SOME GOLDBACH REPRESENTATIONS OF POLYNOMIALS AND FORMAL POWER SERIES

SİNEM BENLİ-GÖRAL[1], HAYDAR GÖRAL[2], AND MUSTAFA KUTAY KUTLU[3,*]

[1,2,3] İZMİR INSTITUTE OF TECHNOLOGY, DEPARTMENT OF MATHEMATICS, 35430, URLA, İZMİR, TÜRKİYE

ABSTRACT. For a unique factorization domain R with zero Jacobson radical and which is not a field, we prove that any polynomial in $F[x]$ can be written as a sum of two irreducible polynomials from $F[x]$, where F is the field of fractions of R. Besides, if the characteristic of R is 0, then any monic polynomial from $R[x]$ can be written as a sum of two irreducible polynomials from $R[x]$, and any non-constant polynomial from $R[x]$ can be written as a sum of at most three irreducible polynomials from $R[x]$. We refer to this representation as a (Weak) Goldbach Property. We also prove that if R is a unique factorization domain which is not local, then any polynomial in $R[x]$ can be written as a sum of at most four irreducible polynomials from $R[x]$. Moreover, we characterize a Goldbach Property for formal power series over discrete valuation rings. Finally, using ultraproducts, we construct some local rings R which are not fields, where another type of a Goldbach Property holds for $R[x]$.

CONTENTS

Date: March 6, 2026.

Key words and phrases. Goldbach's Conjecture, Goldbach Property, polynomial rings, formal power series, ultraproducts.

[3,*] Corresponding author: mustafakutlu@iyte.edu.tr.

[1] sinembenli@iyte.edu.tr, [2] haydargoral@iyte.edu.tr.

2020 *Mathematics subject classification.* 13G05, 11C08, 11U07.

1. Introduction

Goldbach's Conjecture is one of the oldest and best-known unsolved problems in number theory. It states that every even integer greater than 2 can be written as a sum of two prime numbers. Goldbach's Conjecture was first proposed by Christian Goldbach in a letter to Euler in 1742 as:

"*At least it seems that every integer that is greater than* 5 *is a sum of three primes.*"

Then, Euler indicated that the above version of Goldbach's Conjecture is equivalent to every even integer greater than 2 is a sum of two prime numbers. The conjecture has been shown to hold for all integers less than 4×10^{18}. However, Goldbach's Conjecture is still open. On the other hand, Goldbach's Conjecture implies its weak version, namely the Weak Goldbach Conjecture, and it states that every odd number greater than or equal to 7 can be represented as a sum of three primes. In 1937, Vinogradov [36] proved that every sufficiently large odd positive integer is a sum of three primes and the proof is based on the circle method. Later on, using a sieve method, Chen [11] obtained that every sufficiently large even integer is a sum of a prime and a product of at most two primes. More recently, in 2013, Helfgott gave a proof of the Weak Goldbach Conjecture, see [19, 20].

Although the Goldbach Conjecture remains open, one can consider it for other algebraic structures such as polynomial and formal power series rings. This property is called a *Goldbach Property*. For a commutative ring R, we say that the ring $R[x]$ has a Goldbach Property if every (monic) element of $R[x]$ can be written as a sum of two irreducible polynomials from $R[x]$. One of the first major achievements for polynomial rings was made by Hayes [18] in 1965, who proved that in the ring $\mathbb{Z}[x]$, any non-constant polynomial can be written as a sum of two irreducible polynomials from $\mathbb{Q}[x]$. In other words, Hayes showed

that $\mathbb{Q}[x]$ has a Goldbach Property. Hayes also pointed out that his proof indicates that $F[x]$ has a Goldbach Property whenever R is a principal ideal domain with infinitely many prime elements, where F is the field of fractions of R. In 2006, Saidak [31] gave another proof of Hayes' result for $\mathbb{Z}[x]$, and proved that $\mathbb{Z}[x]$ has a Goldbach Property. Moreover, Saidak also gave a quantitative version of his result. Later on, Saidak's quantitative result was further generalized by Kozek [21, 22], Dubickas [14] and Lemos and de Araujo [24]. In 2011, Pollack [29] showed that if R is an integral domain which is Noetherian and if R has infinitely many maximal ideals, then $R[x]$ has a Goldbach Property, and this extends the corresponding results of [18, 31]. If R is a finite field, then a Goldbach Property was obtained in [5]. From another point of view, one can examine a Goldbach Property for formal power series rings. For instance, the complete characterization of a Goldbach Property for $\mathbb{Z}[[x]]$ was given in [28]. For some discussions on the Goldbach Conjecture, we direct the reader to [25].

There is a far-reaching conjecture of Schinzel, the so-called Schinzel Hypothesis, which states that if $\{P_1, \ldots, P_s\}$ is a set of non-constant irreducible polynomials from $\mathbb{Z}[x]$ with the property that there is no prime number $p \in \mathbb{Z}$ dividing the product $\prod_{i=1}^{s} P_i(m)$ for all $m \in \mathbb{Z}$, then there exist infinitely many $m \in \mathbb{Z}$ such that the values $P_1(m), \ldots, P_s(m)$ are all prime numbers. The Schinzel Hypothesis immediately extends Dirichlet's theorem on primes in arithmetic progressions. It also implies the twin prime conjecture by taking $\{x, x+2\}$ as our set of irreducible polynomials from $\mathbb{Z}[x]$. However, the Schinzel Hypothesis is wide open even our set of irreducible polynomials from $\mathbb{Z}[x]$ only consists of one polynomial of degree at least 2. Similar to the Goldbach Property for polynomials, there are several versions of the Schinzel Hypothesis for polynomials as well, see [6–9]. In [6], Bodin, Dèbes and Najib proved that a Schinzel Hypothesis is true for $R[x_1, \ldots, x_n]$ where $n \geq 1$ and R is a unique factorization domain whose field of fractions F has the product formula and F is imperfect when the characteristic of it is positive. To illustrate, if R is the ring of integers of a number field of class number 1, or $k[y_1, \ldots, y_r]$ where k is a field and $r \geq 1$, or R itself is a field with the product formula and R is imperfect when the characteristic of it is positive, then a Schinzel Hypothesis holds for $R[x_1, \ldots, x_n]$ where $n \geq 1$. Therefore, by [6], one can immediately obtain a Goldbach Property [6, Corollary 1.5] for rings which satisfy the assumptions of [6, Theorem 1.1], in particular, a Goldbach Property holds for $\mathbb{Z}[x_1, \ldots, x_n]$ when $n \geq 1$. In [8], the authors obtained another Schinzel

Hypothesis, so-called the Hilbert-Schinzel Specialization Property for many rings. However, this property does not yield the corresponding Goldbach Property for these rings. For a coprime version of the Schinzel Hypothesis, we refer the reader to [7, 9].

In this note, we also focus on a Goldbach Property for polynomials and formal power series. Throughout the paper, R stands for an associative commutative ring with identity $1 \neq 0$, and $\mathrm{J}(R)$ and $\mathrm{U}(R)$ denote the Jacobson radical and the set of unit (invertible) elements of R, respectively.

Here is a brief overview of this note. In the next section, we show that for a unique factorization domain R which is not a field with $\mathrm{J}(R) = 0$, any polynomial in $F[x]$ can be written as a sum of two irreducible polynomials from $F[x]$, where F is the field of fractions of R, see Theorem 2.9. Besides, if the characteristic of R is 0, then any monic polynomial from $R[x]$ can be written as a sum of two irreducible polynomials from $R[x]$, and any non-constant polynomial from $R[x]$ can be written as a sum of at most three irreducible polynomials from $R[x]$ (a Weak Goldbach Property), see Theorem 2.10. In any case, for a unique factorization domain R which is not a field with $\mathrm{J}(R) = 0$, we prove that any polynomial in $R[x]$ of degree $n \geq 1$ can be written as a sum of at most four irreducible polynomials from $R[x]$ of degree at most n (a Weak Goldbach Property), see Theorem 2.10. In fact, our results Theorem 2.9 and Theorem 2.10 hold true when R is an almost unique factorization domain with $\mathrm{J}(R) = 0$, see Definition 2.12 and Theorem 2.14. In the same section, we obtain that if R is a unique factorization domain which is not local, then a Weak Goldbach Property is satisfied for $R[x]$, see Theorem 2.23. As corollaries, we extend the corresponding classical results of Hayes [18] and Saidak [31]. Our results do not generalize Pollack's result [29], however there are many cases for which Pollack's result [29] is insufficient and our results are applicable. Although, the Schinzel Hypothesis in [6] generalizes the corresponding Goldbach Property, the set of rings where the Schinzel Hypothesis in [6] are pertinent is small (elements of this set has a sort of geometric structure) compared to the set of rings where a Goldbach Property holds, as indicated by Pollack's result and our results. We direct the reader to the table in Remark 2.26 for a summary of our results from Section 2. In Section 3, we work with formal power series over discrete valuation rings, and we give a classification result for a Goldbach Property, see Theorem 3.1. In Section 4, using a result of Bender [5] and ultraproducts,

we construct some examples of local rings R that are not fields, and for which a Goldbach Property holds for $R[x]$, see Corollary 4.8. In Section 4, we also extend Wang's result [37] which states that for each characteristic p including 0, there exist infinitely many infinite fields F of characteristic p such that $F[x]$ satisfies a Weak Goldbach Property, see Proposition 4.10.

2. A Goldbach Property for Polynomial Rings

In ring theory, it is well known that the *Jacobson radical* of a commutative ring R is defined as the intersection of all maximal ideals of R. Since it is important in our work, we shall state a characterization of the elements of $\mathrm{J}(R)$ in terms of unit elements.

Proposition 2.1. *[1, Proposition 1.9] Let R be a commutative ring. Then, $x \in \mathrm{J}(R)$ if and only if $1 - xy \in \mathrm{U}(R)$ for every $y \in R$.*

At this point, we recall the following fundamental results for polynomial rings that we need for the manuscript.

Fact 2.2. *(Gauss' Lemma) [15, p. 303, Proposition 5] Let R be a unique factorization domain and F be the field of fractions of R. If a non-constant polynomial in $R[x]$ is irreducible in $R[x]$, then it is irreducible in $F[x]$.*

Fact 2.3. *(Eisenstein's Criterion) [15, p. 309, Proposition 13] Let R be an integral domain and $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a non-constant polynomial in $R[x]$. Suppose that p is a prime in R so that p divides a_i for all $i \in \{0, 1, \ldots, n-1\}$ but p does not divide a_n. If p^2 does not divide a_0, then $f(x)$ is irreducible in $F[x]$, where F is the field of fractions of R.*

Fact 2.4. *[15, p. 304, Corollary 6] Let R be a unique factorization domain and let F be its field of fractions and $f(x) \in R[x]$ be a non-constant polynomial. Suppose the greatest common divisor of the coefficients of $f(x)$ is 1. Then, f(x) is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$.*

The following fact will be needed for the proof of Theorem 2.14. For completeness, we also give its proof.

Fact 2.5. *Let R be an integral domain and F be its field of fractions and $f(x) \in R[x]$ be a non-constant polynomial with the property that any common divisor of the coefficients of $f(x)$ is a unit. Then, the irreducibility of $f(x)$ in $F[x]$ implies the irreducibility of $f(x)$ in $R[x]$.*

Proof. Suppose that f factors in $R[x]$ as $f = gh$ with $g, h \in R[x]$. Viewing this factorization in $F[x]$, the irreducibility of f in $F[x]$ forces one of the factors, say g, to be a unit in $F[x]$. As F is a field, the units of $F[x]$ are precisely the non-zero constants. Hence $g = c$ for some non-zero $c \in F$. Since $g \in R[x]$, we see that $c \in R$ and $c \neq 0$. From $f = ch$, we conclude that c divides all the coefficients of f. By the assumption on f, we deduce that $g = c$ must be a unit in R. Hence, f is also irreducible in $R[x]$. □

The next three lemmas will be crucial for Theorem 2.9 and Theorem 2.10.

Lemma 2.6. *Let R be an integral domain. If p and q are non-associated prime elements in R with $(p, q) = pR + qR = R$, then there are elements c and d in R such that $p \nmid c$ and $q \nmid d$, and also*

$$pc + qd = 1.$$

Proof. As $(p, q) = R$, there exist c_0 and d_0 in R such that

$$pc_0 + qd_0 = 1.$$

If $p \nmid c_0$ and $q \nmid d_0$, then we are done. Without loss of generality, let p divide c_0 and for any $k \in R$, define

$$c_k = c_0 + qk \quad \text{and} \quad d_k = d_0 - pk.$$

Then, we have that

$$pc_k + qd_k = 1$$

for all $k \in R$. Clearly $c_1 = c_0 + q$ and $c_q = c_0 + q^2$. As p does not divide q (they are non-associated), it follows that p does not divide c_1 and c_q. Next, we observe that q cannot divide d_1 and d_q at the same time. If q divides both d_1 and d_q, then q divides $d_1 - d_q = p(q - 1)$. As q is a prime element, it follows that q divides p or $q - 1$. The former case is impossible since $(p, q) = R$ (they are non-associated). For the latter case, if q divides $q - 1$, then q divides -1. This means q is a unit, contradicting that q is a prime element. Therefore, one of (c_1, d_1) or (c_q, d_q) is a solution of equation

$$pc + qd = 1,$$

where $p \nmid c$ and $q \nmid d$. □

Lemma 2.7. *Let R be an integral domain. If p and q are two elements from R with $(p, q) = pR + qR = R$, then $(p^n, q^n) = p^nR + q^nR = R$ for any integer $n \geq 1$.*

Proof. As $(p, q) = R$, there exist a and b in R such that

$$pa + qb = 1.$$

Say $\alpha = pa$ and $\beta = qb$. Then, we have

$$\alpha + \beta = 1.$$

To obtain the lemma, it is enough to show that $(p^2, q^2) = p^2R + q^2R = R$, and hence by induction $(p^n, q^n) = R$ for all $n \geq 1$. Now,

$$\begin{aligned} 1 = 1^3 = (\alpha + \beta)^3 &= \alpha^3 + 3\alpha^2\beta + 3\alpha\beta^2 + \beta^3 \\ &= \alpha^2\big(\alpha + 3\beta\big) + \beta^2\big(3\alpha + \beta\big) \\ &= p^2a^2\big(pa + 3qb\big) + q^2b^2\big(3pa + qb\big) \\ &= p^2k_1 + q^2k_2, \end{aligned}$$

where

$$k_1 = a^2\big(pa + 3qb\big)$$

and

$$k_2 = b^2\big(3pa + qb\big).$$

Thus, we conclude that

$$(p^2, q^2) = p^2R + q^2R = R.$$

□

Lemma 2.8. *Let R be a unique factorization domain which is not a field with $\mathrm{J}(R) = 0$. Then, the following conditions hold:*

(1) *The ring R contains infinitely many non-associated prime elements.*
(2) *Let $a \in R \setminus \{0\}$. There are non-associated primes p, q and an element y in R such that $p \nmid a$ and $q \mid 1 - pay$.*

Proof. (1) As R is not a field, it contains non-unit elements which are not zero. So R contains prime elements, as it is a unique factorization domain. Next, we observe that R contains infinitely many non-associated prime elements. Assume that R contains only finitely many non-associated primes, say $p_1, p_2, \ldots, p_k$. For any $y \in R$, the element $1 - p_1p_2 \cdots p_ky$ is non-zero and is not divisible by any of p_1, p_2, …, p_k. Thus, $1 - p_1p_2 \cdots p_ky \in \mathrm{U}(R)$ for every $y \in R$. By Proposition 2.1, this yields

that $0 \neq p_1p_2\cdots p_k \in \mathrm{J}(R)$, which contradicts the fact that $\mathrm{J}(R) = 0$. Hence, R contains infinitely many non-associated primes.

(2) Let a be a non-zero element of R. Then, condition (1) directly implies that there exists a prime $p \in R$ that does not divide a. We also have $pa \notin \mathrm{J}(R)$ as $pa \neq 0$, and this gives that there exists $y \in R$ such that $1 - pay$ is a non-unit in R by Proposition 2.1. Consequently, we can find a prime element $q \in R$ that divides $1 - pay$, and it follows that p and q are not associated.

□

Now, we are ready to prove our results which provide a Goldbach or a Weak Goldbach Property for unique factorization domains with trivial Jacobson radical.

Theorem 2.9. *Let R be a unique factorization domain which is not a field with $\mathrm{J}(R) = 0$ and F be its field of fractions.*

(1) *Every polynomial $M(x)$ of degree $n \geq 1$ in $F[x]$ can be written as a sum of two irreducible polynomials from $F[x]$ of degree n.*

(2) *Every polynomial $M(x)$ of degree $n \geq 1$ in $R[x]$ can be written as a sum of two irreducible polynomials from $R[x]$ of degree $n + 1$.*

Proof. (1) Let

$$M(x) = m_nx^n + m_{n-1}x^{n-1} + \cdots + m_tx^t$$

be a polynomial in $F[x]$ with $0 \leq t \leq n$. We suppose that $n \geq 1$, $m_n \neq 0$, and $m_t \neq 0$. As the non-zero constants are units in F, multiplying $M(x)$ by a non-zero element from F does not affect the irreducibility of $M(x)$. Thus, we may assume that $M(x)$ is in $R[x]$ by multiplying it by the denominators of its coefficients, if necessary. For the element $m_nm_t \neq 0$, we find non-associated primes p, q and an element y as in Lemma 2.8(2). It follows that

$$R = (p, 1 - pm_nm_ty) \subseteq (p, q).$$

In other words, $(p, q) = R$. Therefore, there exist non-zero elements $a_n^{'}$ and $b_n^{'}$ in R such that

$$qa_n^{'} + pb_n^{'} = m_n.$$

As both p and q do not divide m_n, one sees that p does not divide $qa_n^{'}$ and q does not divide $pb_n^{'}$. Set $a_n = qa_n^{'}$ and $b_n = pb_n^{'}$. Similarly, for $t < i < n$, there exist $a_i^{'}$

and $b_i^{'}$ in R such that

$$pa_i^{'} + qb_i^{'} = m_i.$$

Put $a_i = pa_i^{'}$ and $b_i = qb_i^{'}$ for $t < i < n$. Clearly, p divides a_i and q divides b_i for $t < i < n$. Now, by Lemma 2.6, there exist $a_t^{'}$ and $b_t^{'}$ in R such that

$$pa_t^{'} + qb_t^{'} = 1$$

with $p \nmid a_t^{'}$ and $q \nmid b_t^{'}$. We take $a_t = m_t pa_t^{'}$ and $b_t = m_t qb_t^{'}$. Since p does not divide m_t, it follows that $p \mid a_t$ but $p^2 \nmid a_t$. For a similar reason, we deduce that $q \mid b_t$ but $q^2 \nmid b_t$.

Case 1: Assume $t = 0$. Let

$$A(x) = a_n x^n + \cdots + a_1 x + a_0$$

and

$$B(x) = b_n x^n + \cdots + b_1 x + b_0.$$

Then, $A(x)$ and $B(x)$ are irreducible in $F[x]$ by Fact 2.3, that is, by Eisenstein's Criterion since all the required conditions are satisfied by the above observations. Moreover, we have

$$M(x) = A(x) + B(x).$$

Case 2: Assume $t \geq 1$. Let

$$A(x) = a_n x^n + \cdots + a_t x^t + pq$$

and

$$B(x) = b_n x^n + \cdots + b_t x^t - pq.$$

Thus, both p and q divide pq and both p^2 and q^2 do not divide pq. Then, once again $A(x)$ and $B(x)$ are irreducible in $F[x]$ by Fact 2.3, and

$$M(x) = A(x) + B(x).$$

(2) Let

$$M(x) = m_n x^n + m_{n-1}x^{n-1} + \cdots + m_t x^t$$

be a polynomial in $R[x]$ with $0 \leq t \leq n$. Again, we suppose that $n \geq 1$, $m_n \neq 0$, and $m_t \neq 0$. By Lemma 2.8 and as in the proof of (1) of the theorem, we have $R = (p, q)$ for some non-associated prime elements p and q in R. Now, we choose non-zero elements $a_n^{'}$ and $b_n^{'}$ from R such that

$$pa_n^{'} + qb_n^{'} = m_n.$$

This time, we set $a_n = pa_n^{'}$ and $b_n = qb_n^{'}$ and the remains are the same as before. Let

$$A(x) = x^{n+1} + a_n x^n + \cdots + a_1 x + a_0$$

or

$$A(x) = x^{n+1} + a_n x^n + \cdots + a_t x^t + pq$$

and

$$B(x) = -x^{n+1} + b_n x^n + \cdots + b_1 x + b_0$$

or

$$B(x) = -x^{n+1} + b_n x^n + \cdots + b_t x^t - pq,$$

with respect to t being zero or non-zero. Then, in either case $A(x)$ and $B(x)$ are irreducible in $R[x]$ by Fact 2.3 and Fact 2.4, and

$$M(x) = A(x) + B(x).$$

□

Considering the characteristics of integral domains, we can obtain stronger results, in particular we improve the degree bound in the second part of Theorem 2.9.

Theorem 2.10. *Let R be a unique factorization domain which is not a field with $\mathrm{J}(R) = 0$. Let*

$$M(x) = m_n x^n + m_{n-1}x^{n-1} + \cdots + m_0 \in R[x]$$

be a polynomial of degree $n \geq 1$.

(1) *If the degree of $M(x)$ is 1, then we can write $M(x)$ as a sum of two irreducible polynomials of degree 1 from $R[x]$.*

(2) *If $M(x)$ is of degree 2, then we can write $M(x)$ as a sum of three irreducible polynomials from $R[x]$ of degree at most 2.*

(3) *If $M(x)$ is monic, $n \geq 2$ and $m_{n-1} - 1$ is not a unit element in R, then $M(x)$ can be written as sum of two irreducible polynomials from $R[x]$ of degree n and $n-1$.*

(4) *Suppose that the characteristic* $\mathrm{char}(R)$ *of R does not divide n. If $M(x)$ is monic and $n \geq 2$, then it can be written as a sum of two irreducible polynomials from $R[x]$ of degree n and $n-1$.*

(5) *Suppose that* $\mathrm{char}(R)$ *of R does not divide n or $m_{n-1} - 1$ is not a unit element in R. If $M(x)$ is not a monic polynomial and $n \geq 2$, then we can write $M(x)$ as a sum of three irreducible polynomials from $R[x]$ of degree at most n.*

(6) *Suppose that* $\mathrm{char}(R)$ *divides n. Let $M(x)$ be a polynomial of degree $n \geq 3$. If $m_{n-1} - 1$ is a unit element in R, then $M(x)$ can be written as sum of four irreducible polynomials from $R[x]$ of degree at most n.*

Proof. (1) Let

$$M(x) = m_1 x + m_0.$$

If m_1 is not a unit, then we can write $M(x)$ as the sum of two irreducible polynomials as

$$M(x) = ((m_1 - 1)x + 1) + (x + m_0 - 1).$$

If m_1 is a unit, then we can assume that $M(x) = x + m_0$. Suppose that $m_0 + 1 \neq 0$. By the second part of Lemma 2.8, choose a prime number p that does not divide $m_0 + 1$. By Fact 2.4, the polynomial $M(x)$ is the sum of two irreducible polynomials as

$$M(x) = x + m_0 = (px + m_0 + 1) + ((1 - p)x - 1).$$

If $m_0 - 1 \neq 0$, then again by the second part of Lemma 2.8, choose a prime number q that does not divide $m_0 - 1$. It follows that $M(x)$ can be written as the sum of two irreducible polynomials as

$$M(x) = x + m_0 = (qx + m_0 - 1) + ((1 - q)x + 1).$$

Finally, suppose that $m_0 = 1 = -1$ (so the characteristic is 2). Let r be a prime element in R. Then, we can write $M(x)$ as the sum of two irreducible polynomials as

$$M(x) = x + 1 = (rx + r + 1) + ((1 - r)x - r).$$

(2) Let

$$M(x) = m_2x^2 + m_1x + m_0.$$

Then,

$$M(x) = m_2x^2 - p + (m_1 - 1)x + p + x + m_0,$$

where p is a prime element in R which does not divide m_2. Note that the existence of such a prime p is guaranteed by Lemma 2.8(2). Furthermore, choose p such that it does not divide $m_1 - 1$, if m_1 is not 1. By Facts 2.3 and 2.4, we know that $m_2x^2 - p$, $(m_1 - 1)x + p$ and $x + m_0$ are all irreducible polynomials in $R[x]$. Hence, we write $M(x)$ as a sum of three irreducible polynomials from $R[x]$.

(3) Let

$$M(x) = x^n + m_{n-1}x^{n-1} + \cdots + m_0$$

be a monic polynomial of degree n in $R[x]$. Since $m_{n-1}-1$ is a non-unit, we may pick a prime element p in R that divides $m_{n-1} - 1$. As p is not in $\mathrm{J}(R)$, by Proposition 2.1 there is $y \in R$ such that $1 - py$ is not a unit and choose a prime divisor q of it. Then, it follows that $(p, q) = R$. For $0 < i < n - 1$, there exist $a_i^{'}$ and $b_i^{'}$ in R such that

$$pa_i^{'} + qb_i^{'} = m_i.$$

Put $a_i = pa_i^{'}$ and $b_i = qb_i^{'}$ for $0 < i < n - 1$, and set $a_{n-1} = m_{n-1} - 1$. Now, by Lemma 2.7, there exist $a_0^{'}$ and $b_0^{'}$ in R such that

$$p^2a_0^{'} + q^2b_0^{'} = 1.$$

Put

$$a_0 = p - p^2a_0^{'}(q + p - m_0)$$

and

$$b_0 = m_0 - p + p^2a_0^{'}(q + p - m_0) = m_0 - p + (1 - q^2b_0^{'})(q + p - m_0)$$

$$= q - q^2b_0^{'}(q + p - m_0).$$

Let

$$A(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

and

$$B(x) = x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1x + b_0.$$

By our choice of the a_i's for $i \in \{1, \ldots, n-1\}$, the prime p divides a_i for $i \in \{1, \ldots, n-1\}$. As $a_0 = p - p^2f$ where $f = a_0^{'}(q + p - m_0)$, we conclude that $p \mid a_0$ but $p^2 \nmid a_0$. Similarly, for $0 \leq i < n-1$ the prime q divides b_i, but q^2 does not divide b_0. Then, by Eisenstein's Criterion and Fact 2.4, the polynomials $A(x)$ and $B(x)$ are irreducible in $R[x]$ and

$$M(x) = A(x) + B(x).$$

(4) Let

$$M(x) = x^n + m_{n-1}x^{n-1} + \cdots + m_0$$

be a monic polynomial of degree n in $R[x]$. Note that if $m_{n-1} - 1$ is not a unit element in R, then we are done by (3). We argue that we can ensure that $m_{n-1} - 1$ is not a unit element in R by replacing x by $x + h$ for some h from R. Suppose that $m_{n-1} - 1$ is a unit element in R. As $\mathrm{char}(R)$ of R does not divide n, the element n is not zero when we regard n as an element of R. Thus, n is not in $\mathrm{J}(R)$ as it is trivial. Therefore, there exists $r \in R$ such that $1 + rn$ is not a unit in R. Now, we replace x by $x + r(m_{n-1} - 1)$ to get

$$\overline{M}(x) = M(x + r(m_{n-1} - 1)) = x^n + r_{n-1}x^{n-1} + \cdots + r_0$$

for some suitable r_i in R for $i \in \{0, \ldots, n-1\}$ and $r_{n-1} = m_{n-1} + rn(m_{n-1} - 1)$. Notice that

$$r_{n-1} - 1 = m_{n-1} + rn(m_{n-1} - 1) - 1 = (m_{n-1} - 1)(1 + rn).$$

As $1 + rn \notin \mathrm{U}(R)$, we also deduce that $r_{n-1} - 1 \notin \mathrm{U}(R)$. As the irreducibility is preserved by changing x to $x + h$ for any $h \in R$, we may assume from the beginning that $m_{n-1} - 1$ is not a unit element in R. The proof of the remaining part follows from the proof of (3).

(5) Let

$$M(x) = m_nx^n + m_{n-1}x^{n-1} + \cdots + m_0$$

be a polynomial in $R[x]$ where $m_n \neq 1$. Then, by Lemma 2.8(2), there exists a prime element p in R which does not divide $m_n - 1$. Hence, we can rewrite $M(x)$ as follows:

$$\begin{aligned} M(x) &= (m_n - 1)x^n + x^n + m_{n-1}x^{n-1} + \cdots + m_0 \\ &= (m_n - 1)x^n - p + x^n + m_{n-1}x^{n-1} + \cdots + m_0 + p, \end{aligned}$$

Also, from the above parts (3) or (4), we know that

$$x^n + m_{n-1}x^{n-1} + \cdots + m_0 + p$$

can be written as a sum of two irreducible polynomials from $R[x]$ of degree n and $n-1$. As $(m_n-1)x^n-p$ is an irreducible polynomial in $R[x]$, where the irreducibility follows from Fact 2.3 and Fact 2.4, we can write $M(x)$ as a sum of three irreducible polynomials from $R[x]$ of degree at most n.

(6) Let

$$M(x) = m_n x^n + m_{n-1}x^{n-1} + \cdots + m_1 x + m_0$$

be a polynomial of degree $n \geq 3$ in $R[x]$ with $m_{n-1} - 1 = u$ is a unit element in R. Then,

$$M(x) = m_n x^n + (1 + u)x^{n-1} + \cdots + m_1 x + m_0.$$

We can write $M(x)$ as follows:

$$M(x) = m_n x^n - p + ux^{n-1} + p + x^{n-1} + m_{n-2}x^{n-2} + \cdots + m_1 x + m_0,$$

where p is a prime element in R which does not divide m_n; the existence of such a prime p is again ensured by Lemma 2.8(2). Then, $m_n x^n - p$ and $ux^{n-1} + p$ are irreducible polynomials in $R[x]$ similar to the arguments above. As $\mathrm{char}(R)$ does not divide $n - 1$, by part (4), the polynomial

$$x^{n-1} + m_{n-2}x^{n-2} + \cdots + m_1 x + m_0$$

can be written as a sum of two irreducible polynomials from $R[x]$ of degree $n-1$ and $n - 2$. Consequently, we can write $M(x)$ as a sum of four irreducible polynomials from $R[x]$ of degree at most n.

□

Remark 2.11. In Theorem 2.10, we anticipate that two summands are always sufficient for the aforementioned Goldbach Property, as Pollack [29] demonstrated for Noetherian rings with infinitely many maximal ideals. This result, however, is not attainable with our current approach. We therefore pose this as an open question in the final section.

Next, we will refine Theorem 2.9 and Theorem 2.10. For this purpose, we introduce the following definition, and then relate it to other significant integral domains.

Definition 2.12. Let R be an integral domain which is not a field. We say that R is an *almost unique factorization domain (almost UFD)* if the following two conditions are satisfied:

(1) Any non-unit element x from R is divisible by a prime element p from R.
(2) For any non-zero element $x \in R$, there exists a prime element $q \in R$ such that q does not divide x.

Note that any unique factorization domain with infinitely many non-associated primes is an almost UFD. In particular, if R is a unique factorization domain which is not a field with $\mathrm{J}(R) = 0$, then it is an almost UFD by Lemma 2.8(1).

Now, we contextualize almost UFDs within the existing factorization theory; in other words, we compare them with atomic domains, ACCP domains, and GCD domains. An integral domain R is called *atomic* if every non-zero non-unit element of R can be written as a finite product of irreducible elements (atoms). In that sense, Condition (1) in Definition 2.12 relates almost UFDs to atomic domains. In an atomic domain, irreducible elements are not necessarily prime elements. However, every irreducible element in an almost UFD is prime. This yields that if an integral domain R is atomic and an almost UFD, then it is a unique factorization domain. Moreover, in an almost UFD, we have infinitely many non-associated primes, and this fact is guaranteed by Condition (2) in Definition 2.12. Therefore, the first part of Lemma 2.8 holds for almost UFDs. In the proof of Theorem 2.9 and Theorem 2.10, we use Eisenstein's Criterion, thus we need prime elements to apply our technique. We cannot make this technique applicable if we have atomic domains instead of almost UFDs. Recall that an integral domain R satisfies *ACCP (ascending chain condition on principal ideals)* if there is no infinite strictly ascending chain of principal

ideals. Equivalently, for every ascending chain

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

of principal ideals of R, there exists an integer $n \geq 1$ such that

$$(a_n) = (a_{n+1}) = \cdots .$$

An integral domain R is a *GCD domain (greatest common divisor domain)* if every pair of elements has a greatest common divisor. That is, for any $a, b \in R$ (not both zero), there exists $d \in R$ such that

- $d \mid a$ and $d \mid b$ (d is a common divisor),
- if $c \in R$ satisfies $c \mid a$ and $c \mid b$, then $c \mid d$ (d is greatest in the divisibility order).

The element d is unique up to multiplication by a unit. These three classes, atomic domains, ACCP domains, and GCD domains, are related as follows, and they are all generalizations of unique factorization domains. Every integral domain satisfying ACCP is atomic, but the converse fails (see [17]). GCD domains are not necessarily atomic, nor do they necessarily satisfy ACCP. Also, atomic domains need not be GCD domains. An integral domain that is both an atomic and a GCD domain is exactly a unique factorization domain. Therefore, the ring R is a unique factorization domain if and only if R is an atomic domain and R is an almost UFD or a GCD domain. It is known that irreducible elements are prime elements in GCD domains. In that sense, almost UFDs are closer to GCD domains than to the other two classes. For this reason, understanding the relationship between almost UFDs and GCD domains is an intriguing question, and we pose this as an open problem in the last section.

Now, we will give two more non-trivial examples of rings that are almost UFDs (notice that they are also GCD domains).

Example 2.13. (1) An entire complex function $f(z)$ is said to be of finite order if there exists a number $\alpha > 0$ such that

$$f(z) = O(e^{|z|^\alpha}) \quad \text{as} \quad |z| \to \infty.$$

The lower bound of the numbers α with the above property is called the order of $f(z)$. Let R be the set of entire functions of order 1. Then, via the injective

map sending f to its Maclaurin series, we view R as a subring of $\mathbb{C}[[z]]$. By the Hadamard Factorization Theorem (see [12, Chapter 11]), if $f(z) \in R$, then

$$f(z) = e^{A+Bz} z^m \prod_{n=1}^{\infty} (1 - z/z_n) e^{z/z_n}$$

where $z_1, z_2, \ldots$ are the non-zero zeros of $f(z)$ (multiple zeros being repeated as appropriate and the number of zeros can be finite), m is the order of $f(z)$ at 0, and A, B are two elements from $\mathbb{C}$. For instance, any polynomial, e^z, $\sin z$ and Riemann's famous function

$$\xi(z) = \frac{1}{2} z(z-1) \pi^{-\frac{z}{2}} \Gamma\left(\frac{z}{2}\right) \zeta(z)$$

which plays a key role in the distribution of prime numbers (see [12, Chapter 8]) are in the ring R. One can see from the Hadamard Factorization Theorem that R is an almost UFD. However, it is not a unique factorization domain as some elements can be written as a product of infinitely many prime elements. These are the functions from R which have infinitely many zeros, for example $\xi(z)$. For any $a \in \mathbb{C}$, the element $z - a$ is a prime element in R, and the evaluation map at a from R to $\mathbb{C}$ is surjective with kernel $M_a = (z - a)$. Therefore, the ideal M_a is maximal in R. Hence, we see that $\mathrm{J}(R) = 0$, and this follows from the fact that a non-zero entire function (of order 1) can have at most countably many zeros.

(2) Let R be a unique factorization domain which is not a field with $\mathrm{J}(R) = 0$. The ultrapower S of R with respect to a non-principal ultrafilter is an almost UFD but not a unique factorization domain (see Section 4 for precise definitions). There are elements in S which have infinitely many prime divisors.

A careful analysis of the proofs of Theorem 2.9 and Theorem 2.10 reveals that Theorem 2.9 and Theorem 2.10 are true for an almost UFD with trivial Jacobson radical.

Theorem 2.14. *Let R be an almost UFD with $\mathrm{J}(R) = 0$. Then, Theorem 2.9 and Theorem 2.10 hold.*

Proof. In our construction, the property of being an almost UFD with trivial Jacobson radical is sufficient for the second part of Lemma 2.8. Since the other lemmas, Fact 2.5 and the Eisenstein Criterion hold for arbitrary integral domains, we obtain the conclusion of Theorem 2.9. For the first, second and third parts of Theorem 2.10, the same condition

suffices as we apply the second part of Lemma 2.8 and Fact 2.5 again. This observation indicates that being an almost UFD with trivial Jacobson radical is also sufficient for the remaining parts of Theorem 2.10. Hence, we obtain all the conclusions of Theorem 2.10. □

Corollary 2.15. *Theorem 2.9 and Theorem 2.10 hold true for the ring of entire complex functions of order 1.*

Next, we give some corollaries of our previous theorems (Theorem 2.9 and Theorem 2.10) which extend the corresponding results of Hayes [18] and Saidak [31].

Corollary 2.16. (1) *Let R be a principal ideal domain with infinitely many non-associated prime elements. Then, Theorem 2.9 and Theorem 2.10 hold.*

(2) *Let R be a unique factorization domain with $|\mathrm{U}(R)| < |R|$. Then, Theorem 2.9 and Theorem 2.10 hold.*

(3) *Let R be a unique factorization domain of characteristic 0 with $\mathrm{J}(R) = 0$ and $S = R[[t_1, t_2, \ldots]]$. Then, any monic polynomial $M(x) \in S[x]$ of degree $n \geq 2$ can be written as a sum of two irreducible polynomials from $S[x]$ of degree n and $n-1$.*

Proof. (1) As R is a principal ideal domain, any maximal ideal of R is of the form pR where p is a prime element. Then, the Jacobson radical

$$\mathrm{J}(R) = \bigcap_{p \in I} pR$$

of R is equal to 0, where I is a set of all non-associated prime elements of R. Thus, Theorem 2.9 and Theorem 2.10 hold.

(2) Consider the map $f_r : R \longrightarrow R$ such that $f_r(x) = 1 - xr$ where $r \in \mathrm{J}(R) \setminus \{0\}$. Then by Proposition 2.1, we get $f_r(R) \subseteq \mathrm{U}(R)$. Moreover, f_r is one-to-one. This yields that $|\mathrm{U}(R)| = |R|$, which is a contradiction. Thus, we have $\mathrm{J}(R) = 0$, and hence, Theorem 2.9 and Theorem 2.10 hold.

(3) Let

$$M(x) = \overline{M}(x, \bar{t}) = x^n + m_{n-1}(\bar{t})x^{n-1} + \cdots + m_0(\bar{t})$$

be a monic polynomial in $S[x]$ with $n \geq 1$ and $\bar{t} = (t_1, t_2, \ldots)$. Then, $\overline{M}(x, 0)$ is a monic polynomial in $R[x]$. Therefore, by Theorem 2.10(4) there are two irreducible monic polynomials $A(x)$ and $B(x)$ of degree n and $n-1$ respectively such that $\overline{M}(x, 0) = A(x) + B(x)$. We put $A_1(x) = A(x) + \overline{M}(x, \bar{t}) - \overline{M}(x, 0)$ and

$B_1(x) = B(x)$. Notice that the degree of $A_1(x)$ is n as well. Observe that both of the polynomials $A_1(x)$ and $B_1(x)$ are irreducible in $S[x]$, as they are monic and irreducible in $R[x]$. Hence, we are done as $M(x) = A_1(x) + B_1(x)$.

□

The next example indicates that if R is a field, then a Goldbach Property may fail for $R[x]$.

Example 2.17. As $\mathbb{C}$ is an algebraically closed field, all irreducible polynomials have degree 1 in $\mathbb{C}[x]$, and 1 or 2 in $\mathbb{R}[x]$. Thus, a Goldbach Property does not hold for $\mathbb{C}[x]$ and $\mathbb{R}[x]$.

We also remind that not being a field is not necessary for a Goldbach Property. As $\mathrm{J}(\mathbb{Z}) = 0$, by Theorem 2.9, we know that a Goldbach Property holds for $\mathbb{Q}[x]$.

Remark 2.18. By [29], we know that any polynomial in $\mathbb{Z}[x]$ of degree $n \geq 1$ can be written as a sum of two irreducible polynomials from $\mathbb{Z}[x]$ of degree n. This yields that for any prime number p, the polynomial ring over the localization of $\mathbb{Z}$ at p, namely $\mathbb{Z}_{(p)}[x]$, has a Goldbach Property, where

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}.$$

To see this, let $A(x)$ be a polynomial in $\mathbb{Z}_{(p)}[x]$ of degree $n \geq 1$. Note that there exists an integer N such that $NA(x) \in \mathbb{Z}[x]$ and p does not divide N. In fact, N is a unit in $\mathbb{Z}_{(p)}$. Then, there exist two irreducible polynomials $f_1(x)$ and $f_2(x)$ in $\mathbb{Z}[x]$ such that

$$NA(x) = f_1(x) + f_2(x).$$

As $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, by Gauss' Lemma (Fact 2.2), both of $f_1(x)$ and $f_2(x)$ are also irreducible in $\mathbb{Q}[x]$ and $\mathbb{Z}_{(p)}[x]$, as well. Since N is a unit, we can write $A(x)$ as a sum of two irreducible polynomials in $\mathbb{Z}_{(p)}[x]$ as follows:

$$A(x) = \frac{f_1(x)}{N} + \frac{f_2(x)}{N}.$$

Recall that a commutative ring R is called *local* if it has a unique maximal ideal.

Remark 2.19. Let R be a ring. Then, R is local if and only if for any $a \in R$, the element a or $1 - a$ is a unit. The proof of this fact can be deduced from Proposition 2.1.

Remark 2.20. If a unique factorization domain has infinitely many non-associated primes, then this does not mean that it has a trivial Jacobson radical and even it can be local. For instance if K is a field, then $R = K[[t_1, t_2, \ldots]]$ is a unique factorization domain with infinitely many non-associated primes. Moreover, R is local and its Jacobson radical is $(t_1, t_2, \ldots)$, see [27].

Corollary 2.21. *Let R be a unique factorization domain which is not local. Let*

$$M(x) = a_n x^n + \cdots + m_t x^t$$

be a polynomial with $m_t \in \mathrm{U}(R)$ and $0 \leq t \leq n$. Then, $M(x)$ can be written as a sum of two irreducible polynomials from $R[x]$.

Proof. As R is not local, it is not a field, and so it has at least two non-associated prime elements. Moreover, $\mathrm{J}(R)$ cannot contain all prime elements because it is not maximal. Let p be a prime element which is not in $\mathrm{J}(R)$. By Proposition 2.1, $1 - py \notin \mathrm{U}(R)$ for some $y \in R$. Now, choose a prime q that divides $1 - py$. Then, $(p, q) = R$, and also p and q do not divide m_t. The rest of the proof is similar to the proof of the second part of Theorem 2.9. □

Fact 2.22. *[23, Theorem 9.1] Let F be a field and $n \geq 2$ an integer. Let $a \in F$ be a non-zero element. Assume that for all primes p with $p \mid n$, we have $a \notin F^p$, and if $4 \mid n$, then $a \notin -4F^4$. Then, the polynomial $x^n - a$ is irreducible in $F[x]$.*

Now, we prove that if R is a unique factorization domain which is not local, then a Weak Goldbach Property holds for $R[x]$.

Theorem 2.23. *Let R be a unique factorization domain which is not local and $M(x)$ be a non-constant polynomial.*

1. *If $M(0) = 0$ or $M(0) - 1 \in \mathrm{U}(R) \cup \{0\}$, then $M(x)$ can be written as a sum of four irreducible polynomials from $R[x]$.*
2. *If $M(0) \neq 0$ and $M(0) - 1 \notin \mathrm{U}(R) \cup \{0\}$, then $M(x)$ can be written as a sum of three irreducible polynomials from $R[x]$.*

Proof. Let

$$M(x) = m_n x^n + \cdots + m_t x^t$$

be a non-constant polynomial in $R[x]$. Let ℓ be the number of prime divisors of $m_t - 1$ if $m_t \neq 1$. In other words, if $m_t \neq 1$ and $m_t - 1 = u p_1^{a_1} \cdots p_s^{a_s}$, where u is a unit,

$p_1, \ldots, p_s$ are non-associated prime elements, and $a_1, \ldots, a_s$ are non-negative integers, then $\ell = a_1 + \cdots + a_s$. Let d be an odd prime number larger than $\max\{n, \ell\}$. Write

$$M(x) = A(x) + B(x),$$

where

$$A(x) = x^d + m_n x^n + \cdots + m_{t+1} x^{t+1} + 1$$

and

$$B(x) = -x^d + m_t x^t - 1, \text{ if } n > t$$

or

$$B(x) = -x^d - 1, \text{ if } n = t.$$

Now, we shall separate the argument into two cases.

(1) If $t \geq 1$, that is, if $M(0) = 0$ then by Corollary 2.21, both $A(x)$ and $B(x)$ can be written as a sum of two irreducible polynomials from $R[x]$. Now, let $t = 0$ and suppose that $m_0 - 1 \in \mathrm{U}(R) \cup \{0\}$. Then again by the previous corollary, $B(x) = -x^d + m_0 - 1$ can be written as a sum of two irreducible polynomials from $R[x]$. Hence, in this case $M(x)$ can be written as a sum of four irreducible polynomials from $R[x]$.

(2) Let $t = 0$ and $a = m_0 - 1$ be non-zero and non-unit. We will observe that the polynomial $x^d - a$ has no root in R. On the contrary suppose that $\alpha \in R$ is a root of $x^d - a$. Then, α is non-zero and not a unit as well. Let $p \in R$ be a prime dividing α. Thus, $p^d \mid \alpha^d$ and so $p^d \mid a$. However, $a = u p_1^{a_1} \cdots p_s^{a_s}$ and $a_i < d$ for any $i \in \{1, \ldots, s\}$, which is a contradiction. Therefore, $x^d - a$ has no root in R. Since R is integrally closed in the field of fractions F of R, the polynomial $x^d - a$ also does not have a root in F. By Fact 2.22, the polynomial $x^d - a$ is irreducible in $F[x]$, and so is irreducible in $R[x]$ as it is monic. Hence, in this case $M(x)$ can be written as a sum of three irreducible polynomials from $R[x]$. □

Remark 2.24. Let R be the ring $\mathbb{Z}[[t_1, t_2, \ldots]]$. Then, the ring R is not local and its Jacobson radical is non-zero, and in fact $\mathrm{J}(R) = (t_1, t_2, \ldots)$. Moreover, R is a unique factorization domain, see [10, 27]. Therefore, any polynomial in $R[x]$ can be written as a sum of at most four irreducible polynomials from $R[x]$ by the previous theorem. Besides, R is not

Noetherian, and so one cannot immediately apply the result of [29]. In fact, as $\mathrm{J}(\mathbb{Z}) = 0$, we deduce that $R[x]$ has a Goldbach Property for monic polynomials by the last part of Corollary 2.16.

Assembling Theorem 2.9, Theorem 2.10, Theorem 2.14 and Theorem 2.23, we have proved the following result.

Theorem 2.25. *Let R be a unique factorization domain and $M(x) \in R[x]$ be a polynomial of degree $n \geq 1$. If R is not local, then $M(x)$ can be written as a sum of at most four irreducible polynomials from the polynomial ring $R[x]$. Besides, if $\mathrm{J}(R) = 0$, then the degrees of these irreducible polynomials are at most n. Furthermore, if $\mathrm{char}(R) = 0$, then $M(x)$ can be written as a sum of at most three irreducible polynomials from the polynomial ring $R[x]$ of degree at most n. Moreover, the last two assertions hold true if R is an almost UFD.*

Now, we give a table which summarizes our results of this section as in the previous theorem.

Remark 2.26. Let R be an almost UFD and

$$M(x) = m_n x^n + m_{n-1} x^{n-1} + \cdots + m_0$$

be a polynomial from $R[x]$ with degree $n \geq 1$. Let F be the field of fractions of R.

Properties of R and $M(x)$	**The number of irreducible polynomials from $R[x]$ or $F[x]$ to represent $M(x)$**
$\mathrm{J}(R) = 0$	2 from $F[x]$
$n = 1$	2 from $R[x]$
$\mathrm{J}(R) = 0$ and $n = 2$	3 from $R[x]$
$\mathrm{J}(R) = 0$, $m_n = 1$, $m_{n-1} - 1 \notin \mathrm{U}(R)$ and $n \geq 2$	2 from $R[x]$
$\mathrm{J}(R) = 0$, $m_n = 1$, $\mathrm{char}(R) \nmid n$ and $n \geq 2$	2 from $R[x]$
$\mathrm{J}(R) = 0$, $\mathrm{char}(R) \nmid n$ or $m_{n-1} - 1 \notin \mathrm{U}(R)$ and $n \geq 3$	3 from $R[x]$
$\mathrm{J}(R) = 0$, $\mathrm{char}(R) \mid n$, $m_{n-1} - 1 \in \mathrm{U}(R)$ and $n \geq 3$	4 from $R[x]$
R is a unique factorization domain which is not local	4 from $R[x]$
$\mathrm{J}(R) = 0$ and $\mathrm{char}(R) = 0$	3 from $R[x]$

Summary table of our results: Theorems 2.9, 2.10, 2.14 and 2.23

3. A Goldbach Property in Formal Power Series over Discrete Valuation Rings

Recall that a discrete valuation ring (DVR) is a principal ideal domain with exactly one non-zero maximal ideal. Thus, a DVR is local and not a field. Equivalently, S is a DVR if S is a unique factorization domain with a unique prime element. For instance, one variable formal power series over a field and the p-adic integers are examples of discrete valuation rings. Following some of the ideas from [28], one can obtain the following characterization result.

Theorem 3.1. *Let S be a DVR and set $R = S[[x]]$. Then, a power series f from R can be written as a sum of two primes from R if and only if f is not a unit.*

Proof. Let S be a DVR, p be its unique prime element, and $R = S[[x]]$. As S is a PID, we know that R is a UFD. Therefore, irreducible and prime elements coincide in R. Take a power series f from R and write $f = f_0 + f_1x + f_2x^2 + \cdots$. Note that f is a unit if and only if f_0 is a unit in S if and only if p does not divide f_0. This indicates that if f is a sum of two primes from R, then it is not a unit. Conversely, assume that f is not a unit. Thus,

p divides f_0. Then, $f_0 = up^\ell$ for some $\ell \geq 1$ and $u \in \mathrm{U}(S)$.

Case 1: Suppose that p divides f_1. Put $a_0 = p^{\ell+1}$ and $b_0 = f_0 - p^{\ell+1}$. Then, $f_0 = a_0 + b_0$ and both a_0 and b_0 are non-zero and divisible by p. Also, we see that $f_1 - 1$ is a unit, as it is not divisible by p. Thus, the element f_1 can be written as a sum of two unit elements $a_1 = f_1 - 1$ and $b_1 = 1$ from S. Now, set

$$A = a_0 + (f_1 - 1)x + f_2x^2 + f_3x^3 + \cdots$$

and

$$B = b_0 + x.$$

Then, $f = A + B$. Next, we prove that both A and B are prime elements from R. Write $A = gh$ where $g = g_0 + g_1x + \cdots$ and $h = h_0 + h_1x + \cdots$ from R. Then $a_0 = g_0h_0$. As p divides a_0, we can write $g_0 = u_1p^{\ell_1}$ and $h_0 = u_2p^{\ell_2}$, where $u_1, u_2 \in \mathrm{U}(S)$ and at least one of ℓ_1, ℓ_2 is positive. If both ℓ_1 and ℓ_2 are positive, then this yields that $f_1 - 1 = g_0h_1 + g_1h_0$ is divisible by p, which is a contradiction. Thus, one of g_0 and h_0 is not divisible by p and we conclude that one of g or h is a unit in R. Therefore, A is irreducible and hence it is a prime element. The primality of B is similar.

Case 2: Assume that p does not divide f_1, in other words f_1 is a unit. Let m be a positive odd integer greater than ℓ. Put

$$A = f_0 - p^m + f_1x + (f_2 - 1)x^2 + f_3x^3 + \cdots$$

and

$$B = p^m + x^2.$$

Then, $f = A + B$ and similar to Case 1, the element A is prime. Next, we prove that B is prime by showing that it is irreducible. Write $p^m + x^2 = gh$ where $g = g_0 + g_1x + \cdots$ and $h = h_0 + h_1x + \cdots$ from R. Suppose g and h are not units so g_0 and h_0 are both divisible by p. Moreover, $p^m = g_0h_0$. If we write $g_0 = u_1p^{\ell_1}$ and $h_0 = u_2p^{\ell_2}$ where $u_1, u_2 \in \mathrm{U}(S)$ and both ℓ_1 and ℓ_2 are positive, then one of ℓ_1 and ℓ_2 is even and the other is odd, that is to say, their parities are different. Also, we have $0 = g_0h_1 + g_1h_0$. The previous observation yields that p divides at least one of g_1 and h_1. Moreover, we have $1 = g_0h_2 + g_1h_1 + g_2h_0$, and so we get a contradiction as p divides the right hand side. Hence, the element B is a prime element as well. □

Remark 3.2. By a similar reasoning, one can observe that if K is a field whose characteristic is not 2, then a power series f from $K[[x]]$ can be written as a sum of two primes in $K[[x]]$ if and only if f is not a unit. Besides, as a corollary of the previous theorem, if R is $\mathbb{Z}_p[[x]]$ or $K[[x, y]]$ where K is a field, then a power series f from R is a sum of two primes in R if and only if f is not a unit.

4. A Goldbach Property for Polynomials over Local Rings via Ultraproducts

In Section 2, we discussed a Goldbach Property for $R[x]$ where R is not local. Also in Remark 2.18, we have seen that $\mathbb{Z}_{(p)}[x]$ has a Goldbach Property for any prime number p, and the ring $\mathbb{Z}_{(p)}$ is local. In this section, we consider a Goldbach Property for polynomials over local rings. We also give more examples of local rings R (which are not fields and which do not come from localizations) where $R[x]$ has a Goldbach Property. To do so, we make use of ultraproducts. The fundamental utility of the ultraproduct construction in algebra lies in its ability to transfer first-order properties between a family of structures and their ultraproduct via Łoś' Theorem (the exact statement is below). For a given first-order formula, this theorem states that the formula holds in the ultraproduct if and only if the set of indices for which it holds in the component structures is an element of the underlying ultrafilter. Consequently, statements expressible in first-order logic, such as being a group, a ring, or a field are preserved in the ultraproduct. This enables the systematic construction of new algebraic structures with properties inherited from most of their factors. To motivate the applications of ultraproducts in algebra, we have the following two key results.

- **Ax's Theorem [4] (1969):** Using ultraproducts of finite fields, Ax proved that every injective polynomial map from $\mathbb{C}^n$ to $\mathbb{C}^n$ is surjective. This result relies on the fact that injective functions on finite fields are bijective.
- **The van den Dries–Schmidt Theorem [13] (1984):** Applying ultraproducts (nonstandard analysis), van den Dries–Schmidt established uniform bounds in polynomial rings over fields. For fixed n and d, there exists a bound $A(n, d)$ such that for any field K and polynomials $f, f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ of degree $\leq d$, if f belongs to the ideal $(f_1, \ldots, f_m)$, then $f = \sum_{i=1}^{m} f_i h_i$ with $\deg h_i \leq A(n, d)$. Furthermore, with the help of nonstandard methods, primality testing can be reduced to checking polynomials up to a uniform bound $P(n, d)$.

For more on model theory, we refer the reader to the Appendix section, and more details can be found in [26, 35].

Now, we begin with recalling ultraproducts.

Definition 4.1. A *filter* D on a non-empty set Ω is a set of subsets of Ω such that

(i) If A is in D and $A \subseteq B$, then B is also in D.
(ii) If A and B are in D, then so is $A \cap B$.
(iii) $\Omega \in D$, $\emptyset \notin D$.

A filter D on Ω is called an *ultrafilter* (a *maximal filter*) if for each $A \subseteq \Omega$, exactly one of A and $\Omega \setminus A$ belongs to D. By Zorn's lemma, one can see that every filter is contained in an ultrafilter. An ultrafilter is said to be *non-principal* if it contains all cofinite sets, in other words it does not contain any finite set. Now we fix an ultrafilter D on a non-empty set Ω and let $(\mathcal{M}_i)_{i\in\Omega}$ be a family of $\mathcal{L}$-structures where $\mathcal{L}$ is a language. Two elements (possibly two infinite tuples) $(x_i)_i$ and $(y_i)_i$ from $\prod_{i\in\Omega} \mathcal{M}_i$ are said to be D-*equivalent* and denoted by $(x_i)_i \equiv_D (y_i)_i$, if $\{i : x_i = y_i\} \in D$. The D-equivalence class $(x_i)_i/D$ of $(x_i)_i$ is defined as

$$\{(y_i)_i \in \prod_{i\in\Omega} \mathcal{M}_i : (y_i)_i \equiv_D (x_i)_i\}.$$

The *ultraproduct*

$$\mathcal{U} = \prod_{i\in\Omega} \mathcal{M}_i/D$$

of the structures $\mathcal{M}_i$ is defined by the D-equivalence classes, and it is an $\mathcal{L}$-structure as follows:

- For a function symbol $f \in \mathcal{L}$ of arity k,

$$f^{\mathcal{U}} : \big((a_i^1)_i/D, \ldots, (a_i^k)_i/D\big) \mapsto (f^{\mathcal{M}_i}(a_i^1, \ldots, a_i^k))_i/D.$$

- For a relation symbol $E \in \mathcal{L}$ of arity k,

$$E^{\mathcal{U}} = \left\{ \big((a_i^1)_i/D, \ldots, (a_i^k)_i/D\big) \in \mathcal{U}^k : \{i \in \Omega : (a_i^1, \ldots, a_i^k) \in E^{\mathcal{M}_i}\} \in D \right\}.$$

- For a constant symbol $c \in \mathcal{L}$,

$$c^{\mathcal{U}} = (c^{\mathcal{M}_i})_i/D.$$

One can see that the above definition is well-defined. If all the structures $\mathcal{M}_i$ are the same structure $\mathcal{M}$, then the ultraproduct is called the *ultrapower*. The notion of ultraproducts and their properties apply to many-sorted structures.

The following theorem is due to Łoś, and it is one of the fundamental results of ultraproducts.

Łoś' Theorem: Let D be an ultrafilter on a non-empty set Ω, $(\mathcal{M}_i)_{i\in\Omega}$ be a family of $\mathcal{L}$-structures and $\varphi(x_1, ..., x_k)$ be an $\mathcal{L}$-formula. Set $\mathcal{U} = \prod_{i\in\Omega} \mathcal{M}_i/D$ and take a tuple $\bar{a} = \big((a_i^1)_i/D, ..., (a_i^k)_i/D\big) \in \mathcal{U}^k$. Then $\mathcal{U} \models \varphi(\bar{a})$ if and only if

$$\{i \in \Omega : \mathcal{M}_i \models \varphi(a_i^1, ..., a_i^k)\} \in D.$$

Now, we turn back to our main concern, namely a Goldbach Property. First, we observe that a Goldbach Property can be expressed as a first-order sentence in the language of rings.

Irreducibility for a fixed degree d: For any $d \geq 1$ and coefficients $e_0, \ldots, e_d$ from R, define $\varphi_d(e_0, \ldots, e_d)$ as:

$$\begin{aligned} e_d \neq 0 \quad \wedge\ \neg\exists c\, \exists g_0 \cdots \exists g_d \Big(& c \neq 0 \ \wedge\ \neg\exists u\, (c \cdot u = 1) \\ & \wedge\ g_d \neq 0 \ \wedge\ \bigwedge_{k=0}^{d} (c \cdot g_k = e_k) \Big) \\ \wedge \bigwedge_{m=1}^{d-1} \neg\exists g_0 \cdots \exists g_m\, \exists h_0 \cdots \exists h_{\,d-m} \Big(& g_m \neq 0 \ \wedge\ h_{\,d-m} \neq 0 \\ & \wedge \bigwedge_{k=0}^{d} \Big(\sum_{\substack{0\leq i\leq m \\ 0\leq j\leq d-m \\ i+j=k}} g_i h_j \ =\ e_k \Big) \Big). \end{aligned}$$

The above formula states that the polynomial $e_d x^d + \cdots + e_1 x + e_0$ is irreducible in $R[x]$.

Irreducibility for polynomials of degree $\leq n$: For coefficients $b_0, \ldots, b_n$ from R, define

$$\mathrm{Irr}(b_0, \ldots, b_n) : \bigvee_{d=1}^{n} \Big(b_d \neq 0 \ \wedge\ \bigwedge_{i=d+1}^{n} (b_i = 0) \ \wedge\ \varphi_d(b_0, \ldots, b_d) \Big).$$

The above formula states that the tuple $(b_0, \dots, b_n)$ represents an irreducible, non-constant polynomial of some degree $1 \leq d \leq n$.

Every non-constant polynomial of degree n is a sum of at most k irreducible polynomials of degree $\leq n$: Let $k \geq 1$ be a fixed integer. The following first-order sentence expresses this property:

$$\begin{aligned}\phi_{n,k} : \forall a_0 \cdots \forall a_n \Bigg(a_n \neq 0 \\ \rightarrow \bigvee_{m=1}^{k} \exists b_{10} \cdots \exists b_{1n}\ \exists b_{20} \cdots \exists b_{2n} \\ \dots\ \exists b_{m0} \cdots \exists b_{mn} \Bigg(\bigwedge_{j=1}^{m} \mathrm{Irr}(b_{j0}, \dots, b_{jn}) \\ \wedge \bigwedge_{i=0}^{n} \Big(\sum_{j=1}^{m} b_{ji} = a_i \Big) \Bigg) \Bigg).\end{aligned}$$

If $a_n = 1$ in the above formula, then we denote this formula by $\psi_{n,k}$. Notice that $\psi_{n,k}$ states that any monic polynomial of degree n is a sum of at most k irreducible polynomials of degree at most n. All quantifiers range over elements of the integral domain R. As n and k are fixed parameters, all conjunctions, disjunctions and quantifier blocks are finite, the whole expression $\phi_{n,k}$ (also $\psi_{n,k}$) is indeed a first-order sentence in the language of rings $\mathcal{L}_r = \{+, -, \cdot, 0, 1\}$. By the results of Hayes, Saidak and Pollack, one has the following facts:

- Hayes [18]: $\mathbb{Q} \models \{\phi_{n,2} : n \geq 1\}$,
- Saidak [31]: $\mathbb{Z} \models \{\psi_{n,2} : n \geq 1\}$,
- Pollack [29]: $\mathbb{Z} \models \{\phi_{n,2} : n \geq 1\}$.

Let T_d be the $\mathcal{L}_r$-theory of integral domains and $R \models T_d$, that is, R is an integral domain. By Proposition 2.1, we know that $\mathrm{J}(R)$ is a definable subset of R since $\mathrm{U}(R)$ is definable in R. Therefore, having a trivial Jacobson radical, namely $\mathrm{J}(R) = 0$, is a first-order sentence. Also, observe that being an almost UFD is a first-order sentence (the two conditions in Definition 2.12 are both first-order sentences). Let $T_{d,0}$ be the $\mathcal{L}_r$-theory of almost UFDs with trivial Jacobson radical. In light of Theorem 2.10 and Theorem 2.14, we have the

following fact. If $R \models T_{d,0}$, then

$$R \models \{\phi_{n,4} : n \geq 1\}.$$

With these above observations, we also have the following result, which is an immediate corollary of Łoś' Theorem.

Corollary 4.2. *Let D be an ultrafilter on a non-empty set Ω and $(\mathcal{R}_i)_{i\in\Omega}$ be a family of unique factorization domains which are not fields with $\mathrm{J}(R_i) = 0$ for all $i \in \Omega$. Then, Theorem 2.9 and Theorem 2.10 are true for $\mathcal{U} = \prod_{i\in\Omega} \mathcal{R}_i/D$.*

The above corollary can also be obtained by Theorem 2.14, as $\mathcal{U}$ is an almost UFD with $\mathrm{J}(\mathcal{U}) = 0$. If the filter in the above corollary is non-principal, then $\mathcal{U}$ is an almost UFD but not a unique factorization domain. Some elements from $\mathcal{U}$ have infinitely many prime divisors. For instance, if $\mathcal{U}$ is an ultrapower of $\mathbb{Z}$ with respect to a non-principal ultrafilter, then the element $(n!)_n/D$ from $\mathcal{U}$ is divisible by all primes from $\mathbb{Z}$.

The following theorem was proved by Bender in [5].

Theorem 4.3. *[5, Theorem 1.1] Let $\mathbb{F}_q$ be a finite field of odd characteristic and with q elements, and f be a monic polynomial in $\mathbb{F}_q[x]$ of degree $n \geq 2$. Then if*

$$q > 3n^4 16^{n^4}(n+1)^{8n^4+1},$$

there exist irreducible monic polynomials f_1 and f_2 in $\mathbb{F}_q[x]$ with $\deg(f_1) = n-1$ and $\deg(f_2) = n$ such that

$$f = f_1 + f_2.$$

Recall that the formal power series $\mathbb{F}_q[[t]]$ is a local principal ideal domain, whose unique prime element is t. Using the theorem above, one can obtain a Goldbach Property over $(\mathbb{F}_q[[t]])[x]$.

Theorem 4.4. *Let $\mathbb{F}_q$ be a finite field of odd characteristic and with q elements, and $M(x)$ be a monic polynomial in $(\mathbb{F}_q[[t]])[x]$ of degree $n \geq 2$. Then if*

$$q > 3n^4 16^{n^4}(n+1)^{8n^4+1},$$

there exist irreducible monic polynomials $M_1(x)$ and $M_2(x)$ in $(\mathbb{F}_q[[t]])[x]$ with

$$\deg(M_1(x)) = n-1$$

and

$$\deg(M_2(x)) = n$$

such that

$$M(x) = M_1(x) + M_2(x).$$

Proof. Let $M(x)$ be a monic polynomial in $(\mathbb{F}_q[[t]])[x]$ of degree $n \geq 2$. Write

$$M(x) = g(x,t) = x^n + m_{n-1}(t)x^{n-1} + \cdots + m_0(t),$$

where $m_i(t)$ belongs to $\mathbb{F}_q[[t]]$ for $i \in \{0, \ldots, n-1\}$. Then, $g(x,0)$ is a monic polynomial in $\mathbb{F}_q[x]$ of degree $n \geq 2$. By Theorem 4.3, there exist irreducible monic polynomials $f_1(x)$ and $f_2(x)$ in $\mathbb{F}_q[x]$ with $\deg(f_1(x)) = n-1$ and $\deg(f_2(x)) = n$ such that

$$g(x,0) = f_1(x) + f_2(x).$$

We set $M_1(x) = f_1(x)$ and $M_2(x) = f_2(x) + M(x) - g(x,0)$. Note that the polynomial $M_1(x)$ is also irreducible in $(\mathbb{F}_q[[t]])[x]$. Similarly, the polynomial $M_2(x)$ is a monic polynomial of degree n in $(\mathbb{F}_q[[t]])[x]$. Besides, $M_2(x)$ is also irreducible in $(\mathbb{F}_q[[t]])[x]$ as $f_2(x)$ in $\mathbb{F}_q[x]$ is irreducible and monic. This completes the proof. □

Remark 4.5. Notice that if $R = \mathbb{F}_q[[t_1, t_2, \ldots]]$ with q is odd, then the above theorem also holds for $R[x]$. Moreover, R is not Noetherian. Thus, one cannot make use of the corresponding result of [29].

Let $\mathbb{Z}_p$ be the p-adic integers and $\mathbb{Q}_p$ be the field of fractions of $\mathbb{Z}_p$, which is called the p-adic numbers. The ring $\mathbb{Z}_p$ is a local ring whose unique prime element is p. By a similar proof that of Theorem 4.4, one can obtain a Goldbach Property for $\mathbb{Z}_p[x]$.

Theorem 4.6. *Let p be an odd prime and $M(x)$ be a monic polynomial in $\mathbb{Z}_p[x]$ of degree $n \geq 2$. There exists a constant $c(n)$ depending only on n such that if $p > c(n)$, there exist irreducible monic polynomials $M_1(x)$ and $M_2(x)$ in $\mathbb{Z}_p[x]$ with $\deg(M_1(x)) = n-1$ and $\deg(M_2(x)) = n$ such that*

$$M(x) = M_1(x) + M_2(x).$$

In [2], the authors focused on the model theory of p-adic fields. As a remarkable corollary of their results we have the following fact which was also used to prove a conjecture of Artin, which states that for any positive integer d there is a prime p_0 such that for all primes $p \geq p_0$ every homogeneous polynomial of degree d in $n > d^2$ variables has a non-trivial zero in $\mathbb{Q}_p$.

Fact 4.7. *Let D be a non-principal ultrafilter on the set of primes $\mathbb{P}$. Then*

$$\prod_{p\in\mathbb{P}} \mathbb{Q}_p/D \equiv \prod_{p\in\mathbb{P}} \mathbb{F}_p((t))/D$$

as valued fields.

Notice also that the previous fact yields Theorem 4.6 as well.

Recall that a field F is called *pseudo-finite* if it is an infinite model of the first-order theory of finite fields. By applying our previous two results (Theorem 4.4 and Theorem 4.6), one has the following corollary:

Corollary 4.8. *Let D be a non-principal ultrafilter on the set of primes $\mathbb{P}$. Any monic polynomial $M(x)$ in $R[x]$ of degree $n \geq 2$ can be represented as a sum of two irreducible monic polynomials from $R[x]$ of degree n and $n-1$ if R is one of the following local rings:*

(1) $R = \prod_{p\in\mathbb{P}} \mathbb{Z}_p/D$,
(2) $R = \prod_{p\in\mathbb{P}} \mathbb{F}_p[[t]]/D$,
(3) *R is a pseudo-finite field of characteristic not 2.*

Proof. (1) By Remark 2.19 and Łoś' Theorem, we have that

$$R = \prod_{p\in\mathbb{P}} \mathbb{Z}_p/D$$

is a local ring, which is not a field. By Theorem 4.6 and Łoś' Theorem again, we conclude the result as the aforementioned Goldbach Property is a first-order property.

(2) This part is similar to the first part.

(3) Note that a pseudo-finite field is elementary equivalent to an ultraproduct of finite fields, see [3]. Therefore, this part follows from Theorem 4.3 and Łoś' Theorem once again.

□

Remark 4.9. By Theorem 2.10, we know that if $\mathrm{J}(R) = 0$, then a Goldbach Property for monic polynomials holds for $R[x]$ if R is a unique factorization domain of characteristic 0 which is not a field. Also, the previous corollary yields that there are some local integral domains R which are not fields where a type of Goldbach Property holds for $R[x]$. By

Theorem 2.10, Example 2.17, Remark 2.18 and the third part of the previous corollary, we discussed a Goldbach Property for polynomial rings over fields and for local rings which come from localizations of the integers. Hence, the triviality of the Jacobson radical, or being a field, or being a local ring do not determine a Goldbach Property over polynomial rings.

In 1998, using model theory, Wang [37] showed that for each characteristic $p \neq 2$ including the case $p = 0$, there exist infinitely many infinite fields F of characteristic p such that $F[x]$ satisfies a Weak Goldbach Property: every monic polynomial of degree $n \geq 2$ from $F[x]$ can be written as a sum of three irreducible monic polynomials from $F[x]$ with the property that one of degree n and the other two of degree less than n. In Wang's result, the cardinalities of those fields are not of a fixed cardinality. The first part of the next proposition generalizes Wang's result without model theory. Using more model theory, we can show the existence of such infinitely many infinite fields of any uncountable cardinality.

Proposition 4.10. *Let $p \in \mathbb{P} \cup \{0\}$.*

(1) *There exist infinitely many non-isomorphic infinite fields F of countable cardinality and characteristic p such that every polynomial $M(x)$ from $F[x]$ of degree $n \geq 1$ can be represented as a sum of two irreducible polynomials from $F[x]$ of degree n.*

(2) *Let κ be an uncountable cardinal. There exist 2^κ many non-isomorphic fields F of cardinality κ and characteristic p such that any monic polynomial $M(x)$ from $F[x]$ of degree $n \geq 1$ can be represented as a sum of two irreducible monic polynomials from $F[x]$ of degree n.*

(3) *Let κ be an uncountable cardinal. There exist 2^κ many non-isomorphic fields F of cardinality κ and characteristic $p \neq 2$ such that any monic polynomial $M(x)$ from $F[x]$ of degree $n \geq 2$ can be represented as a sum of two irreducible monic polynomials from $F[x]$ of degree n and $n - 1$.*

Proof. (1) Let $R(p, n) = \mathbb{F}_p[t_1, \ldots, t_n]$ and $F(p, n) = \mathbb{F}_p(t_1, \ldots, t_n)$ where $n \geq 1$, p is in $\mathbb{P} \cup \{0\}$ and $\mathbb{F}_0 = \mathbb{Q}$. Notice that $R(p, n)$ is a unique factorization domain with $\mathrm{J}(R(p, n)) = 0$, and $F(p, n)$ is the field of fractions of $R(p, n)$ whose cardinality is countable. Moreover, $F(p, n)$ is isomorphic to $F(q, m)$ as fields if and only if $p = q$ and $n = m$. Now, the result follows from Theorem 2.9(1).

(2) Let κ be an uncountable cardinal. Set $K_0 = \mathbb{Q}$ and $K_p = \mathbb{F}_p(t)$ when $p > 0$. For any $p \in \mathbb{P} \cup \{0\}$, by Theorem 2.9(1) we know that every polynomial $M(x)$ from

$K_p[x]$ of degree $n \geq 1$ can be represented as a sum of two irreducible polynomials from $K_p[x]$ of degree n. The same Goldbach Property holds over $L_p[x]$ for every field L_p such that K_p and L_p are elementarily equivalent. By [30,32], K_p is unstable and by [33], the theory of K_p has 2^κ non-isomorphic models of cardinality κ for any p. This proves the assertion.

(3) Let κ be an uncountable cardinal and K_p be a pseudo-finite field of characteristic $p \neq 2$. By the last part of Corollary 4.8, any monic polynomial $M(x)$ from $K_p[x]$ of degree $n \geq 2$ can be represented as a sum of two irreducible monic polynomials from $K_p[x]$ of degree n and $n-1$. This Goldbach Property holds true over $L_p[x]$ for every field L_p such that K_p and L_p are elementarily equivalent. By [16], we know that pseudo-finite fields are unstable. Hence, by [33] the theory of K_p has 2^κ non-isomorphic models of cardinality κ. This completes the proof.

□

5. Appendix: Some Model Theory

In this section, we briefly recall the basics of model theory, namely language, structure, formula, model and the compactness theorem. The details can be found in [26, 35].

Definition 5.1 (Language)**.** A *language* $\mathcal{L}$ is given by specifying the following data:

(i) A set of function symbols $\mathcal{F}$ and positive integers n_f for each f in $\mathcal{F}$,
(ii) A set of relation symbols $\mathcal{R}$ and positive integers n_E for each E in $\mathcal{R}$,
(iii) A set of constant symbols $\mathcal{C}$.

The number n_f indicates that f is a function of n_f variables and the number n_E emphasizes that E is an n_E-ary relation. For instance, the language $\{+, -, \cdot, 0, 1\}$ is called the language of rings where $+, -, \cdot$ are binary function symbols and 0,1 are constants.

Now, we define structures with respect to a language $\mathcal{L}$.

Definition 5.2 (Structure)**.** An $\mathcal{L}$-*structure* $\mathcal{M}$ is given by the following data:

(i) A non-empty set M called the domain of $\mathcal{M}$,
(ii) A function $f^{\mathcal{M}} : M^{n_f} \to M$ for each $f \in \mathcal{F}$,
(iii) A set $E^{\mathcal{M}} \subseteq M^{n_E}$ for each $E \in \mathcal{R}$,
(iv) An element $c^{\mathcal{M}} \in M$ for each $c \in \mathcal{C}$.

We regard $f^{\mathcal{M}}, E^{\mathcal{M}}$ and $c^{\mathcal{M}}$ as the interpretations of f, E and c for $\mathcal{M}$, and we write the structure $\mathcal{M}$ as

$$\mathcal{M} = (M, f^{\mathcal{M}}, E^{\mathcal{M}}, c^{\mathcal{M}} : f \in \mathcal{F}, E \in \mathcal{R}, c \in \mathcal{C}).$$

For example, a ring is an $\mathcal{L}$-structure $(R, +, -, \cdot, 0, 1)$ in the language of rings. Another example is

$$(\mathbb{R}, +, -, \cdot, <, 0, 1)$$

and here our language is the language $\{+, -, \cdot, <, 0, 1\}$ of ordered rings. Any graph $G = (V, E)$ is an $\mathcal{L}$-structure and the language just contains a relation, $\mathcal{L} = \{e\}$. The structure $(\mathbb{Z}, +, -, \cdot, |, 0, 1)$ is an $\mathcal{L}$-structure where, $\mathcal{L} = \{+, -, \cdot, |, 0, 1\}$ and the symbol $|$ is the divisibility relation on $\mathbb{Z}$.

Let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures. A map $\alpha : \mathcal{M} \to \mathcal{N}$ is called an $\mathcal{L}$-monomorphism ($\mathcal{L}$-embedding) if α is injective from M to N and

- α preserves all $\mathcal{L}$-functions: $\alpha(f^{\mathcal{M}}(a_1, \ldots, a_n)) = f^{\mathcal{N}}(\alpha(a_1), \ldots, \alpha(a_n))$ for all $a_1, \ldots, a_n$ in M with $n = n_f$.
- α preserves all $\mathcal{L}$-relations: for all $E \in \mathcal{R}$ and $a_1, \ldots, a_n \in M$ with $n = n_E$, $(a_1, \ldots, a_n) \in E^{\mathcal{M}}$ if and only if $((\alpha(a_1), \ldots, \alpha(a_n)) \in E^{\mathcal{N}}$.
- α preserves all $\mathcal{L}$-constants: for any $c \in \mathcal{C}$, we have $\alpha(c^{\mathcal{M}}) = c^{\mathcal{N}}$.

Note that monomorphisms are closed under compositions. A bijective monomorphism is called an isomorphism. If there is an isomorphism between $\mathcal{M}$ and $\mathcal{N}$, we write $\mathcal{M} \simeq \mathcal{N}$. Observe that $\simeq$ is an equivalence relation and if $\mathcal{M}$ is an $\mathcal{L}$-structure, then $(Aut(\mathcal{M}), \circ)$ is a group.

Let $\mathcal{M}$ and $\mathcal{N}$ be two $\mathcal{L}$-structures. We say that $\mathcal{M}$ is a substructure of $\mathcal{N}$ (or $\mathcal{N}$ is an extension of $\mathcal{M}$) if the identity map from $\mathcal{M}$ to $\mathcal{N}$ is a monomorphism. In this case, we write $\mathcal{M} \subseteq \mathcal{N}$. Here are some examples:

- $(2\mathbb{Z}, <) \subseteq (\mathbb{Z}, <)$
- $(\mathbb{Z}, +, -, \cdot, 0, 1) \subseteq (\mathbb{R}, +, -, \cdot, 0, 1) \subseteq (\mathbb{C}, +, -, \cdot, 0, 1)$

Suppose that M is a subset of N and $\mathcal{N}$ is an $\mathcal{L}$-structure. If M is closed under all $\mathcal{L}$-operations (functions and constants), then naturally

$$\mathcal{M} = (M, f^{\mathcal{M}}, E^{\mathcal{M}}, c^{\mathcal{M}} : f \in \mathcal{F}, E \in \mathcal{R}, c \in \mathcal{C})$$

becomes a substructure of $\mathcal{N}$ with $E^{\mathcal{M}} = E^{\mathcal{N}} \cap M^n$ where $n = n_E$ is the arity of $E \in \mathcal{R}$.

5.1. **Formulas.** Basically, an $\mathcal{L}$-*formula* is a string of symbols which is built using the symbols from $\mathcal{L}$, variable symbols $\{v_1, v_2, \ldots\}$, the equality symbol $=$, parentheses (,), the Boolean connectives $\wedge, \vee, \neg$, and the quantifiers $\forall, \exists$. Here is the formal definition.

Definition 5.3 (Formula)**.** Let $\mathcal{L}$ be a language. The set of $\mathcal{L}$-*terms* is the smallest set $\mathcal{T}$ such that

(i) For any constant symbol $c \in \mathcal{C}$, we have $c \in \mathcal{T}$.
(ii) Each variable symbol v_n is in $\mathcal{T}$ for $n \in \{1, 2, 3, \ldots\}$.
(iii) If $t_1, \ldots, t_{n_f}$ are in $\mathcal{T}$ and $f \in \mathcal{F}$, then $f(t_1, \ldots, t_{n_f}) \in \mathcal{T}$.

One can see that each term defines a function on any $\mathcal{L}$-structure $\mathcal{M}$ (inductively): if t is v_i, then $t^{\mathcal{M}}(a_1, \ldots, a_n) = a_i$. If t is c, then $t^{\mathcal{M}}(a_1, \ldots, a_n) = c^{\mathcal{M}}$. If $t = f(t_1, \ldots, t_m)$, then

$$t^{\mathcal{M}}(a_1, \ldots, a_n) = f^{\mathcal{M}}(t_1^{\mathcal{M}}(a_1, \ldots, a_n), \ldots, t_m^{\mathcal{M}}(a_1, \ldots, a_n)).$$

We say that ϕ is an *atomic* $\mathcal{L}$-*formula* if ϕ is given by either $t_1 = t_2$ where t_1, t_2 are $\mathcal{L}$-terms, or $E(t_1, \ldots, t_{n_E})$ where $t_1, \ldots, t_{n_E}$ are $\mathcal{L}$-terms and $E \in \mathcal{R}$. The set of $\mathcal{L}$-*formulas* is the smallest set $\mathcal{J}$ containing the atomic formulas such that

(1) If $\phi \in \mathcal{J}$, then $\neg\phi \in \mathcal{J}$.
(2) If ϕ_1 and ϕ_2 are in $\mathcal{J}$, then so are $\phi_1 \wedge \phi_2$ and $\phi_1 \vee \phi_2$.
(3) If $\phi \in \mathcal{J}$, then so are $\forall v_i \phi$ and $\exists v_i \phi$.

The variable v is said to be *occur freely* in a formula ϕ if it is not inside one of the quantifiers $\forall$ and $\exists$. A formula with no free variables is called a *sentence*. For instance, $\phi(x) : \exists y\ (y^2 + 1 = x)$ is a formula in the language of rings with x being its free variable, and $\forall x\ \exists y\ (y^2 = x)$ is a sentence in the language of rings.

Definition 5.4. Let $\mathcal{M}$ be an $\mathcal{L}$-structure and ϕ be an $\mathcal{L}$-formula with free variables $\bar{v} = (v_1, \ldots, v_k)$. Let $\bar{a} = (a_1, \ldots, a_k) \in M^k$. We inductively define $\mathcal{M} \models \phi(\bar{a})$ as follows.

(1) If ϕ is $t_1 = t_2$ where t_1 and t_2 are $\mathcal{L}$-terms, then $\mathcal{M} \models \phi(\bar{a})$ if $t_1^{\mathcal{M}}(\bar{a}) = t_2^{\mathcal{M}}(\bar{a})$.
(2) If ϕ is of the form $E(t_1, \ldots, t_{n_E})$ where $t_1, \ldots, t_{n_E}$ are $\mathcal{L}$-terms and $E \in \mathcal{R}$, then $\mathcal{M} \models \phi(\bar{a})$ if $(t_1^{\mathcal{M}}(\bar{a}), \ldots, t_{n_E}^{\mathcal{M}}(\bar{a})) \in E^{\mathcal{M}}$.
(3) If ϕ is $\neg\psi$, then $\mathcal{M} \models \phi(\bar{a})$ if $\mathcal{M} \not\models \psi(\bar{a})$.
(4) If ϕ is $\phi_1 \wedge \phi_2$, then $\mathcal{M} \models \phi(\bar{a})$ if $\mathcal{M} \models \phi_1(\bar{a})$ and $\mathcal{M} \models \phi_2(\bar{a})$.

(5) If ϕ is $\phi_1 \vee \phi_2$, then $\mathcal{M} \models \phi(\bar{a})$ if $\mathcal{M} \models \phi_1(\bar{a})$ or $\mathcal{M} \models \phi_2(\bar{a})$.
(6) If ϕ is $\exists w\ \psi(\bar{v}, w)$, then $\mathcal{M} \models \phi(\bar{a})$ if there exists b in M such that $\mathcal{M} \models \psi(\bar{a}, b)$.
(7) If ϕ is $\forall w\ \psi(\bar{v}, w)$, then $\mathcal{M} \models \phi(\bar{a})$ if for all b in M we have $\mathcal{M} \models \psi(\bar{a}, b)$.

We say that $\mathcal{M}$ satisfies $\phi(\bar{a})$ (or $\phi(\bar{a})$ is true in $\mathcal{M}$) if $\mathcal{M} \models \phi(\bar{a})$. For any sentence ϕ, either $\mathcal{M} \models \phi$ or $\mathcal{M} \not\models \phi$. For instance if ϕ is the sentence $\exists v\ (v^2 + 1 = 0)$, then $\mathbb{C} \models \phi$ but $\mathbb{R} \not\models \phi$ and $\mathbb{Z} \not\models \phi$ in the language of rings.

5.2. **Theories and Models.** For a given language $\mathcal{L}$, an *$\mathcal{L}$-theory* T is a set of sentences. An $\mathcal{L}$-structure $\mathcal{M}$ is said to be a *model* of T, denoted by $\mathcal{M} \models T$, if $\mathcal{M} \models \phi$ for any $\phi \in T$. For instance, if $\mathcal{L}_r$ is the language of rings, then the ring axioms is a theory and rings are its models. A theory T is satisfiable if it has a model. We say that two $\mathcal{L}$-structures $\mathcal{M}_1$ and $\mathcal{M}_2$ are *elementarily equivalent*, denoted by $\mathcal{M}_1 \equiv \mathcal{M}_2$, if they satisfy exactly the same $\mathcal{L}$-sentences. For instance $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are not elementarily equivalent as groups. To see this, one can consider the formula

$$\varphi : \exists v \forall x \exists y\ (x = y + y \vee x = y + y + v).$$

Then, $\mathbb{Z} \models \phi$ as any element is either even or odd. However, $\mathbb{Z} \times \mathbb{Z} \not\models \varphi$. Let $Th(\mathcal{M})$ be the full theory of $\mathcal{M}$, that is to say, it is the set of all sentences which are true in $\mathcal{M}$. Then, one can see that $\mathcal{M}_1 \equiv \mathcal{M}_2$ if and only if they have the same full theories, i.e. $Th(\mathcal{M}_1) = Th(\mathcal{M}_2)$.

One can show that two isomorphic structures are elementarily equivalent. Recall that an *isomorphism* is a bijection that preserves the interpretations of all the symbols of the language. However, the converse is not true, and in fact they need not have the same cardinality. To illustrate, the field of algebraic numbers $\overline{\mathbb{Q}}$ and $\mathbb{C}$ are not isomorphic as fields, but $\overline{\mathbb{Q}} \equiv \mathbb{C}$. The converse is true for finite structures: if $\mathcal{M}_1$ is a finite $\mathcal{L}$-structure, then $\mathcal{M}_1 \equiv \mathcal{M}_2$ if and only if they are isomorphic.

Next, we give one of the most fundamental theorems of model theory, namely the compactness theorem.

Compactness Theorem: Let T be a theory in a language $\mathcal{L}$. Then, T has a model if and only if every finite subset of T has a model.

The Compactness Theorem has a proof by applying Łoś' Theorem, and it has plentiful applications to other domains of mathematics, for instance see [3, 4].

Classification theory originated with the work of Morley during the 1960s and Shelah in the 1970s, and it seeks to classify first-order theories. The inquiry regarding the number of models a theory may possess has been at the core of model theory. Stable theories play a crucial role in categorizing their models. If a theory lacks stability, then its models become challenging to manage and various to classify [33]. Let M be an L-structure and $\phi(\bar{x}, \bar{y})$ be an L-formula. The formula $\phi(\bar{x}, \bar{y})$ has the *k-order property* in M if there are $\bar{a_i}, \bar{b_i}$ in M for $1 \leq i \leq k$ such that $\phi(\bar{a_i}, \bar{b_j})$ holds if and only if $i \leq j$. Let T be a complete theory in the language L. A formula $\phi(\bar{x}, \bar{y})$ is called *stable* for T if it does not have the k-order property for any model M of T for some positive integer k. The theory T is said to be *stable* if any L-formula $\phi(\bar{x}, \bar{y})$ is stable for T. For instance, the theory of algebraically closed fields is stable, but the theory of real numbers is not stable in the language of rings. As mentioned before, if R is a pseudo-finite field or $\mathbb{Q}$, then the theory of R is unstable in the language of rings [16, 30]. For more on the stability theory, we refer the reader to [34, 35].

6. Some Open Problems

(1) Let R be a unique factorization domain which is not a field with $\mathrm{J}(R) = 0$. Let $M(x) = m_n x^n + m_{n-1}x^{n-1} + \cdots + m_0 \in R[x]$ be a polynomial of degree $n \geq 1$. Is $M(x)$ a sum of two irreducible polynomials from $R[x]$ of degree at most n?
(2) Let R be a local unique factorization domain, which is not a field. Is it true that $R \models \{\psi_{n,k} : n \geq 1\}$ for some $k \geq 2$?
(3) What is the relation between almost UFDs and GCD domains? Let R be an almost UFD. Is R a GCD domain?

Declaration of competing interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement: We are grateful to the anonymous referee, whose suggestions immensely improved the quality and presentation of the paper. The second author's research is partially supported by the Science Academy's Young Scientist Award (BAGEP 2025).

References

[1] Atiyah M. F., MacDonald I. G., *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, (1969).

[2] Ax J., Kochen S., *Diophantine problems over local fields I*, Amer. J. Math., **87(3)**, (1965), 605–630.

[3] Ax J., *The elementary theory of finite fields*, Ann. of Math. (2), **88(2)** (1968), 239–271.

[4] Ax J., *Injective endomorphisms of varieties and schemes*, Pacific J. Math., **31(1)**, (1969), 1–7.

[5] Bender A. O., *Representing an element in $\mathbb{F}_q[t]$ as the sum of two irreducibles*, Mathematika, **60(1)**, (2014), 166–182.

[6] Bodin A., Dèbes P., Najib S., *The Schinzel hypothesis for polynomials*, Trans. Amer. Math. Soc., **373(12)**, (2020), 8339–8364.

[7] Bodin A., Dèbes P., Najib S., *Prime and coprime values of polynomials*, Enseign. Math., **66(1-2)**, (2020), 173–186.

[8] Bodin A., Dèbes P., König J., Najib S., *The Hilbert-Schinzel specialization property*, J. Reine Angew. Math., **785**, (2022), 55–79.

[9] Bodin A., Dèbes P., *Coprime values of polynomials in several variables*, Israel J. Math., **257(1)**, (2023), 25–54.

[10] Chang G. W., *Rings of formal power series in an infinite set of indeterminates*, Comm. Algebra, **42(10)**, (2014), 4182–4187.

[11] Chen J.-R., *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica, **16(2)**, (1973), 157–176.

[12] Davenport H., *Multiplicative Number Theory*, Springer-Verlag, New York, 2nd edition, (1982).

[13] Dries L. van den, Schmidt K., *Bounds in the theory of polynomial rings over fields. A nonstandard approach*, Inventiones Mathematicae **76(1)** (1984), 77–91.

[14] Dubickas A., *Linear forms in monic integer polynomials*, Canad. Math. Bull., **56(3)**, (2013), 510–519.

[15] Dummit D. S., Foote R. M., *Abstract Algebra*, John Wiley, Hoboken, NJ, 3rd edition, (2004).

[16] Duret J.-L., *Les corps pseudo-algébriquement clos non séparablement clos ont la propriété d'indépendance*, in Model theory of algebra and arithmetic, Proc. Karpacz 1979, Springer LN 834 (1980), 136–161.

[17] Grams A., *Atomic rings and the ascending chain condition for principal ideals*, Mathematical Proceedings of the Cambridge Philosophical Society, **75(3)**, (1974), 321–329.

[18] Hayes D. R., *A Goldbach theorem for polynomials with integral coefficients*, Amer. Math. Monthly, **72(1)**, (1965), 45–46.

[19] Helfgott H. A., *The ternary Goldbach conjecture is true*, arXiv:1312.7748v2, (2014).

[20] Helfgott H. A., *The ternary Goldbach problem*, arXiv:1501.05438v2, (2015).

[21] Kozek M. R., *Applications of covering systems of integers and Goldbach's conjecture for monic polynomials*, Ph.D. Thesis, University of South Carolina, ProQuest LLC, Ann Arbor, MI, (2007), 60pp.

[22] Kozek M., *An asymptotic formula for Goldbach's conjecture with monic polynomials in* $\mathbb{Z}[x]$, Amer. Math. Monthly, **117(4)**, (2010), 365–369.

[23] Lang S., *Algebra*, Revised 3rd ed., Vol. 211, Springer, Graduate Texts in Mathematics, (2002).

[24] Lemos A., de Araujo A. L. A., *An asymptotic formula for Goldbach's conjecture with monic polynomials in* $\mathbb{Z}[\theta][x]$, Colloq. Math., **148(2)**, (2017), 215–223.

[25] Li H., *Some discussions on the Goldbach conjecture*, arXiv:2306.17769v2, (2023).

[26] Marker D., *Model Theory: An Introduction*, Springer-Verlag, New York, (2002).

[27] Nishimura H., *On the unique factorization theorem for formal power series*, J. Math. Kyoto Univ., **7(2)**, (1967), 151–160.

[28] Paran E., *Twin-prime and Goldbach theorems for* $\mathbb{Z}[[x]]$, J. Number Theory, **213**, (2020), 453–461.

[29] Pollack P., *On Polynomial Rings with a Goldbach Property*, Amer. Math. Monthly, **118(1)**, (2011), 71–77.

[30] Robinson J., *Definability and decision problems in arithmetic*, J. Symbolic Logic, **14(2)**, (1949), 98–114.

[31] Saidak F., *On Goldbach's Conjecture for Integer Polynomials*, Amer. Math. Monthly, **113(6)**, (2006), 541–545.

[32] Scanlon T., *Infinite stable fields are Artin-Schreier closed*, unpublished manuscript, https://math.berkeley.edu/~scanlon/papers/ASclos.pdf, (1999).

[33] Shelah S., *The number of non-isomorphic models of an unstable first-order theory*, Israel J. Math., **9(4)**, (1971), 473–487.

[34] Shelah S., *Classification Theory, Studies in Logic and the Foundations of Mathematics*, North Holland, 2nd edition (1990).

[35] Tent K., Ziegler M., *A Course in Model Theory: Lecture Notes in Logic*, ASL, (2012).

[36] Vinogradov I. M., *Representation of an odd number as a sum of three primes*, Dokl. Akad. Nauk SSSR, **15(6-7)**, (1937), 291–294.

[37] Wang S., *The Goldbach 3-primes property for polynomial rings over certain infinite fields*, Chinese Science Bulletin, **43(15)**, (1998), 1256–1260.