Research Article

Giordano Santilli and Daniele Taufer*

First-degree prime ideals of composite extensions

https://doi.org/10.1515/jmc-2024-0036
received October 25, 2024; accepted January 20, 2025

Abstract: Let $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ be linearly disjoint number fields and let $\mathbb{Q}(\theta)$ be their compositum. We prove that the first-degree prime ideals (FDPIs) of $\mathbb{Z}[\theta]$ may almost always be constructed in terms of the FDPIs of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$, and *vice versa*. We identify the cases where this correspondence does not hold, and provide explicit counterexamples for each obstruction. We show that for every pair of coprime integers $d, e \in \mathbb{Z}$, such a correspondence almost always respects the divisibility of principal ideals of the form $(e + d\theta)\mathbb{Z}[\theta]$, with a few exceptions that we characterize. Finally, we establish the asymptotic computational improvement of such an approach, and we verify the reduction in time needed for computing such primes for certain concrete cases.

Keywords: first-degree prime ideals, principal ideal factorization, linearly disjoint extensions

MSC 2020: 11Y05, 11Y40, 12F05

1 Introduction

Let O be the ring of integers of a number field $\mathbb{Q}(\theta)$. It is well known that the norm of its prime ideals is always a prime power p^e, and this property also holds for every sub-order of O, such as $\mathbb{Z}[\theta]$. A special family of primes that deserves particular attention comprises those of degree $e = 1$, namely, those of prime norm. Such *first-degree prime ideals* (FDPIs) have been classically studied as they constitute a set of basic components for ideals. In fact, a positive fraction of prime integers splits only by means of first-degree primes [1, Thm. 84], and any Galois field class group may be generated from products of such ideals [1, Thm. 89].

More recently, similar results have been obtained in a more applied framework: FDPIs of $\mathbb{Z}[\theta]$ have been proved to constitute a basis for principal ideals generated by $e + d\theta$ in $\mathbb{Z}[\theta]$ for every coprime pair $e, d \in \mathbb{Z}$ [2], and this evidence has been exploited for designing the celebrated General Number Field Sieve (GNFS) algorithm [3,4], which is nowadays the most efficient classical algorithm known for factoring large integers. Indeed, after a parameters selection phase, such an algorithm needs to compute large sets of FDPIs of $\mathbb{Z}[\theta]$, which will be employed for factoring the aforementioned principal ideals. Afterward, these factorizations will be sieved in order to detect certain relations, which should lead to the factorization of the input integer with a positive probability. Moreover, the same algorithm has been proven effective for solving the discrete logarithm problem over finite fields, both for prime [5] and power-of-prime [6,7] fields.

In this article, the theory of FDPIs of $\mathbb{Z}[\theta]$ is further enhanced by establishing their relation with the corresponding prime ideals obtained from the minimal (non-trivial) sub-fields of $\mathbb{Q}(\theta)$. The novelty of this work is twofold. From a theoretical perspective, whenever $\mathbb{Q}(\theta)$ is realized as the compositum of two linearly disjoint sub-fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$, the factorization of $(e + d\theta)$ is proved to be almost always readable from the divisibility of its relative norm in $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$. On a computational side, the described procedure leads to

*** Corresponding author: Daniele Taufer,** Department of Computer Science, KU Leuven, Leuven, Belgium, e-mail: daniele.taufer@kuleuven.be
Giordano Santilli: Agenzia per la Cybersicurezza Nazionale, Rome, Italy, e-mail: giordano.santilli@gmail.com

a more efficient method for producing first-degree primes of $\mathbb{Z}[\theta]$, outperforming the standard algorithm of a linear factor which depends on the smoothness of the extension degree $[\mathbb{Q}(\theta) : \mathbb{Q}]$.

More precisely, employing the convenient description of such primes [2] as

$$(t, p) = \ker(\mathbb{Z}[\theta] \to \mathbb{F}_p,\ \theta \mapsto t),$$

the *combination* of first-degree primes $(r, p) \subseteq \mathbb{Z}[\alpha]$ and $(s, p) \subseteq \mathbb{Z}[\beta]$ is defined as $(r + s, p) \subseteq \mathbb{Z}[\theta]$, and such an operation is proved to describe the vast majority of first-degree primes in $\mathbb{Z}[\theta]$. Furthermore, the divisibility of principal ideals $I = (e + d\theta)\mathbb{Z}[\theta]$ is respected in all but exceptional cases, which are fully characterized in terms of the zeroes of the affine map

$$\phi : \mathbb{F}_p \to \mathbb{F}_p,\ x \mapsto -x - d^{-1}e.$$

The main novel results of this study are collected in Table 1. Its first row indicates when the combination of FDPIs in $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ dividing $I_\alpha = I \cap \mathbb{Z}[\alpha]$ and $I_\beta = I \cap \mathbb{Z}[\beta]$ is an FDPI of $\mathbb{Z}[\alpha + \beta]$, and when it divides I. The second row depicts the opposite scenario, namely when an FDPI of $\mathbb{Z}[\alpha + \beta]$ dividing I determines FDPIs in $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$, and when they divide I_α and I_β.

Such results lead to a bottom-up approach that may be employed to accelerate the production of these primes and to design new algorithms based on the smaller extensions, whose usage is often computationally preferable.

In practice, the employed hypotheses are not truly restrictive: every pair of reasonably uncorrelated fields happen to be linearly disjoint [8,9], thus every composite extension may be realized this way, with a suitable choice of sub-extensions. However, *ad hoc* examples are provided to show that every required hypothesis is essential in general.

This study is an extension of a previous work by Santilli and Taufer [10], which addresses the same problem when the field $\mathbb{Q}(\theta)$ is biquadratic. However, the techniques employed and developed in the current study are more sophisticated and lead to a deeper comprehension of ideals in towers of fields. The novel results not only generalize those of Santilli and Taufer [10], but also cover a much wider range of situations and provide theoretical tools that may be exploited for computational and cryptographic purposes, such as factoring and sieving through number fields.

This study is organized as follows: in Section 2, the basic results about resultant and linearly disjoint extensions are recalled and combined to properly identify the field extensions that we address in the present work. Section 3 is devoted to defining the FDPIs combination and establishing when this construction defines a complete correspondence of the considered FDPIs. Such an association is proved to almost always respect the divisibility of prescribed principal ideals in Section 4. In Section 5, the complexity of a combination-based approach for computing FDPIs is discussed, and a computational comparison with the state-of-the-art method is presented. Finally, in Section 6, we review the work and hint at possible future research directions.

Table 1: Overview of the main results of the study

	Existence	**Divisibility**
$(r, p), (s, p) \Rightarrow (t, p)$	Always	unless $\begin{cases} g(\phi(r)) \equiv 0 \bmod p \\ f(\phi(s)) \equiv 0 \bmod p \\ \phi(r) \not\equiv s \bmod p \\ \phi(s) \not\equiv r \bmod p \end{cases}$
	(Proposition 3.3)	(Theorem 4.3)
$(t, p) \Rightarrow (r, p), (s, p)$	when:	
	t is a simple root of $\mathrm{minpol}_{\mathbb{Q}}(\alpha + \beta) \bmod p$, or	Always
	$\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are normal and of coprime degrees	
	(Propositions 3.6 and 3.10)	(Theorem 4.6)

2 Preliminaries

2.1 Resultant

In this section, we recall the main properties of the polynomial resultant over a field.

Definition 2.1. (Resultant) Let $\Bbbk$ be a field and $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i \in \Bbbk[x]$ be polynomials of degree n and m, i.e., $a_n b_m \neq 0$. The resultant $R(f, g)$ of f and g is defined as the determinant of their Sylvester matrix, i.e.,

$$R(f,g) = \det \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & a_n & & \dots & & a_1 & a_0 \\ b_m & b_{m-1} & b_{m-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & b_m & & \dots & & b_1 & b_0 \end{pmatrix}.$$

Hence, the resultant is the determinant of a $(n + m) \times (n + m)$ matrix, whose first m rows contain the coefficients of f padded with zeroes and shifted, respectively, on the right by $0, 1, \dots, m - 1$ positions, while the remaining n rows are made of the coefficients of g padded with zeroes and shifted, respectively, on the right by $0, 1, \dots, n - 1$ positions. The resultant may be directly constructed from the roots f and g.

Proposition 2.2. [11, Prop. IV.8.3] *Let $f, g \in \Bbbk[x]$ as above, and let L be an extension of $\Bbbk$ where both f and g split completely, i.e.,*

$$f = a_n(x - \alpha_1)\dots(x - \alpha_n) \in L[x],$$
$$g = b_m(x - \beta_1)\dots(x - \beta_m) \in L[x].$$

Then,

$$R(f,g) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$

Remark 2.3. The roots of f and g as above need not to be different. Indeed, these polynomials have a common root if and only if $R(f, g) = 0$ [11, Cor. IV.8.4].

Corollary 2.4. [11, p. 203] *Let $f, g \in \Bbbk[x]$ as above, then*

$$R(f,g) = a_n^m \prod_{i=1}^{n} g(\alpha_i), \quad R(f,g) = (-1)^{nm} b_m^n \prod_{j=1}^{m} f(\beta_j).$$

We will apply resultants for constructing minimal polynomials of composite extensions. In this perspective, we employ it to define another polynomial in $\Bbbk[x]$.

Notation 2.5. Let $f, g \in \Bbbk[x]$ as above. For every $y \in \Bbbk$ we denote

$$R_{f,g}(y) = R(f(x), g(y - x)).$$

We can view it as a polynomial $R_{f,g}(y) \in \Bbbk[y]$, which by renaming the variable can be seen again as a polynomial $R_{f,g} \in \Bbbk[x]$. Finally, we will drop the indices f and g when they are clear from the context.

Proposition 2.6. *Let $f, g \in \Bbbk[x]$ be monic with $n = \deg(f)$, $m = \deg(g)$, and let $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_m$ be their respective (not necessarily distinct) roots in an extension L of $\Bbbk$. Then,*

$$R_{f,g} = \prod_{i=1}^{n}\prod_{j=1}^{m}(x - \alpha_i - \beta_j).$$

Proof. Since $g = \prod_{j=1}^{m}(x - \beta_j) \in L[x]$, for every $y \in \Bbbk$, we have $g(y - x) = \prod_{j=1}^{m}(y - x - \beta_j)$. From Corollary 2.4, we obtain

$$R_{f,g}(y) = R(f(x), g(y - x)) = \prod_{i=1}^{n} g(y - \alpha_i) = \prod_{i=1}^{n}\prod_{j=1}^{m}(y - \alpha_i - \beta_j),$$

which evaluated in x as in Notation 2.5 gives the desired result. □

Remark 2.7. It immediately follows from definitions that

$$R(g(y - x), f(x)) = (-1)^{nm} R_{f,g}(y) = R_{g,f}(y).$$

2.2 Linear disjoint extensions

In this section, we recall the basics of linearly disjoint field extensions that will be employed in this study.

Proposition 2.8. [8, §5, Prop. 5.1] *Let $\Bbbk$ be a field and Ω be an algebraic extension of $\Bbbk$. Let A and B be $\Bbbk$-subalgebras of Ω. The following conditions are equivalent*:

- *The $\Bbbk$-algebra homomorphism defined by*

$$A \otimes_{\Bbbk} B \to \Omega, \quad a \otimes b \mapsto ab,$$

  is injective.
- *Any $\Bbbk$-basis of A is linearly independent over B.*
- *Any $\Bbbk$-basis of B is linearly independent over A.*
- *If $\{u_i\}_i$ is a $\Bbbk$-basis of A and $\{v_j\}_j$ is a $\Bbbk$-basis of B, then $\{u_i v_j\}_{i,j}$ are $\Bbbk$-linearly independent.*

In this work, we will always consider $\Bbbk = \mathbb{Q}$. Moreover, A and B will be number fields (seen as subfields of $\mathbb{C}$ after a fixed field embedding), and Ω will be their compositum AB, namely, the smallest number field containing both A and B.

Definition 2.9. (Linearly disjointness) Two number fields satisfying any (every) condition of Proposition 2.8 are called *linearly disjoint*.

The simplest way to detect linear disjointness is by looking at the composite degree. For the reader's convenience, we recall the proof of this fact.

Lemma 2.10. *Two number fields L_1 and L_2 are linearly disjoint if and only if*

$$[L_1 L_2 : \mathbb{Q}] = [L_1 : \mathbb{Q}][L_2 : \mathbb{Q}].$$

Proof. Let $\{u_i\}_{1 \le i \le [L_1:\mathbb{Q}]}$ be a $\mathbb{Q}$-basis of L_1 and $\{v_j\}_{1 \le j \le [L_2:\mathbb{Q}]}$ be a $\mathbb{Q}$-basis of L_2. By definition of compositum, we have

$$L_1 L_2 = \langle \{u_i v_j\}_{i,j} \rangle_{\mathbb{Q}}.$$

The fields L_1 and L_2 are linearly disjoint if and only if $\{u_i v_j\}_{i,j}$ are $\mathbb{Q}$-linearly independent, i.e., they generate a space of dimension $[L_1 : \mathbb{Q}][L_2 : \mathbb{Q}]$ over $\mathbb{Q}$. □

From the above lemma, it is easy to see that when L_1 and L_2 are linearly disjoint, then $L_1 \cap L_2 = \mathbb{Q}$. If at least one of them is normal, the opposite implication also holds.

Proposition 2.11. [8, §5, Thm. 5.5] *Let L_1, L_2 be number fields, of which at least one is a normal extension of $\mathbb{Q}$. Then, they are linearly disjoint if and only if*

$$L_1 \cap L_2 = \mathbb{Q}.$$

If the discriminants of two number fields L_1, L_2 are coprime, then they are known to be linearly disjoint. The opposite also holds whenever $O_{L_1L_2} = O_{L_1}O_{L_2}$ [9].

A primitive element of the compositum of linearly disjoint fields may be easily characterized.

Proposition 2.12. *Let $\mathbb{Q}(\alpha), \mathbb{Q}(\beta)$ be linearly disjoint number fields. Then, their compositum is $\mathbb{Q}(\alpha + \beta)$.*

Proof. It follows from [12, Thm. p. 638], by noticing that the condition $\gcd(\deg\alpha, \deg\beta) = 1$ is only used in its proof to imply the field degrees multiplicativity, which in our assumptions follows by Lemma 2.10. □

Corollary 2.13. *Let $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ be two linearly disjoint number fields and let $f, g \in \mathbb{Q}[x]$ be minimal polynomials of α and β over $\mathbb{Q}$. Then, a defining polynomial for $\mathbb{Q}(\alpha, \beta)$ is $R_{f,g}$.*

Proof. Let $n = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f)$ and $m = [\mathbb{Q}(\beta) : \mathbb{Q}] = \deg(g)$, and let $h \in \mathbb{Q}[x]$ be the minimal polynomial of $\alpha + \beta$ over $\mathbb{Q}$. Proposition 2.12 ensures that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + \beta)$ and since the number fields are linearly disjoint, from Lemma 2.10, we know that $mn = [\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] = \deg(h)$. From Proposition 2.6, the polynomial $R_{f,g}$ is monic, has degree nm, and $\alpha + \beta$ is one of its roots, then $h | R_{f,g}$. Since they have the same degree, we conclude that $h = R_{f,g}$. □

By means of Corollary 2.13, we will always regard the compositum of two linearly disjoint number fields $\mathbb{Q}[x]/(f)$ and $\mathbb{Q}[x]/(g)$ as the field generated by their resultant, namely, $\mathbb{Q}[x]/(R_{f,g})$.

Remark 2.14. Even if $R_{f,g}$ is a generator for the compositum $\mathbb{Q}(\alpha + \beta)$, we are not guaranteed that it is a convenient one. In fact, the minimal polynomials of elements $\{\alpha + k\beta\}_{k\in\mathbb{Z}}$ tend to have large coefficients [13, Remark to Algorithm 2.1.8].

3 FDPIs

We consider the following setting: let $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ be two linearly disjoint number fields and let $f \in \mathbb{Z}[x]$ (resp. $g \in \mathbb{Z}[x]$) be the minimal polynomial of α (resp. β) over $\mathbb{Q}$. We also consider the compositum $\mathbb{Q}(\alpha, \beta)$, which is equal to $\mathbb{Q}(\alpha + \beta)$ by Proposition 2.12. Let L be a field extension of the field $\Bbbk$, we will denote by $N_{L/\Bbbk}(x)$ the norm of the element $x \in L$ over the field $\Bbbk$. Given an algebraic integer $\theta \in \mathbb{C}$, we recall that the norm of a non-zero ideal $\mathfrak{a} \subseteq \mathbb{Z}[\theta]$ is

$$\mathcal{N}(\mathfrak{a}) = [\mathbb{Z}[\theta] : \mathfrak{a}].$$

Definition 3.1. (FDPIs) Let $\theta \in \mathbb{C}$ be an algebraic integer. A non-zero prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\theta]$ is called a *FDPI* if $\mathcal{N}(\mathfrak{p})$ is a prime integer.

These particular ideals admit a practical representation as follows.

Theorem 3.2. [2, pp. 58–59] *Let $f \in \mathbb{Z}[x]$ be an irreducible monic polynomial and $\theta \in \mathbb{C}$ one of its roots. Then, for every integer prime p, there is a bijection between*

$$\{(r, p) | r \in \mathbb{F}_p \text{ such that } f(r) = 0 \in \mathbb{F}_p\}$$

and

$$\{\mathfrak{p} | \mathfrak{p} \in \text{Spec } \mathbb{Z}[\theta] \text{ such that } \mathcal{N}(\mathfrak{p}) = p\}.$$

The bijection considered in the previous theorem is given by the evaluation of θ in a root r of $f \bmod p$, namely, such ideals $\mathfrak{p}$ arise as kernels of the evaluations

$$\text{ev}_{\theta \mapsto r} : \mathbb{Z}[\theta] \to \mathbb{F}_p, \ \theta \mapsto r.$$

Certain ideals of $\mathbb{Z}[\theta]$ can be factored using only FDPIs [2], and this is one of the main facts on which the GNFS relies. For a quick recap on these results, refer [10, Section 2].

Here we are interested in studying the relation among FDPIs of the orders $\mathbb{Z}[\alpha]$, $\mathbb{Z}[\beta]$ and those of $\mathbb{Z}[\alpha + \beta]$. The following result shows that it is always possible to efficiently construct FDPIs of $\mathbb{Z}[\alpha + \beta]$ starting from those of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$.

Proposition 3.3. *Let (r, p) be an FDPI of $\mathbb{Z}[\alpha]$ and (s, p) be an FDPI of $\mathbb{Z}[\beta]$, then $(r + s, p)$ is an FDPI of $\mathbb{Z}[\alpha + \beta]$.*

Proof. From Corollary 2.13, we know that the minimal polynomial of $\alpha + \beta$ is $R_{f,g}$. Since (r, p) is an FDPI of $\mathbb{Z}[\alpha]$, then r is a root of $f \bmod p$. Analogously, s is a root of $g \bmod p$. The definition of $R_{f,g}$ as seen in Proposition 2.6 leads to the desired result. □

Remark 3.4. The previous result applied to biquadratic extensions is precisely [10, Theorem 2].

Proposition 3.3 motivates the following definition.

Definition 3.5. (Combination) We say that the FDPI $(r + s, p) \subseteq \mathbb{Z}[\alpha + \beta]$ is the *combination* of $(r, p) \subseteq \mathbb{Z}[\alpha]$ and $(s, p) \subseteq \mathbb{Z}[\beta]$.

The following proposition shows that almost every FDPI of $\mathbb{Z}[\alpha + \beta]$ arise from a combination of FDPIs of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$.

Proposition 3.6. *Let (t, p) be an FDPI of $\mathbb{Z}[\alpha + \beta]$, where t is a simple root of $R_{f,g} \bmod p$. Then, (t, p) is a combination of FDPIs of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$.*

Proof. Let $\mathbb{F}_q$ be an extension of $\mathbb{F}_p$ where both $f \bmod p$ and $g \bmod p$ split. By Proposition 2.6, the roots of $R = R_{f,g} \bmod p$ are sums of roots in $\mathbb{F}_q$ of $f \bmod p$ and $g \bmod p$, i.e., there are $\gamma_1, \gamma_2 \in \mathbb{F}_q$ such that $t = \gamma_1 + \gamma_2$ and

$$f(\gamma_1) = 0 = g(\gamma_2).$$

It is well known [14, Theorem 2.14] that the conjugates of γ over $\mathbb{F}_p$, namely, $\{\gamma^{p^n}\}_{n \in \mathbb{N}}$, are simple roots of the same irreducible polynomial, hence in particular we have

$$f(\gamma_1^p) = 0 = g(\gamma_2^p).$$

Therefore, $\gamma_1^p + \gamma_2^p$ is also a root of R. However, we have

$$\gamma_1^p + \gamma_2^p = (\gamma_1 + \gamma_2)^p = t^p = t.$$

Thus, either t is a multiple root of R or all the conjugates of γ_1 are equal, and so are those of γ_2. By hypothesis we are in the latter case, then $\gamma_1, \gamma_2 \in \mathbb{F}_p$ and (t, p) is the combination of (γ_1, p) and (γ_2, p). □

Remark 3.7. The resultant polynomial $R_{f,g}$ is irreducible over $\mathbb{Q}$ by Corollary 2.13, then it has no repeated roots. Hence, its discriminant $R(R_{f,g}, R')$ is a non-zero integer, which is therefore divisible only by primes from a finite set $\mathcal{P}$. In particular, for every prime $p \notin \mathcal{P}$, the projected resultant $R_{f,g} \bmod p$ has only simple roots, so every prime ideal of $\mathbb{Z}[\alpha + \beta]$ of norm p arises as a combination of FDPIs in $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ by Proposition 3.6. For a more precise description of this set $\mathcal{P}$, we refer to [13, Lemma 2.1.13].

Remark 3.8. We note that Proposition 3.6 generalizes [10, Theorem 3]. In fact, let $f(x) = x^2 - a$, $g(x) = x^2 - b$, let p be a prime and $\gamma_1, \gamma_2 \in \mathbb{F}_{p^2}$ such that $f(\gamma_1) = 0 = g(\gamma_2)$. It is clear that $-\gamma_1$ (resp. $-\gamma_2$) is also a root of f (resp. g), therefore, the roots of $R_{f,g}$ in $\mathbb{F}_{p^2}$ are $\pm\gamma_1 \pm \gamma_2$. An easy check shows that $R_{f,g}$ has a multiple root if and only if

- $p = 2$, or
- $\gamma_1 = 0$ or $\gamma_2 = 0$, or
- $t = \gamma_1 + \gamma_2 = 0$.

In the first two cases, the FDPI $(t, p) \subseteq \mathbb{Z}[\alpha + \beta]$ arises anyway as a combination, while when $t = 0$ this does not necessarily hold [10, Example 3].

We now prove that when $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are both normal and of coprime degrees, we are guaranteed that every FDPI of $\mathbb{Z}[\alpha + \beta]$ arises as a combination, without exceptions. First, we prove a technical result linking a global property of polynomials with the degrees of their local factors. It is stated independently on the following results, as it has its own theoretical interest.

Proposition 3.9. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial and let L be its splitting field over $\mathbb{Q}$. Let p be an integer prime and $h \in \mathbb{F}_p[x]$ be an irreducible factor of $f \bmod p$. Then,*

$$\deg h \mid [L : \mathbb{Q}].$$

Proof. Let O_L be the ring of integers of L over $\mathbb{Q}$ and let $\mathfrak{p} \subseteq O_L$ be a prime lying over p. Since $L/\mathbb{Q}$ is Galois, the ramification index e and the inertia degree f are independent of $\mathfrak{p}$ [13, Prop. 10.1.3]. Thus, if g is the number of primes lying over p, we have

$$[L : \mathbb{Q}] = \mathrm{efg},$$

and in particular $f \mid [L : \mathbb{Q}]$. Since f is monic with integer coefficients, its roots are in O_L, so it splits in $O_L/\mathfrak{p}$. Thus, this extension of $\mathbb{F}_p$ contains the splitting field of f over $\mathbb{F}_p$. Since h is irreducible, $O_L/\mathfrak{p}$ also contains the field $\mathbb{F}_p[x]/(h)$, which has degree $\deg h$ over $\mathbb{F}_p$. Therefore, we have

$$\deg h \mid [O_L/\mathfrak{p} : \mathbb{F}_p] = f,$$

which concludes the proof. □

We can now prove the combination result.

Proposition 3.10. *Let $f, g \in \mathbb{Z}[x]$ be monic and irreducible polynomials of coprime degrees such that $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$ and $\mathbb{Q}(\beta) = \mathbb{Q}[x]/(g)$ are normal extensions of $\mathbb{Q}$. If (t, p) is an FDPI of $\mathbb{Z}[\alpha + \beta]$, then it is a combination of FDPIs of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$.*

Proof. Since the degrees are coprime, we have $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$, and since $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are normal, by Proposition 2.11 we know that they are linearly disjoint. Thus, by Corollary 2.13, their compositum $\mathbb{Q}(\alpha, \beta)$ is generated by $R = R_{f,g}$, and by hypothesis we have

$$R(t) \equiv 0 \bmod p.$$

Let $\overline{f}, \overline{g} \in \mathbb{F}_p[x]$ be the projections of f and g modulo p, and let $\mathbb{F}_q$ be their common splitting field. By Proposition 2.6 there are $\nu, \mu \in \mathbb{F}_q$ such that

$$\overline{f}(\nu) = 0, \quad \overline{g}(\mu) = 0, \quad t = \nu + \mu.$$

Let h_f and h_g be minimal polynomials of ν and μ over $\mathbb{F}_p$, respectively. Since $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are normal over $\mathbb{Q}$, then they are the splitting fields of α and β, so Proposition 3.9 implies that

$$\deg h_f | \deg f, \quad \deg h_g | \deg g.$$

Since $\deg f$ and $\deg g$ are coprime, also $\gcd(\deg h_f, \deg h_g) = 1$. However, since $\nu + \mu = t \in \mathbb{F}_p$ we have $\mathbb{F}_p(\nu) = \mathbb{F}_p(\mu)$. This may only happen if

$$\mathbb{F}_p(\nu) = \mathbb{F}_p(\mu) = \mathbb{F}_p,$$

which means that $\nu, \mu \in \mathbb{F}_p$. Hence, we conclude that (t, p) is the combination of (ν, p) and (μ, p). □

The following examples show that both normality and coprimality of degrees are necessary conditions for Proposition 3.10.

Example 3.11. Let us consider the following irreducible polynomials:

$$f(x) = x^2 - 3, \quad g(x) = x^3 - 2,$$

and let $\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$ and $\mathbb{Q}(\beta) = \mathbb{Q}[x]/(g)$ be the number fields they generate. We note that the degrees are coprime and $\mathbb{Q}(\alpha)$ is Galois, while $\mathbb{Q}(\beta)$ is not normal. A defining polynomial of the compositum $\mathbb{Q}(\alpha + \beta)$ is the resultant

$$R_{f,g} = x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23.$$

The FDPIs of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ with norm 17 correspond to the roots modulo 17 of f and g. One can directly verify that there are none of them in $\mathbb{Z}[\alpha]$, while $(8, 17)$ is an FDPI in $\mathbb{Z}[\beta]$. However, $(13, 17) \subseteq \mathbb{Z}[\alpha + \beta]$ is an FDPI of norm 17, which cannot be a combination of FDPIs in the underlying extensions. In fact, one can directly check that, with the notation employed in the proof of Proposition 3.10, we obtain $h_g = x^2 + 8x + 13$, whose degree does not divide $\deg g$. This shows that the hypothesis of normality on both extensions is necessary for Proposition 3.10.

Example 3.12. Let f be as in Example 3.11 and consider $g = x^4 + 1$. These polynomials are irreducible over $\mathbb{Q}$ and generate normal extensions $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$. The compositum $\mathbb{Q}(\alpha + \beta)$ is defined by the polynomial

$$R_{f,g} = x^8 - 12x^6 + 56x^4 - 72x^2 + 100.$$

Neither $\mathbb{Z}[\alpha]$ nor $\mathbb{Z}[\beta]$ have FDPIs with norm 5, although there is an FDPI in $\mathbb{Z}[\alpha + \beta]$ of norm 5, that is $(0, 5)$, which again cannot arise from any combination of FDPIs in the underlying extensions. Therefore, we also need coprime degrees in Proposition 3.10.

4 Divisibility of prescribed principal ideals

Given an algebraic integer $\theta \in \mathbb{C}$, it is known that the prime factors of principal ideals of the form $(e + d\theta)\mathbb{Z}[\theta]$ with $\gcd(e, d) = 1$ are all first-degree primes $(t, p) \subseteq \mathbb{Z}[\theta]$ such that $e + dt \equiv 0 \bmod p$ [2, Corollary 5.5]. In this section, we detail how this divisibility can be read from the underlying fields and *vice versa*. The results presented in the study by Santilli and Taufer [10, Section 4] may therefore be seen as particular instances of those discussed in the present section. To pursue this direction, we first need to characterize the intersection of this principal ideal with the underlying rings $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$.

Theorem 4.1. *Let $\alpha, \beta \in \mathbb{C}$ be algebraic integers defining linearly disjoint number fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$, and let $g = \sum_{i=0}^{m} b_i x^i \in \mathbb{Z}[x]$ be the minimal polynomial of β over $\mathbb{Q}$. Let $e, d \in \mathbb{Z}$ be coprime integers and let I be the principal ideal generated by $\xi = e + d(\alpha + \beta)$ in $\mathbb{Z}[\alpha + \beta]$. Then,*

$$I \cap \mathbb{Z}[\alpha] = (\chi)\mathbb{Z}[\alpha]$$

is still principal, generated by $\chi = N_{\mathbb{Q}(\alpha+\beta)/\mathbb{Q}(\alpha)}(\xi)$, *namely,*

$$\chi = \sum_{i=0}^{m} (-d)^i \Omega^{m-i} b_{m-i}, \quad \text{where } \Omega = e + d\alpha \in \mathbb{Z}[\alpha].$$

Proof. We directly prove the two inclusions.

($\subseteq$) Every $z \in I = (\zeta)\mathbb{Z}[\alpha + \beta]$ can be written as

$$z = (\Omega + d\beta)(\lambda_0 + \lambda_1\beta + \ldots + \lambda_{m-1}\beta^{m-1}),$$

for some $\lambda_0, \ldots, \lambda_{m-1} \in \mathbb{Z}[\alpha]$. Since $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are linearly disjoint, then $\{1, \beta, \ldots, \beta^{m-1}\}$ is a basis for $\mathbb{Q}(\alpha + \beta)$ over $\mathbb{Q}(\alpha)$ by Proposition 2.8. Hence, if this z also belongs to $\mathbb{Z}[\alpha]$, all its non-constant coefficients as an element of $\mathbb{Z}[\alpha][\beta]$ need to vanish, i.e.,

$$\begin{cases} \lambda_1\Omega + d\lambda_0 - \lambda_{m-1}db_1 = 0, \\ \lambda_2\Omega + d\lambda_1 - \lambda_{m-1}db_2 = 0, \\ \vdots \\ \lambda_{m-2}\Omega + d\lambda_{m-3} - \lambda_{m-1}db_{m-2} = 0, \\ \lambda_{m-1}\Omega + d\lambda_{m-2} - \lambda_{m-1}db_{m-1} = 0. \end{cases} \tag{1}$$

We first prove that for every $0 \le i \le m-1$ we have $d^i | \lambda_i$. To do so, we prove by induction on $0 \le j \le i$ that $d^j | \lambda_i$. The base step $j = 0$ is trivial. Let us assume that $d^j | \lambda_i$ for all $j \le i \le m-2$. For every $1 \le k \le i - j$, the $(j + k)$th equation of system (1) gives

$$e\lambda_{j+k} = d(\lambda_{m-1}b_{j+k} - \lambda_{j+k-1} - \alpha\lambda_{j+k}).$$

Since $(e, d) = 1$ and by induction $d^j | \lambda_{m-1}b_{j+k} - \lambda_{j+k-1} - \alpha\lambda_{j+k}$, $d^{j+1} | \lambda_{j+k}$ for every $1 \le k \le i - j$, i.e., $d^{j+1} | \lambda_i$ whenever $j + 1 \le i$. We now prove by induction on $2 \le k \le m$ that

$$\lambda_{m-k} = \frac{\lambda_{m-1}}{d^{k-1}} \left(\sum_{j=0}^{k-1} d^j (-\Omega)^{k-1-j} b_{m-j} \right), \tag{2}$$

which is well defined since $\frac{\lambda_{m-1}}{d^{k-1}} \in \mathbb{Z}$, as noted before. The base step $k = 2$ is given by the last equation of (1), indeed

$$\lambda_{m-2} = \frac{\lambda_{m-1}}{d}(db_{m-1} - \Omega).$$

We now suppose that (2) holds for $k \le m-1$ and check that this implies it for $k + 1$. From the $(m - k)$th equation of system (1), we have

$$\lambda_{m-k}\Omega + d\lambda_{m-k-1} - d\lambda_{m-1}b_{m-k} = 0,$$

which by inductive hypothesis becomes

$$\begin{aligned} \lambda_{m-k-1} &= \frac{1}{d} \left(d\lambda_{m-1}b_{m-k} + \frac{\lambda_{m-1}}{d^{k-1}} \left(\sum_{j=0}^{k-1} b_{m-j} d^j (-\Omega)^{k-j} \right) \right) \\ &= \frac{\lambda_{m-1}}{d^k} \left(d^k b_{m-k} + \sum_{j=0}^{k-1} b_{m-j} d^j (-\Omega)^{k-j} \right) \\ &= \frac{\lambda_{m-1}}{d^k} \left(\sum_{j=0}^{k} b_{m-j} d^j (-\Omega)^{k-j} \right). \end{aligned}$$

This proves that (2) holds, and in particular

$$\lambda_0 = \frac{\lambda_{m-1}}{d^{m-1}} \left(\sum_{j=0}^{m-1} b_{m-j} d^j (-\Omega)^{m-1-j} \right). \tag{3}$$

When system (1) holds, we have $z = \lambda_0\Omega - \lambda_{m-1}db_0$, which by means of (3) can be written as

$$\begin{aligned}\lambda_0\Omega - \lambda_{m-1}db_0 &= \frac{\lambda_{m-1}}{d^{m-1}}\left(\sum_{j=0}^{m-1} b_{m-j}d^j(-\Omega)^{m-1-j}\right)\Omega - \lambda_{m-1}db_0\\ &= \frac{\lambda_{m-1}}{d^{m-1}}\left(\sum_{j=0}^{m-1} b_{m-j}d^j(-1)^{m+1-j}\Omega^{m-j} - d^m b_0\right)\\ &= (-1)^{m+1}\frac{\lambda_{m-1}}{d^{m-1}}\left(\sum_{j=0}^{m-1} b_{m-j}(-d)^j\Omega^{m-j} + (-d)^m b_0\right)\\ &= (-1)^{m+1}\frac{\lambda_{m-1}}{d^{m-1}}\chi.\end{aligned}$$

Since $\frac{\lambda_{m-1}}{d^{m-1}} \in \mathbb{Z}[\alpha]$, $z \in (\chi)\mathbb{Z}[\alpha]$.

(⊇) By definition $\chi \in \mathbb{Z}[\alpha]$, and by a straightforward computation, we obtain

$$\chi = \prod_{i=1}^{m}(\Omega + d\beta_i) = N_{\mathbb{Q}(\alpha+\beta)/\mathbb{Q}(\alpha)}(\xi), \tag{4}$$

where β_i's are the roots of $g(x)$ in its splitting field. Since $\xi \in \mathbb{Z}[\alpha+\beta] \subseteq O_{\mathbb{Q}(\alpha+\beta)}$, it satisfies a polynomial with coefficients in $\mathbb{Z}[\alpha]$, namely, there are $h_i \in \mathbb{Z}[\alpha]$ such that

$$h(\xi) = h_t\xi^t + h_{t-1}\xi^{t-1} + \ldots + h_0 = 0.$$

Then,

$$\chi = N_{\mathbb{Q}(\alpha+\beta)/\mathbb{Q}(\alpha)}(\xi) = (-1)^t h_0 = (-1)^{t+1}\xi(h_t\xi^{t-1} + h_{t-1}\xi^{t-2} + \ldots + h_1),$$

so it belongs to $(\xi)\mathbb{Z}[\alpha+\beta]$. □

Remark 4.2. It is easy to verify that the biquadratic case discussed in the study by Santilli and Taufer [10, Proposition 4] is simply an instance of Theorem 4.1, when $\beta^2 \in \mathbb{Z}$ and $g = x^2 - \beta^2$.

We now fix some notation: let $\alpha, \beta \in \mathbb{C}$ be algebraic integers such that $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are linearly disjoint, let $e, d \in \mathbb{Z}$ be coprime integers and let us consider the principal ideal $I = (e + d(\alpha+\beta)) \subseteq \mathbb{Z}[\alpha+\beta]$. Let also $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ be the minimal polynomial of α and $g = \sum_{i=0}^{m} b_i x^i \in \mathbb{Z}[x]$ be the minimal polynomial of β. By Theorem 4.1, we know that

$$I_\alpha = I \cap \mathbb{Z}[\alpha] = (\chi_\alpha)\mathbb{Z}[\alpha], \quad \text{where } \chi_\alpha = \sum_{i=0}^{m}(-d)^i(e + d\alpha)^{m-i}b_{m-i}$$

and

$$I_\beta = I \cap \mathbb{Z}[\beta] = (\chi_\beta)\mathbb{Z}[\beta], \quad \text{where } \chi_\beta = \sum_{i=0}^{n}(-d)^i(e + d\beta)^{n-i}a_{n-i}.$$

Finally, whenever p is a prime not dividing d, we may define the affine map

$$\phi : \mathbb{F}_p \to \mathbb{F}_p,\ x \mapsto -x - d^{-1}e.$$

Theorem 4.3. *In the above notation, let (r, p) be a first-degree prime of $\mathbb{Z}[\alpha]$ dividing I_α and (s, p) be a first-degree prime of $\mathbb{Z}[\alpha]$ dividing I_β. Then, $(r + s, p)$ is a first-degree prime of $\mathbb{Z}[\alpha+\beta]$ dividing I, unless $\phi(r)$ is a root of $g \bmod p$ different from s and, at the same time, $\phi(s)$ is a root of $f \bmod p$ different from r.*

Proof. Since $(r, p)|I_\alpha$, $I_\alpha \subseteq \ker(\mathrm{ev}_{\alpha\mapsto r})$, so we have

$$\sum_{i=0}^{m}(-d)^i(e + dr)^{m-i}b_{m-i} \equiv 0 \bmod p.$$

If $d \equiv 0 \bmod p$, the above equation leads to $e^m \equiv 0 \bmod p$, contradicting the coprimality of e and d. Hence, we may assume $d \not\equiv 0 \bmod p$ and write

$$\sum_{i=0}^{m}(-d)^i(e + dr)^{m-i}b_{m-i} = (-d)^m g\left(\frac{e + dr}{-d}\right) = (-d)^m g(\phi(r)).$$

Since $p\nmid d$, $\phi(r)$ is a root of $g \bmod p$. The same argument also shows that $\phi(s)$ needs to be a root of $f \bmod p$. By hypothesis we may assume that either $\phi(r) = s$ or $\phi(s) = r$, both of which imply

$$r + s + d^{-1}e \equiv 0 \bmod p.$$

Since I is generated by $e + d(\alpha + \beta)$, the above congruence shows that the combination $(r + s, p)$, which is an FDPI of $\mathbb{Z}[\alpha + \beta]$ by Proposition 3.3, divides I. □

The condition $\phi(r) \neq s$ being a root of $g \bmod p$ and $\phi(s) \neq r$ being a root of $f \bmod p$ of Theorem 4.3 will be referred to as the *exceptional case*. It appears to be extremely rare, especially when the considered extensions are small (e.g., Proposition 4.9). However, it can occasionally occur and may not be evident *a priori*, as shown in the following example.

Example 4.4. Let us consider the polynomials

$$f = x^3 + x^2 + x + 19, \quad g = x^4 - 6x^2 - 7x + 5,$$

generating the number fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$, whose composite $\mathbb{Q}(\theta)$ is generated by

$$h = x^{12} + 4x^{11} - 8x^{10} + 11x^9 + 193x^8 + 824x^7 + 5663x^6 + 8910x^5 + 32405x^4 + 120009x^3 + 185557x^2 + 255445x + 24299.$$

Let us consider the principal ideal

$$I = (1 + \theta)\mathbb{Z}[\theta],$$

whose intersections with $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are generated by

$$\chi_\alpha = -4\alpha^2 - 23\alpha - 50, \quad \chi_\beta = \beta^3 + 2\beta^2 + 2\beta - 18.$$

We observe that $(1, 11), (2, 11), (7, 11) \subseteq \mathbb{Z}[\alpha]$ are FDPIs, while the norm-11 first-degree primes of $\mathbb{Z}[\beta]$ are $(3, 11), (9, 11) \subseteq \mathbb{Z}[\beta]$. However, we have

$$\phi(1) \equiv 9 \bmod 11, \quad \phi(3) \equiv 7 \bmod 11.$$

Hence, we are in the exceptional case of Theorem 4.3: the FDPI $(4, 11) \subseteq \mathbb{Z}[\theta]$ given by the combination of $(1, 11) \in \mathbb{Z}[\alpha]$ and $(3, 11) \in \mathbb{Z}[\beta]$ does not divide I, as

$$1 + (1 + 3) \equiv 5 \not\equiv 0 \bmod 11.$$

Remark 4.5. We highlight that Theorem 4.3, applied to biquadratic fields, improves [10, Theorem 4]. In fact, when $f(x) = x^2 - a$ and $g(x) = x^2 - b$, the exceptional case occurs only if

$$\begin{cases} e + dr \equiv ds \bmod p, \\ e + ds \equiv dr \bmod p. \end{cases}$$

If $p = 2$, these equations are both equivalent to $e + d(r + s) \equiv 0 \bmod 2$, so $(r + s, 2)|(e + d(\alpha + \beta))$, thus the exceptional case does not prevent ideal divisibility. If $p \neq 2$, the above equations imply that $e \equiv 0 \bmod p$, which

gives $r \equiv s \bmod p$ since $\gcd(d, e) = 1$. However, we would still have ideal divisibility if $2r \equiv r + s \equiv 0 \bmod p$, hence this may fail only if

$$p \neq 2, \quad e \equiv 0 \bmod p, \quad r \equiv s \not\equiv 0 \bmod p.$$

The above condition is sharper than the condition established in [10, Theorem 4], and it is satisfied by [10, Example 4].

On the other hand, we show that if a combination divides I, then its constituents always divide the correspondent restrictions I_α and I_β.

Theorem 4.6. *In the above notation, let $(t, p) \subseteq \mathbb{Z}[\alpha + \beta]$ be an FDPI dividing I. If there exist first-degree primes $(r, p) \subseteq \mathbb{Z}[\alpha]$ and $(s, p) \subseteq \mathbb{Z}[\beta]$ such that $r + s \equiv t \bmod p$, then $(r, p) | I_\alpha$ and $(s, p) | I_\beta$.*

Proof. If $(r + s, p)$ divides the ideal generated by $e + d(\alpha + \beta)$, then we have

$$e + d(r + s) \equiv 0 \bmod p.$$

Since $(d, e) = 1$, $p \nmid d$, so we can write $r \equiv -d^{-1}e - s \bmod p$. Thus, we have

$$\sum_{i=0}^{m} (-d)^i (e + dr)^{m-i} b_{m-i} \equiv b^m g(-d^{-1}e - r) \equiv b^m g(s) \equiv 0 \bmod p,$$

which proves that $(s, p) | (\chi_\beta)\mathbb{Z}[\beta]$. The proof of $(r, p) | (\chi_\alpha)\mathbb{Z}[\alpha]$ is completely analogous. □

Remark 4.7. We note that [10, Theorem 5] follows by Theorem 4.6, when the considered number fields are quadratic.

The norms over $\mathbb{Q}$ of the considered principal ideals are equal, hence even the exponents of the first-degree divisors of the given principal ideal may be read from the underlying extensions [2].

Lemma 4.8. *Let ξ, χ_α, and χ_β be defined as above, then their norms over $\mathbb{Q}$ are the same, namely,*

$$N_{\mathbb{Q}(\alpha+\beta)/\mathbb{Q}}(\xi) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\chi_\alpha) = N_{\mathbb{Q}(\beta)/\mathbb{Q}}(\chi_\beta).$$

Proof. It follows directly from (4) and the composition of norms (refer [11, Theorem VI.5.1]). □

Finally, we conclude this section by observing that for small extensions, we can prevent exceptional cases with a few assumptions. For instance, the following proposition describes a family of composite fields where the correspondence between the FDPIs is perfect, namely, exceptional cases never occur.

Proposition 4.9. *Let m be an odd integer, $\mathbb{Q}(\theta)$ be a Galois field of degree $2m$ and let $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ be its degree-2 and degree-m subfields, respectively. Let $d, e \in \mathbb{Z}$ be coprime and $I = (e + d\theta)\mathbb{Z}[\theta]$. Then, either $I \cap \mathbb{Z}[\alpha] = (0)$ or the FDPIs of $\mathbb{Z}[\theta]$ dividing I are precisely the combinations of FDPIs of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ dividing $I \cap \mathbb{Z}[\alpha]$ and $I \cap \mathbb{Z}[\beta]$, respectively.*

Proof. We first note that $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are normal extensions of coprime degrees, hence by Proposition 2.11 they are linearly disjoint.

On one side, by Proposition 3.10, every FDPI of $\mathbb{Z}[\theta]$ arises from a combination of $(r, p) \subseteq \mathbb{Z}[\alpha]$ and $(s, p) \subseteq \mathbb{Z}[\beta]$, and by Theorem 4.6, we know that $(r, p) | I_\alpha$ and $(s, p) | I_\beta$.

On the other side, assume that there are FDPIs $(r, p) | I_\alpha$ and $(s, p) | I_\beta$. In this case $p \nmid d$, otherwise

$$0 \equiv \mathrm{ev}_{\alpha \mapsto r}(\chi_\alpha) \equiv e^m,$$

which would contradict the coprimality of e and d. Since $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2$, χ_α is a linear polynomial in α. Thus, either $\chi_\alpha = 0$, or there is at most one solution $w \in \mathbb{F}_p$ to

$$\mathrm{ev}_{\alpha\mapsto w}(\chi_\alpha) = (-d)^m g(\phi(w)).$$

In the latter case, since $(r,p)|I_\alpha$ we conclude that $w = r$ is the unique zero of $\mathrm{ev}_{\alpha\mapsto w}(\chi_\alpha)$ over $\mathbb{F}_p$. Since ϕ is linear and $p\nmid d$, this implies that $s = \phi(r)$ is the unique root of $g \bmod p$, so Theorem 4.3 applies, proving that $(r+s,p)|I$. □

Proposition 4.9 notably applies for $k = 3$ on sextic extensions, which are widely studied for the GNFS optimization [19,20]. We observe that the normality condition is only necessary for ensuring that every first-degree prime of $\mathbb{Z}[\theta]$ is obtained via ideal combination, but it may be dropped whenever finding them all is not a requirement. This is usually the case in algorithmic practice, where we are only interested in efficiently finding plenty of them. Furthermore, in Section 5.3 we will computationally observe that the quantity of FDPIs one may miss by dropping the normality assumption is negligible, especially when their norm is large.

5 Computational improvement

In Sections 3 and 4, we proved that, apart from rare exceptions, we may compute FDPIs in composite extensions by addressing the same problem inside underlying subfields and composing the resulting solutions. This approach is particularly efficient for computing large sets of FDPIs in composite extensions with smooth degrees, although consistent time improvements may also be appreciated in the well studied degree-6 extensions.

In the present section, we discuss the time reduction obtained from such an approach, and we computationally evaluate the results with Magma [15][1].

5.1 Asymptotic complexity

We consider a number field $\mathbb{Q}(\theta) = \mathbb{Q}[x]/(h)$ obtained from the compositum of linearly disjoint number fields $\mathbb{Q}(\alpha_i) = \mathbb{Q}[x]/(f_i)$, and we compare the following approaches for finding FDPIs of $\mathbb{Z}[\theta]$ of norm p (Table 2).

The complexity of both algorithms depends on the complexity of computing the roots of a given degree-n polynomial over $\mathbb{F}_p$, which can be achieved via the renowned Berlekamp algorithm [16], or with more sophisticated approaches [17,18], whose asymptotic complexity depends on the relation between n and p. From a GNFS perspective, one is mostly interested in the asymptotic behavior of p, and the asymptotic complexity for the best-known algorithms when $p \to \infty$ is

$$O(n^{1+o(1)}\log p).$$

A random positive integer $\leq M$ is prime with probability $1/\log M$, and when it is prime, it requires $O(n^{1+o(1)}\log M)$ field operations to compute the first-degree primes of that norm. Thus, the computational cost of computing the FDPIs of norms $\leq M$ is expected to grow linearly with M.

In our setting, since the underlying extensions are linearly disjoint, if $n_i = \deg(f_i)$, then h may be obtained as an iterated resultant and it has degree $\deg(h) = \prod_i n_i$. Hence, the standard approach for finding first-degree primes in $\mathbb{Z}[\theta]$ of norms $\leq M$ should require $O(\deg(h)^{1+o(1)}M)$ field operations.

1 Our testing has been performed on a personal computer running Magma V2.25-3, CPU: Intel(R) Core(TM) i7-8565U @ 1.80GHz. The MAGMA implementation may be found on GitHub at https://github.com/DTaufer/First-degree-prime-ideals/blob/main/MagmaCode.m.

Table 2: Standard and composite approaches for finding FDPIs

Standard approach	Composite approach
Compute the roots $\mathcal{R}$ of $f \bmod p$	Compute the roots $\mathcal{R}_i$ of $f_i \bmod p$
Return $\{(r_j, p)\}_{r_j \in \mathcal{R}}$	Return $\{(\sum_j r_j, p)\}_{(r_j)_j \in \prod_j \mathcal{R}_j}$

On the other side, solving the same problem in the smaller subfields requires repeated roots finding of degree-n_i polynomials over the same base-field $\mathbb{F}_p$, each of which can be accomplished in $O(n_i^{1+o(1)}p)$ fields operations. Afterward, the solutions need to be composed, which requires at most $\prod_i n_i$ additions over $\mathbb{F}_p$, which does not depend on p so it is a constant factor we can neglect.

The above discussion implies that, for large values of p, the two approaches have the same asymptotic linear complexity. However, it also shows that by employing the composite approach we should expect an asymptotically linear reduction in time of about $\frac{\prod_i n_i}{\sum_i n_i}$. In Sections 5.2 and 5.3, we will computationally verify these estimates observing that, although linear, this improvement may actually be conspicuous even in small cases.

5.2 Degree-6 extensions

Here we consider degree-6 extensions, the degree that is often employed for the polynomial-selection phase of the GNFS [19,20]. In the sieving phase of such an algorithm, a large set of FDPIs has to be computed to construct the *algebraic factor base*.

Every degree-2 polynomial is normal, and constructing degree-3 normal polynomials is computationally effortless, hence we have decided to deal with degree-6 Galois extensions. This way, by Proposition 3.10, we are guaranteed that both approaches produce the same outcome.

We randomly selected ten instances of such extensions and computed the average time needed for the two aforementioned approaches to produce the FDPIs of norm $p \leq M$ for $M \leq 10^9$. The results are shown in Figure 1.

As discussed in Section 5.1, the computational time appears to increase linearly with M, and the composite approach proves to be faster by a factor ~ 1.5.

5.3 Extensions of smooth degrees

According to the complexity estimations of Section 5.1, the composite approach is expected to be notably faster whenever the degree of the composite extensions has small prime factors.

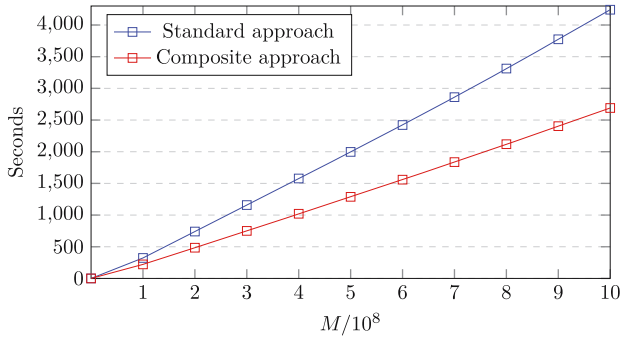

Figure 1: Time needed to compute FDPIs of norm up to M for a degree-6 defining polynomial.

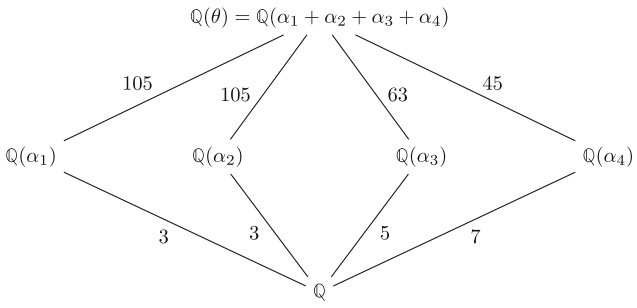

Figure 2: Lattice of the minimal fields in a number field of degree 315. The large extension is realized as the compositum of the small underlying fields.

We consider different number fields of degree $315 = 3^2 \times 5 \times 7$, which can be obtained from their linearly disjoint number sub-fields of small degrees, as shown in Figure 2.

A repeated application of Proposition 3.3 shows that we can compute the first-degree primes of $\mathbb{Z}[\theta]$ by simply composing those of each $\mathbb{Z}[\alpha_i]$. The time improvement with respect to the standard approach is noteworthy, as it is witnessed by Figure 3. In this case, the composite approach is ~39 times faster than the standard one.

In this setting, neither the degrees of the sub-fields are coprime nor the considered extensions are normal, so we should expect to miss a few first-degree primes. We have considered ten randomly generated degree-315 number fields and we have collected the number of ideals constructed with the two approaches in Table 3.

The number of ideals that the composite approach misses in the considered examples is irrelevant, especially when their norm increases. This is expected by Proposition 3.6, as explained in Remark 3.7.

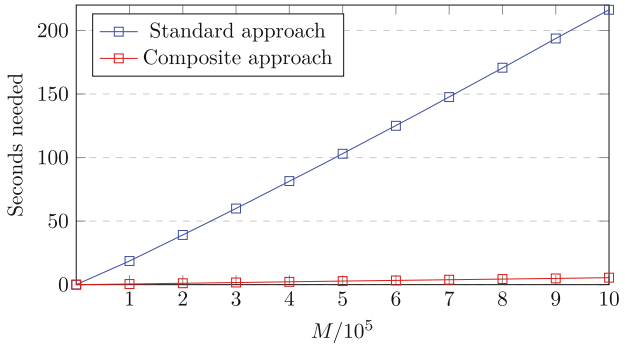

Figure 3: Time needed to compute FDPIs of norm up to M for a degree-315 defining polynomial.

Table 3: Number of norm-p FDPIs constructed with the different approaches

	p ranging from $i \cdot 10^7$ to $(i+1) \cdot 10^7$									
	$i = 0$	$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$	$i = 7$	$i = 8$	$i = 9$
Standard	94759	83520	80137	79167	76478	74732	71694	75699	73324	72671
Composite	94679	83518	80131	79166	76478	74732	71694	75698	73324	72671
Difference	80	2	6	1	0	0	0	1	0	0

6 Conclusion

We have analyzed the behavior of FDPIs in composite number fields in terms of those lying in the underlying extensions, and we have established huge families of cases where such correspondence is completely achieved. Moreover, we have studied the divisibility of special-shaped principal ideals in terms of the FDPIs of the underlying fields dividing the relative norms of the considered ideal.

Our work shows that, in most cases, the information on FDPIs of composite extensions can efficiently be read from the underlying fields. Thus, when designing algorithms that deal with FDPIs, one may conceivably work inside small and easy-to-handle fields to achieve results in more complex extensions. In fact, we demonstrated that knowing the behavior of such prime ideals inside prime-degree number fields is often sufficient and worthwhile.

The largest limitation of the current approach is the shape of minimal polynomials arising from the resultant construction, which is not always ideal for computational applications. For instance, several heuristical properties are usually required in the polynomial selection of the GNFS to speed up the successive phases [21]. However, other types of ideal combinations may be investigated to extend the additive linear combination proposed in this work. Indeed, we considered linearly disjoint number fields, whose generators α, β linearly combine to produce the generator $\theta = \alpha + \beta$ of the composite extension. This led to combining FDPIs by simply adding the first entries in their representations. If, instead, θ was given as a non-linear polynomial expression in the generators α, β, one could look for different types of ideal combinations, which may similarly allow us to read the properties of composite fields from those of their underlying subfields, while at the same time controlling the shape of the polynomial generating the composite extension.

Acknowledgements: The authors would like to thank professors Massimiliano Sala, Michele Elia, and Willem A. de Graaf for their useful advice and discussions, and the anonymous reviewer for the careful reading and observations. This work was presented at CIFRIS24, www.decifris.it/cifris24, the second congress of De Cifris.

Funding information: DT was supported in part by the European Union's H2020 Program, Grant number ERC-669891, and in part by the Research Foundation – Flanders (FWO), project 12ZZC23N.

Author contributions: All authors have equally contributed and accepted responsibility for the entire content of this manuscript.

Conflict of interest: The authors declare no conflicts of interest.

Data availability statement: The computational routines used to generate and analyze the data during the current study are available in the GitHub repository, https://github.com/DTaufer/First-degree-prime-ideals.

References

[1] Hilbert D. The theory of algebraic number fields. Berlin-Heidelberg: Springer; 1998.
[2] Buhler JP, Lenstra HW, Pomerance C. Factoring integers with the number field sieve. in: The development of the number field sieve. Berlin-Heidelberg: Springer; 1993. p. 50–94.
[3] Bernstein DJ, Lenstra AK. A general number field sieve implementation. in: The development of the number field sieve, Berlin-Heidelberg: Springer; 1993. p. 103–26.
[4] Lenstra AK, Lenstra HW, Manasse MS, Pollard JM. The number field sieve. in: The development of the number field sieve, Berlin-Heidelberg: Springer; 1993. p. 11–42.
[5] Gordon DM. Discrete logarithms in GF(p) using the number field sieve. SIAM J Discrete Math. 1993;6(1):124–38.
[6] Barbulescu R, Gaudry P, Kleinjung T. The tower number field sieve. ASIACRYPT 2015;2015:31–55.
[7] Joux A, Pierrot C. The special number field sieve in $\mathbb{F}_{p^n}$. in: Pairing-Based Cryptography - Pairing 2013; 2014. p. 45–61.
[8] Cohn PM. Algebra. Vol. 3. Wiley; 1991.

[9] Khanduja SK. The discriminant of compositum of algebraic number fields. Int J Number Theory. 2019;15(2):353–60.
[10] Santilli G, Taufer D. First-degree prime ideals of biquadratic fields dividing prescribed principal ideals. Mathematics. 2020;8(9):1433.
[11] Lang S. Algebra. New York: Springer; 2002.
[12] Isaacs IM. Degrees of sums in a separable field extension. Proc Am Math Soc. 1970;25(3):638–41.
[13] Cohen H. Advanced topics in computational number theory. New York: Springer; 2000.
[14] Lidl R, Niederreiter H. Finite fields. Cambridge: Cambridge University Press; 1996.
[15] Bosma W, Cannon J, Playoust C. The Magma algebra system. I. The user language.. J Symbolic Comput. 1997;24:235–65.
[16] Berlekamp ER, Factoring polynomials over large finite fields. Math Comp. 1970;24:713–35.
[17] Kaltofen E, Shoup V. Subquadratic-time factoring of polynomials over finite fields. Math Comp. 1998;67:1179–97.
[18] Kedlaya K, Umans C. Fast polynomial factorization and modular composition. SIAM J Comput. 2011;40(6):1767–802.
[19] Bai S, Thomé E, Zimmermann P. Factorisation of RSA-704 with CADO-NFS. 2012; hal-00760322.
[20] Kleinjung T, Aoki K, Franke J, Lenstra AK, Thomé E, Bos JS, et al. Factorization of a 768-bit RSA modulus. In: CRYPTO 2010; 2010. p. 333–50.
[21] Briggs ME. An introduction to the general number field sieve. Ph.D. Dissertation. Virginia Tech; 1998.