Article
First-Degree Prime Ideals of Biquadratic Fields Dividing Prescribed Principal Ideals

Giordano Santilli and Daniele Taufer *
Department of Mathematics, University of Trento, 38123 Trento, Italy; giordano.santilli@unitn.it
* Correspondence: daniele.taufer@gmail.com

Received: 31 July 2020; Accepted: 23 August 2020; Published: 26 August 2020

Abstract: We describe first-degree prime ideals of biquadratic extensions in terms of the first-degree prime ideals of two underlying quadratic fields. The identification of the prime divisors is given by numerical conditions involving their ideal norms. The correspondence between these ideals in the larger ring and those in the smaller ones extends to the divisibility of specially-shaped principal ideals in their respective rings, with some exceptions that we explicitly characterize.

Keywords: first-degree prime ideals; biquadratic extensions; ideal division

MSC: 11R04; 11R11; 11R16

1. Introduction

Biquadratic fields are numerical fields that have been studied extensively [1–6] and are currently in the spotlight as they provide examples of non-principal Euclidean ideal classes [7,8]. They are defined as numerical fields whose Galois group is the Klein group, and they can be obtained by the compositum of two quadratic fields, which is the construction we adopt in the present work.

In a general number field $\mathbb{Q}(\gamma)$, the special subring $\mathbb{Z}[\gamma]$ of the ring of integers plays an important role in applications, since their elements have a natural representation as integer-valued polynomials.

The study of the prime ideals of number field orders and conditions on the ideals they divide are common and often challenging goals in commutative algebra. These topics find a natural application in algebraic number theory, and they have been recently widely adopted for addressing concrete computational problems, such as integer factorization [9].

Among all the prime ideals, those of degree one have seen a fruitful employment in computational number theory. In fact, these first-degree prime ideals may be represented using elementary finite arithmetic and are consequently well suited for practical computing. This feature is crucial for the effectiveness of the general number field sieve (GNFS), which is the most efficient known algorithm to factorize large integers [10–12]. This algorithm searches for the factorization in first-degree prime ideals of a huge amount of specially-shaped principal ideals in an order of a number field, properly defined from the integer we intend to factorize.

In this paper, we start from a biquadratic field $\mathbb{Q}(\gamma)$, and we investigate the relation between the first-degree prime ideals in $\mathbb{Z}[\gamma]$ and the first-degree prime ideals of $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$, with $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ being two underlying quadratic fields.

$$\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha + \beta)$$

$$\mathbb{Q}(\alpha) \quad \mathbb{Q}(\beta)$$

$$\mathbb{Q}$$
Moreover, with their application to the GNFS in mind, we determine conditions under which these special primes in the biquadratic extension divide prescribed principal ideals in terms of their behavior in the quadratic extensions.

In Section 2, we recall the results we need on the structure of first-degree prime ideals. In Section 3, we provide an explicit relation between such ideals in \( \mathbb{Z}[\gamma] \) and those in \( \mathbb{Z}[\alpha] \) and \( \mathbb{Z}[\beta] \), which depends on their ideal norms. In Section 4, we extend this relation to the divisibility of principal ideals in their respective rings, with some exceptions that we explicitly highlight. In Section 5, we hint at applications and further research.

### 2. Notation and Preliminaries

Let \( \mathbb{Q}(\alpha) \) and \( \mathbb{Q}(\beta) \) be two distinct quadratic fields, i.e., \( a = \alpha^2 \) and \( b = \beta^2 \) have distinct non-trivial square-free parts. We may assume these number fields to be generated by the polynomials:

\[
f_a(x) = x^2 - a, \quad f_b(x) = x^2 - b,
\]

where \( a, b \in \mathbb{Z} \). It is well-known [5] that the biquadratic extension they generate is \( \mathbb{Q}(\gamma) \) with \( \gamma = \alpha + \beta \), whose minimal polynomial is:

\[
f_c(x) = x^4 - 2(a + b)x^2 + (a - b)^2.
\]

We denote by \( \mathcal{O} \) the ring of integers of the number field \( \mathbb{Q}(\theta) \), and we call one of its subrings \( A \) an order if \( \mathcal{O} : A \) is finite. In this setting, we focus on ideals in the order \( \mathbb{Z}[\theta] \), which has been deeply studied in [9].

**Definition 1.** Let \( \theta \) be an algebraic integer and \( a \) be a non-zero ideal of \( \mathbb{Z}[\theta] \). The norm of \( a \) is:

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

Moreover, a non-zero prime ideal \( p \) of \( \mathbb{Z}[\theta] \) is called a first-degree prime ideal if \( N(p) \) is a prime integer.

The following theorem characterizes the first-degree prime ideals of \( \mathbb{Z}[\theta] \).

**Theorem 1** ([9], p. 57). Let \( f \in \mathbb{Z}[\theta] \) be an irreducible monic polynomial and \( \theta \in \mathbb{C} \) one of its roots. Then, for every positive prime \( p \) there is a bijection between:

\[
\{(r, p) \mid r \in \mathbb{Z}/p\mathbb{Z} \text{ such that } f(r) \equiv 0 \mod p\}
\]

and:

\[
\{p \mid p \in \text{Spec } \mathbb{Z}[\theta] \text{ such that } N(p) = p\}.
\]

In the above bijections, an ideal \( p \) corresponds to \( (r, p) \) if it is the kernel of the evaluation-in-\( r \) ring morphism:

\[
\pi_\theta : \mathbb{Z}[\theta] \rightarrow \mathbb{Z}/p\mathbb{Z}, \quad a + b\theta \mapsto a + br \mod p.
\]

This function allows us to treat these abstract objects simply as pairs of integers, satisfying the property described in Theorem 1. Such an identification has two consequences: from a theoretical side, we can prove the properties of first-degree prime ideals by only dealing with elementary arithmetic, while on the applied side, they may be stored and systematically processed without dedicated software.

The following is an explicit example that shows how to establish the above bijection. It also highlights that different subrings of \( \mathcal{O} \) may exhibit different behavior in terms of their first-degree prime ideals.

---

*This is a continuation of a longer discussion on the application of algebraic number theory to cryptography, specifically focusing on the GNFS, and the properties of first-degree prime ideals in biquadratic extensions.*
Example 1. Let \( f_2 = x^2 - 2 \) and \( f_{50} = x^2 - 50 \), and let \( \mathbb{Q}(\sqrt{2}) \) and \( \mathbb{Q}(\sqrt{50}) \) be the quadratic number fields they generate. These two fields are clearly isomorphic, and so are their rings of integers. However, the first-degree prime ideals in the two orders \( \mathbb{Z}[\sqrt{2}] \) and \( \mathbb{Z}[\sqrt{50}] \) are different: indeed, let us consider:

\[
I = (5, \sqrt{50}) \subseteq \mathbb{Z}[\sqrt{50}].
\]

This ideal is the kernel of the ring morphism \( \pi_{\sqrt{50}} : \mathbb{Z}[\sqrt{50}] \to \mathbb{Z}/5\mathbb{Z}, a + b\sqrt{50} \mapsto a \mod 5 \); therefore, \( N(I) = 5 \), and it corresponds to the pair \((0, 5)\) by means of Theorem 1.

On the other side, the same theorem ensures that there cannot be any first-degree prime ideals of norm five in \( \mathbb{Z}[\sqrt{2}] \), since two is not a quadratic residue modulo five.

In the following sections, we will use these bijections as identifications.

Divisibility of Principal Ideals Inside Non-Maximal Orders

It is a standard fact \([13]\) that non-zero ideals factor uniquely into primes in the whole ring of integers; however, it is possible to generalize this decomposition even inside non-maximal orders \( \mathbb{Z}[\theta] \) following \([9]\).

Proposition 1 \([9], \text{Proposition 7.1}\). Let \( A \) be an order of a number field \( \mathbb{Q}(\theta) \). For each prime \( p \) of \( A \), there exists a unique group homomorphism:

\[
l_{p, A} : \mathbb{Q}(\theta)^* \to \mathbb{Z},
\]

such that the following hold:

(i) For all non-zero \( x \in A \), we have \( l_{p, A}(x) \geq 0 \);
(ii) For all non-zero \( x \in A \), then \( l_{p, A}(x) > 0 \) if and only if \( x \in p \);
(iii) For each \( x \in \mathbb{Q}(\theta)^* \), then \( l_{p, A}(x) = 0 \) for all but a finite number of \( p \), and:

\[
\prod_{p \in \text{Spec } A} N(p)^{l_{p, A}(x)} = |N(x)|,
\]

where \( N(x) \) is the norm of the element \( x \) in the field \( \mathbb{Q}(\theta) \).

When \( A = \mathcal{O} \) is the maximal order, the functions \( l_{p, A}(x) \) coincide with the exponents appearing in the prime factorization of the principal ideal \( (x) \subseteq \mathcal{O} \). In general, these functions are related to those of larger orders by the following proposition.

Proposition 2 \([9], \text{Proposition 7.2}\). Let \( A \) and \( B \) be orders of \( \mathcal{O} \) such that \( A \subset B \). For every \( p \in \text{Spec } A \), we have:

\[
l_{p, A}(x) = \sum_{q | p} \left[ B : A \right] l_{q, B}(x),
\]

where this sum ranges over all the primes \( q \) of \( B \), such that \( p = q \cap A \).

In this work, we apply these results with \( A = \mathbb{Z}[\theta] \) and \( B = \mathcal{O} \) in order to find first-degree prime factors of the principal ideals generated by \( n + m\theta \), for any pair of coprime integers \( (n, m) \). Under these assumptions, the following result is particularly useful.

Corollary 1 \([9], \text{Corollary 5.5}\). Let \( n, m \) be coprime integers, and let \( p \) be a prime of \( \mathbb{Z}[\theta] \). If \( p \) is not a first-degree prime ideal, then \( l_{p, \mathbb{Z}[\theta]}(n + m\theta) = 0 \). Otherwise, if \( p \) is a first-degree prime ideal corresponding to the pair \((r, p)\), then:
In this setting, the number \( l_{p,\mathbb{Z}[\theta]}(n + m\theta) \) counts the number of times \( p \) divides \( \langle n + m\theta \rangle \). Moreover, Corollary 1 implies that prime divisors of these particular ideals in \( \mathbb{Z}[\theta] \) are all first-degree prime ideals with different norms. However, this does not imply that one can completely factorize a prescribed principal ideal in non-maximal orders, such as \( \mathbb{Z}[\theta] \). The following example portrays this scenario and emphasizes the link between the factorization in \( \mathbb{Z}[\theta] \) and that in \( \mathcal{O} \), as prescribed by the previous results.

**Example 2.** Let \( f = x^2 + 3 \) define the quadratic field \( \mathbb{Q}(\sqrt{-3}) \). It is well known [14] (Theorem 3.2) that in this situation, \( [\mathcal{O} : \mathbb{Z}[\sqrt{-3}]] = 2 \). Let us consider its element \( x = 1 + \sqrt{-3} \), and let \( I = x\mathcal{O} \) and \( \mathcal{T} = x\mathbb{Z}[\sqrt{-3}] \) be the principal ideals it generates. We observe that:

\[ I \subseteq \mathcal{T} \cap \mathbb{Z}[\sqrt{-3}], \]

as it may be checked that \( 2 \in (I \cap \mathbb{Z}[\sqrt{-3}]) \setminus \mathcal{T} \).

We notice that \( I \) is prime with norm four; hence, it is not a first-degree prime. Thus, as remarked after Proposition 1, we trivially have:

\[ l_{I,\mathcal{O}}(x) = 1. \]

On the other side, the ideal \( \mathcal{T} \) is not prime, and its norm is four. From Theorem 1, the only first-degree prime ideal with the norm equal to two is the one corresponding to the pair \((1, 2)\), which is actually the ideal \( \mathcal{T} = (2, 1 + \sqrt{-3}) \subseteq \mathbb{Z}[\sqrt{-3}] \). Moreover, \( x \in \mathcal{T} \), then \( \mathcal{T} \) divides \( \mathcal{I} \), and Corollary 1 gives:

\[ l_{\mathcal{T},\mathbb{Z}[\sqrt{-3}]}(x) = 2. \]

Furthermore, the same corollary also guarantees that \( \mathcal{I} \) is the only first-degree prime ideal dividing \( \mathcal{T} \). This agrees with Proposition 2, since \( I \cap \mathbb{Z}[\sqrt{-3}] = \mathcal{I} \), then:

\[ [\mathcal{O} : I] : [\mathbb{Z}[\sqrt{-3}] : \mathcal{I}] \simeq [\mathcal{F}_4 : \mathcal{F}_2] = 2. \]

In conclusion, the usual ideal factorization of \( I \) in \( \mathcal{O} \) provides all the prime factors of \( \mathcal{T} \) in \( \mathbb{Z}[\sqrt{-3}] \), although these do not produce a complete factorization for \( \mathcal{T} \).

### 3. First-Degree Prime Ideals of Biquadratic Extensions

The following theorem exhibits, by means of Theorem 1, how to construct first-degree prime ideals of a given norm in a biquadratic field by knowing first-degree prime ideals of the same norm in two of its quadratic subfields.

**Theorem 2.** Let \((r, p)\) be a first-degree prime ideal of \( \mathbb{Z}[\alpha] \) and \((s, p)\) a first-degree prime ideal of \( \mathbb{Z}[\beta] \). Then, \((r + s, p)\) is a first-degree prime ideal of \( \mathbb{Z}[\gamma] \).

**Proof.** By the hypothesis, we have:

\[
\begin{align*}
  f_a(r) & = r^2 - a \equiv 0 \mod p, \\
  f_b(s) & = s^2 - b \equiv 0 \mod p.
\end{align*}
\]

By plugging \( r + s \) into \( f_c \), we get:
\[
\begin{align*}
\phi_c(r+s) &= (r+s)^4 - 2(a+b)(r+s)^2 + (a-b)^2 \\
&\equiv (r+s)^4 - 2(r^2 + s^2)(r+s)^2 + (r^2 - s^2)^2 \mod p \\
&\equiv (r+s)^2((r+s)^2 - 2(r^2 + s^2) + (r-s)^2) \mod p \\
&\equiv 0 \mod p.
\end{align*}
\]

Therefore, \((r+s,p)\) is a first-degree prime ideal of \(\mathbb{Z}[\gamma]\). \(\square\)

We will refer to \((r+s,p) \subseteq \mathbb{Z}[\gamma]\) as the combination of the ideals \((r,p) \subseteq \mathbb{Z}[\alpha]\) and \((s,p) \subseteq \mathbb{Z}[\beta]\). Now, we prove that the ideals constructed as combinations are almost all the first-degree prime ideals of \(\mathbb{Z}[\gamma]\).

**Theorem 3.** Let \((t,p)\) be a first-degree prime ideal of \(\mathbb{Z}[\gamma]\). If either \(p = 2\) or \(t \equiv 0 \mod p\), then there exists a unique pair \(r,s \in \mathbb{Z}/p\mathbb{Z}\) such that \(t \equiv r+s \mod p\) and \((r,p),(s,p)\) are first-degree prime ideals of \(\mathbb{Z}[\alpha]\) and \(\mathbb{Z}[\beta]\), respectively.

**Proof.** We treat separately the cases \(p = 2\) and \(p \) odd, explicitly exhibiting such a pair \((r,s)\) in both cases.

- **Case: \(p = 2\).**
  
  Since in \(\mathbb{Z}/2\mathbb{Z}\), every element is equal to its square, the only choice of \(r,s \in \mathbb{Z}/2\mathbb{Z}\) satisfying:
  
  \[
  \begin{cases}
  r^2 - a \equiv 0 \mod 2, \\
  s^2 - b \equiv 0 \mod 2,
  \end{cases}
  \]
  
  is \((r,s) = (a,b)\), which also satisfies \(t = r+s\) because:
  
  \[0 \equiv f_c(t) \equiv t^4 - 2(a+b)t^2 + (a-b)^2 \equiv t + a + b \mod 2.\]

- **Case: \(p \neq 2\) and \(t \neq 0\).**
  
  In this case, \(2t\) is invertible in \(\mathbb{Z}/p\mathbb{Z}\), then we can define \(r_1 = \frac{t^2 + a - b}{2t}\). We notice that from \(f_c(t) \equiv 0 \mod p\), we have:
  
  \[
  r_1^2 = \left(\frac{t^2 + a - b}{2t}\right)^2 = \frac{t^4 + 2at^2 - 2bt^2 + a^2 - 2ab + b^2}{4t^2} \equiv \frac{f_c(t) + 4at^2}{4t^2} \equiv a \mod p.
  \]
  
  Thus, \(r_1\) is a square root of \(a\) modulo \(p\), and since \(\mathbb{Z}/p\mathbb{Z}\) is a finite field, there are at most two solutions to \(r^2 - a \equiv 0 \mod p\); hence, these are:
  
  \[r_1 = \frac{t^2 + a - b}{2t}, \quad r_2 = -r_1 = -\frac{t^2 + a - b}{2t}.\]

  Similarly, there are only two possible values for \(s\), which are:
  
  \[s_1 = \frac{t^2 - a + b}{2t}, \quad s_2 = -s_1 = -\frac{t^2 - a + b}{2t}.\]
It is easy to verify that \( r_1 + s_1 = t \), and we now prove that \((r_1, s_1)\) is in fact the unique choice for such a pair \((r, s)\) in order to satisfy \( r + s = t \).

First, we notice that \((r, s) = (r_2, s_2)\) is not a possible option, since in this case, \( r_2 + s_2 = -t \), but \(-t \not\equiv t \mod p\) since \( p \neq 2 \) and \( t \not\equiv 0 \mod p \).

To conclude the proof, we show that \((r_1, s_2)\) may be a suitable choice only when \( s_1 = s_2 = 0 \); therefore, \((r_1, s_2) = (r_1, s_1)\). Suppose that \( r_1 + s_2 = t \), which means \( a = b = t^2 \). Then:

\[
0 \equiv f_c(t) \equiv 2t^2(t^2 - a - b) \mod p.
\]

Since \( 2t^2 \not\equiv 0 \mod p \), we get \( a + b \equiv t^2 \mod p \), then \( a \equiv t^2 \mod p \) and \( b \equiv 0 \mod p \). This proves that \( s_1 = s_2 = 0 \).

The same argument shows that \((r_2, s_1)\) is a valid pair only if \( r_1 = r_2 = 0 \) so \((r_2, s_1) = (r_1, s_1)\).

In conclusion, there is only one working pair, that is \((r, s) = (r_1, s_1)\).

The uniqueness part of Theorem 3 states that any ideal \((t, p)\) of \( \mathbb{Z} [\gamma] \) with \( t \neq 0 \) may be determined without repetitions from first-degree prime ideals of two underlying quadratic fields. The only ideals left are those of the form \((0, p)\) for \( p \neq 2 \), which are examined in the following proposition.

**Proposition 3.** Let \((0, p)\) be a first-degree prime ideal of \( \mathbb{Z} [\gamma] \) and \( r \in \mathbb{Z} / p\mathbb{Z} \), then the following are equivalent:

- \( f_a(r) \equiv 0 \mod p, \)
- \( f_b(r) \equiv 0 \mod p, \)
- \((r, p)\) and \((-r, p)\) are first-degree prime ideals of \( \mathbb{Z} [\alpha], \)
- \((r, p)\) and \((-r, p)\) are first-degree prime ideals of \( \mathbb{Z} [\beta]. \)

**Proof.** From \( f_c(0) \equiv 0 \mod p \), we get:

\[
(a - b)^2 \equiv 0 \mod p \implies a \equiv b \mod p.
\]

Hence, \( f_a \equiv f_b \mod p \); therefore, \( r \) is a root of \( f_a \) modulo \( p \) if and only if the same holds for \( f_b \). Moreover, if \( f_a(r) \equiv 0 \mod p \), also \( f_b(-r) \equiv 0 \mod p \), implying that \((\pm r, p)\) are first-degree prime ideals of \( \mathbb{Z} [\alpha], \) while the converse is trivial.

**Remark 1.** The above proposition is trivial for \( p = 2 \). In fact, by Theorem 3, if \((0, 2)\) is a first-degree prime ideal of \( \mathbb{Z} [\gamma] \), then all the above equivalent conditions are satisfied for \( r = a \).

According to Proposition 3, one of the following situations takes place, depending on the number \( \nu \) of roots of \( f_a \) modulo \( p \):

- \( \nu = 0: \) \((0, p) \subset \mathbb{Z} [\gamma] \) cannot be found as a combination of first-degree prime ideals of \( \mathbb{Z} [\alpha] \) and \( \mathbb{Z} [\beta], \)
- \( \nu = 1: \) \((0, p) \subset \mathbb{Z} [\gamma] \) is the combination of \((0, p) \subset \mathbb{Z} [\alpha] \) and \((0, p) \subset \mathbb{Z} [\beta], \)
- \( \nu = 2: \) \((0, p) \subset \mathbb{Z} [\gamma] \) is determined by two different combinations of first-degree prime ideals of \( \mathbb{Z} [\alpha] \) and \( \mathbb{Z} [\beta], \)

In the following example, we see that all the above cases may actually occur.

**Example 3.** Let \( \alpha = x^2 - 50 \) and \( \beta = x^2 - 155 \) generate the quadratic fields \( \mathbb{Q} (\alpha) \) and \( \mathbb{Q} (\beta), \) so that the composite biquadratic field \( \mathbb{Q} (\gamma) \) is generated by the polynomial \( f_c = x^4 - 410x^2 + 11025. \)

The unique first-degree prime ideal in \( \mathbb{Z} [\gamma] \) with norm \( p = 3 \) is \((0, 3), \) but there are no such ideals in \( \mathbb{Z} [\alpha] \) or in \( \mathbb{Z} [\beta], \) then \((0, 3)\) cannot be a combination of any of them.

The unique first-degree prime ideal of norm \( p = 5 \) in \( \mathbb{Z} [\gamma] \) is \((0, 5), \) which is determined uniquely as a combination of the ideals \((0, 5) \) in \( \mathbb{Z} [\alpha] \) and \((0, 5) \) in \( \mathbb{Z} [\beta]. \)
There are three first-degree prime ideals of norm \( p = 7 \) in \( \mathbb{Z}[\gamma] \): \((0,7), (2,7), \) and \((5,7)\). The first-degree prime ideals of the same norm for both \( \mathbb{Z}[\alpha] \) and \( \mathbb{Z}[\beta] \) are \((1,7), (6,7)\). As prescribed by Theorem 3, we observe that \((2,7), (5,7)\) are uniquely determined by the combinations of \((1,7), (1,7)\) and \((6,7), (6,7)\), whereas \((0,7)\) arises from both the combinations of \((1,7), (6,7)\) and \((6,7), (1,7)\).

4. Division of Prescribed Principal Ideals

In this section, we consider a special family of principal ideals of \( \mathbb{Z}[\gamma] \), and we study its first-degree prime divisors in terms of first-degree prime ideals dividing its intersections with \( \mathbb{Z}[\alpha] \) and \( \mathbb{Z}[\beta] \). This particular class of ideals is of great interest, since they are the ones usually employed in applications [9]. We begin by characterizing these intersections, as in the following proposition.

**Proposition 4.** Let \( n \neq m \) be coprime integers, and let \( I = (n + m\gamma) \subseteq \mathbb{Z}[\gamma] \). Then, \( I \cap \mathbb{Z}[\alpha] \) is a principal ideal of \( \mathbb{Z}[\alpha] \) generated by:

\[
I \cap \mathbb{Z}[\alpha] = \left\langle (n + m\alpha + m\beta)(n + m\alpha - m\beta) \right\rangle.
\]

**Proof.** We prove both inclusions.

(\(\supseteq\)) The generator \((n + m\alpha + m\beta)(n + m\alpha - m\beta)\) is an element of \( I \) and is equal to

\[
(n + m\alpha)^2 - (m\beta)^2 = n^2 + m^2(a - b) + 2nm\alpha,
\]

which belongs to \( \mathbb{Z}[\alpha] \).

(\(\subseteq\)) Any element \( x \in I \) may be written as:

\[
x = (n + m\alpha + m\beta)(\lambda_0 + \lambda_1\alpha + \lambda_2\beta + \lambda_3\alpha\beta),
\]

for some \( \lambda_0, \ldots, \lambda_3 \in \mathbb{Z} \). Since \( \{1, \alpha, \beta, \alpha\beta\} \) is a \( \mathbb{Q} \)-basis of \( \mathbb{Z}[\gamma] \) [5], then \( x \in \mathbb{Z}[\alpha] \) if and only if its coefficients \( \beta \) and \( \alpha\beta \) are zero, which amounts to:

\[
m\lambda_0 + n\lambda_2 + m\lambda_3 = 0, \quad m\lambda_1 + m\lambda_2 + n\lambda_3 = 0. \tag{1}
\]

From Equation (1), we get:

\[
\lambda_0 + \lambda_1\alpha + \lambda_2\beta + \lambda_3\alpha\beta = - \left( \frac{n}{m} \lambda_2 + a\lambda_3 \right) - a \left( \lambda_2 + \frac{n}{m} \lambda_3 \right) + m\beta \left( \frac{\lambda_2 + \lambda_3\alpha}{m} \right)
\]

\[
= (n + m\alpha - m\beta) \left( - \frac{\lambda_2 + \lambda_3\alpha}{m} \right).
\]

Moreover, since \( (m,n) = 1 \), then Equation (1) also implies that \( m \) divides both \( \lambda_2 \) and \( \lambda_3 \). Hence, we conclude that any \( x \in I \cap \mathbb{Z}[\alpha] \) belongs to the principal ideal generated in \( \mathbb{Z}[\alpha] \) by the element \((n + m\alpha + m\beta)(n + m\alpha - m\beta)\). \(\square\)

With the following theorems, we prove that the divisibility is stable under combination except for an exceptional case.

**Theorem 4.** Let \( n \neq m \) be coprime integers and \( I = (n + m\gamma) \) be a principal ideal of \( \mathbb{Z}[\gamma] \). Let us assume that there are the \( (r, p) \) first-degree prime ideal of \( \mathbb{Z}[\alpha] \) dividing \( I_4 = I \cap \mathbb{Z}[\alpha] \) and the \( (s, p) \) first-degree prime ideal of \( \mathbb{Z}[\beta] \) dividing \( I_0 = I \cap \mathbb{Z}[\beta] \). Then, \( (r + s, p) \) is a first-degree prime ideal of \( \mathbb{Z}[\gamma] \) dividing \( I \) unless the following conditions simultaneously hold:

\[
p \neq 2, \quad n \equiv 0 \mod p, \quad r + s \equiv 0 \mod p.
\]
Proof. By Theorem 2, \((r + s, p)\) is a first-degree prime ideal of \(\mathbb{Z}[\gamma]\), then it is sufficient to show that under the aforementioned conditions, we obtain:

\[
n + m(r + s) \equiv 0 \mod p, \tag{2}
\]

which proves that \(I = (n + m\gamma) \subseteq \ker \pi = (r + s, p)\), hence \((r + s, p) | I\).

- Case: \(p = 2\).
  
  By Proposition 4, a generator of \(I_a\) in \(\mathbb{Z}[\alpha]\) is \(g = n^2 + m^2(a - b) + 2nma\); therefore:
  
  \[
  \pi_a(g) = n^2 + m^2(a - b) + 2nmr \equiv n + m(a^2 + b^2) \equiv n + m(r + s) \mod 2.
  
  Thus, either (2) is satisfied or \(\pi_a(g) \equiv 1 \mod 2\), which implies that there are no first-degree prime ideals \((r, 2)\) dividing \(I_a\).

- Case: \(p \neq 2\) and \(n \not\equiv 0 \mod p\).
  
  By Proposition 4, we have:
  
  \[
  \begin{align*}
  I_a & = (n^2 + m^2(a - b) + 2nma) \subseteq \mathbb{Z}[\alpha], \\
  I_b & = (n^2 + m^2(b - a) + 2nm\beta) \subseteq \mathbb{Z}[\beta].
  \end{align*}
  
  Since \(\ker \pi_a = (r, p) \mid I_a\) and \(\ker \pi_\beta = (s, p) \mid I_b\), then:
  
  \[
  \begin{align*}
  n^2 + m^2(a - b) + 2nmr & \equiv 0 \mod p, \\
  n^2 + m^2(b - a) + 2nms & \equiv 0 \mod p.
  \end{align*}
  
  Summing the above relations, we get:
  
  \[
  2n[n + m(r + s)] \equiv 0 \mod p.
  
  Since \(2n \not\equiv 0 \mod p\), this implies (2).

- Case: \(p \neq 2\), \(n \equiv 0 \mod p\) and \(r + s \equiv 0 \mod p\).
  
  In this case, (2) is trivially satisfied.

Thus, we conclude that \((r + s, p)\) is a first-degree prime ideal of \(\mathbb{Z}[\gamma]\) dividing \(I\) except for the case \(p \neq 2\), \(n \equiv 0 \mod p\), and \(r + s \not\equiv 0 \mod p\). \(\square\)

The next example shows that in the exceptional case mentioned above, the ideal combination may not maintain divisibility.

Example 4. Let \(f_a = x^2 + 4\) and \(f_b = x^2 - 6\) generate the quadratic fields \(\mathbb{Q}(\alpha)\) and \(\mathbb{Q}(\beta)\), so that the composite biquadratic field \(\mathbb{Q}(\gamma)\) is generated by the polynomial \(f_c = x^4 - 4x^2 + 100\).

The first-degree prime ideals of \(\mathbb{Z}[\gamma]\) with norm \(p = 5\) are \((0, 5)\), \((2, 5)\), and \((3, 5)\), while those of \(\mathbb{Z}[\alpha]\) and \(\mathbb{Z}[\beta]\) are \((1, 5)\) and \((4, 5)\).

Let \(I\) be the principal ideal \((5 + \gamma) \subseteq \mathbb{Z}[\gamma]\). By Proposition 4, we have:

\[
I_a = (15 + 10\alpha) \subseteq \mathbb{Z}[\alpha], \quad I_b = (35 + 10\beta) \subseteq \mathbb{Z}[\beta].
\]

It is easy to see that both \((1, 5)\) and \((4, 5)\) divide \(I_a\) and \(I_b\). Besides, the combination of \((1, 5)\) with \((4, 5)\) is \((0, 5)\), which divides \(I\). However, the other options are exceptional, since the combination between \((1, 5)\) and \((1, 5)\) is \((2, 5)\), which does not divide \(I\). The same holds for \((3, 5)\), which is the combination of \((4, 5)\) with \((4, 5)\).
On the other hand, whenever a first-degree prime ideal of $\mathbb{Z}[\gamma]$ dividing a given principal ideal $I$ is obtained as a combination of two first-degree prime ideals, they divide the intersections of $I$ with $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$.

**Theorem 5.** Let $n$ and $m \neq 0$ be coprime integers, $I = (n + m\gamma) \subseteq \mathbb{Z}[\gamma]$, and let $(t, p)$ be a first-degree prime ideal dividing $I$. If there exist first-degree prime ideals $(r, p) \subseteq \mathbb{Z}[\alpha]$ and $(s, p) \subseteq \mathbb{Z}[\beta]$ such that $r + s \equiv t \mod p$, then $(r, p)$ divides $I_a = I \cap \mathbb{Z}[\alpha]$ and $(s, p)$ divides $I_b = I \cap \mathbb{Z}[\beta]$.

**Proof.** If these ideals exist, from $(t, p) \mid I$, we get:

$$0 \equiv n + mt \equiv n + mr + ms \mod p.$$

Let $g_a = n^2 + m^2(a - b) + 2nma$ be a generator of $I_a$ and $g_b = n^2 + m^2(b - a) + 2nmb$ be a generator of $I_b$. From the above equation, we have:

$$\pi_a(g_a) = n^2 + m^2(a - b) + 2nma \equiv n^2 + m^2(a - b) + 2n(-n - ms) \mod p$$

$$\equiv -n^2 - m^2(-a + b) - 2nms \equiv -\pi_b(g_b) \mod p.$$

Hence, since $\pi_a(g_a)$ vanishes if and only if $\pi_b(g_b)$ does, it is sufficient to show that $(r, p) \mid I_a$.

Substituting $n = -mr - ms$, $r^2 \equiv a \mod p$, and $s^2 \equiv b \mod p$, we get:

$$\pi_a(g_a) \equiv (-mr - ms)^2 + m^2(r^2 - s^2) + 2(-mr - ms)mr \equiv 0 \mod p;$$

therefore, $(r, p) \mid I_a$. □

The following corollary enhances the previous result in the generic case.

**Corollary 2.** Let $n$ and $m \neq 0$ be coprime integers, $I = (n + m\gamma) \subseteq \mathbb{Z}[\gamma]$, and let $(t, p)$ be a first-degree prime ideal dividing $I$, with $t \neq 0$ if $p \neq 2$. Then, there exist two unique first-degree prime ideals $(r, p) \subseteq \mathbb{Z}[\alpha]$ and $(s, p) \subseteq \mathbb{Z}[\beta]$ such that $(r, p)$ divides $I \cap \mathbb{Z}[\alpha]$, $(s, p)$ divides $I \cap \mathbb{Z}[\beta]$, and $r + s \equiv t \mod p$.

**Proof.** This follows immediately from Theorem 5 and Theorem 3. □

**Remark 2.** For completeness, we discuss the case $m = 0$, so that $I = (n) \subseteq \mathbb{Z}[\gamma]$. Both intersections of this principal ideal with $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are equal to $(n)$, and for every, $t \in \mathbb{Z} / p\mathbb{Z}$, we have

$$(t, p) \mid (n) \iff n \equiv 0 \mod p.$$

Thus, all or none of the pairs $\{ (t, p) \mid f_c(t) \equiv 0 \mod p \}$ divide $(n) \subset \mathbb{Z}[\gamma]$, so it is still true that the combination preserves divisibility, but in general not uniquely.

### 5. Applications and Further Work

In this work, we show how two first-degree prime ideals in quadratic extensions may be combined to obtain a first-degree prime ideal in the corresponding biquadratic extension lying over them. In addition, this correspondence is proven to preserve the division of prescribed first-degree prime ideals, except for some sporadic, though well-determined, cases.

Nonetheless, further computations suggest that our results might also be extended to more general number fields, possibly requiring additional hypotheses. Such a generalization could be repeatedly applied in order to characterize first-degree prime ideals of a given norm in large extensions: the (at most) $d_1d_2$ first-degree prime ideals of a composite extension may be seen as combinations of $d_1 + d_2$ such ideals into smaller subrings, which are much more convenient to be stored and managed.
Among other applications, first-degree prime ideals are employed in the general number field sieve, where a large number of them are needed to factorize some principal ideals. Even if biquadratic extensions may not be optimal for this algorithm [15,16], a more general form of our results on an ideal combination could lead to better computational performance.

Finally, from a theoretical point of view, it may be worth investigating which algebraic properties are preserved, as happens for divisibility, by first-degree prime ideals’ combination.

Author Contributions: All authors contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors wish to thank professors Massimiliano Sala and Michele Elia for their useful comments and suggestions.

Conflicts of Interest: The authors declare no conflict of interest.

References
1. Bae, S.; Yue, Q. Hilbert genus fields of real biquadratic fields. Ramanujan J. 2011, 24, 161–181. [CrossRef]
2. Dwilewicz, R.; Minč, J.; Schultz, A.; Swallow, J. Hilbert 90 for Biquadratic Extensions. Am. Math. Mon. 2017, 114, 577–587. [CrossRef]
3. Mamoona, S.; Yoshifumi, K.; Toru, N. Monogenicity of Biquadratic Fields Related to Dedekind-Hasse’s Problem. Punjab Univ. J. Math. 2015, 47, 77–82.
4. Ouyang, Y.; Zhang, Z. Hilbert genus fields of biquadratic fields Ramanujan J. 2015, 37, 345–363. [CrossRef]
5. Williams, K.S. Integers of biquadratic fields. Canad. Math. Bull. 1970, 13, 519–526. [CrossRef]
6. Yue, Q. Genus fields of real biquadratic fields. Ramanujan J. 2010, 21, 17–25. [CrossRef]
7. Chattopadhyay, J.; Muthukrishnan, S. Biquadratic fields having a non-principal euclidean ideal class. J. Number Theory 2019, 204, 99–112. [CrossRef]
8. Hu, S.; Yan, L. A new family of biquadratic fields having a non-principal euclidean ideal class. arXiv 2019, arXiv:1907.10850.
9. Buhler, J.P.; Lenstra, H.W.; Pomerance, C. Factoring integers with the number field sieve. In The Development of the Number Field Sieve; Springer: Berlin/Heidelberg, Germany, 1993; pp. 50–94.
10. Lenstra, A.K.; Lenstra, W.H.J. The Development of the Number Field Sieve; Springer Science & Business Media: Berlin/Heidelberg, Germany, 1993.
11. Lenstra, A.K.; Lenstra, W.H.J.; Manasse, M.S.; Pollard, J.M. The number field sieve. In Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing, ACM, Baltimore, MD, USA, 14–16 May 1990; pp. 564–572.
12. Kleijn, T.; Aoki, K.; Franke, J.; Lenstra, A.K.; Thomé, E.; Bos, J.W.; Gaudry, P.; Kruppa, A.; Montgomery, P.L.; Osvik, D.A.; et al. Factorization of a 768-bit RSA modulus, In Annual Cryptology Conference; Springer: Berlin/Heidelberg, Germany, 2010; pp. 333–350.
13. Dedekind, R. Theory of Algebraic Integers; Cambridge University Press: Cambridge, UK, 1996.
14. Stewart, I.; Tall, D. Algebraic Number Theory; AK Peters/CRC Press: Boca Raton, FL, USA, 2001.
15. Kleijn, T. On polynomial selection for the general number field sieve. Math. Comp. 2006, 75, 2037–2047. [CrossRef]
16. Murphy, B. Modelling the yield of number field sieve polynomials, In International Algorithmic Number Theory Symposium; Springer: Berlin/Heidelberg, Germany, 1998; pp. 137–150.