Either $r \leqslant 1$ or any two of them are comaximal[7]. As none of them contains $\mathfrak{I}$, for each $j = 1, \dots, r$, there exists $i_j \in \{1, \dots, \ell\}$ and $m_j \in Z$ such that $P_{i_j}(m_j) \not\equiv 0 \pmod{\mathcal{Q}_j^{g_j+1}}$. The Chinese Remainder Theorem yields an element $m \in Z$ such that $m \equiv m_j \pmod{\mathcal{Q}_j^{g_j+1}}$, for each $j = 1, \dots, r$. It follows that $P_{i_j}(m) \notin \mathcal{Q}_j^{g_j+1}$, and so

$$(P_1(m), \dots, P_\ell(m)) \not\equiv (0, \dots, 0) \pmod{\mathcal{Q}_i^{g_i+1}}, \text{ for each } i = 1, \dots, r.$$

Proposition 2.3(a) below (with $z = 0$ and $\alpha = m$) concludes that $P_1(m), \dots, P_\ell(m)$ are coprime in $Z$, thus ending the proof of Theorem 1.3 for Dedekind domains. The more general statement in Proposition 2.3(a) and the additional statement (b) will be used later.

**Proposition 2.3.** *Under the assumption and notation of §2.2, let $\omega \in Z$ be a multiple of $\delta$ and let $\alpha \in Z$ be an element such that*

(*) $$(P_1(\alpha), \dots, P_\ell(\alpha)) \not\equiv (0, \dots, 0) \pmod{\mathcal{Q}_i^{g_i+1}},\ i = 1, \dots, r.$$

(a) *Then, for every $z \in Z$, the elements $P_1(\alpha + z\omega), \dots, P_\ell(\alpha + z\omega)$ are coprime in $Z$.*

[7]Two ideals $U, V$ of an integral domain $Z$ are *comaximal* if $U + V = Z$.

(b) *Furthermore, if instead of* (AV)*, it is assumed that no prime of $Z$ divides all values $P_1(z), \dots, P_\ell(z)$ with $z \in Z$, then for every $z \in Z$, the elements $P_1(\alpha + z\omega), \dots, P_\ell(\alpha + z\omega)$ have no common prime divisor.*

*Proof.* (a) From Lemma 2.1, it suffices to show that $P_1(\alpha), \dots, P_\ell(\alpha)$ have no non-unit divisors. Assume on the contrary that

$$(P_1(\alpha), \dots, P_\ell(\alpha)) \equiv 0 \pmod{a} \text{ for some non-unit } a \in Z.$$

By the definition of $\delta$ and Lemma 2.1, the element $a$ divides $\delta$. Thus the prime ideal factorization of $aZ$ is of the form $aZ = \prod_{i=1}^{r} \mathcal{Q}_i^{f_i}$, with exponents $f_i \leqslant e_i$. Due to assumption (AV), there must exist an index $i \in \{1, \dots, r\}$ such that $f_i > g_i$: otherwise $\mathfrak{I} \subset aZ$, i.e. $a$ divides all values $P_1(z), \dots, P_\ell(z)$ ($z \in Z$). Consequenty, $f_i \geqslant g_{i+1}$ and so $aZ \subset \mathcal{Q}_i^{g_i+1}$, for the same index $i$. But this contradicts assumption (*).

(b) Merely replace in the proof of (a) the non-unit $a$ by a prime $p$, and resort to the variant of (AV) assumed in (b). □

2.3. **A few words on near UFDs.** This subsection says more on near UFDs for which we will prove the full coprime Schinzel Hypothesis in §3. They will also serve, with Dedekind domains, as landmarks in the discussion of the Hypothesis over other domains in §2.4.

Recall from Remark 1.4 that we call an integral domain $Z$ a *near UFD* if every non-zero element has finitely many prime divisors, and every non-unit has at least one. Of course, a UFD is a near UFD. A simple example showing that the converse does not hold is the ring $\mathbb{Z}_p + X\mathbb{Q}_p[X]$ of polynomials over $\mathbb{Q}_p$ with constant coefficient in $\mathbb{Z}_p$; see Example 2.4.

It is worth noting further that

(a) as for UFDs, every irreducible element $a$ of a near UFD $Z$ is a prime: indeed, such an $a$ is divisible by a prime $p$ of $Z$; being irreducible, $a$ must in fact be associate to $p$.

(b) unlike UFDs, near UFDs do not satisfy the Ascending Chain Condition on Principal Ideals in general, i.e. there exist near UFDs which have an infinite strictly ascending chain of principal ideals; see Example 2.4 below.

It is classical that being a UFD is equivalent to satisfying these two conditions: the Ascending Chain Condition on Principal Ideals holds and every irreducible is a prime. Thus a near UFD is a UFD if and only if it satisfies the Ascending Chain Condition on Principal Ideals. In particular, a near UFD that is Noetherian is a UFD.

*Example* 2.4. Let $R$ be a UFD, not a field, and let $K$ the field of fractions of $R$. Let $Z = R + XK[X]$ be the ring of polynomials over $K[X]$ with constant coefficient in $R$. Then it is well-known that $Z$ is not a UFD. Indeed, any prime element $p$ of $R$ remains prime in $Z$, and one has factorizations $X = (X/p) \cdot p = (X/p^2) \cdot p^2$, corresponding to an infinite ascending chain $(X) \subset (X/p) \subset (X/p^2) \subset \dots$ . Moreover, all irreducible elements of $Z$ are prime, and the non-constant prime elements are (up to associates) exactly the non-constant polynomials with constant coefficient 1. Clearly, every non-constant element of $Z$ has at least one, but finitely many prime divisors of this kind. Assume now additionally that $R$ has only finitely many non-associate prime elements. Then every non-constant polynomial in $Z$ has only finitely many prime divisors altogether, and the same holds more obviously for (non-zero) constants. Therefore, $Z$ is a near UFD in this case.

*Remark* 2.5 (a further advantage of near UFDs). In near UFDs, a non-unit is always divisible by a prime. This is not the case in general. For example $a = 6$ in the ring $\mathbb{Z}[\sqrt{-5}]$ does have irreducible divisors but no prime divisors; or $a = 2$ in the ring of algebraic integers does not even have any irreducible divisors (the ring has no irreducibles). Pick an

element $a \in Z$ as in these two examples. The polynomials $P_1(y) = ay$ and $P_2(y) = a(y+1)$ are coprime in $Q[y]$ and a common prime divisor of all values of $P_1$ and $P_2$ would have to divide $a$ and therefore does not exist. Yet there is no $m \in Z$ such that $P_1(m)$ and $P_2(m)$ are coprime. To avoid such examples, we insist in our assumption (AV) that all elements $P_1(m), \dots, P_\ell(m)$ with $m \in Z$ be coprime, and not just that no prime divides them all. This subtelty vanishes of course if $Z$ is a near UFD.

2.4. **Other domains.** While property $\mathcal{C}opSch(1,1)$ is completely well behaved in the class of Dedekind domains and, as we will see in §3, in that of near UFDs, we show in this subsection that the behavior inside other classes is rather erratic. For example, we produce a non-Noetherian Bézout domain[8] for which $\mathcal{C}opSch(1,1)$ holds (Proposition 2.6) and another one for which it does not (Remark 2.11). We also show that $\mathcal{C}opSch(1,1)$ fails over certain number rings, such as the domain $\mathbb{Z}[\sqrt{5}]$ (Proposition 2.10).

2.4.1. *Non-Noetherian domains satisfying $\mathcal{C}opSch(1,1)$.* Proposition 2.6 shows a ring that is not a near UFD but satisfies $\mathcal{C}opSch(1,1)$. Proposition 2.7 even produces a domain $Z$ that fulfills $\mathcal{C}opSch(1,1)$ even though $Z$ has non-units not divisible by any prime.

**Proposition 2.6.** *The ring $Z$ of entire functions is a Bézout domain which satisfies $\mathcal{C}opSch(1,1)$, but is not Noetherian and is not a near UFD.*

*Proof.* The ring $Z$ is a Bézout domain (see e.g. [Coh68]) whose prime elements, up to multiplication with units, are exactly the linear polynomials $x - c$ ($c \in \mathbb{C}$); indeed, an element of $Z$ is a non-unit if and only if it has a zero in $\mathbb{C}$, and an element with a zero $c$ is divisible by $x - c$ due to Riemann's theorem on removable singularities. In particular, every non-unit of $Z$ has at least one prime divisor. However the set of zeroes of a nonzero entire function may be infinite. This shows that the ring $Z$ is not a near UFD, and is not Noetherian either. Note also that existence of a common prime divisor for a set of elements of $Z$ is equivalent to existence of a common root in $\mathbb{C}$.

Consider now finitely many polynomials $P_1(t), \dots, P_\ell(t) \in Z[t]$ which are coprime in $Q[t]$ and for which no prime of $Z$ divides all values $P_i(m)$ ($i = 1, \dots, \ell$; $m \in Z$). For each $P_i$, we may factor out the gcd $d_i$ of all coefficients and write $P_i(t) = d_i \tilde{P}_i(t)$, where the coefficients of $\tilde{P}_i$ are coprime. Then $d_1, \dots, d_\ell$ are necessarily coprime (since their common prime divisors would divide all values $P_i(m)$ ($i = 1, \dots, \ell$; $m \in Z$)). We now consider specialization of $\tilde{P}_1, \dots, \tilde{P}_\ell$ at *constant* functions $m \in \mathbb{C}$.

Recall that by Lemma 2.1, there exists a nonzero $\delta \in Z$ such that for every $m \in Z$, and in particular for every $m \in \mathbb{C}$, every common divisor of $P_1(m), \dots, P_\ell(m)$ is a divisor of $\delta$. The entire function $\delta$ has a countable set $S$ of zeroes. To prove $\mathcal{C}opSch(1,1)$, it suffices to find $m \in \mathbb{C}$ for which no $z \in S$ is a zero of all of $P_1(m), \dots, P_\ell(m)$. For $i \in \{1, \dots, \ell\}$, denote by $S_i$ the set of all $z \in S$ which are not a root of $d_i$. Since $d_1, \dots, d_\ell$ are coprime, one has $\cup_{i=1}^{\ell} S_i = S$. Now fix $i$ for the moment, and write $\tilde{P}_i(t) = \sum_{j=0}^{k} (\sum_{k=0}^{\infty} a_{jk} x^k) t^j$ with $a_{jk} \in \mathbb{C}$, via power series expansion of the coefficients of $\tilde{P}_i$. Let $z \in S_i$. Since $z$ is not a root of all coefficients of $\tilde{P}_i$, evaluation $x \mapsto z$ yields a nonzero polynomial, which thus has a root at only finitely many values $t \mapsto m \in \mathbb{C}$. This is true for all $z \in S_i$, whence the set of $m \in \mathbb{C}$ such that $P_i(m) = d_i \tilde{P}_i(m)$ has a root at *some* $z \in S_i$ is a countable set. In total, the set of all $m \in \mathbb{C}$ such that $P_1(m), \dots, P_\ell(m)$ have a common root in $S$ (and

[8]Recall that a domain is called *Bézout* if any two elements have a greatest common divisor which is a linear combination of them. Equivalently, the sum of any two principal ideals is a principal ideal.

hence in some $S_i$) is countable as well. Choose $m$ in the complement of this set to obtain the assertion. □

**Proposition 2.7.** *Let $Z = \overline{\mathbb{Z}_p}$ be the integral closure of $\mathbb{Z}_p$ in $\overline{\mathbb{Q}_p}$. Then $Z$ has non-units that are not divisible by any prime and satisfies $\mathcal{C}opSch(1,1)$.*

*Proof.* The domain $Z$ is a (non-Noetherian) valuation ring, whose nonzero finitely generated ideals are exactly the principal ideals $p^r Z$ with $r$ a non-negative rational number. Prime elements do not exist in $Z$, whence the first part of the assertion.

Now take finitely many nonzero polynomials $P_1(t), \dots, P_\ell(t) \in Z[t]$, coprime in $\overline{\mathbb{Q}_p}[t]$, and assume that all values $P_i(m)$ ($i = 1, \dots, \ell$; $m \in Z$) are coprime. Then the coefficients of $P_1, \dots, P_\ell$ must be coprime, and since $Z$ is a valuation ring (i.e., its ideals are totally ordered by inclusion), one of these coefficients, say the coefficient of $t^d$, $d \geqslant 0$, of the polynomial $P_1$, must be a unit. We will proceed to show that there exists $m \in Z$ such that $P_1(m)$ is a unit, which will clearly prove $\mathcal{C}opSch(1,1)$. To that end we draw the Newton polygon (with respect to the $p$-adic valuation) of the polynomial $P_1(t) - u$, with $u \in Z$ a unit to be specified. Since any non-increasing slope in this Newton polygon corresponds to a set of roots of $P_1(t) - u$ of non-negative valuation (i.e. roots contained in $Z$), it suffices to choose $u$ such that there exists at least one segment of non-increasing slope (see, e.g. Proposition II.6.3 in [Neu99] for the aforementioned property of the Newton polygon). This is trivially the case if $d > 0$, so we may assume that the constant coefficient of $P_1$ is the only one of valuation 0. But then simply choose $u = P_1(0)$ and $m = 0$. □

2.4.2. *Rings not satisfying $\mathcal{C}opSch(1,1)$.*

**Proposition 2.8.** *Let $Z$ be a domain and $p, q$ be non-associate irreducible elements of $Z$ such that $Z/(pZ \cap qZ)$ is a finite local ring. Then $\mathcal{C}opSch(1,1)$ fails for $Z$.*

The proof rests on the following elementary fact.

**Lemma 2.9.** *Let $R$ be a finite local ring and let $a, b \in R$ be two distinct elements. Then there exists a polynomial $f \in R[t]$ taking the value $a$ exactly on the units of $R$, and the value $b$ everywhere else.*

*Proof.* Start with $a = 1$ and $b = 0$. The unique maximal ideal of a finite local ring is necessarily the nilradical, i.e., every non-unit of $R$ is nilpotent. In particular, there exists $n \in \mathbb{N}$ (e.g. any sufficiently large multiple of $|R^\times|$) such that $r^n = 0$ for all nilpotent elements $r \in R$, and $r^n = 1$ for all units $r$. Setting $f(t) = t^n$ finishes the proof for $a = 1$, $b = 0$. The general case then follows by simply setting $f(t) = (a - b)t^n + b$. □

*Proof of Proposition 2.8.* Set $J = pZ \cap qZ$. As already used above, locality of $Z/J$ implies that all non-units of $Z/J$ are nilpotent. In particular, $p, q \notin J$, but there exist $m, n \in \mathbb{N}$ such that $p^m \in J$ and $q^n \in J$. By Lemma 2.9, there exist polynomials $P_1, P_2 \in Z[t]$ such that $P_1(z) \in \begin{cases} p + J, & \text{for } z + J \in (Z/J)^\times \\ J, & \text{otherwise} \end{cases}$, and $P_2(z) \in \begin{cases} J, & \text{for } z + J \in (Z/J)^\times \\ q + J, & \text{otherwise} \end{cases}$.
By adding suitable constant terms in $J$ to $P_1$ and $P_2$, one may additionally demand that $p \in P_1(Z)$ and $q \in P_2(Z)$. In particular, $P_1$ and $P_2$ satisfy assumption (AV). However, by construction, $p$ divides both $P_1(z)$ and $P_2(z)$ for all $z$ such that $z + J \in (Z/J)^\times$, and $q$ divides $P_1(z)$ and $P_2(z)$ for all other $z$, showing that $\mathcal{C}opSch(1,1)$ is not satisfied. □

**Proposition 2.10.** *$\mathcal{C}opSch(1,1)$ does not hold for $Z = \mathbb{Z}[\sqrt{5}]$.*

*Proof.* Set $\sigma = \sqrt{5}+1$, so that $Z = \mathbb{Z}[\sigma]$. Note the factorization $2 \cdot 2 = \sigma(\sigma-2)$ in $Z$, in which 2 and $\sigma$ are non-associate irreducible elements. Due to Proposition 2.8, it suffices to verify that $Z/(2Z \cap \sigma Z)$ is a local ring. However, since $4, 2\sigma$ and $\sigma^2$ are all in $2Z \cap \sigma Z$, the set $\{0,1,2,3,\sigma,\sigma+1,\sigma+2,\sigma+3\}$ is a full set of coset representatives, and the non-units (i.e. $0, 2, \sigma, \sigma+2$) are exactly the nilpotents in $Z/(2Z \cap \sigma Z)$. These therefore form the unique maximal ideal, ending the proof. □

*Remark* 2.11 (The *finite* coprime Schinzel Hypothesis). (a) The proof above of Proposition 2.10 even shows that a weaker variant of $\mathcal{C}opSch(1,1)$ fails over $\mathbb{Z}[\sqrt{5}]$, namely the variant, say (FinCopSch), for which the exact same conclusion holds but under the following stronger assumption on values:

(Fin-AV) *The set of values* $\{P_i(m) \mid m \in Z, i = 1,\dots,\ell\}$ *contains a finite subset whose elements are coprime in* $Z$.

(b) Here is an example of a domain fulfilling (FinCopSch) but not $\mathcal{C}opSch(1,1)$. Consider the domain $Z = \mathbb{Z}_p[p^{p^{-n}} \mid n \in \mathbb{N}]$. This is a (non-Noetherian) valuation ring, and in particular a Bézout domain (the finitely generated non-trivial ideals are exactly the principal ideals $(p^{m/p^n})$ with $m, n \in \mathbb{N}$).

Property $\mathcal{C}opSch(1,1)$ does not hold for $Z$. Take $P_1(t) = pt$ and $P_2(t) = t^p - t + p$. These are coprime in $Q[t]$. Furthermore $P_1$ and $P_2$ satisfy assumption (AV) — indeed, any common divisor certainly divides $p = P_1(1)$ as well as $m(m^{p-1}-1)$ for every $m \in Z$; choosing $m$ in the sequence $(p^{p^{-n}})_{n\in\mathbb{N}}$ shows the claim. But note that every $m \in Z$ lies inside some ring $Z_0 = \mathbb{Z}_p[p^{p^{-n}}]$ (for a suitable $n$), and the unique maximal ideal of that ring has residue field $\mathbb{F}_p$, meaning that it necessarily contains $m(m^{p-1}-1)$. Thus $m(m^{p-1}-1)$ is at least divisible by $p^{p^{-n}}$, which is thus a common divisor of $P_1(m)$ and $P_2(m)$.

On the other hand, $Z$ fulfills property (FinCopSch). Indeed, if $P_1(t),\dots,P_\ell(t)$ are polynomials in $Z[t]$ for which finitely many elements $P_i(m)$ with $m \in Z, i \in \{1,\dots,\ell\}$ exist that are coprime, then automatically one of those values must be a unit (since any finite set of non-units has a suitably high root of $p$ as a common divisor!), yielding an $m$ for which $P_1(m),\dots,P_\ell(m)$ are coprime.

2.5. **A UFD not satisfying the gcd stability property.** Recall, for $Z = \mathbb{Z}$, the following result from [BDN20a] already mentioned in the introduction.

**Theorem 2.12.** *Let* $P_1,\dots,P_\ell \in Z[t]$ *be* $\ell \geqslant 2$ *nonzero polynomials, coprime in* $Q[t]$. *Then the set* $\mathcal{D} = \{\gcd(P_1(m),\dots,P_\ell(m)) \mid m \in Z\}$ *is finite and stable under gcd.*

The proof is given for $Z = \mathbb{Z}$ in [BDN20a] but is valid for any PID. Theorem 2.12 implies property $\mathcal{C}opSch(1,1)$. Indeed, asssumption (AV) exactly means that the gcd of elements of $\mathcal{D}$ is 1. By Theorem 2.12, $\mathcal{D}$ is finite and stable by gcd. Therefore $1 \in \mathcal{D}$, i.e. there exists $m \in Z$ such that $P_1(m),\dots,P_\ell(m)$ are coprime. The stability property however cannot be extended to all UFDs.

*Example* 2.13 (a counter-example to Theorem 2.12 for the UFD $Z = \mathbb{Z}[x,y,z]$). Let

$$P_1(t) = \big(x^2y^2z + t^2\big)\big(x^2yz^2 + (t-1)^2\big) \in Z[t]$$
$$P_2(t) = \big(xy^2z^2 + t^2\big)\big(x^2y^2z^2 + (t-1)^2\big) \in Z[t]$$

These nonzero polynomials are coprime in $Q[t]$: they have no common root in $\overline{Q}$.

We prove next that the set $\mathcal{D} = \{\gcd(P_1(m), P_2(m)) \mid m \in Z\}$ is not stable by gcd. Set

$$\begin{cases} d_0 = \gcd(P_1(0), P_2(0)) = \gcd(x^2y^2z, xy^2z^2) = xy^2z \\ d_1 = \gcd(P_1(1), P_2(1)) = \gcd(x^2yz^2, x^2y^2z^2) = x^2yz^2 \end{cases}$$

and $d = \gcd(d_0, d_1) = xyz$. We prove below that $d \notin \mathcal{D}$.

By contradiction, assume that $d = \gcd(P_1(m), P_2(m))$ for some $m = m(x,y,z) \in Z$. As $xyz | P_1(m)$ it follows that $xyz | \big(x^2y^2z + m^2\big)\big(x^2yz^2 + (m-1)^2\big)$ whence $xyz | m^2(m-1)^2$ and $xyz | m(m-1)$. We claim that the last two divisibilities imply that $xyz | m$ or $xyz | m-1$.

Namely, if for instance we had $xy | m$ and $z | m-1$ then, on the one hand, we would have $m = xym'$ for some $m' \in Z$ and so $m(0,0,0) = 0$, but on the other hand, we would have $m(x,y,z) - 1 = zm''$ for some $m'' \in Z$ and so $m(0,0,0) = 1$. Whence the claim.

Now if $xyz | m$, then $x^2y^2z^2 | m^2$. But then $x^2y^2z | P_1(m)$ and $xy^2z^2 | P_2(m)$, whence $xy^2z | d$, a contradiction. The other case for which $xyz | m-1$ is handled similarly.

## 3. The coprime Schinzel Hypothesis - general case

The fully general coprime Schinzel Hypothesis and the almost equivalent Primitive Specialization Hypothesis are introduced in §3.2. Our main result on them, Theorem 3.7, is stated in §3.3. Sections 3.4 and 3.5 show three lemmas needed for the proof, which is given in §3.6. We start in §3.1 with some observations on fixed divisors.

Fix an arbitrary integral domain $Z$.

3.1. **Fixed divisors.** We refer to §1 for the definition of "fixed divisor w.r.t. $\underline{t}$" of a polynomial $P(\underline{t}, \underline{y})$ and for the associated notation $\mathcal{F}_{\underline{t}}(P)$.

**Lemma 3.1.** *Let $Z$ be an integral domain.*
(a) *Let $P \in Z[\underline{t}, \underline{y}]$ be a nonzero polynomial and $p$ be a prime of $Z$ not dividing $P$. If $p$ is in the set $\mathcal{F}_{\underline{t}}(P)$ of fixed divisors of $P$, it is of norm $|Z/pZ| \leqslant \max_{i=1,\dots,k} \deg_{t_i}(P)$.*
(b) *Assume that $Z$ is a near UFD and every prime of $Z$ is of infinite norm. Then, for any polynomials $P_1(\underline{t}, \underline{y}), \dots, P_s(\underline{t}, \underline{y}) \in Z[\underline{t}, \underline{y}]$, primitive w.r.t. $Z$, we have $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s) = \emptyset$.*
(c) *If $Z = R[u_1, \dots, u_r]$ is a polynomial ring over an integral domain $R$, and if either $R$ is infinite or $r \geqslant 2$, then every prime $p \in Z$ is of infinite norm. The same conclusion holds if $Z$ is an integral domain containing an infinite field.*

On the other hand, $\mathbb{Z}$ and $\mathbb{F}_q[x]$ are typical examples of rings that have primes of finite norm. As already noted, (b) is in fact false for these two rings.

*Proof.* (a) is classical. If $p$ is a prime of $Z$ such that $P$ is nonzero modulo $p$ and $|Z/pZ| > \max_{i=1,\dots,k} \deg_{t_i}(P)$, there exists $\underline{m} \in Z^k$ such that $P(\underline{m}, \underline{y}) \not\equiv 0 \pmod{p}$, i.e. $p \notin \mathcal{F}_{\underline{t}}(P)$.
(b) Assume that the set $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s)$ contains a non-unit $a \in Z$. As $Z$ is a near UFD, one may assume that $a$ is a prime of $Z$. It follows from $P_1, \dots, P_s$ being primitive w.r.t. $Z$ that the product $P_1 \cdots P_s$ is nonzero modulo $a$. From (a), the norm $|Z/aZ|$ should be finite, whence a contradiction. Conclude that the set $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s)$ is empty.
(c) With $Z = R[u_1, \dots, u_r]$ as in the statement, assume first that $R$ is infinite. Let $p \in R[u_1, \dots, u_r]$ be a prime element. Suppose first that $p \notin R$, say $d = \deg_{u_r}(p) \geqslant 1$. The elements $1, u_r, \dots, u_r^{d-1}$ are $R[u_1, \dots, u_{r-1}]$-linearly independent in the integral domain $Z/pZ$. As $R$ is infinite, the elements $\sum_{i=0}^{d-1} p_i u_r^i$ with $p_0, \dots, p_{d-1} \in R$ are infinitely many different elements in $Z/pZ$. Thus $Z/pZ$ is infinite. In the case that $p \in R$, the quotient ring $Z/pZ$ is $(R/pR)[u_1, \dots, u_r]$, which is infinite too.

If $Z = R[u_1, \dots, u_r]$ with $r \geqslant 2$, write $R[u_1, \dots, u_r] = R[u_1][u_2, \dots, u_r]$ and use the previous paragraph with $R$ taken to be the infinite ring $R[u_1]$.

If $Z$ is an integral domain containing an infinite field $k$, the containment $k \subset Z$ induces an injective morphism $k \hookrightarrow Z/pZ$ for every prime $p$ of $Z$. The last claim follows. □

3.2. **The two Hypotheses.** Definition 3.2 introduces the coprime Schinzel Hypothesis in the general situation of $s$ sets of polynomials in $k$ variables $t_i$, with $k, s \geqslant 1$. The initial definition from Theorem 1.3 (denoted $\mathcal{C}opSch(1,1)$ in §2) corresponds to the special case $s = k = 1$; in particular assumption (AV) from there is $(\mathrm{AV})_{\underline{t}}$ below with $\underline{t} = t$ and $s = 1$.

*Definition* 3.2. Given an integral domain $Z$ of fraction field $Q$, we say that the *coprime Schinzel Hypothesis holds for* $Z$ if for any integers $k, s \geqslant 1$, the following property is true:
$\mathcal{C}opSch(k,s)$: Consider $s$ sets $\{P_{11}, \dots, P_{1\ell_1}\}, \dots, \{P_{s1}, \dots, P_{s\ell_s}\}$ of nonzero polynomials in $Z[\underline{t}]$ (with $\underline{t} = (t_1, \dots, t_k)$) such that $\ell_i \geqslant 2$ and $P_{i1}, \dots, P_{i\ell_i}$ are coprime in $Q[\underline{t}]$, for each $i = 1, \dots, s$. Assume further that

$(\mathrm{AV})_{\underline{t}}$ *for every non-unit $a \in Z$, there exists $\underline{m} \in Z^k$, such that, for each $i = 1, \dots, s$, the values $P_{i1}(\underline{m}), \dots, P_{i\ell_i}(\underline{m})$ are not all divisible by $a$.*

Then there exists $\underline{m} \in Z^k$ such that, for each $i = 1, \dots, s$, the values $P_{i1}(\underline{m}), \dots, P_{i\ell_i}(\underline{m})$ are coprime in $Z$.

This property is the one used by Schinzel (over $Z = \mathbb{Z}$) in his 2002 paper [Sch02]. The next definition introduces an alternate property, which is equivalent under some assumption, and which better suits our Hilbert-Schinzel context.

*Definition* 3.3. Given an integral domain $Z$, we say that the *Primitive Specialization Hypothesis holds for* $Z$ if for any integers $k, n, s \geqslant 1$ the following property is true:
$\mathcal{P}riSpe(k,n,s)$: Let $P_1(\underline{t}, \underline{y}), \dots, P_s(\underline{t}, \underline{y}) \in Z[\underline{t}, \underline{y}]$ be $s$ nonzero polynomials (in the variables $\underline{t} = (t_1, \dots, t_k)$ and $\underline{y} = (y_1, \dots, y_n)$). Assume that they are primitive w.r.t. $Q[\underline{t}]$ and that $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s) = \emptyset$. Then there exists $\underline{m} \in Z^k$ such that the polynomials $P_1(\underline{m}, \underline{y}), \dots, P_s(\underline{m}, \underline{y})$ are primitive w.r.t. $Z$.

**Lemma 3.4.** (1) *For all integers $k, s \geqslant 1$, we have:*

$$\mathcal{C}opSch(k,s) \Longrightarrow \mathcal{P}riSpe(k,n,s) \text{ for every } n \geqslant 1.$$

(2) *The converse holds as well*
   (a) *if $Z$ has the property that every non-unit is divisible by a prime element, or,*
   (b) *in the special situation that $s = 1$.*

(3) *For all integers $k, n, s \geqslant 1$, we have:*

$$\mathcal{P}riSpe(k,n,1) \Longrightarrow \mathcal{P}riSpe(k,n,s).$$

Thus the coprime Schinzel Hypothesis is stronger than the Primitive Specialization Hypothesis and they are equivalent in either case (a) or (b) from (2), in particular if $Z$ is a near UFD. Assertion (3) allows reducing to the case of one polynomial $P(\underline{t}, \underline{y}) \in Z[\underline{t}, \underline{y}]$ for proving the Primitive Specialization Hypothesis. For a near UFD, the analogous reduction to one family $\{P_1(\underline{t}), \dots, P_\ell(\underline{t})\}$ of polynomials in $Z[\underline{t}]$ also holds for the (equivalent) coprime Schinzel Hypothesis, but this is not clear for a general domain.

*Proof.* (1) Assuming $\mathcal{C}opSch(k,s)$ for some $k, s \geqslant 1$, let $\underline{y} = (y_1, \dots, y_n)$ be $n \geqslant 1$ variables and $P_i(\underline{t}, \underline{y})$ $(i = 1, \dots, s)$ as in $\mathcal{P}riSpe(k,n,s)$. Consider the sets $\{P_{i1}(\underline{t}), \dots, P_{i\ell_i}(\underline{t})\}$ $(i = 1, \dots, s)$ of their respective coefficients in $Z[\underline{t}]$. Condition $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s) = \emptyset$ rewrites:

(*) $\quad (\forall a \in Z \setminus Z^\times)\ (\exists \underline{m} \in Z^k)\ \ (a \text{ does not divide } \prod_{i=1}^s P_i(\underline{m}, \underline{y}))$.

This obviously implies that

(**) $\quad (\forall a \in Z \setminus Z^\times)\ (\exists \underline{m} \in Z^k)\ \ (\forall i = 1, \dots, s)\ (a \text{ does not divide } P_i(\underline{m}, \underline{y}))$,

which is equivalent to condition $(\mathrm{AV})_{\underline{t}}$ for the sets $\{P_{i1}(\underline{t}), \dots, P_{i\ell_i}(\underline{t})\}$ $(i = 1, \dots, s)$. If $\ell_1, \dots, \ell_s$ are $\geqslant 2$, then the coprime Schinzel Hypothesis yields some $\underline{m} \in Z^k$ such

that $P_{i1}(\underline{m}), \dots, P_{i\ell_i}(\underline{m})$ are coprime in $Z$, which equivalently translates as $P_i(\underline{m}, \underline{y})$ being primitive w.r.t. $Z$ ($i = 1, \dots, s$). Taking Remark 3.5(1) below into account, we obtain that $\mathcal{C}opSch(k, s)$ implies $\mathcal{P}riSpe(k, n, s)$.

*Remark* 3.5. (1) If $\ell_i = 1$ for some $i \in \{1, \dots, s\}$, i.e. if the polynomial $P_i(\underline{t}, \underline{y})$ is a monomial in $\underline{y}$, then this polynomial should be treated independently. In this case, $P_i(\underline{t}, \underline{y})$ being primitive w.r.t. $Z[\underline{t}]$, it is of the form $cy_1^{i_1} \cdots y_n^{i_n}$ for some integers $i_1, \dots, i_n \geqslant 0$ and $c \in Z^\times$. Then $P_i(\underline{m}, \underline{y}) = cy_1^{i_1} \cdots y_n^{i_n}$ remains primitive w.r.t. $Z$ *for every* $\underline{m} \in Z^k$.

(2) Suppose given sets $\{P_{i1}(\underline{t}), \dots, P_{i\ell_i}(\underline{t})\}$ as in $\mathcal{C}opSch(k, s)$ for some integers $k, s \geqslant 1$. Consider the polynomials

$$P_i(\underline{t}, \underline{y}) = P_{i1}(\underline{t})y_1 + \cdots + P_{i\ell_i}(\underline{t})y_{\ell_i},\ i = 1, \dots, s,$$

where $\underline{y} = (y_1, \dots, y_\ell)$ is an $\ell$-tuple of new variables and $\ell = \max(\ell_1, \dots, \ell_s)$[9]. Condition $(\mathrm{AV})_{\underline{t}}$ rewrites as (**) above. In either one of the situations (a) or (b) of the statement, condition (**) does imply condition (*), and equivalently $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s) = \emptyset$, for the polynomials $P_i(\underline{t}, \underline{y})$ defined above. Thus if $\mathcal{P}riSpe(k, n, s)$ holds (for every $n \geqslant 1$), we obtain some $\underline{m} \in Z^k$ such that the polynomials $P_1(\underline{m}, \underline{y}), \dots, P_s(\underline{m}, \underline{y})$ are primitive w.r.t. $Z$, which, in terms of the original polynomials $P_{ij}(\underline{t})$, corresponds to the conclusion of the requested property $\mathcal{C}opSch(k, s)$.

(3) Let $P_1(\underline{t}, \underline{y}), \dots, P_s(\underline{t}, \underline{y})$ be as in $\mathcal{P}riSpe(k, n, s)$. Set $P = P_1 \cdots P_s$. We have $P \in Z[\underline{t}, \underline{y}]$, and from Gauss's lemma (applied to the UFD $Q[\underline{t}]$), $P$ is primitive w.r.t. $Q[\underline{t}]$. By hypothesis, $\mathcal{F}_{\underline{t}}(P) = \emptyset$. Assuming $\mathcal{P}riSpe(k, n, 1)$, it follows that there exists $\underline{m} \in Z^k$ such that $P(\underline{m}, \underline{y})$ is primitive w.r.t. $Z$. But then, the polynomials $P_1(\underline{m}, \underline{y}), \dots, P_s(\underline{m}, \underline{y})$ are primitive w.r.t. $Z$ as well. □

3.3. **Main result.** Before stating the main conclusions on our Hypotheses, we introduce the following variant of the Primitive Specialization Hypothesis, which is more precise and more involved but turns out to be quite central and useful.

*Definition* 3.6. Let $Z$ be an integral domain such that every nonzero $a \in Z$ has only finitely many prime divisors (modulo units). We say that the *starred Primitive Specialization Hypothesis holds for* $Z$ if the following property is true for any integers $k, s \geqslant 1$:

$\mathcal{P}riSpe^\star(k, s)$: *Let* $n \geqslant 1$ *and let* $P_1(\underline{t}, \underline{y}), \dots, P_s(\underline{t}, \underline{y}) \in Z[\underline{t}, \underline{y}]$ *be* $s$ *nonzero polynomials (with* $\underline{t} = (t_1, \dots, t_k), \underline{y} = (y_1, \dots, y_n)$*), primitive w.r.t.* $Q[\underline{t}]$ *and such that the product* $P_1 \cdots P_s$ *has no fixed prime divisor in* $Z$ *w.r.t.* $\underline{t}$*. Let* $P_0 \in Z[\underline{t}]$, $P_0 \neq 0$*. Then there exists* $(m_1, \dots, m_{k-1}) \in Z^{k-1}$ *and an arithmetic progression* $\tau_k = (\omega_k \ell + \alpha_k)_{\ell \in Z}$ *with* $\omega_k, \alpha_k \in Z$*,* $\omega_k \neq 0$*, such that for all but finitely many* $m_k \in \tau_k$*, the polynomials*

$$P_1(m_1, \dots, m_k, \underline{y}), \dots, P_s(m_1, \dots, m_k, \underline{y})$$

*have no prime divisors in* $Z$*, and* $P_0(m_1, \dots, m_k) \neq 0$*.*
(*with the convention that for* $k = 1$*, existence of* $(m_1, \dots, m_{k-1}) \in Z^{k-1}$ *is not requested*).

If $Z$ is a near UFD (and so it is equivalent to request that prime or non-unit divisors exist), $\mathcal{P}riSpe^\star(k, s)$ is a more precise form of ($\mathcal{P}riSpe(k, n, s)$ *for all* $n \geqslant 1$) saying where to find the tuples $\underline{m}$, the existence of which is asserted in $\mathcal{P}riSpe(k, n, s)$; thus we have

$$\mathcal{P}riSpe^\star(k, s) \Rightarrow (\mathcal{P}riSpe(k, n, s) \text{ for all } n \geqslant 1) \Leftrightarrow \mathcal{C}opSch(k, s).$$

[9]Any polynomial in $Z[\underline{t}][y_1, \dots, y_{\ell_i}]$ with coefficients $P_{i1}(\underline{t}), \dots, P_{i\ell_i}(\underline{t})$ may be used instead of the polynomial $P_{i1}(\underline{t})y_1 + \cdots + P_{i\ell_i}(\underline{t})y_{\ell_i}$ ($i = 1, \dots, s$).

Because the existence of non unit vs. prime divisors issue is not void in Dedekind domains, Definition 3.3 and Definition 3.6 do not compare so obviously for Dedekind domains.

**Theorem 3.7.** (a) *If $Z$ is a near UFD or a Dedekind domain, then the starred Primitive Specialization Hypothesis holds for $Z$.*
(b) *If $Z$ is a near UFD, then both the Coprime Schinzel Hypothesis and the Primitive Specialization Hypotheses hold.*
(c) *If $Z$ is a Dedekind domain, then the Primitive Specialization Hypothesis holds with $k = 1$ and $n, s \geqslant 1$ (i.e. for polynomials with one variable $t$ to be specialized), and the Coprime Schinzel Hypothesis holds if in addition $s = 1$ (one polynomial $P$).*

Theorem 1.3 for UFDs is the special case $s = k = 1$ of Theorem 3.7(b), and Theorem 1.3 for Dedekind domains (already proved in §2.2) is the second part of Theorem 3.7(c).

3.4. **Two lemmas.** The following lemmas are used in the proof of Theorem 3.7 and of Theorem 1.6. The first one is a refinement of the Chinese Remainder Theorem.

**Lemma 3.8.** *Let $Z$ be an integral domain. Let $I_1, \dots, I_\rho$ be $\rho$ maximal ideals of $Z$ and $I_{\rho+1}, \dots, I_r$ be $r-\rho$ ideals assumed to be prime but not maximal (with $0 \leqslant \rho \leqslant r$). Assume further that $I_j \not\subset I_{j'}$ for any distinct elements $j, j' \in \{1, \dots, r\}$. Let $\underline{t}$, $\underline{y}$ be tuples of variables of length $k, n \geqslant 1$ and let $F \in Z[\underline{t}, \underline{y}]$ be a polynomial, nonzero modulo each ideal $I_j$, $j = \rho+1, \dots, r$. Then for every $(\underline{a}_1, \dots, \underline{a}_\rho) \in (Z^k)^\rho$, there exists $\underline{m} \in Z^k$ such that $\underline{m} \equiv \underline{a}_j \pmod{I_j}$ for each $j = 1, \dots, \rho$, and $F(\underline{m}, \underline{y}) \not\equiv 0 \pmod{I_j}$ for each $j = \rho+1, \dots, r$.*

*Proof.* Assume first $0 \leqslant \rho < r$. A first step is to show by induction on $r - \rho \geqslant 1$ that there exists $\underline{m}_0 \in Z^k$ such that $F(\underline{m}_0, \underline{y}) \not\equiv 0 \pmod{I_j}$, $j = \rho+1, \dots, r$.

Start with $r - \rho = 1$. The quotient ring $Z/I_{\rho+1}$ is an integral domain but not a field, hence is infinite; and $F$ is nonzero modulo $I_{\rho+1}$ (i.e. in $(Z/I_{\rho+1})[\underline{t}, \underline{y}]$). Thus elements $\underline{m}_0 \in Z^k$ exist such that $F(\underline{m}_0, \underline{y}) \not\equiv 0 \pmod{I_{\rho+1}}$. Assume next that there is an element of $Z^k$, say $\underline{m}_1$, such that $F(\underline{m}_1, \underline{y}) \not\equiv 0 \pmod{I_j}$, $j = \rho+1, \dots, s$ with $s < r$. It follows from the assumptions on $I_{\rho+1}, \dots, I_r$ that the product $I_{\rho+1} \cdots I_s$ is not contained in $I_{s+1}$. Pick an element $\pi$ in $I_{\rho+1} \cdots I_s$ that is not in $I_{s+1}$ and consider the polynomial $F(\underline{m}_1 + \pi\underline{t}, \underline{y})$. This polynomial is nonzero modulo $I_{s+1}$ since both $F$ and $\underline{m}_1 + \pi\underline{t}$ are nonzero modulo $I_{s+1}$. As above, the quotient ring $Z/I_{s+1}$ is an infinite integral domain and so there exists $\underline{t}_0 \in Z^k$ such that $F(\underline{m}_1 + \pi\underline{t}_0, \underline{y}) \not\equiv 0 \pmod{I_{s+1}}$; and for each $j = \rho+1, \dots, s$, since $\pi \in I_j$, we have $F(\underline{m}_1 + \pi\underline{t}_0, \underline{y}) \equiv F(\underline{m}_1, \underline{y}) \not\equiv 0 \pmod{I_j}$. Set $\underline{m}_0 = \underline{m}_1 + \pi\underline{t}_0$ to conclude the induction.

Set $J = I_{\rho+1} \cdots I_r$. The ideals $I_1, \dots, I_\rho, J$ are pairwise comaximal. We may apply the Chinese Remainder Theorem, and will, component by component. More specifically write $\underline{m}_0 = (m_{01}, \dots, m_{0k})$ and $\underline{a}_i = (a_{i1}, \dots, a_{ik})$, $i = 1, \dots, \rho$. For each $h = 1, \dots, k$, there is an element $m_h \in Z$ such that $m_h \equiv a_{jh} \pmod{I_j}$ for each $j = 1, \dots, \rho$, and $m_h \equiv m_{0h} \pmod{J}$. Set $\underline{m} = (m_1, \dots, m_k)$. Clearly we have $\underline{m} \equiv \underline{a}_j \pmod{I_j}$ for each $j = 1, \dots, \rho$, and $\underline{m} \equiv \underline{m}_0 \pmod{J}$. The last congruence implies that, for each $j = \rho+1, \dots, r$, we have $\underline{m} \equiv \underline{m}_0 \pmod{I_j}$, and so $F(\underline{m}, \underline{y}) \not\equiv 0 \pmod{I_j}$.

If $r = \rho$, then there is no ideal $J$ and the sole second part of the argument, applied with the maximal ideals $I_1, \dots, I_\rho$, yields the result. □

**Lemma 3.9.** *Let $Z$ be an integral domain such that every nonzero element $a \in Z$ has only finitely many prime divisors (modulo units). Then, for every real number $B > 0$, there are only finitely many prime principal ideals $pZ$ of norm $|Z/pZ|$ less than or equal to $B$.*

The assumption on $Z$ is satisfied in particular if $Z$ is a near UFD or a Dedekind domain.

*Proof.* One may assume that $Z$ is infinite. Fix a real number $B > 0$. For every prime power $q = \ell^r \leqslant B$, pick an element $m_q \in Z$ such that $m_q^q - m_q \neq 0$. Let $a$ be the product of all elements $m_q^q - m_q$ with $q$ running over all prime powers $q \leqslant B$. From the assumption on $Z$, the list, say $\mathcal{D}_a$, of all prime divisors of $a$ (modulo units), is finite.

Consider now a prime $p \in Z$ such that $|Z/pZ| \leqslant B$. The integral domain $Z/pZ$, being finite, is a field. Hence $|Z/pZ|$ is a prime power $q = \ell^r$ ; and $q \leqslant B$. Of course we have $m_q^q - m_q \equiv 0 \pmod{p}$. Hence $p$ divides $a$, i.e. $p \in \mathcal{D}_a$. □

3.5. **A reduction lemma.** This lemma is a central tool of the proof of Theorem 3.7.

**Lemma 3.10.** *Let $Z$ be an integral domain such that every nonzero $a \in Z$ has only finitely many prime divisors (modulo units). Let $k, s \geqslant 1$ be two integers. Assume that property $\mathcal{P}riSpe^\star(1,1)$ holds. Then property $\mathcal{P}riSpe^\star(k,s)$ holds for all integers $k, s \geqslant 1$.*

This reduction is explained in the proof of [Sch02, Theorem 1] (see pages 242–243), with two differences. First, Schinzel uses the coprime Hypothesis formulation instead of the Primitive Specialization one (from Lemma 3.4, they are equivalent if $Z$ is a near UFD). Secondly, Schinzel works over $Z = \mathbb{Z}$. Our proof adapts his arguments to the Primitive Specialization formulation and shows that they carry over to our more general domains $Z$.

*Proof of Lemma 3.10.* Observe that using the same argument as for Lemma 3.4(3), one can reduce from $s$ to one polynomial $P(\underline{t}, \underline{y})$: $\mathcal{P}riSpe^\star(k,1) \Leftrightarrow \mathcal{P}riSpe^\star(k,s)$. Thus we merely need to prove that if $\mathcal{P}riSpe^\star(1,1)$ holds then so does $\mathcal{P}riSpe^\star(k,1)$ $(k \geqslant 1)$.

Assume that $\mathcal{P}riSpe^\star(1,1)$ holds. By the induction principle, we need to prove that

$$\mathcal{P}riSpe^\star(k-1,1) \Rightarrow \mathcal{P}riSpe^\star(k,1) \text{ for } k \geqslant 2.$$

Assume $\mathcal{P}riSpe^\star(k-1,1)$ and let $n$, $P(\underline{t}, \underline{y})$ and $P_0(\underline{t})$ be as in $\mathcal{P}riSpe^\star(k,1)$.

One may assume that $\deg_{t_k}(P) > 0$. Let $\mathcal{P}$ be the set of all primes $p \in Z$ (modulo units) such that $|Z/pZ| \leqslant \max_{1 \leqslant h \leqslant k} \deg_{t_h}(P)$. By Lemma 3.9, the set $\mathcal{P}$ is finite. Let $\pi$ be the product of its elements.

The first step is to construct a $k$-tuple $\underline{u} = (u_1, \ldots, u_k) \in Z^k$ such that

$$P(\underline{u}, \underline{y}) \not\equiv 0 \pmod{p} \text{ for every } p \in \mathcal{P}. \tag{1}$$

By assumption, no prime of $Z$ is a fixed divisor of $P$ w.r.t. $\underline{t}$. Thus for every $p \in \mathcal{P}$, there exists a $k$-tuple $\underline{u}_p = (u_{p1}, \ldots, u_{pk}) \in Z^k$ such that $P(\underline{u}_p, \underline{y}) \not\equiv 0 \pmod{p}$. Denote by $\mathcal{P}_1 \subset \mathcal{P}$ the subset of primes $p$ such that the ideal $pZ$ is maximal in $Z$. We now apply Lemma 3.8. From above, $P$ is nonzero modulo each $p \in \mathcal{P} \setminus \mathcal{P}_1$, and we have $pZ \not\subset p'Z$ for any distinct $p, p' \in \mathcal{P}$. Thus Lemma 3.8 provides a $k$-tuple $\underline{u}_0 = (u_{01}, \ldots, u_{0k}) \in Z^k$ such that $\underline{u}_0 \equiv \underline{u}_p \pmod{p}$ for every prime $p \in \mathcal{P}_1$ and $P(\underline{u}_0, \underline{y}) \not\equiv 0 \pmod{p}$ for every $p \in \mathcal{P} \setminus \mathcal{P}_1$. These congruences imply that $P(\underline{u}_0, \underline{y}) \not\equiv 0 \pmod{p}$ for every $p \in \mathcal{P}$. Furthermore, denoting by $\tau_h$ the arithmetic progression $\tau_h = (\pi\ell + u_{0h})_{\ell \in Z}$ $(h = 1, \ldots, k)$, conclusion (1) holds for every $\underline{u} = (u_1, \ldots, u_k) \in \tau_1 \times \cdots \times \tau_k$. Fix such a $k$-tuple $\underline{u}$.

Consider the following polynomial, where $\underline{v}' = (v_1, \ldots, v_{k-1})$ is a tuple of new variables, and $\underline{u}' = (u_1, \ldots, u_{k-1})$:

$$\widetilde{P}(\underline{v}', t_k, \underline{y}) = P(\pi \underline{v}' + \underline{u}', t_k, \underline{y}) \in Z[\underline{v}', t_k, \underline{y}].$$

We check below that as a polynomial in the $n+1$ variables $t_k, \underline{y}$ with coefficients in $Z[\underline{v}']$, it satisfies the assumptions allowing using the induction hypothesis $\mathcal{P}riSpe^\star(k-1,1)$.

Clearly $\widetilde{P}$ is nonzero. Set $\underline{t}' = (t_1, \ldots, t_{k-1})$. The polynomial $P$ is primitive w.r.t. $Q[\underline{t}']$. Hence $\widetilde{P}$ is primitive w.r.t. $Q[\underline{v}']$. Also note that by (1), we have, for every $p \in \mathcal{P}$,

(2) $$\widetilde{P}(\underline{\ell}', u_k, \underline{y}) \not\equiv 0 \pmod{p} \quad \text{for every } \underline{\ell}' \in Z^{k-1}.$$

The next paragraph shows that $\widetilde{P}$ has no fixed prime divisor in $Z$ w.r.t. $\underline{v}'$.

Assume that there is a prime $p \in Z$ such that $\widetilde{P}(\underline{\ell}', t_k, \underline{y}) \equiv 0 \pmod{p}$ for every $\underline{\ell}' \in Z^{k-1}$. It follows from (2) that $p \notin \mathcal{P}$. This gives that for every $h = 1, \dots, k-1$, we have $\pi v_h + u_h \not\equiv 0 \pmod{p}$ (as a polynomial in $v_h$). This, conjoined with $P(\underline{t}', t_k, \underline{y}) = P(\underline{t}, \underline{y}) \not\equiv 0 \pmod{p}$ shows that $P(\pi\underline{v}' + \underline{u}', t_k, \underline{y}) \not\equiv 0 \pmod{p}$. In other words, $\widetilde{P}$ is nonzero modulo $p$. A contradiction then follows from Lemma 3.1(a) and

$$|Z/pZ| > \max_{1 \leqslant h \leqslant k-1} (\deg_{t_h}(P)) = \max_{1 \leqslant h \leqslant k-1} (\deg_{v_h}(\widetilde{P})).$$

We will apply assumption $\mathcal{P}riSpe^{\star}(k-1, 1)$ to $\widetilde{P} \in Z[\underline{v}'][t_k, \underline{y}]$, and for the following choice of a nonzero polynomial $\widetilde{P}_0 \in Z[\underline{v}']$. The polynomial $P$ is primitive w.r.t. $Q[\underline{t}]$. Thus if $\{P_j(\underline{t}) \,|\, j \in J\}$ is the set of coefficients of $P$ (viewed as a polynomial in $\underline{y}$), by writing a Bézout relation in the PID $Q(\underline{t}')[t_k]$ and then clearing the denominators, we obtain elements $A_j \in Z[\underline{t}]$ and $\Delta \in Z[\underline{t}']$, $\Delta \neq 0$, such that

(3) $$\sum_{j \in J} A_j(\underline{t}', t_k) P_j(\underline{t}', t_k) = \Delta(\underline{t}').$$

Set then

$$\widetilde{P}_0(\underline{v}') = P_{0\infty}(\pi\underline{v}' + \underline{u}') \times \Delta(\pi\underline{v}' + \underline{u}')$$

where $P_{0\infty}(\underline{t}') \in Z[\underline{t}']$ is the leading coefficient of $P_0$ viewed as a polynomial in $t_k$.

From $\mathcal{P}riSpe^{\star}(k-1, 1)$, there exists $\underline{\ell}' = (\ell_1, \dots, \ell_{k-1}) \in Z^{k-1}$ such that

(4) the polynomial $\widetilde{P}(\underline{\ell}', t_k, \underline{y}) = P(\pi\underline{\ell}' + \underline{u}', t_k, \underline{y})$ has no prime divisors in $Z$,

and

(5) $$\widetilde{P}_0(\underline{\ell}') = P_{0\infty}(\pi\underline{\ell}' + \underline{u}') \times \Delta(\pi\underline{\ell}' + \underline{u}') \neq 0.$$

It follows from (3) and (5) that the polynomial $\widetilde{P}(\underline{\ell}', t_k, \underline{y})$ is nonzero and primitive w.r.t. $Q[t_k]$. We check below that $\widetilde{P}(\underline{\ell}', t_k, \underline{y})$ has no fixed prime divisor in $Z$ w.r.t. the variable $t_k$.

Assume that for some prime $p \in Z$, we have $\widetilde{P}(\underline{\ell}', m_k, \underline{y}) \equiv 0 \pmod{p}$ for every $m_k \in Z$. In view of (1), we have $p \notin \mathcal{P}$. Hence, by choice of $\mathcal{P}$, we have

(6) $$|Z/pZ| > \deg_{t_k}(P) = \deg_{t_k}(\widetilde{P}) \geqslant \deg_{t_k}\left(\widetilde{P}(\underline{\ell}', t_k, \underline{y})\right)$$

By (4), the polynomial $\widetilde{P}(\underline{\ell}', t_k, \underline{y})$ is nonzero modulo $p$ (i.e. nonzero in $(Z/pZ)[t_k, \underline{y}]$). This, conjoined with (6), contradicts Lemma 3.1(a).

Use next assumption $\mathcal{P}riSpe^{\star}(1, 1)$ to conclude that there exists an arithmetic progression $\tau_k = (\omega_k \ell + \alpha_k)_{\ell \in Z}$, with $\omega_k, \alpha_k \in Z$, $\omega_k \neq 0$, such that for every $m_k \in \tau_k$, the polynomial

$$\widetilde{P}(\underline{\ell}', m_k, \underline{y}) = P(\pi\underline{\ell}' + \underline{u}', m_k, \underline{y})$$

has no prime divisors in $Z$. Furthermore, taking into account that $P_{0\infty}(\pi\underline{\ell}' + \underline{u}') \neq 0$ (by (5)), we have $P_0(\pi\underline{\ell}' + \underline{u}', m_k) \neq 0$ for all finitely many $m_k \in \tau_k$. The requested conclusion is thus proved for $(m_1, \dots, m_{k-1}) = \pi\underline{\ell}' + \underline{u}'$ and the arithmetic progression $\tau_k$. □

### 3.6. **Proof of Theorem 3.7.**

3.6.1. *Proof of (a).* Let $Z$ be a near UFD or a Dedekind domain. By Lemma 3.10, proving $\mathcal{P}riSpe^{\star}(1, 1)$ will give $\mathcal{P}riSpe^{\star}(k, s)$ for all integers $k, s \geqslant 1$, i.e. the starred Primitive Specialization Hypothesis.

*1st case: $Z$ is a near UFD.* Let $P(t,\underline{y})$ be as in $\mathcal{P}ri\mathit{Spe}^\star(1,1)$. From Remark 3.5(1), one may assume that $P$ is not a monomial in $\underline{y}$. Let $\delta \in Z$ be the parameter associated in §2.1 with the nonzero coefficients $P_1(t),\dots,P_\ell(t) \in Z[t]$ of $P(t,\underline{y})$ viewed as a polynomial in $\underline{y}$.

Let $p_1,\dots,p_r$ be the prime divisors of $\delta$ (distinct modulo units). From condition $\mathcal{F}_t(P)=\emptyset$, for every $h=1,\dots,r$, there exists $m_h \in Z$ such that $P(m_h,\underline{y}) \not\equiv 0 \pmod{p_h}$.

We may assume without loss of generality that, for some $\rho \in \{0,1,\dots,r\}$, the ideals $p_1Z,\dots,p_\rho Z$ are maximal in $Z$, whereas the ideals $p_{\rho+1}Z,\dots,p_rZ$ are not. From above, $P$ is nonzero modulo each $p_h$, $h=\rho+1,\dots,r$, and we have $p_iZ \not\subset p_{i'}Z$ for any distinct $i,i' \in \{1,\dots,r\}$. Lemma 3.8 (with $\underline{t}=t$), applied with $I_h=p_hZ$, $h=1,\dots,r$, yields that there exists an element $m_0 \in Z$ such that $m_0 \equiv m_h \pmod{p_h}$, $h=1,\dots,\rho$, and $P(m_0,\underline{y}) \not\equiv 0 \pmod{p_h}$, $h=\rho+1,\dots,r$. These congruences imply that $P(m_0,\underline{y}) \not\equiv 0 \pmod{p_h}$, for each $h=1,\dots,r$.

Conclude that the polynomial $P(m_0,\underline{y})$ is primitive w.r.t. $Z$. Indeed assume that some non-unit $a \in Z$ divides $P(m_0,\underline{y})$. From Lemma 2.1, $a$ then divides $\delta$. But using that $Z$ is a near UFD, we obtain that some prime divisor of $a$ divides $\delta$ and $P(m_0,\underline{y})$, contrary to what we have established. Furthermore, our conclusion "$P(m,\underline{y})$ *is primitive w.r.t.* $Z$" is not only true for $m=m_0$, but also for every $m$ in the arithmetic progression $(\delta\ell+m_0)_{\ell\in Z}$.

*Remark* 3.11. More generally, if several polynomials $P_i(t,\underline{y})$ are given as in $\mathcal{P}ri\mathit{Spe}(1,n,s)$, then, denoting the corresponding $\delta$-parameters by $\delta_1,\dots,\delta_s$, the conclusion of the Primitive Specialization Hypothesis "$P_1(m,\underline{y}),\dots,P_s(m,\underline{y})$ *are primitive w.r.t.* $Z$" holds for every $m$ in some arithmetic progression $(\omega\ell+\alpha)_{\ell\in Z}$. Specifically one can take $\omega,\alpha \in Z$ such that every prime divisor $p$ of $\delta=\delta_1\cdots\delta_s$ divides $\omega$ and satisfies $\prod_{i=1}^s P_i(\alpha,\underline{y}) \not\equiv 0 \pmod{p}$.

*2nd case: $Z$ is a Dedekind domain.* We noted in Proposition 2.3 that the proof from §2.2 of the Dedekind domain part of Theorem 1.3 gives a more precise form of $\mathcal{C}op\mathit{Sch}(1,1)$. Namely it produces a whole arithmetic progression, the elements of which satisfy the conclusion of the $\mathcal{C}op\mathit{Sch}(1,1)$ (Proposition 2.3(a)). Furthermore, Proposition 2.3(b) shows that the same holds if non-unit divisors are replaced by prime divisors in the statement of the property. Finally, adjusting the observation made in Lemma 3.4(1) to show that "Coprime Schinzel" is stronger than "Primitive Specialization", what we eventually obtain from this chain of arguments is that the proof from §2.2 indeed gives property $\mathcal{P}ri\mathit{Spe}^\star(1,1)$.

3.6.2. *Proof of (b).* This clearly follows from (a) as for near UFDs, the *starred* Primitive Specialization Hypothesis is stronger than the Primitive Specialization Hypothesis, and that by Lemma 3.4(2-a), the latter and the coprime Schinzel Hypothesis are equivalent.

3.6.3. *Proof of (c).* Let $Z$ be a Dedekind domain. As already pointed out, the second part of (c), i.e. $\mathcal{C}op\mathit{Sch}(1,1)$, is the Dedekind domain part of Theorem 1.3 proved in §2.2. By Lemma 3.4(1), we deduce $\mathcal{P}ri\mathit{Spe}(1,n,1)$ for every $n \geqslant 1$. Combined with Lemma 3.4(3), we obtain $\mathcal{P}ri\mathit{Spe}(1,n,s)$ for all integers $n,s \geqslant 1$. □

## 4. The Hilbert-Schinzel specialization property

The goal of this section is to show Theorem 1.6. We distinguish two cases: $k=1$ in §4.1 and $k \geqslant 1$ in §4.2. We consider refinements of Theorem 1.6 in §4.3.

A new assumption on $Z$ in this section is that it is a *Hilbertian ring*.

*Definition* 4.1. Let $Z$ be an integral domain such that the fraction field $Q$ is of characteristic 0 or imperfect. The ring $Z$ is a *Hilbertian ring* if the following holds:

Let $\underline{t} = (t_1, \dots, t_k)$, $\underline{y} = (y_1, \dots, y_n)$ be tuples of variables $(k, n \geqslant 1)$, $P_1(\underline{t}, \underline{y}), \dots, P_s(\underline{t}, \underline{y})$ be $s$ polynomials $(s \geqslant 1)$, irreducible in $Q[\underline{t}, \underline{y}]$, of degree at least 1 in $\underline{y}$, and $F(\underline{t}) \in Q[\underline{t}]$ be a nonzero polynomial. Then the so-called Hilbert subset

$$H_Q(P_1, \dots, P_s; F) = \left\{ \underline{m} \in Q^k \;\middle|\; \begin{array}{c} P_i(\underline{m}, \underline{y}) \text{ is irreducible in } Q[\underline{y}] \\ (i = 1, \dots, s) \\ \text{and } F(\underline{m}) \neq 0. \end{array} \right\}$$

contains a $k$-tuple $\underline{m} \in Z^k$. If $Z$ is a field, it is called a *Hilbertian field*.

The original definition of Hilbertian ring from [FJ08, §13.4] has the defining condition only requested for $n = 1$ and polynomials $P_1(\underline{t}, y_1), \dots P_s(\underline{t}, y_1)$ that are further assumed to be separable in $y_1$. But [BDN20b, Proposition 4.2] shows that it is equivalent to Definition 4.1 under the imperfectness condition. Note further that since Zariski open subsets of Hilbert subsets remain Hilbert subsets, it is equivalent to require in Definition 4.1 that $H_Q(P_1, \dots, P_s; F)$ contains a Zariski-dense subset of tuples $\underline{m} \in Z^k$. In particular, a Hilbertian ring $Z$ is necessarily infinite.

For the proof of Theorem 1.6, note that one may assume that none of the polynomials $P_1, \dots, P_s$ are monomials in $\underline{y}$ (with coefficients in $Z[\underline{t}]$): to fulfill the assumptions of Theorem 1.6, such a monomial must be of the form $cy_i$ for some $c \in Z^\times$ and $i \in \{1, \dots, n\}$; the required conclusion for this monomial then trivially holds for every $\underline{m} \in Z^k$.

4.1. **Proof of Theorem 1.6 - case $k = 1$.** We will prove more generally that the Hilbert-Schinzel property holds with $k = 1$ and given integers $n, s \geqslant 1$ if $Z$ is a Hilbertian ring and the Primitive Specialization Hypothesis holds for $Z$ with $k = 1$ and the integers $n$ and $s$. From Theorem 3.7, the latter holds if $Z$ is a near UFD or a Dedekind domain.

Let $P_1(t, \underline{y}), \dots, P_s(t, \underline{y})$ be $s$ polynomials, irreducible in $Q[t, \underline{y}]$, primitive w.r.t. $Z$, of degree $\geqslant 1$ in $\underline{y}$ and such that $\mathcal{F}_t(P_1 \cdots P_s) = \emptyset$. The polynomials $P_1(t, \underline{y}), \dots, P_s(t, \underline{y})$ are also primitive w.r.t. $Q[t]$, as they are irreducible in $Q[t, \underline{y}]$. The Primitive Specialization Hypothesis with $k = 1$ provides an element $\alpha \in Z$ such that $P_1(\alpha, \underline{y}), \dots, P_s(\alpha, \underline{y})$ are primitive w.r.t. $Z$. Let $\delta_i$ be the parameter associated in Lemma 2.1 with the coefficients $P_{ij}(t) \in Z[t]$ of $P_i$ $(i = 1, \dots, s)$, and let $\omega$ be a multiple of $\delta = \delta_1 \cdots \delta_s$. From Lemma 2.1, for every $\ell \in Z$, the polynomials

$$P_1(\alpha + \ell\omega, \underline{y}), \dots, P_s(\alpha + \ell\omega, \underline{y})$$

are primitive w.r.t. $Z$. Consider next the polynomials

$$P_1(\alpha + \omega t, \underline{y}), \dots, P_s(\alpha + \omega t, \underline{y}).$$

They are in $Z[t, \underline{y}]$ and are irreducible in $Q[t, \underline{y}]$. As $Z$ is a Hilbertian ring, infinitely many $\ell \in Z$ exist such that the polynomials

$$P_1(\alpha + \omega\ell, \underline{y}), \dots, P_s(\alpha + \omega\ell, \underline{y})$$

are irreducible in $Q[\underline{y}]$. From above, these polynomials are also primitive w.r.t. $Z$.

4.2. **Proof of Theorem 1.6 - case $k \geqslant 1$.** We may assume that we are in case (a), and $Z$ is a near UFD. Let $P_1(\underline{t}, \underline{y}), \dots, P_s(\underline{t}, \underline{y})$ be $s$ polynomials, irreducible in $Q[\underline{t}, \underline{y}]$, primitive w.r.t. $Z$, of degree $\geqslant 1$ in $\underline{y}$ and such that $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s) = \emptyset$. Fix a nonzero polynomial $P_0 \in Z[\underline{t}]$. We need to produce a $k$-tuple $\underline{m} \in Z^k$ such that $P_1(\underline{m}, \underline{y}), \dots, P_s(\underline{m}, \underline{y})$ are irreducible in $Q[\underline{y}]$ and primitive w.r.t. $Z$, and $P_0(\underline{m}) \neq 0$. This clearly follows from successive applications of the following lemma to each of the variables $t_1, \dots, t_k$.

**Lemma 4.2.** *If $Z$ is a near UFD and a Hilbertian ring, then $Z$ has the following property, for all $k, n, s \geqslant 1$:*

*$\mathcal{H}ilSch^\star(k,n,s)$: With $\underline{t}=(t_1,\dots,t_k)$, $\underline{y}=(y_1,\dots,y_n)$, let $P_1(\underline{t},\underline{y}),\dots,P_s(\underline{t},\underline{y})$ be $s$ polynomials, irreducible in $Q[\underline{t},\underline{y}]$, of degree $\geqslant 1$ in $\underline{y}$ and such that the product $P=P_1\cdots P_s$ has no fixed prime divisor in $Z$ w.r.t. $\underline{t}$. Then there is an arithmetic progression $\tau=(\omega\ell+\alpha)_{\ell\in Z}$ ($\omega,\alpha\in Z$, $\omega\neq 0$) such that, for infinitely many $m_1\in\tau$, the polynomials*

$$P_1(m_1,t_2,\dots,t_k,\underline{y}),\dots,P_s(m_1,t_2,\dots,t_k,\underline{y})$$

*are irreducible in $Q[t_2,\dots,t_k,\underline{y}]$, of degree $\geqslant 1$ in $\underline{y}$, and such that their product, i.e. the polynomial $P(m_1,t_2,\dots,t_k,\underline{y})$, has no fixed prime divisor in $Z$ w.r.t. $(t_2,\dots,t_k)$.*

(For the application to Theorem 1.6(a), note that for near UFDs, the fixed prime divisor condition, both in the assumption and the conclusion of the property, implies that each of the $s$ polynomials in question are primitive w.r.t. $Z$. Also note that the extra condition in the general definition of Hilbert subsets that $F(\underline{m})\neq 0$ for some given nonzero polynomial $F\in Q[\underline{t}]$ is easily guaranteed: in the successive applications of Lemma 4.2 to each variable $t_i$, it suffices to exclude finitely many values $m_i$, $i=1,\dots,k$).

*Proof of Lemma 4.2.* Set $\underline{t}'=(t_2,\dots,t_k)$. Consider $P_1,\dots,P_s$ as polynomials in $\underline{t}',\underline{y}$ and with coefficients in $Z[t_1]$. As such, they are primitive w.r.t $Q[t_1]$ (being irreducible in $Q[\underline{t},\underline{y}]$). For each $i=1,\dots,s$, denote by $\delta_i\in Z$ the parameter associated in §2.1 with the coefficients of $P_i$ (which are in $Z[t_1]$ and coprime).

Set $\delta=\delta_1\cdots\delta_s$ and let $\mathcal{P}$ be the set of primes $p\in Z$ that divide $\delta$ or such that $|Z/pZ|\leqslant \max_{2\leqslant h\leqslant k}\deg_{t_h}(P)$. From Lemma 3.9, the set $\mathcal{P}$ is finite (up to units). Let $\omega$ be the product of all primes in $\mathcal{P}$.

The first step is to construct a $k$-tuple $\underline{u}=(u_1,\dots,u_k)\in Z^k$ such that

$$P(\underline{u},\underline{y})\not\equiv 0 \pmod p \text{ for every } p\in\mathcal{P}. \tag{1}$$

As $P$ has no fixed prime divisor w.r.t. $\underline{t}$, for every $p\in\mathcal{P}$, there is a $k$-tuple $\underline{u}_p\in Z^k$ such that $P(\underline{u}_p,\underline{y})\not\equiv 0 \pmod p$. Using Lemma 3.8 and arguing as in the proof of Lemma 3.10 (1st step), one finds $\underline{u}_0=(u_{01},\dots,u_{0k})\in Z^k$ satisfying (1). Furthermore, denoting by $\tau_h$ the arithmetic progression $\tau_h=(\omega\ell+u_{0h})_{\ell\in Z}$ ($h=1,\dots,k$), the conclusion holds for every $\underline{u}=(u_1,\dots,u_k)\in\tau_1\times\cdots\times\tau_k$. Fix such a $k$-tuple $\underline{u}$ and set $\alpha=u_1$.

It follows from the fixed prime divisor assumption w.r.t. $\underline{t}$ that $P$ has no fixed prime divisor w.r.t. the variable $t_1$. From Remark 3.11, we have that, for every $\ell_1\in Z$,

(2) the polynomials $P_i(\omega\ell_1+\alpha,\underline{t}',\underline{y})$, $i=1,\dots,s$, have no prime divisors in $Z$.

(Note that condition from Remark 3.11 that $P(\alpha,\underline{t}',\underline{y})\not\equiv 0 \pmod p$ and every prime divisor of $\delta$ is guaranteed by (1)).

Consider the following polynomials, where $v_1$ is a new variable:

$$\widetilde{P}_i(v_1,\underline{t}',\underline{y})=P_i(\omega v_1+\alpha,\underline{t}',\underline{y})\in Z[v_1,\underline{t}',\underline{y}],\ \ i=1,\dots,s.$$

The polynomials $\widetilde{P}_1,\dots,\widetilde{P}_s$ are irreducible in $Q[\underline{t}'][v_1,\underline{y}]$ and of degree at least 1 in $\underline{y}$. As $Z$ is a Hilbertian ring, there exist infinitely many $\ell_1\in Z$ such that

(3) the polynomials $\widetilde{P}_i(\ell_1,\underline{t}',\underline{y})$ ($i=1,\dots,s$) are irreducible in $Q[\underline{t}',\underline{y}]$, of degree $\geqslant 1$ in $\underline{y}$.

Fix $\ell_1\in Z$ as in (3) and set $\widetilde{P}=\prod_{i=1}^s\widetilde{P}_i$. To end the proof, it remains to check that $\widetilde{P}(\ell_1,\underline{t}',\underline{y})$ has no fixed prime divisor w.r.t. $\underline{t}'$. Assume that for some prime $p\in Z$, we have $\widetilde{P}(\ell_1,\underline{m}',\underline{y})\equiv 0 \pmod p$ for every $\underline{m}'\in Z^{k-1}$. Note that due to (1) we have

$$\widetilde{P}(\ell_1,u_2,\dots,u_k,\underline{y})\not\equiv 0 \pmod p, \text{ for every } p\in\mathcal{P}.$$

Therefore $p\notin\mathcal{P}$. Hence, by choice of $\mathcal{P}$,

$$|Z/pZ| > \max_{2\leqslant h\leqslant k} \deg_{t_h}(P) \geqslant \max_{2\leqslant h\leqslant k} \deg_{t_h}\left(\widetilde{P}(\ell_1, \underline{t}', \underline{y})\right) \tag{4}$$

By (2), $\widetilde{P}_1(\ell_1, \underline{t}', \underline{y}), \dots, \widetilde{P}_s(\ell_1, \underline{t}', \underline{y})$ are nonzero modulo $p$ (in $(Z/pZ)[\underline{t}', \underline{y}]$). Hence so is their product $\widetilde{P}(\ell_1, \underline{t}', \underline{y})$. This, conjoined with (4) contradicts Lemma 3.1(a). □

## 4.3. **Variants of Theorem 1.6.**

4.3.1. *Relaxing the fixed divisor assumption.* Let $Z$ be a near UFD and $P_1, \dots, P_s$ be as in Definition 1.5, except that $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s) = \emptyset$ is no longer assumed. By Lemma 3.1, the set of primes in $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s)$ is finite (modulo units). Let $\varphi$ be the product of them. One can then conclude that

(*) *there is a Zariski-dense subset $H \subset Z[1/\varphi]^k$ such that for every $\underline{m} \in H$, the polynomials $P_1(\underline{m}, \underline{y}), \dots, P_s(\underline{m}, \underline{y})$ are irreducible in $Q[\underline{y}]$ and primitive w.r.t. $Z[1/\varphi]$.*

Of course, if $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s) = \emptyset$, then $\varphi = 1$ and we merely have Theorem 1.6. Conversely, the improved conclusion follows from Theorem 1.6 by just taking $Z$ to be $Z[1/\varphi]$: simply note that the assumptions on $Z$ are preserved by passing to $Z[1/\varphi]$.

*Remark* 4.3. One can avoid inverting $\varphi$ and still not assume $\mathcal{F}_{\underline{t}}(P_1 \cdots P_s) = \emptyset$, but then specializing to points $\underline{m} \in Z^k$ should be replaced by specializing to points $\underline{m}(\underline{y}) \in Z[\underline{y}]^k$: a Zariski-dense subset of $\underline{m}(\underline{y}) \in Z[\underline{y}]^k$ exists such that $P_1(\underline{m}(\underline{y}), \underline{y}), \dots, P_s(\underline{m}(\underline{y}), \underline{y})$ are irreducible in $Z[\underline{y}]$ [BDN20b, Theorem 1.1].

4.3.2. *A variant of Theorem 1.6 for Dedekind domains with $k \geqslant 1$.* Compared to Theorem 1.6(b) where $k = 1$, the following result, for Dedekind domains, has $k \geqslant 1$ but $s = 1$, i.e. concerns one polynomial with $k \geqslant 1$ variables $t_i$ to be specialized.

**Theorem 4.4.** *Let $Z$ be a Dedekind domain and a Hilbertian ring. Let $P(\underline{t}, \underline{y})$ be a polynomial, irreducible in $Q[\underline{t}, \underline{y}]$, of degree $\geqslant 1$ in $\underline{y}$ (with $k, n \geqslant 1$). Assume that $P$ has no fixed <u>prime</u> divisor w.r.t. $\underline{t}$. There is a Zariski-dense subset $H \subset Z^k$ such that for every $\underline{m} \in H$, the polynomial $P(\underline{m}, \underline{y})$ is irreducible in $Q[\underline{y}]$ and has no <u>prime</u> divisor in $Z$.*

The cost of the generalization to $k \geqslant 1$ is that the primitivity w.r.t. $Z$ of the polynomial $P(\underline{m}, \underline{y})$ in the conclusion is replaced by the non-divisibility by any prime $p \in Z$. On the other hand the assumption is weaker: $P(\underline{t}, \underline{y})$ is not assumed to be primitive w.r.t. $Z$ and the fixed divisor assumption is restricted to primes.

*Proof.* As before, one may assume that $P$ is not a monomial in $\underline{y}$. The statement clearly follows from successive applications of property $\mathcal{H}ilSch^\star(k, n, 1)$ from Lemma 4.2 to each of the variables $t_1, \dots, t_k$. In Lemma 4.2, this property was proved in the case that $Z$ is a near UFD. We prove it below in the case that $Z$ is a Dedekind domain (and a Hilbertian ring as also assumed in Lemma 4.2). The strategy is the same.

Recall that here $s = 1$. Let $P_1(t_1), \dots, P_N(t_1) \in Z[t_1]$ be the coefficients of $P$ viewed as a polynomial in $\underline{t}', \underline{y}$, where $\underline{t}' = (t_2, \dots, t_k)$. They are coprime in $Q[t_1]$ (a consequence of $P$ being irreducible in $Q[\underline{t}, \underline{y}]$). Let $\delta \in Z$ be the associated parameter from §2.1 and let $\mathcal{Q}_1, \dots, \mathcal{Q}_r$ be the prime ideals of $Z$ dividing $\delta$. One may assume that the first ones, say $\mathcal{Q}_1, \dots, \mathcal{Q}_\rho$, are principal, generated by prime elements $q_1, \dots, q_\rho$ respectively, while the last ones $\mathcal{Q}_{\rho+1}, \dots, \mathcal{Q}_r$ are not principal.

Let $\mathcal{P}$ be the union of the set $\{q_1, \dots, q_\rho\}$ and of the set of primes $p \in Z$ such that $|Z/pZ| \leqslant \max_{2\leqslant h\leqslant k} \deg_{t_h}(P)$. From Lemma 3.9, the set $\mathcal{P}$ is finite. Let $\omega$ be the product of all primes in $\mathcal{P}$.

Let $\mathfrak{I}$ be the ideal of $Z$ generated by all values $P_1(z), \dots, P_N(z)$ with $z \in Z$. Denote by $g_1, \dots, g_r \geqslant 0$ the respective exponents of $\mathcal{Q}_1, \dots, \mathcal{Q}_r$ in the prime ideal factorization of $\mathfrak{I}$.

As $P$ has no fixed prime divisor in $Z$ w.r.t. $\underline{t}$, for every $p \in \mathcal{P}$, there is a $k$-tuple $\underline{u}_p = (u_{p1}, \dots, u_{pk}) \in Z^k$ such that

$$P(\underline{u}_p, \underline{y}) \not\equiv 0 \pmod{p}.$$

Consider next the ideals $\mathcal{Q}_{\rho+1}^{g_{\rho+1}+1}, \dots, \mathcal{Q}_r^{g_r+1}$. As none of these ideals contains $\mathfrak{I}$, for each $j = \rho+1, \dots, r$, there exists $i_j \in \{1, \dots, N\}$ and $u_{j1} \in Z$ such that $P_{i_j}(u_{j1}) \not\equiv 0 \pmod{\mathcal{Q}_j^{g_j+1}}$, or equivalently,

$$(P_1(u_{j1}), \dots, P_N(u_{j1})) \not\equiv (0, \dots, 0) \pmod{\mathcal{Q}_j^{g_j+1}},$$

or, again equivalently,

$$P(u_{j1}, \underline{t}', \underline{y}) \not\equiv 0 \pmod{\mathcal{Q}_j^{g_j+1}}.$$

Any two ideals in the set $\mathcal{P} \cup \{\mathcal{Q}_{\rho+1}^{g_{\rho+1}}, \dots, \mathcal{Q}_r^{g_\rho}\}$ are comaximal (or this set is empty or a singleton). The Chinese Remainder Theorem gives a tuple $\underline{u} = (u_1, \dots, u_k) \in Z^k$ such that

(1) (a) $$P(\underline{u}, \underline{y}) \not\equiv 0 \pmod{p}, \text{ for each } p \in \mathcal{P},$$

(b) $$\text{and } P(u_1, \underline{t}', \underline{y}) \not\equiv 0 \pmod{\mathcal{Q}_j^{g_j+1}}, \text{ for each } j = \rho+1, \dots, r.$$

Note that condition (1-a) implies that $P(u_1, \underline{t}', \underline{y}) \not\equiv 0 \pmod{q_j^{g_j+1}}$, for each $j = 1, \dots, \rho$. So condition (1-b) in fact holds for each $j = 1, \dots, r$. Note further that the fixed prime divisor assumption w.r.t. $\underline{t}$ implies that $P$ has no fixed prime divisor w.r.t. the variable $t_1$. Set $\alpha = u_1$. Proposition 2.3(b) can be applied to conclude that

(2) the polynomial $P(\omega\ell_1 + \alpha, \underline{t}', \underline{y})$ has no prime divisors $p \in Z$ for every $\ell_1 \in Z$.

The end of the proof of Lemma 4.2 can now be reproduced *mutatis mutandi*. Consider the following polynomial, where $v_1$ is a new variable:

$$\widetilde{P}(v_1, \underline{t}', \underline{y}) = P(\omega v_1 + \alpha, \underline{t}', \underline{y}) \in Z[v_1, \underline{t}', \underline{y}].$$

The polynomial $\widetilde{P}$ is irreducible in $Q[\underline{t}'][v_1, \underline{y}]$ and of degree at least 1 in $\underline{y}$. As $Z$ is a Hilbertian ring, there exist infinitely many $\ell_1 \in Z$ such that

(3) the polynomial $\widetilde{P}(\ell_1, \underline{t}', \underline{y})$ is irreducible in $Q[\underline{t}', \underline{y}]$, of degree $\geqslant 1$ in $\underline{y}$.

Fix $\ell_1 \in Z$ as in (3). It remains to check that $\widetilde{P}(\ell_1, \underline{t}', \underline{y})$ has no fixed prime divisor w.r.t. $\underline{t}'$. Assume that for some prime $p \in Z$, we have $\widetilde{P}(\ell_1, \underline{m}', \underline{y}) \equiv 0 \pmod{p}$ for every $\underline{m}' \in Z^{k-1}$. Note that due to (1-a), we have

$$\widetilde{P}(\ell_1, u_2, \dots, u_k, \underline{y}) \not\equiv 0 \pmod{p}, \text{ for every } p \in \mathcal{P}.$$

Therefore $p \notin \mathcal{P}$. Hence, by choice of $\mathcal{P}$,

$$(4) \qquad |Z/pZ| > \max_{2 \leqslant h \leqslant k} \deg_{t_h}(P) \geqslant \max_{2 \leqslant h \leqslant k} \deg_{t_h}\left(\widetilde{P}(\ell_1, \underline{t}', \underline{y})\right)$$

As, by (2), $\widetilde{P}(\ell_1, \underline{t}', \underline{y})$ is nonzero modulo $p$, this contradicts Lemma 3.1(a). □

## References


[BDN20a] Arnaud Bodin, Pierre Dèbes, and Salah Najib. Prime and coprime values of polynomials. *Enseign. Math.*, 66(1-2):173–186, 2020.

[BDN20b] Arnaud Bodin, Pierre Dèbes, and Salah Najib. The Schinzel hypothesis for polynomials. *Trans. Amer. Math. Soc.*, 373(12):8339–8364, 2020.

[Coh68] Paul M. Cohn. Bezout rings and their subrings. *Proc. Cambridge Philos. Soc.*, 64:251–264, 1968.

[Eke91] Torsten Ekedahl. An infinite version of the Chinese remainder theorem. *Comment. Math. Univ. St. Paul.*, 40(1):53–59, 1991.

[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.

[FP17] Péter E. Frenkel and József Pelikán. On the greatest common divisor of the value of two polynomials. *Amer. Math. Monthly*, 124(5):446–450, 2017.

[Lan65] Serge Lang. *Algebra*. Addison-Wesley, 1965.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Poo03] Bjorn Poonen. Squarefree values of multivariable polynomials. *Duke Math. J.*, 118(2):353–373, 2003.

[Sch02] Andrzej Schinzel. A property of polynomials with an application to Siegel's lemma. *Monatsh. Math.*, 137(3):239–251, 2002.

[Ser92] Jean-Pierre Serre. *Topics in Galois Theory*. Research Notes in Mathematics. Jones and Bartlett Publishers, 1992.

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

[SS20] Alexei N. Skorobogatov and Efthymios Sofos. Schinzel Hypothesis with probability 1 and rational points. *preprint*, 2020. arXiv:2005.02998.

*Email address*: arnaud.bodin@univ-lille.fr
*Email address*: pierre.debes@univ-lille.fr
*Email address*: jkoenig@knue.ac.kr
*Email address*: slhnajib@gmail.com

Université de Lille, CNRS, UMR 8524, Laboratoire Paul Painlevé, F-59000 Lille, France

Université de Lille, CNRS, UMR 8524, Laboratoire Paul Painlevé, F-59000 Lille, France

Department of Mathematics Education, Korea National University of Education, 28173 Cheongju, South Korea

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