Università degli Studi Roma Tre

Dipartimento di Matematica e Fisica

PhD Thesis in Mathematics

by

Antonio Cigliola

Split quaternions, generalized quaternions and integer-valued polynomials

Supervisor

Prof. Francesca Tartarone

ACADEMIC YEAR 2013-2014

Contents

To my parents

Introduction

In 1843, sir R. Hamilton introduced the algebra of the *real quaternions* in order to give a geometric interpretation of the 3-dimensional Euclidean real space. He wanted to replicate what Gauss did with complex numbers and the Euclidean plane over the real numbers. In this way Hamilton obtained the 4-dimensional real division algebra $\mathbb{H}_{\mathbb{R}} = \{a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \mid a, b, c, d \in \mathbb{R},\ \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{i}\,\mathbf{j}\,\mathbf{k} = -1\}$ (cf. Section 1.2). The key of Hamilton's work is the interpretation of the multiplication of the imaginary units as the wedge product of the canonical basis $\left\{ \vec{i}, \vec{j}, \vec{k} \right\}$ of the 3-dimensional Euclidean space.

Some years later, in [6] J. Cokle introduced new examples of real algebras: *coquaternions, tessarines* and *cotessarines.* The first ones are exactly the *real split quaternions* (or *paraquaternions*), $\mathbb{P}_{\mathbb{R}}$. As for the hamiltonian quaternions, a split quaternion q is a linear combination of the form $\mathrm{q} = a{+}b\,\mathbf{i}{+}c\,\mathbf{j}{+}d\,\mathbf{k}$ where the the coefficients a, b, c and d are real numbers and the imaginary units are such that $-\,\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{i}\,\mathbf{j}\,\mathbf{k} = 1$ (cf. Section 1.2).

At the beginning, split quaternions were used by physicists for studying the representations of the Lorentz group (see [2]) and, more recently, for describing rotations of the Minkowski 3-space, (see [19]). Moreover in the last decade, split-quaternions have been used in differential geometry for studyng the parahermitian and paraquaternionic manifolds and the transormations of the hyperbolic space, (see [13] and [20]). In these last ten years, (see for example [16]) a generalization of quaternions and split quaternions have been introduced.

This thesis is essentially divided into two main macrosections, one about split quaternions and one about integer-valued polynomials over integer split quaternions.

Let R be a unitary commutative ring. In Chapter 1, taking inspiration from [16, Chapter III], we define the rings $\mathbb{H}_R$ and $\mathbb{P}_R$ as

$$\mathbb{H}_R = \{a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \mid a, b, c, d \in R\}$$
$$\mathbb{P}_R = \{a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \mid a, b, c, d \in R\}$$

where the relations on $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$ are the same as for $\mathbb{H}_{\mathbb{R}}$ and $\mathbb{P}_{\mathbb{R}}$, respectively (cf. Section 1.2). Part of this thesis is devoted to describe properties of the algebras $\mathbb{P}_R$ and, in particular, of $\mathbb{P}_{\mathbb{Z}}$, the algebra of split quaternions with integer coefficients.

At the very beginning of this work we give a representation of $\mathbb{P}_R$ as a subring of the matrix ring $M_2(R)$ (see Propositions 1.3.1 and 1.3.4). This representation simplifies many questions. In Sections 1.4 and 1.5, using the definitions of bar conjugate, norm and trace of elements of $\mathbb{P}_R$ we completely describe central elements, zero-divisors, units, nilpotent and idempotent elements of $\mathbb{P}_R$. We prove that $\mathbb{P}_R$ is an integral extension of R. In particular, the minimal polynomials of the elements of $\mathbb{P}_{\mathbb{Z}}$ turn out to be important to characterize some classes of prime and maximal ideals of the ring $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ (cf. Chapter 3). In Section 1.6 we describe the ideal structure of $\mathbb{P}_{\mathbb{Z}}$. In particular we find out that the prime ideals of $\mathbb{P}_{\mathbb{Z}}$ are exactly (0), $\mathscr{M} = (1 + \mathbf{i}, 1 + \mathbf{j})$ and $p\mathbb{P}_{\mathbb{Z}}$, for an odd prime integer p (cf. Proposition 1.6.23). Excepted (0), they are also maximal.

In order to deepen the investigation on the ideal structure of $\mathbb{P}_{\mathbb{Z}}$ and, later, of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$, we will need to handle the localization of such rings at prime ideals. While for commutative rings the theory of localization is quite wide and well-known, the literature about localizations and, in particular, rings of fractions of noncommutative rings, is not much extended. In Chapter 2 some of the ideas contained in [15] have been developed so to obtain useful results about localization of $\mathbb{P}_{\mathbb{Z}}$. Since for noncommutative rings the complement of a prime ideal is not in general a multiplicative closed subset (see Example 2.1.4), it is not possible to build localizations with respect to prime ideals in the usual way of the commutative case. More suitable sets $\mathscr{C}(Q)$ suggested by Goldie are used to approach this problem (cf. Definition 2.1.5). We show that these sets are an example of the so-called *denominator sets* of [15] (cf. Section 2.1.2). In $\mathbb{P}_{\mathbb{Z}}$ the sets $\mathbb{Z} \smallsetminus (0)$, $\mathbb{Z} \smallsetminus p\mathbb{Z}$ (for a prime integer p) and $\mathscr{C}(Q)$ (for a prime ideal Q of $\mathbb{P}_{\mathbb{Z}}$) are denominator sets. Using these sets we obtain the localizations of $\mathbb{P}_{\mathbb{Z}}$ listed in Proposition 2.2, which are essentially the rings $\mathbb{P}_{\mathbb{Q}}$ (which is the total ring of fractions of $\mathbb{P}_{\mathbb{Z}}$) and $\mathbb{P}_{\mathbb{Z}_{(p)}}$, for a prime integer p.

Let D be a commutative domain and K its quotient field, the *integer-valued polynomial ring on* D is

$$\mathrm{Int}(D) = \{f \in K[x] \mid f(D) \subseteq D\}.$$

The ring $\mathrm{Int}(D)$ and related constructions have inspired much research in recent decades (see [4]). Recently, integer-valued polynomial constructions over noncommutative rings and algebras have been investigated. There are different approaches to this topic. Some authors ([7], [8], [9]) begin with a

D-algebra A over the commutative domain D, and consider polynomials in $K[x]$ (where K is the quotient field of D) that map A into A. The set of such polynomials is a commutative subring of $K[x]$, and this ring may be studied in much the same way as $\mathrm{Int}(D)$.

Another point of investigation ([9], [22], [23]) is to take any ring extension $A \subseteq B$ and studying the set $\mathrm{Int}(A) = \{f \in B[x] \mid f(A) \subseteq A\}$. Even in the case A is not commutative, the properties of $\mathrm{Int}(A)$ reflect somehow the commutative case, although the proofs and methods of analysis are quite different.

In the second part of this thesis we deal with integer-valued polynomials on $\mathbb{P}_{\mathbb{Z}}$, $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) = \{f \in \mathbb{P}_{\mathbb{Q}}[x] \mid f(\mathbb{P}_{\mathbb{Z}}) \subseteq \mathbb{P}_{\mathbb{Z}}\}$ (Definition 3.1.2). A relevant inspiration for this study is the work done by Werner (cf. [22]) about integer-valued polynomials over the *Lipschitz quaternions*, $\mathbb{H}_{\mathbb{Z}}$. However, since $\mathbb{P}_{\mathbb{Z}}$ contains nilpotent elements and zero-divisors while $\mathbb{H}_{\mathbb{Z}}$ does not, the techniques used in this thesis are quite distinct from those used in [22].

The first (and main) difficulty in handling $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ is based on the fact that the polynomial evaluation is not a homomorphism. This makes quite tricky to show that $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ is a ring (cf. Proposition 3.1.4). Once it is known that $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ is a ring, we proceed to investigate the prime and maximal ideal structure of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. Again, localization process assumes a central role.

When D is a commutative noetherian domain and S is a multiplicative subset of D, it is known that $S^{-1}\mathrm{Int}(D) = \mathrm{Int}(S^{-1}D)$ [4, Thm. I.2.3] (in general there is only the containment $S^{-1}\mathrm{Int}(D) \subseteq \mathrm{Int}(S^{-1}D)$). This equality also holds for $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$, as long as S is a denominator set of $\mathbb{P}_{\mathbb{Z}}$ of the type $\mathbb{Z} \setminus p\mathbb{Z}$, for some prime integer p or $p = 0$ (cf. Proposition 3.3.1). This fact turns out to be very useful to describe some classes of elements and, more generally, the ring structure of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$.

For polynomial rings with coefficients in a commutative domain D there are standard ways to describe some prime ideals of $\mathrm{Int}(D)$ (see [4, Chap. V]). In particular, primes above (0) have the form $M(x) \cdot K[x] \cap \mathrm{Int}(D)$, where $M(x) \in K[x]$ is monic and irreducible. We will find a similar result for the primes upper to zero of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ (cf. Theorem 3.4.22). Then we proceed with the study of the primes of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ containing a prime integer p: we will partially classify them and find some sufficient conditions for their maximality.

When I is a nonzero ideal of D and $a \in D$, it is easily seen that the set $\mathfrak{P}_{I,a} = \{f \in \mathrm{Int}(D) \mid f(a) \in I\}$ is an ideal of $\mathrm{Int}(D)$ above I and if I is prime then $\mathfrak{P}_{I,a}$ is prime too. This kind of prime ideals are used in many cases to calculate the Krull dimension (i.e., the maximum length of prime ideals) of $\mathrm{Int}(D)$. We will attempt similar constructions for $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. We will distinguish the two cases $p = 2$ and p odd prime integer.

In the first case we will find that the primes of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ containing 2 are exactly the ones above the ideal $\mathscr{M} = (1 + \mathbf{i}, 1 + \mathbf{j})$ of $\mathbb{P}_{\mathbb{Z}}$. For these ideals the analysis is quite different from the case p odd prime, since $\mathscr{M}$ is not generated by integers as it happens for $p\mathbb{P}_{\mathbb{Z}}$. We consider the following sets, that turn out to be maximal ideals

$$\mathfrak{M}_{\mathrm{q}} := \{f \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) \mid f(\mathrm{q}) \in \mathscr{M}\},$$

for suitable $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$. The difficulty in working with $\mathfrak{M}_{\mathrm{q}}$ is not in showing that it is a maximal or prime ideal, but that it is exactly an ideal. In Section 3.4.3, we give some partial results of maximality depending on the quaternion q chosen for $\mathfrak{M}_{\mathrm{q}}$.

To construct primes of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ containing an odd prime integer p we need some adaptations for definitions (cf. Definition 3.4.2) in order to settle the noncommutative multiplication in $\mathbb{P}_{\mathbb{Z}}$. In fact, the analogous of the sets $\mathfrak{M}_{\mathrm{q}}$ in which $\mathscr{M}$ is replaced by $p\mathbb{P}_{\mathbb{Z}}$, which would be the natural extension of the case $p = 2$, are not ideals.

For each $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$, let $C(\mathrm{q}) := \{a \pm b\,\mathbf{i} \pm c\,\mathbf{j} \pm d\,\mathbf{k}\}$ and I an ideal of $\mathbb{P}_{\mathbb{Z}}$. We define the set

$$\mathfrak{P}_{I,\mathrm{q}} := \{f \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) \mid f(\mathrm{p}) \in I \text{ for all } \mathrm{p} \in C(\mathrm{q})\}.$$

When $\mathrm{q} \in \mathbb{Z}$ or the ideal I is generated by an integer n, it is easy to prove that $\mathfrak{P}_{I,\mathrm{q}}$ is an ideal and we give conditions for it being a prime ideal (see Proposition 3.4.3). It is much more complicate to handle the case when $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}} \setminus \mathbb{Z}$. We first study the primality of $\mathfrak{P}_{(0),\mathrm{q}}$ in terms of the minimal polynomial of q (Theorem 3.4.19) and, as already stated above, we completely classify the primes of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ above (0) (cf. Theorem 3.4.22). In Theorem 3.4.40 we give a sufficient and necessary condition for $\mathfrak{P}_{p\mathbb{P}_{\mathbb{Z}},\mathrm{q}}$ being a prime in $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ again in terms of minimal polynomials. We prove that, if $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$ and $p \nmid \gcd(b, c, d)$, then $\mathfrak{P}_{p\mathbb{P}_{\mathbb{Z}},\mathrm{q}}$ is a maximal ideal if and only if the minimal polynomial of q is irreducible modulo p. Moreover, if this is the case, we have the isomorphism $\frac{\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})}{\mathfrak{P}_{p,\,\mathrm{q}}} \simeq \mathcal{M}_2(\mathbb{F}_{p^2})$.

The investigation on the prime and maximal spectra of the ring $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ is also central in Chapter 4, where we focus our attention on localization properties of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. In this chapter we initially deal with localization of $\mathrm{Int}(R)$, for a right noetherian (noncommutative) ring R, at a noncentral right denominator set S without zero-divisors. We generalize Proposition 3.3.1

and prove that $\mathrm{Int}(R)S^{-1} = \mathrm{Int}(RS^{-1})$ (cf. Theorem 4.1.2). Our further researches about the prime spectrum of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$, start from studying the commutative ring

$$\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right) = \left\{\, f(x) \in \mathbb{Q}[x] \mid f(\mathbb{P}_{\mathbb{Z}_{(p)}}) \subseteq \mathbb{P}_{\mathbb{Z}_{(p)}} \,\right\}$$

because it is shown that

$$\mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) = \bigcap_{p \text{ primo}} \mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}(\mathbb{P}_{\mathbb{Z}_{(p)}}).$$

Since we show that $\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}(\mathbb{P}_{\mathbb{Z}_{(p)}}) = \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})(\mathbb{Z} \smallsetminus p\mathbb{Z})^{-1}$, it follows that the prime ideals of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ can be totally described when one knows the primes of $\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$. More information about the ring $\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$, for an odd prime p, can be recovered using the matrix representation and the isomorphism stated in Proposition 4.1.12:

$$\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right) \simeq \mathcal{M}_2\left(\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)\right).$$

This turns out to be useful since $\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$ is a subring of $\mathbb{Q}[x]$ and thus it is commutative. So one can use some classical tools like, for instance, the ones of [4]. Moreover, to study the ring $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ it is possible to follow the arguments of [17] on the characterization of integrally closed overrings of $\mathbb{Z}[X]$. In particular we show here that the prime ideals of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ above an odd prime integer are all maximal (Corollary 4.3.5).

Chapter 0

Notations and terminology

In this chapter we briefly recall some definitions and notions about ring theory that will be used throughout the work. We will also fix some conventions and symbols used in the text. For the notions not recalled here we refer to [14], [15] and [12]. For convenience, the notions of noncommutative rings of fractions and noncommutative localizations are recalled later in Chapter 2.

0.1 Classical notations

As usual, we will indicate with the symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ the sets of natural, integer, rational, real and complex numbers respectively. Given an integer $n \geqslant 1$, we indicate here with $\mathbb{Z}_n$ the ring $\frac{\mathbb{Z}}{n\mathbb{Z}}$ of the integers modulo n. To indicate the localization of $\mathbb{Z}$ at a prime ideal (p), we use $\mathbb{Z}_{(p)}$. The finite field with q elements is, as usual, $\mathbb{F}_q$. When p is a prime number, we will use interchangeably $\mathbb{Z}_p$ and $\mathbb{F}_p$.

0.2 Rings

In the following, unless otherwise specified, with the term *ring* we will mean always a nonzero ring with identity. We will specify the commutativity of multiplication when needed. We indicate the set of nonzero elements of R with the symbol R^* and $\mathrm{char}(R)$ indicates the *characteristic* of R.

Units

An element a in a ring R is said to be *right-invertible* if there exists $b \in R$ such that $ab = 1$. Such an element b is called *right inverse* of a. Left-invertible elements and their left inverse are defined similarly. If a has both a right inverse b and a left inverse b' then $b = b'$. In this case we say that a is *invertible* or a *unit* and we call b its *inverse.* We indicate by $\mathcal{U}(R)$ the set of all invertible elements of R. It is easy to see that $\mathcal{U}(R)$ is a multiplicative group with the identity 1_R. A ring where every nonzero element is invertible is said to be a *division ring.* Fields differ from division rings only for the commutativity of multiplication. For this reason, division rings are also called *skew fields.*

Conjugacy class

We say that two elements a and b of a ring R are *(multiplicatively) conjugate* if $b = cac^{-1}$, for some $c \in \mathcal{U}(R)$. The multiplicative conjugacy is an equivalence relation over R. We define the *conjugacy class* of an element $a \in R$ to be the set

$$\mathrm{Co}_R(a) = \left\{ cac^{-1} \mid c \in \mathcal{U}(R) \right\},$$

that is the equivalence class associated to a under multiplicative conjugacy. In commutative rings the conjugacy classes are clearly singletons.

Center

We recall that given a ring R, the *center* $\mathcal{Z}(R)$ of R is defined as the set of all elements of R that commute with all other elements of R under multiplication. Obviously, if R is commutative, then $R = \mathcal{Z}(R)$. An element of $\mathcal{Z}(R)$ will be called a *central* element of R.

Zero-divisors and regular elements

A nonzero element $a \in R$ is said to be a *left zero-divisor* if there exists a nonzero element $b \in R$ such that $ab = 0$ in R. Right zero-divisors are defined analogously. In the commutative case, obviously, right and left zero-divisors coincide. For noncommutative rings a left zero-divisor need not to be a right zero-divisor (for some examples in matrix rings see [14, Chapter 1]). When an element of R is both right and left zero-divisor, we call it a zero-divisor *tout court*. We indicate by $\mathcal{D}(R)$ the set of all zero-divisors of R. An element of R which is not a right zero-divisor is said to be a *right regular element*. Similarly on the left. An element which is regular on the left and on the right is called *regular element*. We indicate the set of all right regular elements, left regular elements and regular elements of R by $\mathcal{R}_r(R)$, $\mathcal{R}_l(R)$ and $\mathcal{R}(R)$ respectively. Notice that a right-invertible element cannot be a right zero-divisor. Similarly on the left.

A *domain* (or *integral domain*) is a nontrivial ring without left or right zero-divisor. This means that $ab = 0$ in R implies that $a = 0$ or $b = 0$. In a domain every element is a regular element.

Nilpotent and idempotent elements

An element $a \in R$ is a *nilpotent element* if $a^n = 0$ for some $n \in \mathbb{N}^*$. The least n with this property is the *nilpotence index* of a. Nilpotent elements are not regular. A ring without nonzero nilpotent elements is said to be *reduced.* Domains, skew fields and fields are reduced rings.

An element $a \in R$ is said to be *idempotent* if $a^2 = a$. A regular element $a \neq 0, 1$ of a ring R cannot be an idempotent. Domains have only *trivial idempotent*: 0 and 1.

0.3 Ideals

Let be given an additive subgroup $\mathscr{I}$ of a ring R. We say that $\mathscr{I}$ is a *left ideal* if for each $a \in \mathscr{I}$ and $r \in R$ then $ra \in \mathscr{I}$. We say that $\mathscr{I}$ is a *right ideal* if for each $a \in \mathscr{I}$ and $r \in R$ then $ar \in \mathscr{I}$. Lastly, $\mathscr{I}$ is a *two-sided ideal* of R if $\mathscr{I}$ is both a left and right ideal. For commutative rings left, right and two-sided ideals coincide. In a noncommutative ring a left-ideal needs not to be a right one and *vice versa.* Take for example the set of all $n \times n$ matrices with entries in a ring R where the last column is zero. This set is a left ideal but not a right one. From now on, with the term *ideal* we mean always a two-sided ideal. We can give an equivalent condition for determining if a subset of a ring R is an ideal.

Proposition A. *Let R be a ring. Let $\mathscr{I}$ be an additive subgroup of R. Then $\mathscr{I}$ is an ideal of R if and only if $r\mathscr{I}s \subseteq \mathscr{I}$, for all $r, s \in R$.*

Proof. Suppose that $\mathscr{I}$ is both a left and right ideal. Let $a \in \mathscr{I}$ and $r, s \in R$. Then $ra \in \mathscr{I}$ since $\mathscr{I}$ is a left ideal and $(ra)s \in \mathscr{I}$ since $\mathscr{I}$ is a right ideal. For the converse, let $\mathscr{I}$ be an additive subgroup of R such that $r\mathscr{I}s \subseteq \mathscr{I}$, for all $r, s \in R$. Take $a \in \mathscr{I}$ and $r \in R$. Then it is easy to see that $ar = 1 \cdot ar \in \mathscr{I}$ and $ra = ra \cdot 1 \in \mathscr{I}$ which mean that $\mathscr{I}$ is both a right and left ideal of R. **QED**

Given a ring R, we call *trivial* ideals of R the zero ideal $(0) \overset{\text{def}}{=} \{ 0 \}$ and R itself. A ring R is said to be *simple* if it has only trivial ideals. Fields and skew fields are simple rings. Proposition K gives other examples of simple rings.

Principal ideals

Given an element $a \in R$, we will indicate by

$$(a) \overset{\text{def}}{=} RaR = \left\{ \sum_{i=1}^{n} r_i a s_i \;\middle|\; n \in \mathbb{N}^*,\ 1 \leqslant i \leqslant n,\ r_i, s_i \in R \right\}$$

the *ideal generated* by a. The ideal (a) is the smallest ideal of R containing a. Similarly, we define the *left ideal generated* by a to be the set

$$Ra = \{ ra \mid r \in R \},$$

that is the smallest left ideal of R containing a. Finally, we define the *right ideal generated* by a to be the set

$$aR = \{ ar \mid r \in R \},$$

that is the smallest right ideal of R containing a. If a is a central element of R then $(a) = aR = Ra$. In this case, we will use these notations interchangeably. A left ideal is *principal* if it equals the left ideal generated by one of its elements. The same definition is given for right ideals and ideals. A ring is said to be a *principal ideal ring* if all its ideals are principal. In a commutative ring R, given $a \in R$, it is well known that $(a) = R$ if and only if $a \in \mathcal{U}(R)$. In a noncommutative ring the ‘only if’ part is not true in general. In Proposition 1.6.27 we will see an example of this situation.

Finitely generated ideals

We recall now some notions about ideals that are generated by a finite number of elements. Let R be a ring and let $a_1, a_2 \dots, a_n \in R$, for $n \in \mathbb{N}^*$. We define the *left ideal generated* by the a_i's to be the smallest left ideal of R containing the a_i's. It is the set

$$Ra_1 + \cdots + Ra_n = \{\, r_1 a_1 + \cdots + r_n a_n \mid r_i \in R,\ 1 \leqslant i \leqslant n \,\}.$$

Similarly, we define the *right ideal generated* by the a_i's to be the smallest right ideal of R containing the a_i's. It is the set

$$a_1 R + \cdots + a_n R = \{\, a_1 r_1 + \cdots + a_n r_n \mid r_i \in R,\ 1 \leqslant i \leqslant n \,\}.$$

Finally, we define the *ideal generated* by the a_i's to be the smallest ideal of R containing the a_i's. Mutuating the notation used for commutative rings, it is

$$(a_1, a_2, \dots, a_n) \overset{\text{def}}{=} Ra_1R + Ra_2R + \cdots + Ra_nR.$$

The expression of its elements can be very complicated if n is large. When $n = 2$, then

$$(a_1, a_2) = \left\{ \sum_{i=1}^{l} r_i a_1 s_i + \sum_{j=1}^{m} r_j a_2 s_j \;\middle|\; l, m \in \mathbb{N}^*,\ r_i, s_i, r_j, s_j \in R \right\}.$$

In our work we will consider ideals generated by at most two elements.

A left ideal $\mathscr{I}$ of a ring R is said to be *finitely generated* if there exist $a_1, \dots, a_n \in \mathscr{I}$ such that $\mathscr{I}$ equals the left ideal generated by the a_i's. Similar definitions are given for right finitely generated ideals and finitely generated ideals.

Maximal ideals

An ideal $\mathscr{I}$ of a ring R is *proper* if $\mathscr{I} \neq R$.

Definition B. Let R be a ring. A proper ideal $\mathscr{M} \subseteq R$ is said to be *maximal* if, for all proper ideal $\mathscr{I}$ such that $\mathscr{M} \subseteq \mathscr{I}$, then $\mathscr{I} = \mathscr{M}$.

The maximal ideals are the proper ideals not contained in any other proper ideal of R. Given an ideal $\mathscr{M}$ of a ring R, then $\mathscr{M}$ is maximal if and only if the quotient ring $\frac{R}{\mathscr{M}}$ is a simple ring. In the commutative case this is equivalent to say that $\frac{R}{\mathscr{M}}$ is a field. Given a ring R, by Zorn's lemma, it can be showed that any proper ideal of R is contained in a maximal ideal. For commutative rings we have also that any noninvertible element is contained in a maximal ideal. For noncommutative rings this is not true in general. It can happen that the ideal generated by a noninvertible element a of a ring R is the whole ring R. In Remark 1.6.28 we shall see an explicit example. We call the set of all maximal ideals of a ring R the *maximal spectrum* of R.

A ring is said to be *local* if it has at most one maximal ideal. We write that $(R, \mathscr{M})$ is a local ring for saying explicitly that $\mathscr{M}$ is the maximal ideal of R.

Prime ideals

Another important class of ideals of a ring are the prime ideals.

Definition C. Let R be a ring. A proper ideal $\mathscr{P}$ of R is *prime* if given $a, b \in R$ such that $aRb \subseteq \mathscr{P}$, then $a \in \mathscr{P}$ or $b \in \mathscr{P}$.

Often, it is useful the following equivalent definition of prime ideals.

Proposition D. [12, Proposition 3.1] *Let R be a ring and let $\mathscr{P}$ be a proper ideal of R. Then $\mathscr{P}$ is a prime ideal if whenever $\mathscr{I}$ and $\mathscr{J}$ are ideals of R such that $\mathscr{I}\mathscr{J} \subseteq \mathscr{P}$, then either $\mathscr{I} \subseteq \mathscr{P}$ or $\mathscr{J} \subseteq \mathscr{P}$.*

We recall a property of prime ideals that is well-known in the commutative case.

Proposition E. [12, Proposition 3.2] *Let R be a ring. Then every maximal ideal of R is a prime ideal.*

A characterization of prime ideals follows. For a proof see the reference.

Proposition F. [12, Proposition 3.1] *Let R be a ring. Let $\mathscr{P}$ be a proper ideal of R. Then $\mathscr{P}$ is a prime ideal of R if and only if in $\frac{R}{\mathscr{P}}$ the trivial ideal (0) is a prime ideal.*

We call the set of all prime ideals of a ring R the *prime spectrum* of R and indicate it by $\mathrm{Spec}(R)$.

0.4 Modules over rings

For the notion of left (or right) module over a ring we refer to the bibliography [14], [15] and [12]. We will recall here what is needed for our purposes.

As usual, we will use the left notation ${}_RM$ for indicating a left module M over a ring R. For the right notation we use M_R. The left and right module over a commutative ring coincide. In the following we use the left notation; for right modules similar definitions and properties are given.

A *free* left module ${}_RM$ over a ring R is a module with a *basis* over R, *i.e.* an *R-linearly independent generating set* $E \subset R$. If E is the finite set

$E = \{ e_1, e_2, \dots, e_m \}$, we write that $M = Re_1 \oplus Re_2 \oplus \cdots \oplus Re_m$. When the number m is an invariant of M, we call it the *rank* of M, $\operatorname{rank}(M)$. Since the commutative rings have the *invariant basis number property*, the rank of a module over a commutative ring is well defined.

Given a ring R and a finite set of indeterminates $X = \{ x_1, x_2, \dots, x_m \}$ (that we always assume to be independent over R), the free left module generated by X over R is the set $M = Rx_1 \oplus Rx_2 \oplus \cdots \oplus Rx_m$. Its elements are the formal linear combinations of the elements of X with left coefficients in R. We equip this R-module by the obvious operations. In particular, if R is commutative, X is a basis for M and $\operatorname{rank}(M) = m$.

0.5 Algebras over rings

We recall now some notions about algebras over rings. An *algebra* A over a ring R is an R-module ${}_RA$ equipped by a binary operation, called the *multiplication* of A, which is *bilinear* over R. This means that, given any $a, b \in R$ and $x, y, z \in M$, then $(ax + by)z = a(xz) + b(yz)$ and $x(ay + bz) = a(xy) + b(xz)$.

If the multiplication defined over A is associative we say that A is an *associative algebra.* Since we will work here only with associative algebras, from now on, with the term algebra we mean associative algebra. Similarly, if the multiplication of A is commutative, we call A *commutative algebra.*

If A contains a multiplicative *identity*, we say that A is a *unitary algebra* or an algebra with identity. The most of algebras considered here are unitary.

Given a unitary algebra A, if we focus only on the addition and multiplication between elements of A, we get a ring to whom we refer as the *ring* *structure* of A. In this way, looking at the ring structure of the algebra, we can borrow the notions introduced for rings. The center $\mathcal{Z}(A)$ of an algebra A is the center of its ring structure. The (left or right) zero-divisors, the (left or right) regular elements of A are obviously defined. We say that A is a *division algebra* if A is a unitary algebra where every nonzero element has a multiplicative inverse. Then, a division algebra is an algebra whose ring structure is a division ring. The set of all invertible elements (*units*) of A is denoted by $\mathcal{U}(A)$.

An R-algebra A is said to be *finite* if A is finitely generated as an R-module. This means that $A = Re_1 \oplus Re_2 \oplus \cdots \oplus Re_m$, for some e_1, e_2, $\ldots$, $e_m \in A$. Using the same definitions as in module theory, we speak of linear independence, basis, rank *etc.* for algebras.

Algebra homomorphism

A *homomorphism* between two R-algebras A and B is a map $f : A \to B$ such that, for all $a \in R$ and $x, y \in A$, we have $f(ax) = af(x)$, $f(x+y) = f(x)+f(y)$ and $f(xy) = f(x)f(y)$. Roughly speaking, an algebra homomorphism is an R-linear R-module homomorphism that preserves the multiplication too. Moreover, since we work with unitary algebras, we suppose that every algebra homomorphism $f : A \to B$ preserves the units; that is to say $f(1_A) = 1_B$. A bijective algebra homomorphism is an algebra *isomorphism.* An isomorphism of an algebra into itself is an algebra *automorphism.*

An anti-automorphism f of an algebra A is an algebra isomorphism from A to the opposite ring structure A^{op} associated to A. Briefly, for all $a, b \in A$, then $f(ab) = f(b)f(a)$.

Polynomial evaluation

Taken $r \in R$, we define the *evaluation* at r to be the map $\Phi_r : R[x] \to R$, such that $\Phi_r : f(x) = \sum_{i=0}^n a_i x^i \mapsto f(r) \overset{\text{def}}{=} \sum_{i=0}^n a_i r^i$.

Proposition G. *Let $r \in R$. Then Φ_r is a ring homomorphism if and only if $r \in \mathcal{Z}(R)$.*

In particular, if R is commutative, then Φ_r is a homomorphism for any $r \in R$.

We say that $r \in R$ is a *root* of the polynomial $f(x) \in R[x]$, if $f(r) = 0$. The division with remainder and the relation of *divisibility* between polynomials ar defined as usual.

Proposition H (Ruffini)**.** *Let $f(x) \in R[x]$ and $r \in R$. Then r is a root of $f(x)$ if and only if $f(x)$ is in the left ideal $R[x](x - r)$.*

0.6 Noetherian rings

We say that a ring R is *left noetherian* if the left ideals of R are finitely generated. A ring R is *right noetherian* if the right ideals of R are finitely generated. A ring R is said to be *noetherian* if it is both left and right noetherian. Obviously, in a noetherian ring all ideals are finitely generated. In general, the notions of left and right noetherianity do not coincide. Take for example the upper triangular 2×2 matrices with entries in $\mathbb{Q}$ where the $(1, 1)$ entry is in $\mathbb{Z}$. This set is a right but not left noetherian ring.

We state a result that is a sufficient condition for of an algebra over a ring being noetherian.

Proposition I. [12, Proposition 1.6] *Let R be a commutative noetherian ring. Let A be an R-algebra finitely generated. Then A is a noetherian ring.*

Thus, for instance, the algebras finitely generated over $\mathbb{Z}$ are noetherian rings. This is the case of the ring of the squared matrices with integer entries of any order.

0.7 Matrix rings

Given a ring R and a positive integer n, we will indicate by $\mathcal{M}_n(R)$ the R-algebra of the squared matrices of order n with entries in R. The *identity matrix* of order n will be indicated by I_n. We will call *scalar matrices* those matrices of the form aI_n, where $a \in R$. The notions of determinant (det) and trace (tr) of a squared matrix over a commutative ring are defined as usual.

Let us indicate by E_{ij}, for all $1 \leqslant i, j \leqslant n$, the matrix whose (i,j)-entry is 1 and all other entries are 0. It is clear that $\{ E_{ij} \mid 1 \leqslant i, j \leqslant n \}$ is a generating set for $\mathcal{M}_n(R)$. We will call the E_{ij}'s the *matrix units.* A matrix $A = (a_{ij}) \in \mathcal{M}_n(R)$ is said to be *diagonal* if $a_{ij} = 0$ for all $i \neq j$. Often, for simplicity, a diagonal matrix A of order n is written as a vector of length n: $A = \operatorname{diag}(a_1, a_2, \dots, a_n)$.

We recall here the following crucial properties of matrix rings since we will use them throughout this work. The first one regards the center of the matrix ring: this is made by all scalar matrices with entries in the center of the coefficient ring.

Proposition J. *Let R be a ring and $\mathcal{M}_n(R)$ be the ring of $n \times n$ matrices over R. Then the center of $\mathcal{M}_n(R)$ is made by all scalar matrices aI_n with*

$a \in \mathcal{Z}(R)$. *In particular, if R is commutative, the center of $\mathcal{M}_n(R)$ is the set of scalar matrices.*

Proof. It is immediate to see that, given $a \in \mathcal{Z}(R)$, then $aI_n \in \mathcal{Z}(\mathcal{M}_n(R))$. Let us show the other inclusion. Let $A = (a_{ij}) \in \mathcal{Z}(\mathcal{M}_n(R))$. The matrix $E_{ii}A$ is the matrix that has the same i-th row as A and all other rows are zero. Similarly, the matrix AE_{ii} is the matrix that has the same i-th column as A and all other columns are zero. Since A is a central element, then $E_{ii}A = AE_{ii}$, for each $1 \leqslant i \leqslant n$. This implies that $A = \mathrm{diag}(a_{11}, \ldots, a_{nn})$ is a diagonal matrix. Moreover, for all $1 \leqslant i, j \leqslant n$, we have the identities $AE_{ij} = a_{ii}E_{ij}$ and $E_{ij}A = a_{jj}E_{ij}$. Since A is central, then $a_{ii} = a_{jj}$, for all $1 \leqslant i, j \leqslant n$. This means that $A = aI_n$, for some $a \in R$. Finally, A commutes with $B = bI_n$, for all $b \in R$. Then from the identity $(aI_n)(bI_n) = (bI_n)(aI_n)$, for all $b \in R$, we conclude that $a \in \mathcal{Z}(R)$. Our proof is now complete. **QED**

The next result deals with the ideal structure of matrix rings. We will see that it is not true in general for left or right ideals.

Proposition K. *Let R be a ring and $\mathcal{M}_n(R)$ be the ring of $n \times n$ matrices over R. Then any ideal $\mathscr{I}$ of $\mathcal{M}_n(R)$ has the form $\mathcal{M}_n(I)$ for a uniquely determined ideal I of R. In particular:*

(i) if R is a simple ring, so is $\mathcal{M}_n(R)$;

(ii) if R is a commutative principal ideal ring, then $\mathcal{M}_n(R)$ is a principal ideal ring;

(iii) if (R, M) is a local ring, so is $(\mathcal{M}_n(R), \mathcal{M}_n(M))$.

Proof. If I is an ideal of R, clearly $\mathcal{M}_n(I)$ is an ideal in $\mathcal{M}_n(R)$. Moreover, taken two ideals I and J in R, it is also clear that $I = J$ if and only if $\mathcal{M}_n(I) = \mathcal{M}_n(J)$. Now let $\mathscr{I}$ be an ideal of $\mathcal{M}_n(R)$ and let I be the set of all the (1,1)-entries of the matrices contained in $\mathscr{I}$. It is easy to see that I is an ideal in R. The last step is to show that $\mathscr{I} = \mathcal{M}_n(I)$. Using the matrix units E_{ij}, given any matrix $M = (m_{ij}) \in \mathcal{M}_n(R)$, we have the identity:

$$E_{ij} M E_{kl} = m_{jk} E_{il}. \tag{0.1}$$

Assume $M \in \mathscr{I}$. Taking $i = l = 1$, by the (0.1), we have that $m_{jk}E_{11} \in \mathscr{I}$, and so $m_{jk} \in I$, for each indexes j and k. Thus $\mathscr{I} \subseteq \mathcal{M}_n(I)$. Conversely, take a matrix $A = (a_{ij}) \in \mathcal{M}_n(I)$. We must show that $A \in \mathscr{I}$. It is enough to show that $a_{il}E_{il} \in \mathscr{I}$ for all i and l. Using the equation (0.1), find a matrix $M = (m_{ij}) \in \mathscr{I}$ such that $a_{il} = m_{11}$. Then for $j = k = 1$, the relation (0.1) gives $a_{il}E_{il} = m_{11}E_{il} = E_{i1}ME_{1l} \in \mathscr{I}$. The first statement of the theorem is now clear. Let us show the remaining facts.

(i) If R has no nontrivial ideals, then in $\mathcal{M}_n(R)$ it is impossible to have nontrivial ideals.

(ii) Let R be a principal ideal ring. Let $\mathscr{I}$ be an ideal of $\mathcal{M}_n(R)$. Then there exists an ideal I of R such that $\mathscr{I} = \mathcal{M}_n(I)$. Since I is a principal ideal, then $I = aR$, for some $a \in R$. Thus any element of $\mathscr{I}$ has the form aA, for some $A \in \mathcal{M}_n(R)$.

(iii) Let (R, M) be a local ring. We first show that $\mathscr{M} \overset{\text{def}}{=} \mathcal{M}_n(M)$ is a maximal ideal of $\mathcal{M}_n(R)$. It is easy then to show that it is the only one. Let $\mathscr{I}$ be a proper ideal of $\mathcal{M}_n(R)$ such that $\mathscr{M} \subseteq \mathscr{I}$. Let I be the ideal of R such that $\mathscr{I} = \mathcal{M}_n(I)$. Since R is local, then $I \subseteq M$

and $\mathcal{M}_n(I) \subseteq \mathcal{M}_n(M)$. Thus $\mathscr{I} \subseteq \mathscr{M}$. Finally $\mathscr{I} = \mathscr{M}$ and $\mathscr{M}$ is a maximal ideal. **QED**

The previous result is not true in general for ideals that are only right or left ideals. For instance, take a ring R. Let S be the set of all $n \times n$ matrices over R where the last column is made by zeros. It is easy to see that S is a left but not right ideal of $\mathcal{M}_n(R)$. If $S = \mathcal{M}_n(I)$, for some ideal I of R, then $1 \in I$. Thus $I = R$ and $S = \mathcal{M}_n(R)$, which is a contradiction.

Chapter 1

Algebra of split quaternions: $\mathbb{P}_{\mathbb{Z}}$

In this chapter we deal with a particular class of noncommutative $\mathbb{Z}$-algebras, the generalized quaternion algebras and in particular with the integer split quaternions $\mathbb{P}_{\mathbb{Z}}$. We first study some classes of its elements: zero-divisors, central elements, units etc. Then we completely describe prime and maximal ideals of $\mathbb{P}_{\mathbb{Z}}$. In Chapter 2 we will analyze some localization properties of the same ring. In Chapters 3 and 4 we will focus on the ring of integer-valued polynomials over these algebras.

1.1 Generalized Quaternion Algebras

Generalized quaternions and quaternion algebras have been introduced in the last decade as a tool for studying quadratic form theory. This construction is essentially a natural generalization of $\mathbb{H}_{\mathbb{R}}$, the well-known quaternion algebra over the real numbers introduced by sir Hamilton.

In [16, Chapter III] Lam works with quaternion algebras with coefficients over an arbitrary field of characteristic distinct from 2. More generally, preserving Lam's notations, we will consider here quaternion algebras over a commutative integral domain with characteristic different from 2.

We start giving the main definition.

Definition 1.1.1. Let D be a commutative integral domain of characteristic not two. Let $\alpha, \beta \in D^*$. We define the *quaternion algebra* $\left(\frac{\alpha,\beta}{D}\right)$ over D to be the D-algebra with two generators $\mathbf{i}$ and $\mathbf{j}$ with the defining relations

$$\mathbf{i}^2 = \alpha, \qquad \mathbf{j}^2 = \beta, \qquad \mathbf{i}\,\mathbf{j} = -\,\mathbf{j}\,\mathbf{i}. \tag{1.1}$$

For simplicity let $\mathbf{k} \overset{\text{def}}{=} \mathbf{i}\,\mathbf{j}$. Then we have

$$\mathbf{k}^2 = (\,\mathbf{i}\,\mathbf{j})(\,\mathbf{i}\,\mathbf{j}) = -\,\mathbf{i}^2\,\mathbf{j}^2 = -\alpha\beta. \tag{1.2}$$

We say that two elements a, b in a ring R *anticommute* if $ab = -ba$. We state the following result.

Proposition 1.1.2. *With the notation introduced above, any two elements of* $\{\ \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$ *anticommute. Moreover the algebra* $\left(\frac{\alpha,\beta}{D}\right)$ *is a noncommutative unitary algebra (finitely) generated by* 1, $\boldsymbol{i}$, $\boldsymbol{j}$ *and* $\boldsymbol{k}$ *over* D.

Proof. By (1.1) $\mathbf{i}$ and $\mathbf{j}$ anticommute. By means of easy calculations, we get:

$$\mathbf{i}\,\mathbf{k} = -\,\mathbf{k}\,\mathbf{i} = \alpha\,\mathbf{j}, \qquad \mathbf{k}\,\mathbf{j} = -\,\mathbf{j}\,\mathbf{k} = \beta\,\mathbf{i}, \tag{1.3}$$

this assures the other anticommutativity relations. Finally, the (1.1) say us that 1, $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ are generators of $\left(\frac{\alpha,\beta}{D}\right)$ over D. **QED**

We are ready to show that $\{\,1, \mathbf{i}, \mathbf{j}, \mathbf{k}\,\}$ is a D-basis for $\left(\frac{\alpha,\beta}{D}\right)$. We will adapt the proof of [16, Proposition III.1.0] to the case of a commutative integral domain D with $\operatorname{char}(D) \neq 2$.

Proposition 1.1.3. *With the notation above,* $\{1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$ *is a* D*-basis for* $\left(\frac{\alpha,\beta}{D}\right)$*. In particular* $\operatorname{rank}_D\left(\frac{\alpha,\beta}{D}\right) = 4$.

Proof. Let K be the quotient field of D and let E be the algebraic closure of K. Notice that also $\operatorname{char}(E) \neq 2$. Fix $\alpha', \beta' \in E$ such that $(\alpha')^2 = -\alpha$ and $(\beta')^2 = \beta$ and consider the two matrices $M = \left(\begin{smallmatrix} 0 & \alpha' \\ -\alpha' & 0 \end{smallmatrix}\right)$ and $N = \left(\begin{smallmatrix} 0 & \beta' \\ \beta' & 0 \end{smallmatrix}\right)$ in $\mathcal{M}_2(E)$. By direct computations one gets:

$$M^2 = \alpha I_2, \qquad N^2 = \beta I_2, \qquad MN = \left(\begin{smallmatrix} \alpha'\beta' & 0 \\ 0 & -\alpha'\beta' \end{smallmatrix}\right) = -NM. \tag{1.4}$$

We show that the matrices I_2, M, N and MN are linearly independent over E. For seeing this, take some $a, b, c, d \in E$ such that

$$aI_2 + bM + cN + dMN = \begin{pmatrix} a + d\alpha'\beta' & b\alpha' + c\beta' \\ -b\alpha' + c\beta' & a - d\alpha'\beta' \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Since E is a field of characteristic different by 2, this matrix equation implies that $a = b = c = d = 0$.

Let φ be the map such that $\varphi(1) = I_2$, $\varphi(\mathbf{i}) = M$, $\varphi(\mathbf{j}) = N$ and $\varphi(\mathbf{k}) = MN$. Now extend φ linearly over D to the elements of $\left(\frac{\alpha,\beta}{D}\right)$. Thanks to (1.1), (1.2), (1.3) and (1.4), we get that $\varphi : \left(\frac{\alpha,\beta}{D}\right) \to \mathcal{M}_2(E)$ is a well-defined D-algebra homomorphism. In fact, taken $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \left(\frac{\alpha,\beta}{D}\right)$, for our assumption, $\varphi(\mathrm{q}) = aI_2 + bM + cN + dMN$ which is an element of $\mathcal{M}_2(E)$. Further, φ is D-linear by definition. Moreover, it preserves the multiplication since it behaves well with the generators:

$$\varphi(\mathbf{i}\,\mathbf{j}) = \varphi(\mathbf{k}) = MN = \varphi(\mathbf{i})\varphi(\mathbf{j}),$$

$$\varphi(\mathbf{j}\,\mathbf{i}) = \varphi(-\mathbf{k}) = -\varphi(\mathbf{k}) = -MN = MN = \varphi(\mathbf{j})\varphi(\mathbf{i}).$$

The other rules of multiplication of generators can be obtained similarly. Suppose now that the generators 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ of $\left(\frac{\alpha,\beta}{D}\right)$ are D-linearly dependent.

Then $a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} = 0$, for some $a, b, c, d \in D$. Since φ is a homomorphism, then $\varphi(a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}) = aI_2 + bM + cN + dMN = 0$. As we said above, I_2, M, N and MN are linearly independent over E, thus $a = b = c = d = 0$. Then $\{\, 1, \mathbf{i}, \mathbf{j}, \mathbf{k} \,\}$ is a basis of $\left(\frac{\alpha,\beta}{D}\right)$. Since D is a commutative domain, it has the invariant basis number property and $\operatorname{rank}_D \left(\frac{\alpha,\beta}{D}\right) = 4$. **QED**

Thanks to Proposition 1.1.3, we can state that every element $\mathrm{q} \in \left(\frac{\alpha,\beta}{D}\right)$ is of the form

$$\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k},$$

for some coefficients $a, b, c, d \in D$. Moreover, we have that

$$\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} = 0$$

if and only if $a = b = c = d = 0$. Lastly, we can explicitly write that

$$\left(\frac{\alpha,\beta}{D}\right) = \left\{\, a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \,\middle|\, a, b, c, d \in D,\ \mathbf{i}^2 = \alpha,\ \mathbf{j}^2 = \beta,\ \mathbf{i}\,\mathbf{j} = -\mathbf{j}\,\mathbf{i} = \ \mathbf{k} \,\right\}.$$

When D is a field, we come back to the definition given by Lam at the beginning of Chapter III in [16]. Then $\left(\frac{\alpha,\beta}{D}\right)$ is a vector space over D and we will say that $\left(\frac{\alpha,\beta}{D}\right)$ has *dimension* 4 over D.

1.2 Quaternions and Split quaternions

Now, we simplify the above notation for the rings we will use in the following. In Definition 1.1.1, if we take $\alpha = \beta = -1$ and $D = \mathbb{R}$, we obtain exactly the algebra of *real quaternions* introduced by Hamilton, $\mathbb{H}_{\mathbb{R}}$. Similarly, we set $\mathbb{H}_{\mathbb{Q}} \overset{\text{def}}{=} \left(\frac{-1,-1}{\mathbb{Q}}\right)$ the ring of *rational quaternions* and $\mathbb{H}_{\mathbb{Z}} \overset{\text{def}}{=} \left(\frac{-1,-1}{\mathbb{Z}}\right)$, the ring of *integer* or *Lipschitz quaternions.* The following containments hold: $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H}_{\mathbb{R}}$ and $\mathbb{H}_{\mathbb{Z}} \subset \mathbb{H}_{\mathbb{Q}} \subset \mathbb{H}_{\mathbb{R}}$.

More in general we use the following notation.

Notation 1.2.1. Let D be a commutative integral domain with $\mathrm{char}(D) \neq 2$. Then, with the notation introduced above,

$$\mathbb{H}_D \overset{\text{def}}{=} \left(\frac{-1,-1}{D} \right) = \left\{ a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \,\middle|\, a,b,c,d \in D,\ \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{i}\,\mathbf{j}\,\mathbf{k} = -1 \right\}.$$

In the Definition 1.1.1, taking $\alpha = -1$, $\beta = 1$ and $D = \mathbb{R}$, we get the algebra of Cokle's *real split quaternions.* For simplicity, we set $\mathbb{P}_{\mathbb{R}} \overset{\text{def}}{=} \left(\frac{-1,1}{\mathbb{R}}\right)$. Similarly, we indicate $\mathbb{H}_{\mathbb{Q}} \overset{\text{def}}{=} \left(\frac{-1,1}{\mathbb{Q}}\right)$, the ring of *rational split quaternions* and $\mathbb{H}_{\mathbb{Z}} \overset{\text{def}}{=} \left(\frac{-1,1}{\mathbb{Z}}\right)$, the ring *integer split quaternions.* The following containments hold: $\mathbb{R} \subset \mathbb{C} \subset \mathbb{P}_{\mathbb{R}}$ and $\mathbb{P}_{\mathbb{Z}} \subset \mathbb{P}_{\mathbb{Q}} \subset \mathbb{P}_{\mathbb{R}}$.

As for quaternions, we introduce the following notation.

Notation 1.2.2. Let D be a commutative integral domain with $\mathrm{char}(D) \neq 2$. Then, with the notation introduced above,

$$\mathbb{P}_D \overset{\text{def}}{=} \left(\frac{-1,1}{D} \right) = \left\{ a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \,\middle|\, a,b,c,d \in D,\ -\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{i}\,\mathbf{j}\,\mathbf{k} = 1 \right\}.$$

More generally, imitating Notations (1.2.1) and (1.2.2), one can define quaternions and split quaternions with coefficients over any commutative ring R where the relations between $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ are the same as for $\mathbb{H}_{\mathbb{R}}$ and $\mathbb{P}_{\mathbb{R}}$ respectively.

Definition 1.2.3. Let R be a commutative ring. We define the set of quaternions with coefficients in R to be the set

$$\mathbb{H}_R \overset{\text{def}}{=} \left\{ a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \,\middle|\, a,b,c,d \in R,\ \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{i}\,\mathbf{j}\,\mathbf{k} = -1 \right\}$$

and the set of split quaternions with coefficients in R to be the set

$$\mathbb{P}_R \overset{\text{def}}{=} \left\{ a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \,\middle|\, a,b,c,d \in R,\ -\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{i}\,\mathbf{j}\,\mathbf{k} = 1 \right\}.$$

Similarly to the case when coefficients are taken in a commutative domain, we can state the following about $\mathbb{P}_R$ and $\mathbb{H}_R$, for a generic commutative ring R.

Proposition 1.2.4. *Let R be a commutative ring. With the definitions given above, $\mathbb{H}_R$ and $\mathbb{P}_R$ are R-algebras.*

Proof. It is a direct calculation. **QED**

In particular, we will see in Proposition 1.4.4 that $\mathbb{P}_R$ is noncommutative unless R has characteristic 2.

As we did above for generalized quaternions over a commutative domain, we point out the following fact that we will use throughout this work.

Proposition 1.2.5. *An element $\mathrm{q} = a + b\,\boldsymbol{i} + c\,\boldsymbol{j} + d\,\boldsymbol{k}$ of $\mathbb{H}_R$ or $\mathbb{P}_R$ is zero if and only if $a = b = c = d = 0$.*

Proof. We will work with $\mathbb{H}_R$; for $\mathbb{P}_R$ one can argue in the same way. For proving the thesis, we first build $\mathbb{H}_R$ explicitly. Let 1, $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ be indeterminates linearly independent over R. Call F the free R-module generated by 1, $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ over R. As usual we identify 0_R with 0_F and, for simplicity, the generator 1 with the unit of R. Thus we get $F = R \oplus R\,\mathbf{i} \oplus R\mathbf{j} \oplus R\,\mathbf{k}$. Its elements are the R-linear combinations of 1, $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$. Clearly, by definition, if $a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in F$ is zero, then $a = b = c = d = 0$. The R-module F can be turned into an algebra if we say how to multiply the generators. For building $\mathbb{H}_R$ we set $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ and $\mathbf{i}\,\mathbf{j} = -\mathbf{j}\,\mathbf{i} = \mathbf{k}$ (for $\mathbb{P}_R$ use instead $-\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = 1$ and $\mathbf{i}\,\mathbf{j} = -\mathbf{j}\,\mathbf{i} = \mathbf{k}$). Extending this relations linearly over R, we obtain the algebra $\mathbb{H}_R$. The linear independence over R of 1, $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ is still true in $\mathbb{H}_R$ since the ring structure built on F does not effect the R-module structure. Similar considerations give the thesis also for $\mathbb{P}_R$. **QED**

It is important to notice that $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ are invertible elements in both $\mathbb{H}_R$ and $\mathbb{P}_R$ as it is shown here after.

Proposition 1.2.6. *With the notation above, the elements* $\mathbf{i}$, $\mathbf{j}$ *and* $\mathbf{k}$ *are units in both* $\mathbb{H}_R$ *and* $\mathbb{P}_R$.

Proof. As regards $\mathbb{H}_R$ we have that $\mathbf{i}^{-1} = -\mathbf{i}$, $\mathbf{j}^{-1} = -\mathbf{j}$ and $\mathbf{k}^{-1} = -\mathbf{k}$. In $\mathbb{P}_R$ instead we have that $\mathbf{i}^{-1} = -\mathbf{i}$, $\mathbf{j}^{-1} = \mathbf{j}$ and $\mathbf{k}^{-1} = \mathbf{k}$. **QED**

From Proposition 1.2.6, since $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ are units, it makes sense to give the following definition.

Definition 1.2.7. With the notation above, we refer to 1, $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ as the *basis units* of $\mathbb{H}_R$ and $\mathbb{P}_R$.

While the expression of a general element of the two rings $\mathbb{H}_R$ and $\mathbb{P}_R$ is the same, there are important differences between the two rings. For instance, the defining relations on the basis units imply that $\mathbf{j}\,\mathbf{k} = \mathbf{i}$ in $\mathbb{H}_R$, while $\mathbf{j}\,\mathbf{k} = -\mathbf{i}$ in $\mathbb{P}_R$. Thus, the two rings have different multiplication tables if $\mathrm{char}(R) \neq 2$. Moreover, the Lipschitz quaternions $\mathbb{H}_{\mathbb{Z}}$ are a subring of the division ring $\mathbb{H}_{\mathbb{Q}}$ (which is contained in the classical Hamiltonian quaternions $\mathbb{H}_{\mathbb{R}}$). Consequently, $\mathbb{H}_{\mathbb{Z}}$ contains no zero-divisors. However, $\mathbb{P}_{\mathbb{Z}}$ contains zero-divisors and nilpotent elements. For example, in $\mathbb{P}_{\mathbb{Z}}$ we have $(1+\mathbf{j})(1-\mathbf{j}) = 0$ and $(\mathbf{i}+\mathbf{j})^2 = 0$.

In the following we focus on split quaternions, $\mathbb{P}_R$. We start describing deeply this ring and its properties.

1.3 Matrix representation

There is a matrix representation for split quaternions.

Theorem 1.3.1. *Let R be a commutative ring such that $2 \in \mathcal{U}(R)$. Then $\mathbb{P}_R \simeq \mathcal{M}_2(R)$ as R-algebras.*

Proof. Consider the map $\varphi : \mathbb{P}_R \to \mathcal{M}_2(R)$ defined by

$$\varphi : a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \longmapsto \begin{pmatrix} a+d & b+c \\ c-b & a-d \end{pmatrix} \tag{1.5}$$

and $\psi : \mathcal{M}_2(R) \to \mathbb{P}_R$ defined by

$$\psi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \frac{1}{2}\left[(a+d) + (b-c)\,\mathbf{i} + (b+c)\,\mathbf{j} + (a-d)\,\mathbf{k}\right]. \tag{1.6}$$

It is straightforward to check that φ and ψ are inverse functions of each other. It is also immediate to see that they are R-linear. The two bijections φ and ψ determine a correspondence between an R-basis of $\mathbb{P}_R$ and one of $\mathcal{M}_2(R)$. More precisely we have: $1 \leftrightarrow \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathbf{i} \leftrightarrow \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $\mathbf{j} \leftrightarrow \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\mathbf{k} \leftrightarrow \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. It can be easily calculated that φ preserves the multiplication between $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$. Then φ preserves the product of elements of $\mathbb{P}_R$ and ψ does as well. **QED**

Remark 1.3.2. When 2 is not invertible in the ring R, Theorem 1.3.1 does not hold. For example, we have that $\mathbb{P}_\mathbb{Z} \subsetneq \mathcal{M}_2(\mathbb{Z})$. In fact the integer square matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ corresponds to the rational split quaternion $\frac{1+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2} \notin \mathbb{P}_\mathbb{Z}$. Nevertheless, when R is a domain with $\mathrm{char}(R) \neq 2$, we may use the (injective) map φ to see that $\mathbb{P}_R \subseteq \mathcal{M}_2(R)$.

Remark 1.3.3. In Theorem 1.3.1, the condition on the characteristic of R is necessary. For instance, $\mathbb{P}_{\mathbb{Z}_2}$ is a commutative ring with 8 elements and it cannot be isomorphic to a subring of $\mathcal{M}_2(\mathbb{Z}_2)$, whose center contains just two elements.

The next proposition shows the proper subring of $\mathcal{M}_2(\mathbb{Z})$ isomorphic to $\mathbb{P}_{\mathbb{Z}}$.

Theorem 1.3.4. *Let $\mathcal{A} \subseteq \mathcal{M}_2(\mathbb{Z})$ be the set*

$$\mathcal{A} \overset{def}{=} \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a \equiv d,\ b \equiv c \ (\text{mod. } 2) \} .$$

Then we have that $\mathcal{A} \simeq \mathbb{P}_{\mathbb{Z}}$.

Proof. For proving the isomorphism we use again the maps φ and ψ of Theorem (1.3.1). We need just some light modifications. If we consider $\varphi : \mathbb{P}_{\mathbb{Z}} \to \mathcal{M}_2(\mathbb{Z})$, it is easy to understand that $\mathrm{Im}(\varphi) = \mathcal{A}$. This implies that $\mathcal{A}$ is a subring of $\mathcal{M}_2(\mathbb{Z})$. We will work with the reduction $\varphi' : \mathbb{P}_{\mathbb{Z}} \to \mathcal{A}$. Because of the definition of the ring $\mathcal{A}$, the restriction $\psi' : \mathcal{A} \to \mathbb{P}_{\mathbb{Z}}$ is also well defined. It is clear that φ' and ψ' are $\mathbb{Z}$-linear, invertible and that they are inverse functions of each other. Our proof is now complete. **QED**

1.4 Bar conjugation, Norm and Trace.

The following definitions will be given simultaneously for quaternions and split quaternions with coefficients in any commutative ring. We will specify the differences between the two cases soon afterwards.

Definition 1.4.1. Let R be a commutative ring. Given $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{H}_R$ or $\mathbb{P}_R$, we say that a, b, c, and d are the *coefficients* of q. In particular we call a the *real part* of q and $b\,\mathbf{i}+c\,\mathbf{j}+d\,\mathbf{k}$ the *imaginary part* of q. We define the *bar conjugate* of q to be

$$\bar{\mathrm{q}} \overset{\mathrm{def}}{=} a-b\,\mathbf{i}-c\,\mathbf{j}-d\,\mathbf{k},$$

that is the element with the same real part of q and its opposite imaginary part.

It is well-known that the bar conjugation is an *anti-automorphism* of the ring $\mathbb{H}_{\mathbb{R}}$. This is true in general for $\mathbb{H}_R$ and $\mathbb{P}_R$, for any commutative ring R. More precisely we have the following result whose proof is straightforward.

Proposition 1.4.2. *Let R be a commutative ring. Take q and p both in $\mathbb{H}_R$ or $\mathbb{P}_R$. Then:*

(i) $\overline{\overline{\mathrm{q}}}=\mathrm{q}$*;*

(ii) $\overline{\mathrm{q}+\mathrm{p}}=\overline{\mathrm{q}}+\overline{\mathrm{p}}$*;*

(iii) $\overline{\mathrm{q}\mathrm{p}}=\overline{\mathrm{p}}\,\overline{\mathrm{q}}$*;*

(iv) $\mathrm{q}+\overline{\mathrm{q}}\in R$*;*

(v) $\mathrm{q}\overline{\mathrm{q}}\in R$*.*

We can state this simple result for central split quaternions.

Proposition 1.4.3. *Let R be a commutative ring and let $\mathrm{q}=a+b\,\mathbf{i}+c\,\mathbf{j}+d\,\mathbf{k}\in\mathbb{P}_R$. Then the following are equivalent:*

(i) $\mathrm{q}\in\mathcal{Z}(\mathbb{P}_R)$*;*

(ii) q *commutes with both* $\mathbf{i}$ *and* $\mathbf{j}$*;*

(iii) $2b = 2c = 2d = 0$;

(iv) $\mathrm{q} = \overline{\mathrm{q}}$.

Proof. (i)⇒(ii) is obvious.

(ii)⇒(i) We have that $\mathrm{q}\,\mathbf{k} = \mathrm{q}\,\mathbf{i}\,\mathbf{j} = \mathbf{i}\mathrm{q}\,\mathbf{j} = \mathbf{i}\,\mathbf{j}\mathrm{q} = \mathbf{k}\mathrm{q}$. So q commutes with $\mathbf{k}$ too. Since q commutes with the generators of $\mathbb{P}_R$, we have $\mathrm{q} \in \mathcal{Z}(\mathbb{P}_R)$.

(ii)⇔(iii) q commutes with both $\mathbf{i}$ and $\mathbf{j}$ if and only if $0 = \mathrm{q}\,\mathbf{i} - \mathbf{i}\mathrm{q} = 2d\,\mathbf{j} - 2c\,\mathbf{k}$ and $0 = \mathrm{q}\,\mathbf{j} - \mathbf{j}\mathrm{q} = 2d\,\mathbf{i} + 2b\,\mathbf{k}$. This is equivalent to having $2b = 2c = 2d = 0$.

(iii)⇔(iv) Note that $\mathrm{q} - \overline{\mathrm{q}} = 2b\,\mathbf{i} + 2c\,\mathbf{j} + 2d\,\mathbf{k}$. So $\mathrm{q} = \overline{\mathrm{q}} \Leftrightarrow \mathrm{q} - \overline{\mathrm{q}} = 0 \Leftrightarrow 2b = 2c = 2d = 0$. **QED**

Thanks to Proposition 1.4.3 we can calculate the center of $\mathbb{P}_R$ for some classes of rings R.

Proposition 1.4.4. *Let R be a commutative ring. If* $\mathrm{char}(R) = 2$ *then* $\mathcal{Z}(\mathbb{P}_R) = \mathbb{P}_R$*, that is $\mathbb{P}_R$ is a commutative ring.*

Proof. The non obvious inclusion ($\mathbb{P}_R \subseteq \mathcal{Z}(\mathbb{P}_R)$) follows from Proposition 1.4.3. In fact, since $2 \cdot 1_R = 0$, for all $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_R$ we have that $2b = 2c = 2d = 0$, so $\mathrm{q} \in \mathcal{Z}(\mathbb{P}_R)$. **QED**

Proposition 1.4.5. *Let R be a commutative ring. If 2 is not a zero-divisor, then $\mathcal{Z}(\mathbb{P}_R) = R$.*

Proof. We only show the nontrivial inclusion $\mathcal{Z}(\mathbb{P}_R) \subseteq R$. Take a central split quaternion $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$. By Proposition 1.4.3, we have that $2b = 2c = 2d = 0$. By hypothesis, 2 is not a zero-divisor, then $b = c = d = 0$. **QED**

The previous results (Proposition 1.4.3 – Proposition 1.4.5) about central elements are also true for quaternions with coefficients in a commutative ring ($\mathbb{H}_R$). The proofs are analogous.

Remark 1.4.6. When $\mathbb{P}_R$ is isomorphic to a full matrix ring (see Section 1.3), one can obtain Proposition 1.4.5 as a corollary of Proposition J. In fact, in this case the center of $\mathcal{M}_2(R)$ is isomorphic to R itself.

Remark 1.4.7. The hypothesis on the characteristic of R is essential in Proposition 1.4.5. If $\mathrm{char}(R)$ is nonzero and even, then in $\mathbb{P}_R$ there can be central elements with a nonzero imaginary part (let us call them *nontrivial central elements*). For instance, if $\mathrm{char}(R) = 2n \neq 0$ and R has more than two elements, then $a + n\,\mathbf{i} + n\,\mathbf{j} + n\,\mathbf{k}$ is a central element for any $a \in R$, as a direct calculation can show.

For our future purposes, it is the worth summing up the previous facts about central elements in the next corollary that states that scalar elements are central.

Corollary 1.4.8. *Let R be a commutative ring. Then $R \subseteq \mathcal{Z}(\mathbb{P}_R)$.*

Sometimes, when $R = \mathcal{Z}(\mathbb{P}_R)$, we call central the elements of R for meaning that they are scalars of $\mathbb{P}_R$, that are elements with zero imaginary part.

The next notions of trace and norm are introduced in [16, Chapter III.2] for generalized quaternions over fields. For our aims, we will give the following definitions for quaternions and split quaternions with coefficients in commutative rings. When needed, we will distinguish the two cases.

Definition 1.4.9. Let R be a commutative ring. Let q be an element of $\mathbb{H}_R$ or $\mathbb{P}_R$. We define the *trace* of q to be $\mathrm{T}(\mathrm{q}) \overset{\text{def}}{=} \mathrm{q} + \overline{\mathrm{q}}$ and the *norm* of q to be $\mathrm{N}(\mathrm{q}) \overset{\text{def}}{=} \mathrm{q}\overline{\mathrm{q}}$

We prove immediately the following statements.

Proposition 1.4.10. *With the notation above, let* $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{H}_R$. *Then* $\mathrm{T}(\mathrm{q}) = 2a$ *and* $\mathrm{N}(\mathrm{q}) = a^2 + b^2 + c^2 + d^2$.

Proof. It is easily proved by direct calculation. **QED**

Similarly, for split quaternions we have the next one.

Proposition 1.4.11. *With the notation above, let* $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_R$. *Then* $\mathrm{T}(\mathrm{q}) = 2a$ *and* $\mathrm{N}(\mathrm{q}) = a^2 + b^2 - c^2 - d^2$.

Proof. It follows by direct calculation. **QED**

Proposition 1.4.11 explains why split quaternions are called this way. This is because their norm splits in a positive and a negative part.

It is convenient to state this immediate property.

Proposition 1.4.12. *Let* R *be a commutative ring. Let* $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{H}_R$ *or in* $\mathbb{P}_R$. *Then* $\mathrm{T}(\mathrm{q}) = \mathrm{T}(\overline{\mathrm{q}})$ *and* $\mathrm{N}(\mathrm{q}) = \mathrm{N}(\overline{\mathrm{q}})$.

Proof. It follows immediately by calculation. **QED**

The norm and the trace of a split quaternion are, respectively, the determinant and the trace of the matrix associated under the matrix representation. More precisely, we have the following result.

Proposition 1.4.13. *Let* R *be (any) commutative ring and let* $\varphi : \mathbb{P}_R \to \mathcal{M}_2(R)$ *defined as in (1.5) of Proposition 1.3.1. Let* $\mathrm{q} \in \mathbb{P}_R$. *Then* $\mathrm{T}(\mathrm{q}) = \mathrm{tr}(\varphi(\mathrm{q}))$ *and* $\mathrm{N}(\mathrm{q}) = \det(\varphi(\mathrm{q}))$.

Proof. It is straightforward. **QED**

We generalize here a well-known result true for real quaternions: the norm is multiplicative. We will often use this fact in the following.

Proposition 1.4.14. *Let R be a commutative ring. Let* $\mathrm{q}, \mathrm{p} \in \mathbb{H}_R$ *or* $\mathbb{P}_R$. *Then*

$$\mathrm{N}(\mathrm{q}\,\mathrm{p}) = \mathrm{N}(\mathrm{q})\,\mathrm{N}(\mathrm{p}).$$

Proof. $\mathrm{N}(\mathrm{q}\,\mathrm{p}) = \mathrm{q}\,\mathrm{p}(\overline{\mathrm{q}\,\mathrm{p}}) = \mathrm{q}\,\mathrm{p}\,\overline{\mathrm{p}}\,\overline{\mathrm{q}} = \mathrm{q}\,\mathrm{N}(\mathrm{p})\overline{\mathrm{q}} = \mathrm{N}(\mathrm{q})\,\mathrm{N}(\mathrm{p}).$ **QED**

Given a division ring K, its center F results to be a field. We say that an element $a \in K$ is *algebraic* over F if there exists a nonzero polynomial $f(x) \in F[x]$ such that $f(a) = 0$. The monic polynomial of least degree with this property is called the *minimal polynomial* of a over F. If every $a \in K$ is algebraic over F we say that K is algebraic over its center.

In the same way, given a commutative ring R, we can give the notion of algebraic elements of $\mathbb{H}_R$ and $\mathbb{P}_R$ over their centers. In particular, it results that $\mathbb{H}_R$ and $\mathbb{P}_R$ are algebraic extensions of the ring of coefficients R (which is contained in the center of both $\mathbb{H}_R$ and $\mathbb{P}_R$). We will prove this by using the norm and the trace defined above.

Proposition 1.4.15. *Let R be a commutative ring. Let* q *be an element of* $\mathbb{H}_R$ *or* $\mathbb{P}_R$. *Then* q *is a root of the quadratic polynomial*

$$x^2 - \mathrm{T}(\mathrm{q})\,x + \mathrm{N}(\mathrm{q}) \in R[x].$$

Proof. From the relation $\mathrm{q} = \mathrm{T}(\mathrm{q}) - \overline{\mathrm{q}}$, we obtain that $\mathrm{q}^2 = (\mathrm{T}(\mathrm{q}) - \overline{\mathrm{q}})\mathrm{q} = \mathrm{T}(\mathrm{q})\mathrm{q} - \overline{\mathrm{q}}\mathrm{q} = \mathrm{T}(\mathrm{q})\mathrm{q} - \mathrm{N}(\mathrm{q})$. **QED**

For both quaternions and split quaternions, it makes sense to give the following definition.

Definition 1.4.16. Let R be a commutative ring. Given $\mathrm{q} \in \mathbb{H}_R$ or in $\mathbb{P}_R$, we define the *minimal polynomial of* q to be

$$m_{\mathrm{q}}(x) = \begin{cases} x - \mathrm{q} & \text{if } \mathrm{q} \in R \\ x^2 - \mathrm{T}(\mathrm{q})x + \mathrm{N}(\mathrm{q}) & \text{if } \mathrm{q} \notin R. \end{cases}$$

Remark 1.4.17. In Definition 1.4.16 there is a relevant difference between the quaternion and split quaternion cases (while the definitions and the properties we analyzed until now are similar). It happens that the minimal polynomial over $\mathbb{R}$ of a real quaternion is an irreducible polynomial, instead for real split quaternions this is not true in general.

Proposition 1.4.18. *Let* $\mathrm{q} \in \mathbb{H}_{\mathbb{R}}$*. Then the minimal polynomial* $m_{\mathrm{q}}(x) \in \mathbb{R}[x]$ *is irreducible over* $\mathbb{R}$*.*

Proof. If $\mathrm{q} \in \mathbb{R}$, by Definition 1.4.16, $m_{\mathrm{q}}(x)$ is linear so irreducible over $\mathbb{R}$. Let $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \notin \mathbb{R}$ be now a noncentral quaternion. We recall that $\mathrm{N}(\mathrm{q}) = a^2 + b^2 + c^2 + d^2$ (see Proposition 1.4.10). So the discriminant of its minimal polynomial $m_{\mathrm{q}}(x) = x^2 - \mathrm{T}(\mathrm{q})\,x + \mathrm{N}(\mathrm{q})$ is $\Delta = \mathrm{T}(\mathrm{q})^2 - 4\,\mathrm{N}(\mathrm{q}) = -4(b^2 + c^2 + d^2) < 0$. This means that $m_{\mathrm{q}}(x)$ is an irreducible polynomial over $\mathbb{R}$. **QED**

For split quaternions the previous result is not true in general. In the following remark we give some examples.

Remark 1.4.19. Let $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{R}}$ be a real split quaternion. Let $m_{\mathrm{q}}(x)$ be its minimal polynomial. The discriminant of the minimal polynomial becomes

$$\Delta = \mathrm{T}(\mathrm{q})^2 - 4\,\mathrm{N}(\mathrm{q}) = -4(b^2 - c^2 - d^2)$$

which can equal any real value: zero, positive or negative. This implies that the minimal polynomial of a real split quaternion can be irreducible (as for quaternions), reducible or in some cases, the square of a linear polynomial.

For example we have that $\mathbf{i}$ is a root of the irreducible polynomial x^2+1 but $\mathbf{j}$ and $\mathbf{i}+\mathbf{j}$ are respectively roots of the polynomials x^2-1 and x^2, both reducible over $\mathbb{R}$.

It may sound strange to call *minimal* a polynomial that is reducible. Here we are forced to do so since no real split quaternion with nonzero imaginary part can be a root of a linear polynomial belonging to $\mathbb{R}[x]$.

Let K be a noncommutative division ring and let $a, b \in K$ be algebraic over $\mathcal{Z}(K)$. A well known result by E. Dickson states that a and b are conjugate in K if and only if they have the same minimal polynomial over $\mathcal{Z}(K)$, see [14, Theorem 16.8].

For split quaternions something similar is true.

Proposition 1.4.20. *Let R be a commutative ring. Let q and p be conjugate in $\mathbb{P}_R$. Then p and q have the same norm and trace. In particular p and q share the same minimal polynomial.*

Proof. Let N and T be the norm and trace of q. Let $\mathrm{p} = c\mathrm{q}c^{-1}$, for some invertible $c \in \mathbb{P}_R$. We have:

$$\begin{aligned}
\mathrm{N}(\mathrm{p}) &= \mathrm{N}(c\mathrm{q}c^{-1}) \\
&= c\mathrm{q}c^{-1}\overline{(c\mathrm{q}c^{-1})} \\
&= c\mathrm{q}c^{-1}\overline{c^{-1}}\,\overline{\mathrm{q}}\,\overline{c} \\
&= \mathrm{N}(c)^{-1}\,\mathrm{N}(q)\,\mathrm{N}(c) \\
&= \mathrm{N}(q).
\end{aligned}$$

As regards trace we have:

$$\begin{aligned}
\mathrm{T}(\mathrm{p}) &= \mathrm{T}(c\mathrm{q}c^{-1})\\
&= c\mathrm{q}c^{-1} + \overline{\left(c\mathrm{q}\frac{1}{\mathrm{N}(c)}\overline{c}\right)}\\
&= c\mathrm{q}c^{-1} + \overline{\overline{c}}\,\overline{\mathrm{q}}\,\frac{1}{\mathrm{N}(c)}\overline{c}\\
&= c\mathrm{q}c^{-1} + c\overline{\mathrm{q}}c^{-1}\\
&= c(\mathrm{q}+\overline{\mathrm{q}})c^{-1}\\
&= \mathrm{T}(\mathrm{q}).
\end{aligned}$$

QED

Remark 1.4.21. The converse of Proposition 1.4.20 is not true in general. We have that $\mathbf{j}$ and $\mathbf{k}$ in $\mathbb{P}_{\mathbb{Z}}$ have the same norm and trace and they are both root of $x^2+1 \in \mathbb{Z}[x]$. Nevertheless they are not conjugate in $\mathbb{P}_{\mathbb{Z}}$. If it were so, we would have $\mathbf{j}\mathrm{q} = \mathrm{q}\,\mathbf{k}$, for some $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathcal{U}(\mathbb{P}_{\mathbb{Z}})$. By calculation one gets: $a = -b$ and $c = d$. Since q is supposed to be invertible in $\mathbb{P}_{\mathbb{Z}}$, we must have $\mathrm{N}(\mathrm{q}) = 2a^2 - 2c^2 = \pm 1$, which is impossible in $\mathbb{Z}$.

1.5 Units, zero-divisors, idempotent and nilpotent elements of $\mathbb{P}_R$

In what follows we use norm and trace defined in Section 1.4 in order to characterize units, zero-divisors, idempotent and nilpotent elements of $\mathbb{P}_R$.

Since $\mathbb{P}_R$ is in general a noncommutative ring, we should distinguish left zero-divisors by right ones. The same should be for right and left-invertible elements. Nevertheless, we will see in the following that in $\mathbb{P}_R$ we can avoid the side specification.

We give now a characterization for units.

Proposition 1.5.1. *Let R be a commutative ring. Let* $\mathrm{q} \in \mathbb{P}_R$. *Then the following are equivalent:*

(i) q *is right-invertible with right-inverse* $\frac{1}{\mathrm{N}(\mathrm{q})}\,\overline{\mathrm{q}}$*;*

(ii) q *is left-invertible with left-inverse* $\frac{1}{\mathrm{N}(\mathrm{q})}\,\overline{\mathrm{q}}$*;*

(iii) $\mathrm{N}(\mathrm{q}) \in \mathcal{U}(R)$.

Proof. We will prove only (i)⇔(iii). The equivalence (ii)⇔(iii) is similar. If $\mathrm{qp} = 1$, for some $\mathrm{p} \in \mathbb{P}_R$, since the norm is multiplicative, we have $\mathrm{N}(\mathrm{q})\,\mathrm{N}(\mathrm{p}) = 1$. This means that the norm of q is invertible in R. For the converse, suppose that $\mathrm{N}(\mathrm{q})$ is invertible. By calculation one can see that $\frac{1}{\mathrm{N}(\mathrm{q})}\,\overline{\mathrm{q}}$ is a right-inverse of q. **QED**

Since Proposition 1.5.1 assures that right-invertible elements are also left-invertible and vice versa, it makes sense to consider $\mathcal{U}(\mathbb{P}_R)$, the set of invertible elements of $\mathbb{P}_R$. We give the following immediate corollary.

Corollary 1.5.2. *Let R be a commutative ring. Let* $\mathrm{q} \in \mathbb{P}_R$. *Then* $\mathrm{q} \in \mathcal{U}(\mathbb{P}_R)$ *if and only if* $\mathrm{N}(\mathrm{q})$ *is invertible in R.*

In particular we have the following statement.

Corollary 1.5.3. *Let k be a field. Then*

$$\mathcal{U}(\mathbb{P}_k) = \{\, \mathrm{q} \in \mathbb{P}_k \;\mid\; \mathrm{N}(\mathrm{q}) \neq 0 \,\}\,.$$

Moreover,

$$\mathcal{U}(\mathbb{P}_{\mathbb{Z}}) = \{\, \mathrm{q} \in \mathbb{P}_{\mathbb{Z}} \;\mid\; \mathrm{N}(\mathrm{q}) = \pm 1 \,\}\,.$$

In literature, for instance see [14, Example 1.1], it is known that

$$\mathcal{U}(\mathbb{H}_{\mathbb{Z}}) = Q_8$$

the group of the eight quaternions. The unit group of $\mathbb{P}_{\mathbb{Z}}$ is instead an infinite group. We can state something more general for split quaternions with coefficients over commutative rings.

Proposition 1.5.4. *Let R be an infinite commutative ring. Then $\mathcal{U}(\mathbb{P}_R)$ is an infinite group.*

Proof. Let $a \in R^*$. Then consider the split quaternion $\mathrm{q} = 1 + a\,\mathbf{i} + a\,\mathbf{j}$. By Corollary 1.5.2, since $\mathrm{N}(\mathrm{q}) = 1 + a^2 - a^2 = 1$, we have that q is invertible. Since there infinitely many elements in R, there are infinite such invertible elements in $\mathbb{P}_R$. **QED**

The following result characterizes the zero-divisors of $\mathbb{P}_R$.

Proposition 1.5.5. *Let R be a commutative ring. Let $\mathrm{q} \in \mathbb{P}_R$. Then the following are equivalent:*

(i) q *is a left zero-divisor;*

(ii) q *is a right zero-divisor;*

(iii) $\mathrm{N}(\mathrm{q})$ *is a zero-divisor in R.*

Proof. We will prove only (i)⇔(iii). The equivalence (ii)⇔(iii) is similar since $\mathrm{q}\overline{\mathrm{q}} = \overline{\mathrm{q}}\mathrm{q}$, for any $\mathrm{q} \in \mathbb{P}_R$. If q is a left zero-divisor, then there exists a $\mathrm{p} \in \mathbb{P}_R$ such that $\mathrm{qp} = 0$. Then $\mathrm{N}(\mathrm{qp}) = \mathrm{N}(\mathrm{q})\,\mathrm{N}(\mathrm{p}) = 0$, which means that $\mathrm{N}(\mathrm{q})$ is a zero-divisor in R. For the converse, suppose that $\mathrm{N}(\mathrm{q})$ is a zero-divisor in R. Then $\mathrm{N}(\mathrm{q})a = 0$, for some $a \in R$. Thus $\mathrm{q}(\overline{\mathrm{q}}a) = \mathrm{N}(\mathrm{q})a = 0$, which means that q is a left zero-divisor. **QED**

Since in $\mathbb{P}_R$ every left zero-divisor is also a right zero-divisor and *vice versa*, it makes sense to consider $\mathcal{D}(\mathbb{P}_R)$, the set of all zero-divisors of $\mathbb{P}_R$.

The following result immediately follows.

Corollary 1.5.6. *Let D be a commutative domain. Let $\mathrm{q} \in \mathbb{P}_D$. Then $\mathrm{q} \in \mathcal{D}(\mathbb{P}_D)$ if and only if $\mathrm{N}(\mathrm{q}) = 0$.*

We recall again that while $\mathbb{H}_\mathbb{R}$, $\mathbb{H}_\mathbb{Q}$ and $\mathbb{H}_\mathbb{Z}$ are noncommutative integral domains (in particular $\mathbb{H}_\mathbb{R}$ and $\mathbb{H}_\mathbb{Q}$ are skew fields) we have that $\mathbb{P}_\mathbb{R}$, $\mathbb{P}_\mathbb{Q}$ and $\mathbb{P}_\mathbb{Z}$ contains zero-divisors. Take for instance $1 - \mathbf{j}$. This is a zero-divisor also in $\mathbb{P}_D$, for all commutative domains D. In this way we see that even if D is a commutative domain, then $\mathbb{P}_D$ can contain zero-divisors. We show in the next result instead, that no scalar element of D can vanish the elements of $\mathbb{P}_D$.

Proposition 1.5.7. *Let D be a commutative domain. Let $a \in D$ and $\mathrm{q} \in \mathbb{P}_D$. Suppose that $a\mathrm{q} = 0$. Then $a = 0$ or $\mathrm{q} = 0$. In particular $\mathbb{Z} \cap \mathcal{D}(\mathbb{P}_\mathbb{Z}) = \varnothing$.*

Proof. It is immediate since D does not contain any zero-divisors. **QED**

We study now the idempotent elements of a split quaternion ring.

Proposition 1.5.8. *Let D be a commutative domain. Then $\mathrm{q} \in \mathbb{P}_D \setminus D$ is an idempotent if and only if $\mathrm{T}(\mathrm{q}) = 1$ and $\mathrm{N}(\mathrm{q}) = 0$.*

Proof. Let us consider a split quaternion $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$. By Proposition 1.4.15, we can write $\mathrm{q}^2 = \mathrm{T}(\mathrm{q})\mathrm{q} - \mathrm{N}(\mathrm{q})$. If $\mathrm{T}(\mathrm{q}) = 1$ and $\mathrm{N}(\mathrm{q}) = 0$, it is clear that $\mathrm{q}^2 = \mathrm{q}$. Conversely, take an idempotent $\mathrm{q} \in \mathbb{P}_D \setminus D$. Then we get the conditions:

$$\begin{cases}(\mathrm{T}(\mathrm{q})-1)a=\mathrm{N}(\mathrm{q})\\(\mathrm{T}(\mathrm{q})-1)b=0\\(\mathrm{T}(\mathrm{q})-1)c=0\\(\mathrm{T}(\mathrm{q})-1)d=0\end{cases}$$

If $\mathrm{T}(\mathrm{q})=1$ then $\mathrm{N}(\mathrm{q})=0$. If $\mathrm{T}(\mathrm{q})\neq 1$, then $b=c=d=0$. This means that $\mathrm{q}=a$ is an idempotent in the domain D which is absurd. **QED**

The next result shows that split quaternion rings can also contain nilpotent elements.

Proposition 1.5.9. *Let D be a commutative domain. Then a nilpotent element of $\mathbb{P}_D$ has at most nilpotence index 2. Moreover $\mathrm{q}\in\mathbb{P}_D$ is nilpotent if and only if $\mathrm{T}(\mathrm{q})=\mathrm{N}(\mathrm{q})=0$.*

Proof. By Proposition 1.4.15, we can write $\mathrm{q}^2=\mathrm{T}(\mathrm{q})\mathrm{q}-\mathrm{N}(\mathrm{q})$. Clearly, if $\mathrm{T}(\mathrm{q})=\mathrm{N}(\mathrm{q})=0$, then q is nilpotent of index 2. For the converse, assume that q is nilpotent and nonzero with nilpotence index n, for some integer $n\geqslant 2$. We will show that $\mathrm{T}(\mathrm{q})=\mathrm{N}(\mathrm{q})=0$ and that $n=2$. Since the norm is multiplicative, $0=\mathrm{N}(\mathrm{q}^n)=(\mathrm{N}(\mathrm{q}))^n$. Being D a domain, $\mathrm{N}(\mathrm{q})=0$. Then $q^2=\mathrm{T}(\mathrm{q})\mathrm{q}$. By induction, we get $\mathrm{q}^n=(\mathrm{T}(\mathrm{q}))^{n-1}\mathrm{q}$ and $(\mathrm{T}(\mathrm{q}))^{n-1}\mathrm{q}=0$. This forces $(\mathrm{T}(\mathrm{q}))^{n-1}=0$, and hence $\mathrm{T}(\mathrm{q})=0$. Thus $\mathrm{q}^2=\mathrm{T}(\mathrm{q})\mathrm{q}=0$ and $n=2$. **QED**

1.6 Ideal structure of $\mathbb{P}_{\mathbb{Z}}$

In this section we describe the ideal structure of the ring $\mathbb{P}_{\mathbb{Z}}$. In order to make our calculations easier, we will often use the matrix representation (1.5) of

$\mathbb{P}_{\mathbb{Z}}$ introduced in Section 1.3, the norm and the trace of the elements of $\mathbb{P}_{\mathbb{Z}}$ we studied in Section 1.4.

We will see that the maximal and primes ideals of $\mathbb{P}_{\mathbb{Z}}$ are generated by at most two elements. Moreover, the Proposition I assures that $\mathbb{P}_{\mathbb{Z}}$ is a noetherian ring: all the ideals of $\mathbb{P}_{\mathbb{Z}}$ are finitely generated.

Proposition 1.6.1. *Let R be a commutative noetherian ring. Then $\mathbb{P}_R$ is a noetherian ring.*

Proof. Recall that R is contained in the center of $\mathbb{P}_R$, by Proposition 1.4.8. Further, 1, $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ are generators of $\mathbb{P}_R$ over R. The conclusion follows by Proposition I. **QED**

We see now that the ideals of $\mathbb{P}_R$ are closed under norm.

Proposition 1.6.2. *Let R be a commutative ring. Let $\mathscr{I}$ be an ideal of $\mathbb{P}_R$ and let $\mathrm{q} \in \mathscr{I}$. Then $\mathrm{N}(\mathrm{q}) \in \mathscr{I}$ as well.*

Proof. It follows from the definition of norm (see Definition 1.4.9). **QED**

The rings $\mathbb{H}_{\mathbb{R}}$ and $\mathbb{H}_{\mathbb{Q}}$ have only trivial ideals since they are skew fields. In [12, Exercise 3A] it is shown that the prime ideals of $\mathbb{H}_{\mathbb{Z}}$ are (0), $p\mathbb{H}_{\mathbb{Z}}$, for all odd prime integers p, and the doubly generated ideal $(1+\mathbf{i}, 1+\mathbf{j})$, which contains 2.

By using the matrix representation (1.5) of split quaternions we can state some preliminary results about the ideals of $\mathbb{P}_R$ depending on the ideal structure of R. The key is the bijection between the ideals of R and $\mathcal{M}_n(R)$ stated in Proposition K.

Proposition 1.6.3. *With the notations introduced above, we have that:*

(i) For any field F with $\mathrm{char}(F) \neq 2$, *the ring $\mathbb{P}_F$ is a simple ring. In particular, $\mathbb{P}_{\mathbb{R}}$, $\mathbb{P}_{\mathbb{Q}}$ and $\mathbb{P}_{\mathbb{Z}_p}$, for any odd prime integer p, are simple rings.*

(ii) For any odd integer m, the ring $\mathbb{P}_{\mathbb{Z}_m}$ is a principal ideal ring.

(iii) For any odd prime integer p, the ring $\mathbb{P}_{\mathbb{Z}_{(p)}}$ is a local principal ideal ring.

Proof. It is an immediate consequence of Proposition 1.3.1 and Proposition K. **QED**

It is important to notice that Proposition 1.6.3,(ii) does not hold in general for even values of the integer m. Later, in Proposition 1.6.15, we will see that $\mathbb{P}_{\mathbb{Z}_2}$ has a doubly generated ideal.

After Proposition K, we can also state that the ring $\mathcal{M}_n(\mathbb{Z})$ is a principal ideal ring. This does not imply necessarily that $\mathbb{P}_{\mathbb{Z}} \simeq \mathcal{A} \subsetneq \mathcal{M}_2(\mathbb{Z})$ is a principal ideal ring too. In fact, we will see in Theorem 1.6.22 that $\mathbb{P}_{\mathbb{Z}}$ contains the doubly generated ideal $\mathscr{M} = (1 + \mathbf{i}, 1 + \mathbf{j})$.

Norm, trace and the algebraicity of the elements of $\mathbb{P}_{\mathbb{Z}}$ over $\mathbb{Z}$ will play a fundamental role in this context.

Let us start with the ideal (0) of $\mathbb{P}_{\mathbb{Z}}$. In a commutative ring R the condition that (0) is a prime ideal is equivalent for R being a domain. In a noncommutative ring this equivalence is not true in general. We are going to show that, although there are zero-divisors in the ring $\mathbb{P}_{\mathbb{Z}}$, the trivial ideal (0) is prime. The proof of this fact needs some preliminary and technical results.

Lemma 1.6.4. *Let $\mathscr{I} \neq (0)$ be an ideal of $\mathbb{P}_{\mathbb{Z}}$. Let* q *be a nonzero element of $\mathscr{I}$ and let a be one of the nonzero coefficients of* q. *Then $\mathscr{I}$ contains an element* q' *such that the real part of* q' *equals a.*

Proof. Let $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$. By some simple calculations we have that

$$\begin{aligned} \mathrm{q}(-\,\mathbf{i}) &= b - a\,\mathbf{i} - d\,\mathbf{j} + c\,\mathbf{k} \\ \mathrm{q}\,\mathbf{j} &= c + d\,\mathbf{i} + a\,\mathbf{j} + b\,\mathbf{k} \\ \mathrm{q}\,\mathbf{k} &= d - c\,\mathbf{i} - b\,\mathbf{j} + a\,\mathbf{k}. \end{aligned} \tag{1.7}$$

Since $\mathscr{I}$ is an ideal, all these products are elements of $\mathscr{I}$ too. So the equations (1.7) show how we can build other elements of $\mathscr{I}$ whose real part is equal to one of the imaginary coefficients of q. **QED**

Lemma 1.6.5. *Let $\mathscr{I}$ be an ideal of $\mathbb{P}_{\mathbb{Z}}$. Let $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathscr{I}$. Then $\mathscr{I}$ contains* $4a$, $4b$, $4c$ *and* $4d$.

Proof. Starting from q we can build the following elements of $\mathscr{I}$.

$$\begin{aligned} -\,\mathbf{i}\,\mathrm{q}\,\mathbf{i} &= a + b\,\mathbf{i} - c\,\mathbf{j} - d\,\mathbf{k}, \\ \mathbf{j}\,\mathrm{q}\,\mathbf{j} &= a - b\,\mathbf{i} + c\,\mathbf{j} - d\,\mathbf{k}, \\ \mathbf{k}\,\mathrm{q}\,\mathbf{k} &= a - b\,\mathbf{i} - c\,\mathbf{j} + d\,\mathbf{k}. \end{aligned} \tag{1.8}$$

The sum $\mathrm{q} - \ \mathbf{i}\,\mathrm{q}\,\mathbf{i} + \ \mathbf{j}\,\mathrm{q}\,\mathbf{j} + \ \mathbf{k}\,\mathrm{q}\,\mathbf{k} = 4a \in \mathscr{I}$. Similarly for the others, if we permute coefficients as in Lemma 1.6.4. **QED**

Proposition 1.6.6. *Every nonzero ideal of $\mathbb{P}_{\mathbb{Z}}$ contains an element of nonzero norm.*

Proof. Let us suppose *ab absurdo* that the ideal $\mathscr{I} \neq (0)$ of $\mathbb{P}_{\mathbb{Z}}$ is a subset of $\mathcal{D}(\mathbb{P}_{\mathbb{Z}})$. By Lemma 1.6.4 we can find in $\mathscr{I}$ an element with a nonzero real part, call it a. By Lemma 1.6.5, $4a \neq 0$ is an element of $\mathscr{I}$. This means that $\mathrm{N}(4a) = 16a^2 \neq 0$ and that $4a$ is not a zero-divisor (Proposition 1.5.7). This contradicts our hypothesis on $\mathscr{I}$. **QED**

Immediately, we have the following result.

Corollary 1.6.7. *Every nonzero ideal of* $\mathbb{P}_{\mathbb{Z}}$ *contains a nonzero element of* $\mathbb{Z}$.

Proof. It follows from Proposition 1.6.2 and Proposition 1.6.6. **QED**

Lemma 1.6.8. *A nonzero prime ideal of* $\mathbb{P}_{\mathbb{Z}}$ *contains exactly one prime integer.*

Proof. Let $\mathscr{I}$ be a nonzero prime ideal of $\mathbb{P}_{\mathbb{Z}}$. By Corollary 1.6.7, in $\mathscr{I}$ we can find an integer $m > 1$. Let us suppose that $m = p_1 p_2 \cdots p_t$, for some not necessarily distinct primes p_i. This means that $p_1 p_2 \cdots p_t \mathbb{P}_{\mathbb{Z}} \subseteq \mathscr{I}$. Since the p_i's are central, we can write $p_1 \mathbb{P}_{\mathbb{Z}} p_2 \cdots p_t \subseteq \mathscr{I}$. By our hypothesis $\mathscr{I}$ is a prime ideal, and it follows that $p_1 \in \mathscr{I}$ or $p_2 \cdots p_t \in \mathscr{I}$. By induction we can state that $\mathscr{I}$ must contain one of the p_i's. Finally, $\mathscr{I}$ cannot contain two different prime numbers. Otherwise it would be the whole ring $\mathbb{P}_{\mathbb{Z}}$ by using a Bézout identity. **QED**

Now we are ready to state our first result about prime ideals of $\mathbb{P}_{\mathbb{Z}}$.

Proposition 1.6.9. *The zero ideal* (0) *is a prime ideal of* $\mathbb{P}_{\mathbb{Z}}$.

Proof. Let $\mathscr{I}$ and $\mathscr{J}$ be ideals of $\mathbb{P}_{\mathbb{Z}}$ such that $\mathscr{I}\mathscr{J} \subseteq (0)$. We must show that $\mathscr{I} = (0)$ or $\mathscr{J} = (0)$. If $\mathscr{I} = (0)$ we are done. If it is not so, thanks to Corollary 1.6.7, we can take in $\mathscr{I}$ an integer $n \neq 0$. Since n is central, for every $\mathrm{p} \in \mathscr{J}$ we have $n\mathrm{p} = 0$. By Proposition 1.5.7, this implies that $\mathrm{p} = 0$ and that $\mathscr{J}$ is the zero ideal. **QED**

Now we study the primality of the ideals of the form $p\mathbb{P}_{\mathbb{Z}}$, generated by an odd prime integer p. We will make use of split quaternions with coefficients in the finite field $\mathbb{Z}_p$ of order a prime p.

We recall here that, by Proposition 1.3.1, if p is odd, we have the isomorphism

$$\mathbb{P}_{\mathbb{Z}_p} \simeq \mathcal{M}_2(\mathbb{Z}_p). \tag{1.9}$$

Proposition 1.6.10. *Let m be a nonzero integer. Then*

$$\frac{\mathbb{P}_{\mathbb{Z}}}{m\mathbb{P}_{\mathbb{Z}}} \simeq \mathbb{P}_{\mathbb{Z}_m} \tag{1.10}$$

Proof. Consider the map $\psi : \mathbb{P}_{\mathbb{Z}} \to \mathbb{P}_{\mathbb{Z}_m}$ such that $\psi(a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}) = \overline{a} + \overline{b}\,\mathbf{i} + \overline{c}\,\mathbf{j} + \overline{d}\,\mathbf{k}$, where $\overline{a}, \overline{b}, \overline{c}, \overline{d}$ are the residues modulo m of the respective coefficients of q. The map ψ is obviously surjective. Take now an integer split quaternion $a+b\,\mathbf{i}+c\,\mathbf{j}+d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$ such that $\psi(a+b\,\mathbf{i}+c\,\mathbf{j}+d\,\mathbf{k}) = \overline{a}+\overline{b}\,\mathbf{i}+\overline{c}\,\mathbf{j}+\overline{d}\,\mathbf{k} = 0$ in $\mathbb{P}_{\mathbb{Z}_m}$. Then m divides the coefficients a, b, c and d in $\mathbb{Z}$. Thus it is easy to see that $\ker\psi = m\mathbb{P}_{\mathbb{Z}}$. The thesis follows from the first isomorphism theorem for rings. **QED**

We get the following result.

Proposition 1.6.11. *Let p be an odd prime integer. We have the isomorphism*

$$\frac{\mathbb{P}_{\mathbb{Z}}}{p\mathbb{P}_{\mathbb{Z}}} \simeq \mathcal{M}_2(\mathbb{Z}_p). \tag{1.11}$$

Proof. It is easily obtained putting together (1.9) and (1.10). **QED**

Proposition 1.6.12. *Let p be an odd prime integer. Then the ideal $p\mathbb{P}_{\mathbb{Z}}$ is a maximal ideal of $\mathbb{P}_{\mathbb{Z}}$.*

Proof. By Proposition 1.6.11 the quotient ring $\frac{\mathbb{P}_{\mathbb{Z}}}{p\mathbb{P}_{\mathbb{Z}}}$ is isomorphic to the matrix ring $\mathcal{M}_2(\mathbb{Z}_p)$, which by Proposition K,(i) is a simple ring. By the correspondence theorem for rings we can say that there are no proper ideals over $p\mathbb{P}_{\mathbb{Z}}$ in $\mathbb{P}_{\mathbb{Z}}$. In other words $p\mathbb{P}_{\mathbb{Z}}$ is a maximal ideal in the ring $\mathbb{P}_{\mathbb{Z}}$. **QED**

Corollary 1.6.13. *Let p be an odd prime integer. Then the ideal $p\mathbb{P}_{\mathbb{Z}}$ is a prime ideal of $\mathbb{P}_{\mathbb{Z}}$.*

Proof. By Proposition E and Proposition 1.6.12. **QED**

Remark 1.6.14. In Chapter 0 we recalled that the quotient ring of a maximal ideal is a simple ring and, if the ring is commutative, this quotient is a field. In general, in a noncommutative setting the quotient at a maximal ideal may not be a skew field. For instance, in Proposition 1.6.12 we showed that $p\mathbb{P}_{\mathbb{Z}}$ is a maximal ideal of $\mathbb{P}_{\mathbb{Z}}$, for odd primes p. Nevertheless the ring $\mathbb{P}_{\mathbb{Z}_p}$ is not a domain. Here we have that $(\overline{1} + \mathbf{j})(\overline{1} - \mathbf{j}) = 0$.

The case $p = 2$ requires a distinct discussion. Unfortunately, in this case we cannot use the matrix representation as we did for odd primes. We will proceed with direct calculations. By Proposition 1.6.10 we know that

$$\frac{\mathbb{P}_{\mathbb{Z}}}{2\mathbb{P}_{\mathbb{Z}}} \simeq \mathbb{P}_{\mathbb{Z}_2}. \tag{1.12}$$

Proposition 1.6.15. *The ring $\mathbb{P}_{\mathbb{Z}_2}$ is a commutative local ring with sixteen elements. Its maximal ideal is the ideal generated by $1 + \mathbf{i}$ and $1 + \mathbf{j}$ and the correspondent residue ring is $\mathbb{F}_2$.*

Proof. We have that

$$\begin{aligned}\mathbb{P}_{\mathbb{Z}_2} =\{&0,\ 1,\ \mathbf{i},\ \mathbf{j},\ \mathbf{k},\ 1+\mathbf{i},\ 1+\mathbf{j},\ 1+\mathbf{k},\ \mathbf{i}+\mathbf{j},\ \mathbf{i}+\mathbf{k},\ \mathbf{j}+\mathbf{k},\\ &1+\mathbf{i}+\mathbf{j},\ 1+\mathbf{i}+\mathbf{k},\ 1+\mathbf{j}+\mathbf{k},\ \mathbf{i}+\mathbf{j}+\mathbf{k},\ 1+\mathbf{i}+\mathbf{j}+\mathbf{k}\}.\end{aligned}$$

So it has sixteen elements. Since it has characteristic 2, by Proposition 1.4.4, $\mathbb{P}_{\mathbb{Z}_2}$ is a commutative ring. Given $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}_2}$, we have that q is invertible if and only if $\mathrm{N}(\mathrm{q}) = 1$ and q is noninvertible if and only if $\mathrm{N}(\mathrm{q}) = 0$, thus it is a zero-divisor (see Propositions 1.5.2 and 1.5.5). Moreover, for all $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}_2}$, we have that $\mathrm{q} = \overline{\mathrm{q}}$. From this it follows that norm is additive as well as multiplicative. For seeing this, notice first that for any $\mathrm{q}, \mathrm{q}_1 \in \mathbb{P}_{\mathbb{Z}_2}$ we have $\mathrm{q}\overline{\mathrm{q}_1} = \overline{\mathrm{q}_1}\mathrm{q}$, by the commutativity of multiplication. Finally, it follows that

$$\begin{aligned} \mathrm{N}(\mathrm{q}+\mathrm{q}_1) &= (\mathrm{q}+\mathrm{q}_1)\overline{(\mathrm{q}+\mathrm{q}_1)} \\ &= \mathrm{q}\overline{\mathrm{q}} + \mathrm{q}\overline{\mathrm{q}_1} + \mathrm{q}_1\overline{\mathrm{q}} + \mathrm{q}_1\overline{\mathrm{q}_1} \\ &= \mathrm{q}\overline{\mathrm{q}} + \mathrm{q}_1\overline{\mathrm{q}_1} + 2\mathrm{q}\overline{\mathrm{q}_1} \\ &= \mathrm{q}\overline{\mathrm{q}} + \mathrm{q}_1\overline{\mathrm{q}_1} \\ &= \mathrm{N}(\mathrm{q}) + \mathrm{N}(\mathrm{q}_1). \end{aligned}$$

By this, it is easy to show that the zero-divisors form a maximal ideal M. In particular

$$M = \mathcal{D}(\mathbb{P}_{\mathbb{Z}_2}) = \{\, 0,\ 1+\mathbf{i},\ 1+\mathbf{j},\ 1+\mathbf{k},\ \mathbf{i}+\mathbf{j},\ \mathbf{i}+\mathbf{k},\ \mathbf{j}+\mathbf{k},\ 1+\mathbf{i}+\mathbf{j}+\mathbf{k}\,\},$$

which is generated by $1+\mathbf{i}$ and $1+\mathbf{j}$. Since M contains eight elements we have the isomorphism

$$\frac{\mathbb{P}_{\mathbb{Z}_2}}{M} \simeq \mathbb{F}_2.$$

Our proof is now complete. **QED**

Remark 1.6.16. In the proof of Proposition 1.6.15 we show that the norm in $\mathbb{P}_{\mathbb{Z}_2}$ is additive as well as multiplicative. This property is not true in general for the norm in $\mathbb{P}_{\mathbb{Z}}$ or $\mathbb{P}_{\mathbb{Z}_p}$, for odd primes p. For instance take $\mathrm{q} = 1+\mathbf{j}$. Then $\mathrm{N}(\mathrm{q}) + \mathrm{N}(\overline{\mathrm{q}}) = 2\,\mathrm{N}(\mathrm{q}) = 0$ but $\mathrm{N}(1+\mathbf{j}+1-\mathbf{j}) = \mathrm{N}(2) = 4$. Thus norm is not additive in $\mathbb{P}_{\mathbb{Z}}$. Since $p \nmid 4$ then norm is not additive in $\mathbb{P}_{\mathbb{Z}_p}$ too.

By this preliminary result, we can determine the unique maximal ideal of $\mathbb{P}_{\mathbb{Z}}$ that contains $2\mathbb{P}_{\mathbb{Z}}$. We start with this definition.

Definition 1.6.17. We will indicate by $\mathscr{M}$ the ideal generated in $\mathbb{P}_{\mathbb{Z}}$ by $1 + \mathbf{i}$ and $1 + \mathbf{j}$. Thus

$$\mathscr{M} \overset{\text{def}}{=} (1 + \mathbf{i}, 1 + \mathbf{j}).$$

A priori, the elements of $\mathscr{M}$ consist of finite sums of the form

$$\sum_i \mathrm{q}_i(1 + \mathbf{i})\mathrm{p}_i + \sum_j \mathrm{r}_j(1 + \mathbf{j})\mathrm{s}_j,$$

where each $\mathrm{q}_i, \mathrm{p}_i, \mathrm{r}_j, \mathrm{s}_j \in \mathbb{P}_{\mathbb{Z}}$ (see Section 0.3). Such an expression is very tricky to work with, but we can give a simpler description available.

Lemma 1.6.18. *Let* $\mathrm{q} \in \mathscr{M}$. *Then, there exist* $\mathrm{p}, \mathrm{r} \in \mathbb{P}_{\mathbb{Z}}$ *such that*

$$\mathrm{q} = \mathrm{p}(1 + \mathbf{i}) + \mathrm{r}(1 + \mathbf{j}).$$

Proof. Working in the commutative ring $\frac{\mathbb{P}_{\mathbb{Z}}}{2\mathbb{P}_{\mathbb{Z}}}$, we have

$$\mathrm{q} \equiv \mathrm{q}_1(1 + \mathbf{i}) + \mathrm{q}_2(1 + \mathbf{j}),$$

for some $\mathrm{q}_1, \mathrm{q}_2 \in \mathbb{P}_{\mathbb{Z}}$. Lifting this to $\mathbb{P}_{\mathbb{Z}}$, we have

$$\mathrm{q} = \mathrm{q}_1(1 + \mathbf{i}) + \mathrm{q}_2(1 + \mathbf{j}) + 2\mathrm{q}_3,$$

for some $\mathrm{q}_3 \in \mathbb{P}_{\mathbb{Z}}$. Since $2 = (1 - \mathbf{i})(1 + \mathbf{i})$, we get

$$\mathrm{q} = (\mathrm{q}_1 + \mathrm{q}_3(1 - \mathbf{i}))(1 + \mathbf{i}) + \mathrm{q}_2(1 + \mathbf{j}).$$

Taking $\mathrm{p} = \mathrm{q}_1 + \mathrm{q}_3(1 - \mathbf{i})$ and $\mathrm{r} = \mathrm{q}_2$ yields the result. **QED**

We can state the following immediate corollary.

Corollary 1.6.19. *The left, right and two-sided ideals generated by* $1 + \mathbf{i}$ *and* $1 + \mathbf{j}$ *in* $\mathbb{P}_{\mathbb{Z}}$ *concide.*

Proof. Let $\mathscr{I}_l$ and $\mathscr{I}_r$ be the left and the right ideals generated by $1 + \mathbf{i}$ and $1 + \mathbf{j}$ respectively. It is straightforward that $\mathscr{I}_l \subseteq \mathscr{M}$ and $\mathscr{I}_r \subseteq \mathscr{M}$. Lemma 1.6.18 assures that $\mathscr{M} \subseteq \mathscr{I}_l$. Since $\mathbb{P}_{\mathbb{Z}_2}$ is a commutative ring, Lemma 1.6.18 is true also in the right version. Finally, it follows that $\mathscr{M} \subseteq \mathscr{I}_r$. **QED**

Now we are ready to show that $\mathscr{M}$ is a maximal ideal containing 2.

Proposition 1.6.20. *Let* P *be a prime ideal of* $\mathbb{P}_{\mathbb{Z}}$ *containing* 2*. Then,* P *must be a maximal ideal.*

Proof. Since $\frac{\mathbb{P}_{\mathbb{Z}}}{2\mathbb{P}_{\mathbb{Z}}}$ is a finite commutative ring, then $\frac{\mathbb{P}_{\mathbb{Z}}}{P}$ must be a finite commutative ring too. Since P is a prime ideal, by Proposition F, in $\frac{\mathbb{P}_{\mathbb{Z}}}{P}$ the ideal (0) is a prime ideal. Thus $\frac{\mathbb{P}_{\mathbb{Z}}}{P}$ is a finite commutative domain. In other words, $\frac{\mathbb{P}_{\mathbb{Z}}}{P}$ is a field. Thus, P must be a maximal ideal of $\mathbb{P}_{\mathbb{Z}}$. **QED**

Now, we show that $\mathscr{M}$ is the unique maximal ideal of $\mathbb{P}_{\mathbb{Z}}$ over 2.

Proposition 1.6.21. *The ideal* $\mathscr{M} = (1 + \mathbf{i}, 1 + \mathbf{j})$ *of* $\mathbb{P}_{\mathbb{Z}}$ *is maximal, and it is the unique prime ideal of* $\mathbb{P}_{\mathbb{Z}}$ *above 2.*

Proof. It is clear that $2 \in \mathscr{M}$. In fact $\mathrm{N}(1 + \mathbf{i}) = 2$. In particular, $2\mathbb{P}_{\mathbb{Z}} \subseteq \mathscr{M}$. By Proposition 1.6.20, $\mathscr{M}$ is a maximal ideal. Let us show that it is the unique above 2. Given a maximal ideal $\mathscr{I}$ of $\mathbb{P}_{\mathbb{Z}}$ above 2, the image of $\mathscr{I}$ in $\frac{\mathbb{P}_{\mathbb{Z}}}{2\mathbb{P}_{\mathbb{Z}}}$ must be a maximal ideal of $\frac{\mathbb{P}_{\mathbb{Z}}}{2\mathbb{P}_{\mathbb{Z}}}$. By Lemma 1.6.15, we know that the only maximal ideal of $\frac{\mathbb{P}_{\mathbb{Z}}}{2\mathbb{P}_{\mathbb{Z}}}$ is the ideal generated by $1 + \mathbf{i}$ and $1 + \mathbf{j}$. The thesis follows by the correspondence theorem for rings. **QED**

Theorem 1.6.22. *The only maximal ideals of* $\mathbb{P}_{\mathbb{Z}}$ *are* $\mathscr{M} = (1+\mathbf{i},\ 1+\mathbf{j})$ *and the principal ideals* $p\mathbb{P}_{\mathbb{Z}}$*, generated by an odd prime* p*.*

Proof. Let $\mathscr{I}$ be a maximal ideal of $\mathbb{P}_{\mathbb{Z}}$. Let p be the prime number of $\mathscr{I}$ whose existence is assured in Lemma 1.6.8. Then $p\mathbb{P}_{\mathbb{Z}} \subseteq \mathscr{I}$. If p is odd then $p\mathbb{P}_{\mathbb{Z}}$ is a maximal ideal and $p\mathbb{P}_{\mathbb{Z}} = \mathscr{I}$. If $p = 2$, because of our previous investigations, the ideal $\mathscr{I}$ must equal $\mathscr{M} = (1+\mathbf{i},\ 1+\mathbf{j})$, the unique maximal ideal that contains 2. **QED**

As an immediate consequence of Theorem 1.6.22 we have the following

Proposition 1.6.23. *The prime ideals of* $\mathbb{P}_{\mathbb{Z}}$ *are* (0)*,* $\mathscr{M} = (1+\mathbf{i},\ 1+\mathbf{j})$ *and the principal ideals* $p\mathbb{P}_{\mathbb{Z}}$*, generated by an odd prime* p*.*

Proof. The thesis follows from Lemma 1.6.8, Proposition 1.6.9 and Theorem 1.6.22. **QED**

After Propositions 1.6.22 and 1.6.23, we can state that the prime and the maximal spectra of $\mathbb{P}_{\mathbb{Z}}$ and $\mathbb{H}_{\mathbb{Z}}$ have the same pattern.

We now prove an interesting fact about prime ideals that we will use to investigate localization properties of $\mathbb{P}_{\mathbb{Z}}$ in Chapter 2.

Proposition 1.6.24. *The prime ideals of* $\mathbb{P}_{\mathbb{Z}}$ *are closed under bar conjugation.*

Proof. For the zero ideal it is obvious. Take $\mathrm{q} \in p\mathbb{P}_{\mathbb{Z}}$, for an odd prime integer p. If $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$, then $\overline{\mathrm{q}} = a - b\,\mathbf{i} - c\,\mathbf{j} - d\,\mathbf{k}$. Now it is obvious to see that $p \mid \mathrm{q} \Leftrightarrow p \mid \overline{\mathrm{q}}$. To prove the thesis for $\mathscr{M}$, observe first that $\overline{1+\mathbf{i}} = 1 - \mathbf{i} = 2 - (1+\mathbf{i}) \in \mathscr{M}$. Analogously for $\overline{1+\mathbf{j}} \in \mathscr{M}$. Take now $\mathrm{q} \in \mathscr{M}$. Thanks to Lemma 1.6.18, we can suppose that $\mathrm{q} = \mathrm{q}_1(1+\mathbf{i}) + \mathrm{q}_2(1+\mathbf{j})$, for some q_1 and $q_2 \in \mathbb{P}_{\mathbb{Z}}$. Then $\overline{q} = (1 - \mathbf{i})\overline{q_1} + (1 - \mathbf{j})\overline{q_2}$ which is an element of $\mathscr{M}$. **QED**

In our study about prime and maximal ideals of $\mathbb{P}_{\mathbb{Z}}$, we essentially focused on principal ideals generated by central prime integers. Now we briefly analyze what happens when we consider the principal ideal generated by any split quaternion, not necessarily central. For example, let $\mathscr{I} = (1 + 2\mathbf{i})$. We know that $N(1 + 2\mathbf{i}) = 5 \in \mathscr{I}$, thus $5\mathbb{P}_{\mathbb{Z}} \subseteq \mathscr{I}$. Since $5\mathbb{P}_{\mathbb{Z}}$ is a maximal ideal, then we must have $\mathscr{I} = 5\mathbb{P}_{\mathbb{Z}}$ either $\mathscr{I} = \mathbb{P}_{\mathbb{Z}}$. The former case is impossible since $5 \nmid 1 + 2\mathbf{i}$. So we have that $\mathscr{I} = \mathbb{P}_{\mathbb{Z}}$. (In particular, by Proposition 1.6.5, $4 \in \mathscr{I}$, so $1 = 5 - 4 \in \mathscr{I}$). This fact is true in general as we show in the following.

Definition 1.6.25. Let $q = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$. We say that q is *primitive* if $\gcd(a, b, c, d) = 1$.

The ideal generated by non primitive split quaternions leads us to the maximal ideals of $\mathbb{P}_{\mathbb{Z}}$ classified above. In fact, let us take a split quaternion q which is not primitive. Then there is a prime p dividing its coefficients. If p is odd, it is obvious that (q) is contained in the maximal ideal $p\mathbb{P}_{\mathbb{Z}}$. If $p = 2$, then $(q) \subseteq (2) \subseteq (1 + \mathbf{i}, 1 + \mathbf{j})$. So in order to avoid trivial cases we will work now on with primitive split quaternions.

Proposition 1.6.26. *Let* q *be an integer split quaternion such that* $N(q) = p$, *where* p *is a prime number. Then* q *is irreducible and primitive.*

Proof. If $q = q_1 q_2$, then $p = N(q) = N(q_1)\,N(q_2)$. Since p is prime then $N(q_1) = \pm 1$ or $N(q_2) = \pm 1$, that is to say $q_1 \in \mathcal{U}(\mathbb{P}_{\mathbb{Z}})$ or $q_2 \in \mathcal{U}(\mathbb{P}_{\mathbb{Z}})$. This assures the irreducibility of q. If there were a prime n dividing the coefficients of q, we would have $p = \mathrm{N}(\mathrm{q}) = n^2 m$, for some $m \in \mathbb{Z}$. But this violates the Fundamental Theorem of Arithmetic. **QED**

Now we prove that split quaternions of odd prime norm generate the whole ring $\mathbb{P}_{\mathbb{Z}}$. The elements of norm 2 instead, are associated each other: they are all generators of the ideal $(1 + \mathbf{i})$.

Proposition 1.6.27. *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$ *such that* $\mathrm{N}(\mathrm{q}) = p$*, where* p *is an odd prime number. Then* $(\mathrm{q}) = \mathbb{P}_{\mathbb{Z}}$*. In particular* q *is not contained in any maximal ideal of* $\mathbb{P}_{\mathbb{Z}}$*.*

Proof. By the previous result q is primitive, so p does not divide at least one coefficient of q. By Lemma 1.6.4, we may suppose it is the constant term, say a. By Lemma 1.6.5 we know that $4a \in (\mathrm{q})$ and since $\gcd(p, 4a) = 1$, using a Bézout identity, we have that $1 \in \mathbb{P}_{\mathbb{Z}}$ and $(\mathrm{q}) = \mathbb{P}_{\mathbb{Z}}$. **QED**

Remark 1.6.28. The Proposition 1.6.27 helps us in building an element of a noncommutative ring which is not contained in any maximal ideal of the ring. The split quaternion $1 + 2\,\mathbf{i} \in \mathbb{P}_{\mathbb{Z}}$ is a concrete example.

The next preliminary result assures that an integer split quaternion q of norm 2 must have exactly two even coefficients.

Lemma 1.6.29. *Let* q *be an integer split quaternion such that* $\mathrm{N}(\mathrm{q}) = 2$*. Then* $\mathrm{q} = 2a + 2b\,\mathbf{i} + (2c+1)\,\mathbf{j} + (2d+1)\,\mathbf{k}$*, or* $\mathrm{q} = (2a+1) + (2b+1)\,\mathbf{i} + 2c\,\mathbf{j} + 2d\,\mathbf{k}$*, for some* $a, b, c, d \in \mathbb{Z}$*.*

Proof. Suppose the thesis is not true. If all coefficients of q are even, *e.g.* $\mathrm{q} = 2\mathrm{q}'$, for some $\mathrm{q}' \in \mathbb{P}_{\mathbb{Z}}$, we have $\mathrm{N}(\mathrm{q}) = 4\,\mathrm{N}(\mathrm{q}')$. This can not be equal to 2, since $\mathrm{N}(\mathrm{q}') \in \mathbb{Z}$. If the coefficients of q are all odd we have again that

$\mathrm{N}(\mathrm{q}) \in 4\mathbb{Z}$. Lastly, if exactly one or three coefficients are even, then $\mathrm{N}(\mathrm{q})$ is an odd integer. Finally, it turns out that q can have the form $2a + 2b\,\mathbf{i} + (2c + 1)\,\mathbf{j} + (2d + 1)\,\mathbf{k}$ or $(2a + 1) + (2b + 1)\,\mathbf{i} + 2c\,\mathbf{j} + 2d\,\mathbf{k}$, for some a, b, c, $d \in \mathbb{Z}$. In the other possible combinations of parity of the four coefficients, $\mathrm{N}(\mathrm{q})$ cannot equal 2. **QED**

Lemma 1.6.30. *Let* q *and* r *be elements of* $\mathbb{P}_{\mathbb{Z}}$ *such that* $\mathrm{N}(\mathrm{q}) = \mathrm{N}(\mathrm{r}) = 2$. *Then* $\frac{1}{2}\mathrm{qr} \in \mathbb{P}_{\mathbb{Z}}$.

Proof. The result is equivalent to saying that $\mathrm{qr} = 0$ in $\mathbb{P}_{\mathbb{Z}_2}$. By Lemma 1.6.29, we may suppose that q and r are $1 + \mathbf{i}$ or $\mathbf{j} + \mathbf{k}$ modulo 2. Since in $\mathbb{P}_{\mathbb{Z}_2}$ we have that $(1 + \mathbf{i})^2 = 0$, $(\mathbf{j} + \mathbf{k})^2 = 0$ and $(1 + \mathbf{i})(\mathbf{j} + \mathbf{k}) = 0$, the result follows easily. **QED**

The following result states that the ideal generated by an integer split quaternion of norm 2 coincide with the ideal generated by $1 + \mathbf{i}$.

Proposition 1.6.31. *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$ *be such that* $\mathrm{N}(\mathrm{q}) = 2$. *Then* $\mathrm{q} = \mathrm{u}(1 + \mathbf{i})$, *where* $\mathrm{u} \in \mathcal{U}(\mathbb{P}_{\mathbb{Z}})$. *Moreover* $(\mathrm{q}) = (1 + \mathbf{i})$.

Proof. By Lemma 1.6.30 $\mathrm{q}(1 + \mathbf{i})^{-1} = \frac{1}{2}\mathrm{q}(1 - \mathbf{i}) \in \mathbb{P}_{\mathbb{Z}}$. So if we take $\mathrm{u} \overset{\text{def}}{=} \mathrm{q}(1 + \mathbf{i})^{-1}$, we have that $\mathrm{u} \in \mathcal{U}(\mathbb{P}_{\mathbb{Z}})$, because $\mathrm{N}(\mathrm{u}) = 1$. Since $\mathrm{q} = \mathrm{u}(1 + \mathbf{i})$, q and $1 + \mathbf{i}$ generate the same ideal. **QED**

Now we say something more about the zero-divisors. It turns out that they are all contained in the ideal $\mathscr{M}$.

Proposition 1.6.32. *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$ *such that* $2 \mid \mathrm{N}(\mathrm{q})$. *Then* $\mathrm{q} \in \mathscr{M}$. *In particular* $(\mathrm{q}) \subsetneq \mathscr{M}$.

Proof. Let $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$ be such that $\mathrm{N(q)} = a^2 + b^2 - c^2 - d^2 = 2m$, for some $m \in \mathbb{Z}$. Reducing $\mathrm{N(q)}$ modulo 2, we see that q must have zero, two or four even coefficients. In the case that all of them are even, then trivially $\mathrm{q} \in (2) \subseteq \mathscr{M}$. Suppose now that q has all odd coefficients. Then $\mathrm{q} \equiv 1+\mathbf{i}+\mathbf{j}+\mathbf{k}$ (mod. 2). Lifting it up to $\mathbb{P}_{\mathbb{Z}}$, we obtain that $\mathrm{q} = 1+\mathbf{i}+\mathbf{j}+\mathbf{k}+2\mathrm{q}_1$, for some $\mathrm{q}_1 \in \mathbb{P}_{\mathbb{Z}}$. Since $1 + \mathbf{i} + \mathbf{j} + \mathbf{k} = (1+\mathbf{i})(1+\mathbf{j}) \in \mathscr{M}$, then also $\mathrm{q} \in \mathscr{M}$. If q has exactly two even coefficients, then q (mod. 2) is congruent to one of the following: $1+\mathbf{i}$, $1+\mathbf{j}$, $1+\mathbf{k} = (1+\mathbf{i})\,\mathbf{k} + 1 + \mathbf{j}$, $\mathbf{i}+\mathbf{j} = (1+\mathbf{i})\,\mathbf{j} + (1+\mathbf{j})\,\mathbf{i}$, $\mathbf{j}+\mathbf{k} = (1+\mathbf{i})\,\mathbf{j}$, $\mathbf{i}+\mathbf{k} = \mathbf{i}(1+\mathbf{j})$. Since all of them are elements of $\mathscr{M}$, we conclude as above lifting q up to $\mathbb{P}_{\mathbb{Z}}$. Finally $(\mathrm{q}) \subseteq \mathscr{M}$. The inclusion is strict because $\mathscr{M}$ is the unique maximal ideal containing 2 and it is not principal by definition. **QED**

Corollary 1.6.33. *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$ *be a zero-divisor. Then* $\mathrm{q} \in \mathscr{M}$.

Proof. It is a particular case of Proposition 1.6.32. **QED**

Summing up the results we just proved about principal ideals, we obtain the following statement.

Proposition 1.6.34. *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$. *We have the following possible cases:*

(i) $\mathrm{q} = 0$ *if and only if* $(\mathrm{q}) = (0)$.

(ii) If $\mathrm{q} = p\mathrm{u}$, *for an odd prime integer* p *and* $u \in \mathbb{P}_{\mathbb{Z}}$, *then* $(\mathrm{q}) \subseteq p\mathbb{P}_{\mathbb{Z}}$. *Moreover, if* $\mathrm{u} \in \mathcal{U}(\mathbb{P}_{\mathbb{Z}})$, *then* $(\mathrm{q}) = p\mathbb{P}_{\mathbb{Z}}$.

(iii) If $2 \mid \mathrm{q}$, *then* $(\mathrm{q}) \subsetneq \mathscr{M}$.

(iv) If $\mathrm{N(q)} = 0$, *then* $(\mathrm{q}) \subsetneq \mathscr{M}$.

(v) *If* $\mathrm{N}(\mathrm{q}) = \pm 1$*, then* $(\mathrm{q}) = \mathbb{P}_{\mathbb{Z}}$*.*

(vi) *If* $\mathrm{N}(\mathrm{q}) = p$*, for an odd prime integer* p*, then* $(\mathrm{q}) = \mathbb{P}_{\mathbb{Z}}$*.*

(vii) *If* $\mathrm{N}(\mathrm{q}) = 2$*, then* $(\mathrm{q}) = (1 + \mathbf{i})$*.*

Proof. (i) The nontrivial implication follows from Proposition 1.5.7.

(ii) Let us suppose that $\mathrm{q} = p\mathrm{u}$, for some $\mathrm{u} \in \mathbb{P}_{\mathbb{Z}}$. The inclusion $(\mathrm{q}) \subseteq p\mathbb{P}_{\mathbb{Z}}$ is straightforward. If u is invertible, for the other inclusion, notice that also $\mathrm{u}^{-1} \in \mathbb{P}_{\mathbb{Z}}$. So $p = \mathrm{qu}^{-1} \in (\mathrm{q})$.

(iii) If $2 \mid \mathrm{q}$, then $(\mathrm{q}) \subseteq (2) \subsetneq \mathscr{M}$.

(iv) It is the above Corollary 1.6.33.

(v) It is obvious because under these hypothesis q results to be invertible.

(vi) See Proposition 1.6.27.

(vii) See Proposition 1.6.31. **QED**

Remark 1.6.35. We observe that the converse of the second part Proposition 1.6.34,(ii) is not necessarily true. In fact, by the point (vi) of the same proposition, $(1 + 2\,\mathbf{i}) = \mathbb{P}_{\mathbb{Z}}$. Thus $(3 + 6\,\mathbf{i}) = 3\mathbb{P}_{\mathbb{Z}}$, but $1 + 2\,\mathbf{i}$ is not invertible in $\mathbb{P}_{\mathbb{Z}}$. Here follows the most general case we can have.

Proposition 1.6.36. *Let* p *be an odd prime integer and let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$*. Then* $(\mathrm{q}) = p\mathbb{P}_{\mathbb{Z}}$ *if and only if* $\mathrm{q} = p\mathrm{q}'$ *for some* $q' \in \mathbb{P}_{\mathbb{Z}}$ *such that* $(q') = \mathbb{P}_{\mathbb{Z}}$*.*

Proof. The *if* part is immediate since $(\mathrm{q}) = p(\mathrm{q}') = p\mathbb{P}_{\mathbb{Z}}$. For the converse, suppose that $(\mathrm{q}) = p\mathbb{P}_{\mathbb{Z}}$. Then $\mathrm{q} = p\mathrm{q}'$, for some $\mathrm{q}' \in \mathbb{P}_{\mathbb{Z}}$. Moreover $p \in (\mathrm{q})$, so $p = \sum_{h=1}^{n} \mathrm{p}_h \, \mathrm{q} \, \mathrm{r}_h = p \sum_{h=1}^{n} \mathrm{p}_h \, \mathrm{q}' \, \mathrm{r}_h$, for some $\mathrm{p}_h, \mathrm{r}_h \in \mathbb{P}_{\mathbb{Z}}$. By Proposition 1.5.7, it is possible to simplify p from this equality. Then we get $\sum_{h=1}^{n} \mathrm{p}_h \, \mathrm{q}' \, \mathrm{r}_h = 1$, that is to say $1 \in (\mathrm{q}')$, as wanted. **QED**

Chapter 2

Localizations properties of $\mathbb{P}_{\mathbb{Z}}$

A tool of investigation in commutative ring theory is the localization of domains at suitable multiplicative subsets. Localization theory is very used to describe the prime spectrum of domains.

In this chapter we shall first introduce a general theory of noncommutative localizations studying a particular kind of multiplicative subsets, the denominator sets (cf. [15]). In the second section we apply this theory to $\mathbb{P}_{\mathbb{Z}}$. These results will be useful in Chapter 4 in order to describe the prime spectrum of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$.

2.1 Noncommutative localizations

In this section we recall some notion about the localizations (or rings of fractions). We will generalize the more well-known commutative case, for which a universal reference is [1, Chapter 3]. In particular, we shall deal with the necessary theory to our aims; more details and a more general treatment can be found in [15, chapter 4].

2.1.1 Multiplicative subsets

We start with this definition.

Definition 2.1.1. Let be given a ring R and a subset $S \subseteq R$. We say that S is a *multiplicative subset* of R if the following conditions hold:

(i) $1 \in S$;

(ii) $0 \notin S$;

(iii) $S \cdot S \subseteq S$.

We list some examples of multiplicative subsets.

Proposition 2.1.2. *Let R be a ring (not necessarily commutative). Then the following are multiplicative subsets of R:*

(i) the intersection of a family of multiplicative subsets;

(ii) the set of left-invertible elements of R;

(iii) the set of right-invertible elements of R;

(iv) the set of invertible elements $\mathcal{U}(R)$;

(v) the set $\mathcal{R}_l(R)$ of left-regular elements of R;

(vi) the set $\mathcal{R}_r(R)$ of right-regular elements of R;

(vii) the set $\mathcal{R}(R)$ of regular elements of R;

(viii) if $\mathbb{Z} \subseteq R$, then any multiplicative subset of $\mathbb{Z}$ is a multiplicative subset of R.

Proof. It is straightforward. **QED**

If the ring R is commutative, then there exists an important class of multiplicative subsets of R.

Proposition 2.1.3. *Let R be a commutative ring. If Q is a prime ideal of R, then the complement $R \setminus Q$ is a multiplicative subset of R. In particular, the complement in R of the union of a family of prime ideals is a multiplicative subset of R.*

Proof. It is an equivalent condition for Q being prime in R. **QED**

If R is a noncommutative ring, Proposition 2.1.3 is not necessarily true. We can give this example in $\mathbb{P}_{\mathbb{Z}}$.

Example 2.1.4. Take an odd prime integer p. In Proposition 1.6.23 we saw that $p\mathbb{P}_{\mathbb{Z}}$ is a prime ideal of $\mathbb{P}_{\mathbb{Z}}$. The complement of $p\mathbb{P}_{\mathbb{Z}}$ in $\mathbb{P}_{\mathbb{Z}}$ is not multiplicatively closed in $\mathbb{P}_{\mathbb{Z}}$. For instance, write $p = 2k + 1$. The split quaternions $\mathrm{q} = (k + 1) + k\,\mathbf{j}$ and $\overline{\mathrm{q}}$ are primitive so they are not in $p\mathbb{P}_{\mathbb{Z}}$. Nevertheless $\mathrm{q}\overline{\mathrm{q}} = (k + 1)^2 - k^2 = p \in p\mathbb{P}_{\mathbb{Z}}$.

For this reason, in the noncommutative setting it is needed to introduce a new family of multiplicative subsets associated to prime ideals. In [11] Goldie suggests the following definition using prime ideals. We use it in a more general way working with a proper subset.

Definition 2.1.5. Let be given a ring R. Let Q be a proper subset of R. We define the *left Goldie complement* of Q to be

$$\mathscr{C}(Q) \overset{\text{def}}{=} \{\, x \in R \mid xr \notin Q,\ \forall r \notin Q \,\}.$$

Similarly, it is defined the *right Goldie complement* of Q to be

$$\mathscr{C}'(Q) \overset{\text{def}}{=} \{\, x \in R \mid rx \notin Q,\ \forall r \notin Q \,\} .$$

For completeness we set $\mathscr{C}(R) = \mathscr{C}'(R) \overset{\text{def}}{=} \varnothing$.

In order to make no confusion with $\mathscr{C}(Q)$, we will often call the complement $R \smallsetminus Q$ of a subset Q as the *set theoretic complement* of Q. We will see that in general $\mathscr{C}(Q)$ and $R \smallsetminus Q$ are not equal.

We can immediately give some examples of Goldie complements.

Example 2.1.6. Let R be a ring. Then

$$\mathscr{C}(0) = \{\, x \in R \mid xr \neq 0,\ \forall\, r \neq 0 \,\} = \mathcal{R}_l(R),$$

the set of the left regular elements of R and

$$\mathscr{C}'(0) = \{\, x \in R \mid rx \neq 0,\ \forall\, r \neq 0 \,\} = \mathcal{R}_r(R),$$

the set of the right regular elements of R. Recall that, after Proposition 2.1.2, these sets result to be multiplicative subsets. Finally, if R is not a domain, then $\mathscr{C}(0)$ and $\mathscr{C}'(0)$ are strictly contained in R^*.

The following properties are immediate consequences of Definition 2.1.5.

Proposition 2.1.7. *Let R be a ring and let $Q \subsetneq R$ be a prime ideal of R. Then*

(i) $1 \in \mathscr{C}(Q)$.

(ii) $0 \notin \mathscr{C}(Q)$.

(iii) If $a, b \in \mathscr{C}(Q)$ then $ab \in \mathscr{C}(Q)$.

(iv) $\mathscr{C}(Q) \subseteq R \smallsetminus Q$.

Similar properties are true for $\mathscr{C}'(Q)$.

Proof. (i) For each $r \notin Q$, then $1 \cdot r = r \notin Q$.

(ii) Since $0 \in Q$, for all $r \notin Q$, we have that $0 \cdot r \in Q$.

(iii) Let $r \notin Q$. Since $b \in \mathscr{C}(Q)$, then $br \notin Q$. Now again, since $a \in \mathscr{C}(Q)$, $a(br) \notin Q$. Finally for all $r \notin Q$ then $(ab)r \notin Q$.

(iv) Let $x \in \mathscr{C}(Q)$. Since $1 \notin Q$, then $x \cdot 1 = x \notin Q$. So as we wanted, $x \in R \smallsetminus Q$. **QED**

Now we have the following corollary.

Corollary 2.1.8. *Let* R *be a ring. Let* $Q \subsetneq R$ *be a prime ideal of* R*. Then* $\mathscr{C}(Q)$ *is a multiplicative subset of* R*, in particular* $\mathscr{C}(Q) \subseteq R \smallsetminus Q$*. The same is for* $\mathscr{C}'(Q)$.

Proof. Since Q is a prime ideal, the thesis follows from Proposition 2.1.7. **QED**

If R is a commutative ring, $\mathscr{C}(Q)$ gives back the complement of the prime ideal Q.

Proposition 2.1.9. *Let* R *be a commutative ring and* Q *be a proper prime ideal of* R*. Then* $\mathscr{C}(Q) = \mathscr{C}'(Q) = R \smallsetminus Q$.

Proof. After Corollary 2.1.8 we need to prove the inclusion $\mathscr{C}(Q) \supseteq R \smallsetminus Q$. Since Q is a prime ideal in a commutative ring, by Proposition 2.1.3, $R \smallsetminus Q$ is a multiplicative subset. Take $x \notin Q$. Then, for all $r \notin Q$, $xr \notin Q$. Finally $x \in \mathscr{C}(Q)$. **QED**

In Example 2.1.4 we also proved that if $Q = p\mathbb{P}_{\mathbb{Z}}$, for an odd prime p, then $\mathscr{C}(Q) \subsetneq \mathbb{P}_{\mathbb{Z}} \setminus Q$.

When Q is a prime ideal of the ring R, we have an interesting characterization of $\mathscr{C}(Q)$ and $\mathscr{C}'(Q)$.

Proposition 2.1.10. *Let R be a ring. Let Q be a prime ideal of R. Then $\mathscr{C}(Q)$ is the set of left regular elements of R modulo Q and $\mathscr{C}'(Q)$ is the set of right regular elements of R modulo Q.*

Proof. Take $x \in R$. Then x is a left zero-divisor modulo Q if and only if there is $r \in \frac{R}{Q}$, $r \neq 0$, such that $xr = 0$. This is equivalent to say that there is an $r \notin Q$ such that $xr \in Q$. In other words, $x \notin \mathscr{C}(Q)$. Similarly for $\mathscr{C}'(Q)$. **QED**

Now we establish a sufficient criterion for $\mathscr{C}(Q)$ and $\mathscr{C}'(Q)$ being equal.

Proposition 2.1.11. *Let R be noetherian ring and Q be a prime ideal of R. Then $\mathscr{C}(Q) = \mathscr{C}'(Q)$.*

Proof. See [11, Section 3] **QED**

Thus in a noetherian ring, when we construct the ring of fractions with denominators in the Goldie complement of a prime ideal, we do not care on which side we are working on: we will obtain the same structure. Later we will see this in details.

An immediate corollary of Proposition 2.1.11 is the following.

Corollary 2.1.12. *Let R be a noetherian ring and let Q be a prime ideal of R. Then $\mathscr{C}(Q)$ is the set of the regular element of R modulo Q.*

Proof. It follows from Propositions 2.1.10 and 2.1.11. **QED**

After this general discussion, we study more precisely the Goldie complement associated to the prime ideals of $\mathbb{P}_{\mathbb{Z}}$.

Proposition 2.1.13. *Let Q be a prime ideal of $\mathbb{P}_{\mathbb{Z}}$. Then*

(i) $\mathscr{C}(Q)$ *is closed under bar conjugation.*

(ii) $\mathscr{C}(Q)$ *is closed under norm.*

(iii) $\mathscr{C}(Q) = \{ x \notin Q \mid \mathrm{N}(x) \notin Q \}$.

(iv) $\mathscr{C}(Q)$ *does not contain any zero-divisor.*

Proof. Recall that $\mathbb{P}_{\mathbb{Z}}$ is a noetherian ring (it follows from Proposition 1.6.1). Then, for what we told in Proposition 2.1.11, $\mathscr{C}(Q) = \mathscr{C}'(Q)$, for each prime ideal Q of $\mathbb{P}_{\mathbb{Z}}$.

First of all take the prime ideal $Q = (0)$. Then $\mathscr{C}(Q) = \mathcal{R}(\mathbb{P}_{\mathbb{Z}})$, since by Proposition 1.5.5, right and left zero-divisors of $\mathbb{P}_{\mathbb{Z}}$ coincide. Moreover they are exactly the elements with zero norm. Then $\mathscr{C}(Q) = \mathscr{C}'(Q) = \mathcal{R}(\mathbb{P}_{\mathbb{Z}}) = \{ x \neq 0 \mid \mathrm{N}(x) \neq 0 \}$. In this way we have proved (i)-(iv) for the case $Q = (0)$.

Now we prove the (i)-(iv) for the other prime ideals of $\mathbb{P}_{\mathbb{Z}}$.

(i) Suppose that $Q = p\mathbb{P}_{\mathbb{Z}}$, for an odd prime p. Take $x \in \mathscr{C}'(Q)$ and $r \notin Q$. Then, equivalently, $\bar{r} \notin Q$. Thus $\bar{r}x \notin Q$, which is equivalent to say that $\overline{\bar{r}x} = \bar{x}r \notin Q$. Finally, $\overline{x} \in \mathscr{C}(Q)$.

The case $Q = (1 + \mathbf{i}, 1 + \mathbf{j})$ can be proved exactly in the same way by Proposition 1.6.24.

(ii) It is an immediate consequence of the previous property and the multiplicative closure of $\mathscr{C}(Q)$.

(iii) Suppose now that $Q = p\mathbb{P}_{\mathbb{Z}}$, for an odd prime p. The thesis follows if we show that that, taken an $x \notin Q$, then we have the equivalence: $x \in \mathscr{C}(Q) \Leftrightarrow \mathrm{N}(x) \notin Q$. Let $x \in \mathscr{C}(Q)$. Since $\mathscr{C}(Q) \subseteq \mathbb{P}_{\mathbb{Z}} \setminus Q$, then $p \nmid x$ and $p \nmid \overline{x}$. Suppose that $p \mid \mathrm{N}(x)$. We have that $\overline{x} \notin Q$ and $\mathrm{N}(x) = x\overline{x} \in Q$, against the choice of x. For the reverse implication, take an $x \in \mathbb{P}_{\mathbb{Z}}$ such that $\mathrm{N}(x) \notin Q$. If $x \notin \mathscr{C}(Q)$, then it would exist an $r \notin Q$ such that $xr \in Q$. So $p \mid \bar{x}xr = \mathrm{N}(x)r$. Since $\mathrm{N}(x)$ is an integer, this means that $p \mid \mathrm{N}(x)$ or $p \mid r$, but both of these conditions are absurd.

It remains the case $Q = (1+\mathbf{i}, 1+\mathbf{j})$. If $x \in \mathscr{C}(Q)$, then $x \notin Q$ and $\overline{x} \notin Q$. Since $Q \cap \mathbb{Z} = 2\mathbb{Z}$, if $\mathrm{N}(x) \in Q$, then $2 \mid \mathrm{N}(x) = x\overline{x}$. But this violates the fact that $x \in \mathscr{C}(Q)$, being $\overline{x} \notin Q$. Take now $x \notin Q$, such that $2 \nmid \mathrm{N}(x)$. By contradiction, if $x \notin \mathscr{C}(Q)$, it would exist an $r \notin Q$ such that $xr \in Q$. *A fortiori*, for all $s \in \mathbb{P}_{\mathbb{Z}}$, $s\overline{x}xr \in Q$. So $s\,\mathrm{N}(x)r \in Q$, for all $s \in \mathbb{P}_{\mathbb{Z}}$. In particular , $\mathrm{N}(x)\mathbb{P}_{\mathbb{Z}}r \subseteq Q$. Since Q is a prime ideal, then $\mathrm{N}(x) \in Q$ or $r \in Q$, but both conditions are absurd.

(iv) Let $Q = p\mathbb{P}_{\mathbb{Z}}$, for an odd prime p and suppose that $xr' = 0$, for some $x \in \mathscr{C}(Q)$ and $r' \neq 0 \in \mathbb{P}_{\mathbb{Z}}$. If we write $r' = p^m r$, for some $r \notin Q$, and an integer $m \geqslant 0$, we get $xr = 0 \in Q$ which is an absurd. Lastly, if $Q = (1+\mathbf{i}, 1+\mathbf{j})$, this statement is a consequence of Corollary 1.6.33 and Proposition 2.1.7, (iv). **QED**

It is useful to outline the following

Corollary 2.1.14. *With the notation above, we have that:*

$$\mathscr{C}(0) = \mathcal{R}(\mathbb{P}_{\mathbb{Z}});$$

$$\mathscr{C}(p\mathbb{P}_{\mathbb{Z}}) = \{\, x \in \mathbb{P}_{\mathbb{Z}} \mid p \not| \, x \text{ and } p \not| \, \mathrm{N}(x) \,\};$$

and

$$\mathscr{C}(1 + \mathbf{i}, 1 + \mathbf{j}) = \{\, x \in \mathbb{P}_{\mathbb{Z}} \mid 2 \not| \, x \text{ and } 2 \not| \, \mathrm{N}(x) \,\}.$$

Proof. It immediately follows from Proposition 2.1.13, (iii). **QED**

The multiplicative subsets of $\mathbb{P}_{\mathbb{Z}}$ we will work with in the following are: $\mathcal{U}(\mathbb{P}_{\mathbb{Z}})$, the multiplicative subsets of $\mathbb{Z}$, $\mathscr{C}(0)$, $\mathscr{C}(1+\mathbf{i}, 1+\mathbf{j})$ and $\mathscr{C}(p\mathbb{P}_{\mathbb{Z}})$, for any odd prime integer p.

2.1.2 Denominator sets and Localizations

We start with this definition.

Definition 2.1.15. Let be given two rings R and R'. Let S be a multiplicative subset of R. A ring homomorphism $\varphi : R \to R'$ is said to be S-inverting if $\varphi(S) \subseteq \mathcal{U}(R')$.

Given a commutative ring R and a multiplicative subset $S \subseteq R$, in Commutative Ring theory is well-known the construction of the ring R_S, called the localization of R at S and of the ring homomorphism $\varphi : R \to R_S$ which is S-inverting and is *universal* with this property (this means that the data R_S and φ are unique). In particular, it is possible to prove that:

(CL1) Every element of R_S has the form $\varphi(r)\varphi(s)^{-1}$ (for brevity we write $\frac{r}{s}$), for some $r \in R$ and $s \in S$.

(CL2) $\ker \varphi = \{\, r \in R \mid rs = 0, \text{ for some } s \in S \,\}$ (which is an ideal in R).

The addition in R_S is defined by taking a common denominator between fractions and the multiplication is defined by multiplying numerators and denominators of fractions. The embedding of a commutative domain D into its field of quotients corresponds to the localization of D at the set D^*.

The following notions take inspiration from what happens in the commutative case. We formulate them in a general context, also for noncommutative rings.

In [15] it is proven the following result.

Proposition 2.1.16. [15, Proposition 9.2] *Let R be a ring and let S be a multiplicative subset of R. Then there exists an S-inverting homomorphism ε from R to a ring R_S with the following universal property: for any S-inverting homomorphism $\alpha : R \to R'$, there exists a unique ring homomorphism $f : R_S \to R'$ such that $\alpha = f \circ \varepsilon$.*

The universal property of ε stated in Proposition 2.1.16 guarantees the uniqueness of the data $\varepsilon : R \to R_S$. For this reason in the notation of the theorem we are allowed to use R_S for indicating the receiving ring of the *universal S-inverting homomorphism ε*. Lastly, note that Proposition 2.1.16 is true for any subset S (not necessarily multiplicative) but in some cases R_S may be trivial. For example, as in the commutative case, if $0 \in S$ then R_S is the zero ring. The use of multiplicative subsets avoids the trivial cases.

Remark 2.1.17. In opposition to the commutative case, R_S may be the zero ring even though $0 \notin S$. In [15, Example 9.3] and [15, Exercise 9.5] there are such examples.

In a noncommutative context the nature of R_S is not easily predictable. The properties (CL1) and (CL2) of the commutative case are not true in general. The elements of R_S are indeed sums like

$$\varepsilon(r)\varepsilon(s)\varepsilon(r') + \varepsilon(s')^{-1}\varepsilon(r'')\varepsilon(s'')^{-1}, \tag{2.1}$$

for some $r, r', r'' \in R$ and $s, s', s'' \in S$. In a noncommutative setting an expression like the (2.1) is far from being equal to $\varepsilon(r_1)\varepsilon(s_1)^{-1}$, for some $r_1 \in R$ and $s_1 \in S$.

The most unexpected situation is maybe the following. In [15, Theorem 9.11] Lam builds a noncommutative domain which cannot be embedded into any division ring. This domain is known in literature as the *Mal'cev counterexample.*

For these reasons in a noncommutative setting we need additional conditions on the multiplicative subset for building a useful localization ring.

In what follows we first give the definition of a ring of fractions (or localization) and after we describe the family of multiplicative subsets used to construct them. Observe that we initially need to distinguish the right and left *fractions.*

Definition 2.1.18. Let be given a ring R and a multiplicative subset $S \subseteq R$. A ring R' is said to be a *right ring of fractions* or *right localization* of R with respect to S if it is given a ring homomorphism $\varphi : R \to R'$ such that:

(i) φ is S-inverting.

(ii) Every element of R' has the form $\varphi(a)\varphi(s)^{-1}$, for some $a \in R$ and $s \in S$.

(iii) $\ker\varphi = \{\, r \in R \mid rs = 0, \text{ for some } s \in S \,\}$.

To simplify the notation, we write the elements of R' as rs^{-1}, instead of $\varphi(r)\varphi(s)^{-1}$. We define similarly the *left ring of fractions* whose elements have the form $s^{-1}r$.

Remark 2.1.19. When such a ring R' exists, then $R' \neq 0$. Otherwise, in view of (iii), 1 would be a zero-divisor.

The existence of a right (or left) ring of fractions is not given *a priori.* As told above, we need more conditions on the multiplicative subset S. In the next definition we require two conditions on S that essentially let us to find a *common denominator* for (a finite number of) fractions in such a way that we can add or multiply them and obtain an element of the form rs^{-1}.

Definition 2.1.20. Let R be a ring and S a multiplicative subset in R. We say that S is a *right denominator set* if

(i) For any $a \in R$ and $s \in S$, $aS \cap sR \neq \varnothing$. (We also say that S is *right permutable*).

(ii) For $a \in R$, if $s'a = 0$ for some $s' \in S$, then $as = 0$ for some $s \in S$. (We also say that S is *right reversible*).

The left-analogous properties are defined similarly. For a commutative ring the (right and left) permutability and reversibility are trivially true. So the denominator sets for a commutative ring coincide with the multiplicative subsets. Moreover, the multiplicative subsets contained in the center of the ring are trivially denominator subsets.

The following important result due to Ore and Asano (known by Noether too in a noetherian context), gives a necessary and sufficient condition for building a right ring of fractions with respect to a multiplicative subeset.

Proposition 2.1.21. [15, Theorem 10.6] *Let R be a ring and S a multiplicative subset in R. Then R has a right ring of fractions with respect to S if and only if S is a right denominator set.*

For the proof of this result we refer to [15, Section 10]. We outline here only the aspects we will need later.

Definition 2.1.22. In view of Proposition 2.1.21 we can construct the following ring of fractions

$$RS^{-1} = \left\{ as^{-1} \;\middle|\; a \in R,\ s \in S \right\}$$

whose element are the *right fractions with denominator in S*.

Remark 2.1.23. The conditions (i) and (ii) of Definition 2.1.20 are necessary for finding a common denominator when we sum or multiply two fractions in RS^{-1} and so for proving that RS^{-1} is finally a ring.

We complete this general dissertation about localizations with universality of the construction RS^{-1}.

Proposition 2.1.24. *Let R be a ring and S a denominator set in R. Consider the map $\varphi : R \to RS^{-1}$ such that $\varphi(r) = \frac{r}{1}$, for all $r \in R$. Then φ is a universal S-inverting homomorphism. In particular, there is a unique isomorphism $g : R_S \to RS^{-1}$ such that $g \circ \varepsilon = \varphi$, where R_S and $\varepsilon : R \to R_S$ are as in Proposition 2.1.16.*

This result assures that if S is a right denominator set in R then the rings R_S (cf. Proposition 2.1.16) and RS^{-1} (cf. Proposition 2.1.21) coincide.

Similarly we can construct the ring

$$S^{-1}R = \left\{ s^{-1}a \;\middle|\; a \in R,\ s \in S \right\},$$

with respect to a left denominator set S.

Proposition 2.1.25. [15, Corollary 10.14] *Let R be a ring and let S be a right and left denominator set in R. Then we have the isomorphism*

$$RS^{-1} \simeq S^{-1}R.$$

Take now $S = \mathcal{R}(R)$ of all regular elements of the ring R. We saw in Proposition 2.1.2 that it is a multiplicative subset of R. Since S does not contain zero-divisors, RS^{-1} is a localization of R at S if and only if S is right permutable. If this is the case, we call RS^{-1} the *total right ring of fractions of* R, denoted by $\mathcal{Q}^r(R)$. The notion of the total left ring of quotients $\mathcal{Q}^l(R)$ is given similarly. If $\mathcal{Q}^l(R) = \mathcal{Q}^r(R)$, we speak of the *total ring of quotients of* R without any mention of the side. Observe that if D is a commutative domain, $\mathcal{Q}^r(D) = \mathcal{Q}^l(D) = \mathcal{Q}(D)$, the field of quotients of D. The adjective *total* is justified by the fact that $\mathcal{R}(R)$ is the biggest multiplicative subset of R whose elements can be inverted (the rejected ones are zero-divisors). For this reason any other ring of fractions of R can be embedded in $\mathcal{Q}(R)$, when it exists.

2.2 Ring of quotients and Localizations of $\mathbb{P}_{\mathbb{Z}}$

In what follows we aim to investigate the structure of some localizations of $\mathbb{P}_{\mathbb{Z}}$ that we will use to study the ideals of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$.

Before building localizations of $\mathbb{P}_{\mathbb{Z}}$, we must first look for suitable denominator sets in the ring $\mathbb{P}_{\mathbb{Z}}$.

Proposition 2.2.1. *The multiplicative subsets of $\mathbb{Z}$ introduced in Section 2.1.1 (*id est *$\mathbb{Z}^*$ and the sets $\mathbb{Z} \setminus p\mathbb{Z}$, for p prime integers) are denominator sets of $\mathbb{P}_{\mathbb{Z}}$.*

Proof. Let S be one of the multiplicative subsets of the statement. Since by Proposition 1.5.7 the elements of $\mathbb{Z}$ are not zero-divisors in $\mathbb{P}_{\mathbb{Z}}$, we have only to show that S is right and left permutable. This fact is easy to see since S

is contained in the center of $\mathbb{P}_{\mathbb{Z}}$. We can conclude that S is a right and left denominator set of $\mathbb{P}_{\mathbb{Z}}$. **QED**

Proposition 2.2.2. *Let Q be a prime ideal of $\mathbb{P}_{\mathbb{Z}}$. Then $\mathscr{C}(Q)$ is a right and left denominator set of $\mathbb{P}_{\mathbb{Z}}$.*

Proof. We saw in Corollary 2.1.8 that $\mathscr{C}(Q)$ is a multiplicative subset. By Proposition 2.1.13 $\mathscr{C}(Q)$ does not contain zero-divisors, so $\mathscr{C}(Q)$ is right and left reversible. It remains to show that $\mathscr{C}(Q)$ is right permutable. This is trivially done. Given $a \in \mathbb{P}_{\mathbb{Z}}$ and $s \in \mathscr{C}(Q)$, we can permute using the equality $a \cdot \mathrm{N}(s) = s \cdot \bar{s}a$. Similarly for the left permutability. Thus $\mathscr{C}(Q)$ is a right and left denominator set of $\mathbb{P}_{\mathbb{Z}}$. **QED**

We can give the first concrete example.

Proposition 2.2.3. *Let $S = \mathcal{R}(\mathbb{P}_{\mathbb{Z}})$. Then*

$$\mathbb{P}_{\mathbb{Z}}S^{-1} = S^{-1}\mathbb{P}_{\mathbb{Z}} = \mathcal{Q}(\mathbb{P}_{\mathbb{Z}}) = \mathbb{P}_{\mathbb{Q}},$$

which is the total ring of fractions of $\mathbb{P}_{\mathbb{Z}}$.

Proof. Recall that by Corollary 2.1.14, $\mathcal{R}(\mathbb{P}_{\mathbb{Z}}) = \mathscr{C}(0)$ which is a denominator set by Proposition 2.2.2. So the ring $\mathbb{P}_{\mathbb{Z}}S^{-1}$ exists and its elements are the fractions rs^{-1}, where $r, s \in \mathbb{P}_{\mathbb{Z}}$ and $\mathrm{N}(s) \neq 0$. It is easy to understand that $rs^{-1} = \frac{1}{\mathrm{N}(s)}r\overline{s} \in \mathbb{P}_{\mathbb{Q}}$. In this way we showed that $\mathbb{P}_{\mathbb{Z}}S^{-1} \subseteq \mathbb{P}_{\mathbb{Q}}$. Let us show the reverse inclusion. Given $\mathrm{q} \in \mathbb{P}_{\mathbb{Q}}$, write q in the form $\mathrm{p} \cdot a^{-1}$, where $\mathrm{p} \in \mathbb{P}_{\mathbb{Z}}$ and a is a common denominator for the coefficients of q. Obviously, $a \in \mathcal{R}(\mathbb{P}_{\mathbb{Z}})$. Thus $\mathbb{P}_{\mathbb{Z}}S^{-1} = \mathbb{P}_{\mathbb{Q}}$. Similarly, $S^{-1}\mathbb{P}_{\mathbb{Z}} = \mathbb{P}_{\mathbb{Q}}$. Finally since we localized with respect to the set of regular elements of $\mathbb{P}_{\mathbb{Z}}$, we obtained the that $\mathbb{P}_{\mathbb{Q}}$ is the total ring of fractions of $\mathbb{P}_{\mathbb{Z}}$. **QED**

Using the same argument of the proof of the previous result we can state the following.

Proposition 2.2.4. *Let* $S = \mathbb{Z} \setminus \{ 0 \}$. *Then*

$$\mathbb{P}_{\mathbb{Z}} S^{-1} = S^{-1} \mathbb{P}_{\mathbb{Z}} = \mathbb{P}_{\mathbb{Q}}.$$

Proof. By Proposition 2.2.1, S is a denominator set of $\mathbb{P}_{\mathbb{Z}}$. The proof proceeds as in Proposition 2.2.3. The key is taking a common denominator for the coefficients of the elements of $\mathbb{P}_{\mathbb{Q}}$. **QED**

If we localize $\mathbb{P}_{\mathbb{Z}}$ at $S = \mathbb{Z} \setminus p\mathbb{Z}$ or $S = \mathscr{C}(Q)$, where $Q = p\mathbb{P}_{\mathbb{Z}}$, we get the algebra of split quaternions with coefficients in $\mathbb{Z}_{(p)}$, the localization of $\mathbb{Z}$ at p.

Proposition 2.2.5. *Let* $S = \mathbb{Z} \setminus p\mathbb{Z}$. *Then*

$$\mathbb{P}_{\mathbb{Z}} S^{-1} = S^{-1} \mathbb{P}_{\mathbb{Z}} = \mathbb{P}_{\mathbb{Z}_{(p)}}.$$

Proof. We already know that S is a denominator set of $\mathbb{P}_{\mathbb{Z}}$ by Proposition 2.2.1. So the ring $\mathbb{P}_{\mathbb{Z}} S^{-1}$ exists. A right fraction $as^{-1} \in \mathbb{P}_{\mathbb{Z}} S^{-1}$, for some $a \in \mathbb{P}_{\mathbb{Z}}$ and $s \in S$, can be seen as a rational split quaternion $\mathrm{q} \in \mathbb{P}_{\mathbb{Q}}$, whose coefficients are rational numbers with a denominator which is not divisible by p. In other words $\mathbb{P}_{\mathbb{Z}} S^{-1} \subseteq \mathbb{P}_{\mathbb{Z}_{(p)}}$. For the reverse inclusion, notice that the minimum common denominator of some elements of $\mathbb{Z}_{(p)}$ is an element of $\mathbb{Z} \setminus p\mathbb{Z}$. So $\mathbb{P}_{\mathbb{Z}} S^{-1} = \mathbb{P}_{\mathbb{Z}_{(p)}}$. Similarly it can be proved that $S^{-1} \mathbb{P}_{\mathbb{Z}} = \mathbb{P}_{\mathbb{Z}_{(p)}}$. **QED**

Symmetrically we have the following result.

Proposition 2.2.6. *Let p be an odd prime integer,* $Q = p\mathbb{P}_{\mathbb{Z}}$ *and* $S = \mathscr{C}(Q)$. *Then*

$$\mathbb{P}_{\mathbb{Z}} S^{-1} = S^{-1} \mathbb{P}_{\mathbb{Z}} = \mathbb{P}_{\mathbb{Z}_{(p)}}.$$

Proof. We saw that S is a denominator set of $\mathbb{P}_{\mathbb{Z}}$ (Proposition 2.2.2). So the ring $\mathbb{P}_{\mathbb{Z}}S^{-1}$ exists. Since by Corollary 2.1.14, the norm of the elements of S is not divisible by p, a right fraction $\mathrm{p}s^{-1} \in \mathbb{P}_{\mathbb{Z}}S^{-1}$, for some $\mathrm{p} \in \mathbb{P}_{\mathbb{Z}}$ and $s \in S$, can be seen as a rational split quaternion $\mathrm{q} = \frac{1}{\mathrm{N}(s)}\mathrm{p}\overline{s} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$, where $a, b, c, d \in \mathbb{Q}$ and their denominators are not divisible by p. In other words, $a, b, c, d \in \mathbb{Z}_{(p)}$. In particular $\mathbb{P}_{\mathbb{Z}}S^{-1} \subseteq \mathbb{P}_{\mathbb{Z}_{(p)}}$. For the reverse inclusion let $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}_{(p)}}$. Taking a common denominator, write $\mathrm{q} = \frac{1}{n}\mathrm{p}$, for some $\mathrm{p} \in \mathbb{P}_{\mathbb{Z}}$ and $n \in \mathbb{Z}$. Since the minimum common denominator of some elements of $\mathbb{Z}_{(p)}$ is an element of $\mathbb{Z} \setminus p\mathbb{Z}$, then n is not divisible by p. Thus neither $n^2 = \mathrm{N}(n)$ is divisible by p. So $n \in S$ and $\mathbb{P}_{\mathbb{Z}}S^{-1} = \mathbb{P}_{\mathbb{Z}_{(p)}}$. In the same manner we can prove that $S^{-1}\mathbb{P}_{\mathbb{Z}} = \mathbb{P}_{\mathbb{Z}_{(p)}}$. **QED**

We conclude this section calculating the total ring of fractions of $\mathbb{P}_{\mathbb{Z}_{(p)}}$, for a prime integer p. Working as we did for $\mathbb{P}_{\mathbb{Z}}$, it can be proved that the total ring of fractions of $\mathbb{P}_{\mathbb{Z}_{(p)}}$, for a prime integer p, is the whole ring $\mathbb{P}_{\mathbb{Q}}$.

Proposition 2.2.7. *Let p be a prime integer. Then*

$$\mathcal{Q}(\mathbb{P}_{\mathbb{Z}_{(p)}}) = \mathbb{P}_{\mathbb{Q}}.$$

Proof. Call $S = \mathcal{R}(\mathbb{P}_{\mathbb{Z}_{(p)}})$. We have that S is a multiplicative subset of $\mathbb{P}_{\mathbb{Z}_{(p)}}$. As in proof of Proposition 2.2.2, we get that S is a two-sided denominator set in $\mathbb{P}_{\mathbb{Z}_{(p)}}$. Now we can localize $\mathbb{P}_{\mathbb{Z}_{(p)}}$ at S. By Corollary 1.5.6, we have that S is the set of the elements of $\mathbb{P}_{\mathbb{Z}_{(p)}}$ with nonzero norm. As in proof of Proposition 2.2.3, we can see that any fraction $as^{-1} \in \mathbb{P}_{\mathbb{Z}_{(p)}}S^{-1}$ is an element of $\mathbb{P}_{\mathbb{Q}}$. Take now $\mathrm{q} \in \mathbb{P}_{\mathbb{Q}}$. Then $\mathrm{q} = \frac{1}{n}\mathrm{p}$, for some $\mathrm{p} \in \mathbb{P}_{\mathbb{Z}}$ and $n \in \mathbb{Z}^*$. Obviously, since $n \in \mathbb{Z}^*$, then $n \in S$. Thus finally $\mathbb{P}_{\mathbb{Z}_{(p)}}S^{-1} = \mathbb{P}_{\mathbb{Q}}$. Similarly, $S^{-1}\mathbb{P}_{\mathbb{Z}_{(p)}} = \mathbb{P}_{\mathbb{Q}}$. **QED**

Imitating Propositions 2.2.3 and 2.2.7 we can give this general result.

Proposition 2.2.8. *Let R be a commutative ring and let $\mathcal{Q}(R)$ be its total ring of fractions. Then*

$$\mathcal{Q}(\mathbb{P}_R) = \mathbb{P}_{\mathcal{Q}(R)}.$$

Proof. By hypothesis, every non zero-divisor of R has an inverse in $\mathcal{Q}(R)$. Moreover it is possible to build the split quaternion algebra $\mathbb{P}_{\mathcal{Q}(\mathbb{P}_R)}$ over the total ring of fractions of R.

Call $S = \mathcal{R}(\mathbb{P}_R)$, the set of the regular elements of $\mathbb{P}_R$. We already know that S is a multiplicative subset of $\mathbb{P}_R$, see 2.1.2. Since S does not contain zero-divisors, for S being a right denominator set is equivalent to being right permutable. For seeing this, take $\mathrm{q} \in \mathbb{P}_R$ and $\mathrm{s} \in S$. We must show that $\mathrm{q}S \cap \mathrm{s}\mathbb{P}_R \neq \varnothing$. Since s is a regular element, by Proposition 1.5.5, $\mathrm{N(s)}$ is regular in R. Moreover $\mathrm{N}(s)$ is regular in $\mathbb{P}_R$. In fact, if there is an $a \in \mathbb{P}_R^*$ such that $\mathrm{N(s)}a = 0$, then $\mathrm{N}(\mathrm{N(s)}a) = \mathrm{N}(\mathrm{N(s)})\,\mathrm{N}(a) = \mathrm{N(s)}^2\,\mathrm{N}(a) = 0$ which implies that $\mathrm{N(s)}$ is a zero-divisor in R. This contradicts our assumption, then $\mathrm{N(s)} \in S \cap R$. Recall now that $R \subseteq \mathcal{Z}(\mathbb{P}_R)$, by Corollary 1.4.8. Finally using the equality $a\,\mathrm{N(s)} = \mathrm{s}(\bar{\mathrm{s}}a)$, we get that S is right permutable and so a right denominator set. Similarly S is a left denominator set. It makes sense then to build $\mathbb{P}_R S^{-1}$ and $S^{-1}\mathbb{P}_R$. We show now that $\mathbb{P}_R S^{-1} = \mathbb{P}_{\mathcal{Q}(R)}$. Take $\mathrm{q} \in \mathbb{P}_R$ and $s \in S$. We must show that $\mathrm{qs}^{-1} \in \mathbb{P}_{\mathcal{Q}(R)}$. Since $\mathrm{N(s)}$ is invertible in $\mathcal{Q}(R)$, by Proposition 1.5.2 we have that $\mathrm{s} \in \mathcal{U}(\mathbb{P}_{\mathcal{Q}(R)})$ and $\mathrm{s}^{-1} = \frac{1}{\mathrm{N(s)}}\bar{s}$. So $\mathrm{q}s^{-1} = \frac{1}{\mathrm{N(s)}}\mathrm{q}\bar{\mathrm{s}} \in \mathbb{P}_{\mathcal{Q}(R)}$. Let us show the reverse inclusion: $\mathbb{P}_{\mathcal{Q}(R)} \subseteq \mathbb{P}_R S^{-1}$. Take an element $\mathrm{q} \in \mathbb{P}_{\mathcal{Q}(R)}$. Then

$$\mathrm{q} = a_1 s_1^{-1} + a_2 s_2^{-1}\,\mathbf{i} + a_3 s_3^{-1}\,\mathbf{j} + a_4 s_4^{-1}\,\mathbf{k},$$

for some $a_i \in R$ and $s_i \in \mathcal{R}(R)$. By the condition (i) of the Definition 2.1.20 we infer that it is possible to take a common denominator $\mathrm{s} \in S$ for the coefficients $a_i s_i^{-1}$ of q. Thus we can write q = ps^{-1}, where p $\in \mathbb{P}_R$ and s $\in S$. This means that q $\in \mathbb{P}_R S^{-1}$. Then $\mathbb{P}_R S^{-1} = \mathbb{P}_{\mathcal{Q}(R)}$. Similarly $S^{-1}\mathbb{P}_R = \mathbb{P}_{\mathcal{Q}(R)}$. Thus, the total ring of fractions of $\mathbb{P}_R$ is defined: we have

$$\mathcal{Q}(\mathbb{P}_R) = \mathbb{P}_{\mathcal{Q}(R)}$$

and our proof is now complete. **QED**

Chapter 3

Integer-valued polynomials over $\mathbb{P}_{\mathbb{Z}}$

We recall that if D is a commutative domain with field of quotients K, the set of integer-valued polynomials over D is defined as

$$\operatorname{Int}(D) = \{\, f(x) \in K[x] \mid f(a) \in D, \forall\, a \in D \,\}\,.$$

In a commutative setting it is easy to show that $\operatorname{Int}(D)$ is a ring. This simply follows from the fact that polynomial evaluation at an element $a \in D$ is a ring homomorphism: $D[x] \to D$, $f(x) \mapsto f(a)$.

This property is not true in general if we take a polynomial with coefficients in a noncommutative ring. In $\mathbb{P}_{\mathbb{Z}}[x]$ consider, for example, the polynomials $f(x) = x - \mathbf{i}$ and $g(x) = x - \mathbf{j}$. Their product is $fg(x) = x^2 - (\mathbf{i} + \mathbf{j})x + \mathbf{k}$. Although $f(\mathbf{i})g(\mathbf{i}) = 0$, we have that $fg(\mathbf{i}) = 2\,\mathbf{k} \neq 0$. In general, it can be easily shown that the polynomial evaluation at an element $a \in R$ is a ring homomorphism if and only if a is contained in the center $\mathcal{Z}(R)$ of R. In this chapter, after showing that $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})$ is a ring, we will analyze its multiplicative ideal structure with a special attention to its spectrum.

3.1 The ring $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$

We first give this general definition.

Definition 3.1.1. Let R be a commutative ring with total ring of quotients $\mathcal{Q}(R)$. We define the set of integer-valued polynomials over R to be:

$$\mathrm{Int}(R) = \{\, f(x) \in \mathcal{Q}(R)[x] \mid f(\mathrm{q}) \in R, \, \forall\, \mathrm{q} \in R \,\}\,.$$

In Chapter 2.2 we showed that the total ring of fractions of $\mathbb{P}_{\mathbb{Z}}$ coincides with $\mathbb{P}_{\mathbb{Q}}$. Then we can give our main definition in this Chapter.

Definition 3.1.2. We define the set of integer-valued polynomials over $\mathbb{P}_{\mathbb{Z}}$ to be:

$$\mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) = \{\, f(x) \in \mathbb{P}_{\mathbb{Q}}[x] \mid f(\mathrm{q}) \in \mathbb{P}_{\mathbb{Z}}, \, \forall\, \mathrm{q} \in \mathbb{P}_{\mathbb{Z}} \,\}\,.$$

In [22, chapter 3] Werner shows that the analogous set $\mathrm{Int}(\mathbb{H}_{\mathbb{Z}})$ is a ring. His proof can be extended to more general rings as follows.

Theorem 3.1.3. *Let $R \subseteq S$ be a ring extension. Let $u_1, u_2, \ldots, u_n$ be units of R. If every element $a \in R$ can be written as $a = s_1u_1 + s_2u_2 + \cdots + s_nu_n$, for some $s_i \in \mathcal{Z}(S)$, then $\mathrm{Int}_S(R) = \{\, f(x) \in S[x] \mid f(R) \subseteq R \,\}$ is a ring.*

Proof. See [23, Theorem 1.2] or [8, Theorem 2.1].

Corollary 3.1.4. *Let R be a commutative ring. Then the set $\mathrm{Int}(\mathbb{P}_R)$ is a ring. In particular, $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ is a ring.*

Proof. It is a consequence of Theorem 3.1.3. In fact $\mathbb{P}_R$ is a four-dimensional R-algebra generated by the units 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ over R and R is contained in the center of $\mathbb{P}_R$. **QED**

We spend here few words on an interesting open problem we dealt with in our researches. Given any noncommutative ring extension $A \subseteq B$, define the set

$$\operatorname{Int}_B(A) = \{\, f(x) \in B[x] \mid f(A) \subseteq A \,\},$$

of the polynomials of $B[x]$ that are integer-valued over A. The most important open problem remains to establish if $\operatorname{Int}_B(A)$ is closed under multiplication and if it is hence a ring.

In literature there are only partial results about this topic that invest matrix rings, quaternion algebras and split-quaternion algebras, after this thesis. The most general result known is by Werner (see [23, Theorem 1.2]). It assures that if every element of A is finitely generated by units over the center of B, then $\operatorname{Int}_B(A)$ is a ring. Thus, if it is not given such a unit basis for A, we can not prove in general that $\operatorname{Int}_B(A)$ is closed under multiplication. For instance, let A be the generalized quaternion algebra $\left(\frac{\alpha,\beta}{\mathbb{Z}}\right)$, for some $\alpha, \beta \in \mathbb{Z}$ (see Definition 1.1.1). If $\alpha \neq \pm 1$ (or $\beta \neq \pm 1$) then $\mathbf{i}$ (respectively $\mathbf{j}$) is not invertible. Then we can not use Theorem 3.1.3 for proving that, taken where $B = \left(\frac{\alpha,\beta}{\mathbb{Q}}\right)$, $\operatorname{Int}_B(A)$ is a ring. Another ring extension we tried to approach is $\mathbb{P}_{\mathbb{Z}}\langle\mu\rangle \subseteq \mathbb{P}_{\mathbb{Q}}$, where $\mathbb{P}_{\mathbb{Z}}\langle\mu\rangle$ is the algebra generated by $\mathbb{P}_{\mathbb{Z}}$ and $\mu = \frac{1+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2} \in \mathbb{P}_{\mathbb{Q}}$. The elements of $\mathbb{P}_{\mathbb{Z}}\langle\mu\rangle$ turn out to be the $\mathbb{Z}$-linear combinations of 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ and μ. Since μ is not invertible, (it is in fact a zero-divisor) we can not use Theorem 3.1.3. New techniques are needed for establishing if $\operatorname{Int}\mathbb{P}_{\mathbb{Z}}\langle\mu\rangle$ is a ring.

We give now a short description of some of the elements of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. Certainly, we have $\mathbb{P}_{\mathbb{Z}}[x] \subseteq \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$, but there are other polynomials in $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. In general, given a polynomial $f \in \mathbb{P}_{\mathbb{Q}}[x]$, we may write $f(x) = g(x)/n$ for some $g \in \mathbb{P}_{\mathbb{Z}}[x]$ and some integer $n > 0$. Then, $f \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ if and only if $g(\mathrm{q}) \in n\mathbb{P}_{\mathbb{Z}}$ for all $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$. Equivalently, $f \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ if and only if g sends each element of the finite ring $\frac{\mathbb{P}_{\mathbb{Z}}}{n\mathbb{P}_{\mathbb{Z}}}$ to 0 in $\frac{\mathbb{P}_{\mathbb{Z}}}{n\mathbb{P}_{\mathbb{Z}}}$. Using these equivalences, one may produce many polynomials in $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) \smallsetminus \mathbb{P}_{\mathbb{Z}}[x]$. For example, it is easy to verify that $\frac{(1+\mathbf{i}+\mathbf{j}+\mathbf{k})(x^2-x)}{2} \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. Moreover, it is known ([3, Thm. 3]) that the polynomial $(x^{p^2} - x)(x^p - x)$ kills each matrix in $M_2(\mathbb{F}_p)$. Thus, by Proposition 1.6.10 and Theorem 1.3.1, $\frac{(x^{p^2}-x)(x^p-x)}{p} \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$, for each odd prime p.

In what follows we illustrate some general properties of the ring of polynomials with coefficients over a split quaternion algebra. We will use these results later in studying the ideals of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$.

Definition 3.1.5. Let R be a ring. We define a split quaternion with coefficients in $R[x]$ as an expression of the form $F = f_0(x)+f_1(x)\,\mathbf{i}+f_2(x)\,\mathbf{j}+f_3(x)\,\mathbf{k}$, where the $f_i(x)$'s are in $R[x]$. We will indicate their collection with the obvious symbol $\mathbb{P}_{R[x]}$.

Here a useful result follows. It is intuitive but requires a quite technical proof.

Theorem 3.1.6. *Let R be a commutative ring. Then*

$$\mathbb{P}_R[x] \simeq \mathbb{P}_{R[x]}.$$

Proof. Let us consider the map $\Psi : \mathbb{P}_R[x] \longrightarrow \mathbb{P}_{R[x]}$ such that for all $f(x) \in \mathbb{P}_R[x]$, $f(x) = \sum_{r=0}^{n}(a_r + b_r\,\mathbf{i} + c_r\,\mathbf{j} + d_r\,\mathbf{k})x^r$, then

$$\Psi(f(x)) \overset{\text{def}}{=} \sum_{r=0}^{n} a_r x^r + \sum_{r=0}^{n} b_r x^r\,\mathbf{i} + \sum_{r=0}^{n} c_r x^r\,\mathbf{j} + \sum_{r=0}^{n} d_r x^r\,\mathbf{k}.$$

For instance, take the polynomial $f(x) = 1 - \mathbf{j} + (1 - 2\,\mathbf{i} + \mathbf{j} + \mathbf{k})x + (2\,\mathbf{j} - \mathbf{i})x^3 \in \mathbb{P}_{\mathbb{Z}}[x]$. Then $\Psi(f(x)) = (1 + x) + (-2x - x^3)\,\mathbf{i} + (-1 + x + 2x^3)\,\mathbf{j} + (x)\,\mathbf{k}$.

Let us prove now that given $f(x)$ and $g(x)$ in $\mathbb{P}_R[x]$, then $\Psi(f(x)+g(x)) = \Psi(f(x)) + \Psi(g(x))$ and $\Psi(f(x)g(x)) = \Psi(f(x))\Psi(g(x))$.

For simplicity, when we sum two polynomials, we consider them as if they have the same degree, adjoining zero coefficients where necessary. As regards the additivity of Ψ, defined $n' \overset{\text{def}}{=} \max\{\, m, n\,\}$, we have:

$$\begin{aligned}
&\Psi(f(x) + g(x)) = \\
&= \Psi\left(\left(\sum_{r=0}^{n} (a_r + b_r\,\mathbf{i} + c_r\,\mathbf{j} + d_r\,\mathbf{k})\, x^r\right) + \left(\sum_{s=0}^{m} (a'_s + b'_s\,\mathbf{i} + c'_s\,\mathbf{j} + d'_s\,\mathbf{k})\, x^s\right)\right) \\
&= \Psi\left(\sum_{r=0}^{n'} ((a_r + a'_r) + (b_r + b'_r)\ \mathbf{i} + (c_r + c'_r)\ \mathbf{j} + (d_r + d'_r)\ \mathbf{k})\, x^r\right) \\
&= \sum_{r=0}^{n'}(a_r + a'_r)x^r + \sum_{r=0}^{n'}(b_r + b'_r)x^r\,\mathbf{i} + \sum_{r=0}^{n'}(c_r + c'_r)x^r\,\mathbf{j} + \sum_{r=0}^{n'}(d_r + d'_r)x^r\,\mathbf{k} \\
&= \left(\sum_{r=0}^{n} a_r x^r + \sum_{r=0}^{n} b_r x^r\,\mathbf{i} + \sum_{r=0}^{n} c_r x^r\,\mathbf{j} + \sum_{r=0}^{n} d_r x^r\,\mathbf{k}\right) + \\
&\qquad + \left(\sum_{r=0}^{m} a'_r x^r + \sum_{r=0}^{m} b'_r x^r\,\mathbf{i} + \sum_{r=0}^{m} c'_r x^r\,\mathbf{j} + \sum_{r=0}^{m} d'_r x^r\,\mathbf{k}\right) \\
&= \Psi(f(x)) + \Psi(g(x)).
\end{aligned}$$

Obviously, by induction, it can be proved that Ψ behaves well with finite sums.

We now deal with the multiplicativity of Ψ. We will follow some steps depending on the number of terms in the polynomials we multiply. First of all observe that Ψ *essentially* fixes monomials of the form $f(x) = aux^r$, where $a \in R$ and u is one of the unit generators 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$. In fact we have $\Psi(aux^r) = ax^r u$. Now take $g(x) = a'vx^s$, with $a' \in R$ and $v \in \{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$. Then $\Psi(f(x)g(x)) = \Psi(aux^r \cdot a'vx^s) = \Psi(aa'uvx^{r+s}) = aa'x^{r+s}uv$, since uv is one of the generator units (modulo the sign). On the other hand $\Psi(f(x))\Psi(g(x)) = ax^r u \cdot a'x^s v = aa'x^{r+s}uv = \Psi(f(x)g(x))$ (with the same sign for uv as above).

Let us now suppose that $g(x) = (a' + b'\,\mathbf{i} + c'\,\mathbf{j} + d'\,\mathbf{k})x^s$, for some $a', b', c', d' \in R$. Then $\Psi(f(x)g(x)) = \Psi(aux^r \cdot (a' + b'\,\mathbf{i} + c'\,\mathbf{j} + d'\,\mathbf{k})x^s) = aa'x^{r+s}u + ab'x^{r+s}u\,\mathbf{i} + ac'x^{r+s}u\,\mathbf{j} + ad'x^{r+s}u\,\mathbf{k}$, here we used additivity of Ψ. If we calculate $\Psi(f(x))\Psi(g(x))$, we simply obtain the same result.

Take now a generic polynomial $g(x)$. Then, using again that Ψ is additive over $g(x)$, we get the thesis. Simmetrically, if we increase the number of terms of $f(x)$ as we did with $g(x)$ above, we finally get that Ψ behaves well with the multiplication too and that it is a ring homomorphism.

It remains to prove that Ψ is bijective. Surjectivity of Ψ is obvious, but we must settle some details. Take $F \in \mathbb{P}_{R[x]}$, $F = \sum_{s=0}^{n_0} a_s x^s + \sum_{t=0}^{n_1} b_t x^t\,\mathbf{i} + \sum_{u=0}^{n_2} c_u x^u\,\mathbf{j} + \sum_{v=0}^{n_3} d_v x^v\,\mathbf{k}$. Let $n \overset{\text{def}}{=} \max\{\, n_0, n_1, n_2, n_3 \,\}$. Then define $f(x) \overset{\text{def}}{=} \sum_{r=0}^{n}(a_r + b_r\,\mathbf{i} + c_r\,\mathbf{j} + d_r\,\mathbf{k})x^r$ where we suppose to take the value zero for a_r, b_r, c_r and d_r's when $n > n_l$, for $0 \leqslant l \leqslant 3$. It is clear that $\Psi(f(x)) = F$. As regards the injectivity, we prove that $\ker(\Psi)$ is trivial. Suppose $\Psi(f(x)) = 0$, for a polynomial $f(x) = \sum_{r=0}^{n}(a_r + b_r\,\mathbf{i} + c_r\,\mathbf{j} + d_r\,\mathbf{k})x^r$. Then $\sum_{r=0}^{n} a_r x^r + \sum_{r=0}^{n} b_r x^r\,\mathbf{i} + \sum_{r=0}^{n} c_r x^r\,\mathbf{j} + \sum_{r=0}^{n} d_r x^r\,\mathbf{k} = 0$. This implies that $\sum_{r=0}^{n} a_r x^r = \sum_{r=0}^{n} b_r x^r = \sum_{r=0}^{n} c_r x^r = \sum_{r=0}^{n} d_r x^r = 0$ which is obviously equivalent to say that all a_r's, b_r's, c_r's and d_r's are zero for all r. Then $f(x)$ itself is zero. Then Ψ is an isomorphism and $\mathbb{P}_R[x] \simeq \mathbb{P}_{R[x]}$, as we wanted. **QED**

In what follows we will use this definition.

Definition 3.1.7. Let R be a commutative ring. Take a polynomial $f(x) = \sum_{r=0}^{n} \mathrm{q}_r x^r \in \mathbb{P}_R[x]$. We define the bar conjugate of $f(x)$ to be the polynomial $\overline{f}(x) \overset{\text{def}}{=} \sum_{r=0}^{n} \overline{\mathrm{q}}_r x^r$, obtained by taking the bar conjugate of all coefficients of $f(x)$. Moreover we define the norm and the trace of $f(x)$ to be respectively $\mathrm{N}(f(x)) \overset{\text{def}}{=} f(x) \cdot \overline{f}(x)$ and $\mathrm{T}(f(x)) \overset{\text{def}}{=} f(x) + \overline{f}(x)$.

As for split quaternions, the bar conjugation of polynomials is an *anti-automorphism* of the ring $\mathbb{P}_R[x]$. We list some properties:

Proposition 3.1.8. *Let R be a commutative ring. Let $f(x)$ and $g(x)$ be two polynomials of $\mathbb{P}_R[x]$. Then:*

(i) $\overline{\overline{f}}(x) = f(x)$;

(ii) $\overline{f(x) + g(x)} = \overline{f}(x) + \overline{g}(x)$;

(iii) $\overline{f(x)g(x)} = \overline{g}(x)\,\overline{f}(x)$;

(iv) $f(x) + \overline{f}(x) \in R[x]$;

(v) $f(x)\overline{f}(x) \in R[x]$;

(vi) $\mathcal{Z}(\mathbb{P}_R[x]) = \mathcal{Z}(\mathbb{P}_R)[x]$.

Proof. By the isomorphism stated in Theorem 3.1.6, the points (i)-(v) can be proved exactly as for split quaternions with coefficients in a commutative ring. Point (vi) is easy to show. **QED**

Corollary 3.1.9. *Let R be a commutative ring. Then the isomorphism of Theorem 3.1.6 behaves well with the bar conjugation. In particular if* $f(x) =$

$f_0(x) + f_1(x)\,\mathbf{i} + f_2(x)\,\mathbf{j} + f_3(x)\,\mathbf{k} \in \mathbb{P}_R[x]$, *then*

$$\overline{f}(x) = f_0(x) - f_1(x)\,\mathbf{i} - f_2(x)\,\mathbf{j} - f_3(x)\,\mathbf{k},$$

$$\mathrm{T}(f(x)) = 2f_0(x)$$

and

$$\mathrm{N}(f(x)) = f_0^2(x) - f_1^2(x) - f_2^2(x) - f_3^2(x).$$

Proof. It can be easily seen by direct calculation. **QED**

Lemma 3.1.10. *Let $f(x), h(x) \in \mathbb{Q}[x]$, $f(x) \neq 0$ and $g(x) \in \mathbb{P}_{\mathbb{Q}}[x]$. If $f(x) = h(x)g(x)$, then $g(x) \in \mathbb{Q}[x]$. Similarly, if $f(x) = g(x)h(x)$, then $g(x) \in \mathbb{Q}[x]$.*

Proof. By the equality $f(x) = h(x)g(x)$, we get $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$. Since by hypothesis, $f(x)$ and $h(x)$ have central coefficients, then $f(x) = \overline{g}(x)h(x)$. Thus $\overline{g}(x)h(x) = g(x)h(x)$ and $(\overline{g}(x) - g(x))h(x) = 0$. Since the coefficients of $h(x)$ are in $\mathbb{Q}$, then $h(x)$ itself can not be a zero-divisor. So $\overline{g}(x) = g(x)$ that is to say, $g(x) \in \mathbb{Q}[x]$. **QED**

The following result is a generalization of Euclid's lemma. We will use it later for classifying the prime ideals of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ above (0) (cf. Section 3.4.1).

Proposition 3.1.11. *Let $f(x) \in \mathbb{Q}[x]$ and $g(x) \in \mathbb{P}_{\mathbb{Q}}[x]$. Let $M(x) \in \mathbb{Q}[x]$ be an irreducible polynomial. Suppose that $M(x) \mid f(x)g(x)$ and $M(x) \nmid f(x)$, then $M(x) \mid g(x)$ in $\mathbb{P}_{\mathbb{Q}}[x]$.*

Proof. By Theorem 3.1.6, we can write $g(x) = g_0(x) + g_1(x)\,\mathbf{i} + g_2(x)\,\mathbf{j} + g_3(x)\,\mathbf{k}$, for some $g_r(x) \in \mathbb{Q}[x]$, uniquely determined. By hypothesis, we can write $f(x)g(x) = M(x)q(x)$, for some $q(x) \in \mathbb{P}_{\mathbb{Q}}[x]$. Applying the bar conjugation, we get $f(x)\overline{g}(x) = M(x)\overline{q}(x)$, since $f(x)$ and $M(x)$ have central coefficients. Thus $f(x)\left(g(x)+\overline{g}(x)\right) = M(x)\left(q(x)+\overline{q}(x)\right)$. Since the last equality involves polynomials with rational coefficients, we must have that $M(x) \mid (g(x)+\overline{g}(x)) = 2g_0(x)$, that is to say $M(x) \mid g_0(x)$. Take now the polynomial $\mathbf{i}g(x) = -g_1(x) + g_0(x)\,\mathbf{i} - g_3(x)\,\mathbf{j} + g_2(x)\,\mathbf{k}$. Arguing as above with $\mathbf{i}g(x)$ instead of $g(x)$ we obtain that $M(x) \mid g_1(x)$. Multiplying $g(x)$ with $\mathbf{j}$ and $\mathbf{k}$ in the same way we get respectively that $M(x) \mid g_2(x)$ and $M(x) \mid g_3(x)$. Finally $M(x) \mid g(x)$ in $\mathbb{P}_{\mathbb{Q}}[x]$. **QED**

3.2 Some ideals of $\mathrm{Int}(\mathbb{H}_{\mathbb{Z}})$

Given a commutative domain D, an ideal $\mathscr{I}$ of D and an element $a \in D$, it is defined

$$\mathfrak{P}_{\mathscr{I},a} \overset{\text{def}}{=} \{\, f(x) \in \mathrm{Int}(D) \mid f(a) \in \mathscr{I} \,\}\,.$$

It is easy to see that $\mathfrak{P}_{\mathscr{I},a}$ is an ideal of $\mathrm{Int}(D)$ and if $\mathscr{P}$ is a prime ideal of D, then $\mathfrak{P}_{\mathscr{P},a}$ is a prime ideal of $\mathrm{Int}(D)$. The proof of this is based on the fact that the polynomial evaluation at $a \in D$, call it $\Phi_a : \mathrm{Int}(D) \to D$, $\Phi_a(f(x)) = f(a)$, is a ring homomorphism with kernel $\mathfrak{P}_{\mathscr{P},a}$. As we already remarked, in a noncommutative setting, Φ_a may not be an homomorphism of rings.

In [22], Werner gives the following definition.

Definition 3.2.1. Let $\mathscr{I}$ be an ideal of $\mathbb{H}_{\mathbb{Z}}$ and $\alpha \in \mathbb{H}_{\mathbb{Z}}$. Then

$$\mathfrak{P}_{\mathscr{I},\alpha} \overset{\text{def}}{=} \{\, f(x) \in \mathrm{Int}(\mathbb{H}_{\mathbb{Z}}) \mid f(\beta) \in \mathscr{I},\ \forall\, \beta \in \mathrm{Co}_{\mathbb{H}_{\mathbb{Z}}}(\alpha) \,\}\,.$$

Since the group $\mathcal{U}(\mathbb{H}_{\mathbb{Z}})$ is a finite set, only a finite number of tests are needed to check whether a polynomial of $\mathrm{Int}(\mathbb{H}_{\mathbb{Z}})$ is an element of $\mathfrak{P}_{\mathscr{I},\alpha}$.

In this section we briefly recall some results by Werner about the $\mathfrak{P}_{\mathscr{I},\alpha}$-like sets. In particular we will see that it is not in general an ideal of $\mathrm{Int}(\mathbb{H}_{\mathbb{Z}})$ (if $\alpha \in \mathbb{Z}$ or $\mathscr{I} = n\mathbb{H}_{\mathbb{Z}}$, for some $n \in \mathbb{Z}$, it is easy to see that $\mathfrak{P}_{\mathscr{I},\alpha}$ is an ideal).

We recall that the prime spectrum of $\mathbb{H}_{\mathbb{Z}}$ is (formally) similar to that of $\mathbb{P}_{\mathbb{Z}}$. The prime ideals are (0), $p\mathbb{H}_{\mathbb{Z}}$ for all odd prime integers p and the non-principal ideal $(1+\mathbf{i}, 1+\mathbf{j})$ that contains $2\mathbb{H}_{\mathbb{Z}}$. These ideals, except (0), are also maximal ideals.

Proposition 3.2.2. [22, Theorem 4.5] *Let $n \in \mathbb{Z}$, $\mathscr{I} = n\mathbb{H}_{\mathbb{Z}}$ and $\alpha \in \mathbb{H}_{\mathbb{Z}}$. Then $\mathfrak{P}_{\mathscr{I},\alpha}$ is an ideal of* $\mathrm{Int}(\mathbb{H}_{\mathbb{Z}})$. *Moreover if $n \neq 0$, then $\frac{\mathrm{Int}(\mathbb{H}_{\mathbb{Z}})}{\mathfrak{P}_{\mathscr{I},\alpha}}$ is a finite ring.*

When $\mathscr{I} = (0)$, which is prime in $\mathbb{H}_{\mathbb{Z}}$, we have:

Proposition 3.2.3. [22, Proposition 4.6] *For all $\alpha \in \mathbb{H}_{\mathbb{Z}}$, the ideal $\mathfrak{P}_{(0),\alpha}$ is a prime ideal of* $\mathrm{Int}(\mathbb{H}_{\mathbb{Z}})$.

When we work with a prime ideal of $\mathbb{H}_{\mathbb{Z}}$ generated by an odd prime integer and a central element a, we simply get:

Proposition 3.2.4. [22, Theorem 4.12] *Let $\mathscr{P} = p\mathbb{H}_{\mathbb{Z}}$, for an odd prime integer p. Then for all $a \in \mathbb{Z}$ the set $\mathfrak{P}_{\mathscr{P},a}$ is a maximal ideal of* $\mathrm{Int}(\mathbb{H}_{\mathbb{Z}})$.

Instead, when we work with the prime ideal $\mathscr{P} = p\mathbb{H}_{\mathbb{Z}}$ as above and with a non-central quaternion α we have:

Proposition 3.2.5. [22, Theorem 4.12] *Let $\mathscr{P} = p\mathbb{H}_{\mathbb{Z}}$, for an odd prime integer p. Let $\alpha \in \mathbb{H}_{\mathbb{Z}}$ and let $m_\alpha(x)$ be its minimal polynomial (as in Definition 1.4.16). Then* *(i)* $\mathfrak{P}_{\mathscr{P},\alpha}$ *is a maximal ideal of* $\mathrm{Int}(\mathbb{H}_{\mathbb{Z}})$ *if and only if* $m_\alpha(x)$ *is irreducible modulo* p.

(ii) If $m_\alpha(x)$ *is quadratic and reducible modulo* p *and* $x - A$ *is a factor of* $m_\alpha(x)$ *modulo* p*, then* $\mathfrak{M} \overset{def}{=} (\mathfrak{P}_{\mathscr{P},\alpha}, x - A)$ *is a maximal ideal of* $\mathrm{Int}(\mathbb{H}_{\mathbb{Z}})$.

In the following we will deal with prime ideals in $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ generalizing to $\mathbb{P}_{\mathbb{Z}}$ many results that hold for $\mathbb{H}_{\mathbb{Z}}$.

3.3 A localization theorem

We aim now to prove for $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ a result similar to Proposition 3.2.5 for $\mathbb{H}_{\mathbb{Z}}$. We will start by some preliminary statements. In his thesis Werner showed that the ring of integer-valued polynomials over $\mathbb{H}_{\mathbb{Z}}$ behaves well when we localize with respect to a multiplicative subset $S \subseteq \mathbb{Z}$, see [21, Theorem 3.3.2]. The keys of the proof are essentially the centrality of the elements of S and the noetherianity of $\mathbb{H}_{\mathbb{Z}}$. These hypothesis are also true for $\mathbb{P}_{\mathbb{Z}}$. Then we can state:

Proposition 3.3.1. *Let* S *be a multiplicative closed subset of* $\mathbb{Z}$*. Then*

$$\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1} = \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}S^{-1}).$$

Proof. Our proof is an adaptation of [4, Theorem I.2.3], with modifications done to account for the noncommutative rings. Both sets (they are subsets of $\mathbb{P}_{\mathbb{Q}}[x]$) considered in the equality are well-defined. As regards $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1}$, the closure under addition follows by taking a common denominator. The multiplicative closure can be proved since the set S^{-1} is central in $\mathbb{P}_{\mathbb{Q}}$. As regards $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}}S^{-1})$, it is a ring by Theorem 3.1.3.

Let now $f \in \operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1}$, and let $\frac{\mathrm{q}}{s} \in \mathbb{P}_{\mathbb{Z}}S^{-1}$, where $s \in S$ and $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$. We use induction on $n = \deg(f)$ to show that $f(\frac{\mathrm{q}}{s}) \in \mathbb{P}_{\mathbb{Z}}S^{-1}$. There is nothing to prove if $n = 0$, so assume that $n > 0$ and that every polynomial in $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1}$ of degree less than n is an element of $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}}S^{-1})$. Let $g(x) = s^n f(x) - f(sx)$. Since $s \in \mathbb{Z}$ is central in $\mathbb{P}_{\mathbb{Q}}$, $f(sx)$ is a polynomial in $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1}$, so $g \in \operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1}$. Furthermore, $\deg(g) < n$, so $g \in \operatorname{Int}(\mathbb{P}_{\mathbb{Z}}S^{-1})$. Note that $f(\mathrm{q}) \in \mathbb{P}_{\mathbb{Z}}S^{-1}$, so $s^n f(\frac{\mathrm{q}}{s}) = g(\frac{\mathrm{q}}{s}) + f(\mathrm{q}) \in \mathbb{P}_{\mathbb{Z}}S^{-1}$. But, s is a unit in $\mathbb{P}_{\mathbb{Z}}S^{-1}$, so we get $f(\frac{\mathrm{q}}{s}) \in \mathbb{P}_{\mathbb{Z}}S^{-1}$. Hence, $f \in \operatorname{Int}(\mathbb{P}_{\mathbb{Z}}S^{-1})$ and $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1} \subseteq \operatorname{Int}(\mathbb{P}_{\mathbb{Z}}S^{-1})$.

To prove that $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}}S^{-1}) \subseteq \operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1}$, let $h(x) \in \operatorname{Int}(\mathbb{P}_{\mathbb{Z}}S^{-1})$, let M be the right $\mathbb{P}_{\mathbb{Z}}$-module generated by the coefficients of $h(x)$, and let M' be the right $\mathbb{P}_{\mathbb{Z}}$-module generated by $\{h(\mathrm{q})\}_{\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}}$. Then, $\mathbb{P}_{\mathbb{Z}}$ is noetherian (as a right module over itself) and M is finitely generated, so M is noetherian as a right $\mathbb{P}_{\mathbb{Z}}$-module. Since $M' \subseteq M$, M' is also finitely generated. Let $\mathrm{p}_1, \mathrm{p}_2, \dots, \mathrm{p}_m \in \mathbb{P}_{\mathbb{Z}}S^{-1}$ be generators for M' as a right $\mathbb{P}_{\mathbb{Z}}$-module.

By finding a common denominator, we see that there exists $u \in S$ such that $u\mathrm{p}_i \in \mathbb{P}_{\mathbb{Z}}$ for each i. Then, $uM' = M'u \subseteq \mathbb{P}_{\mathbb{Z}}$, which gives $uh(x) \in \operatorname{Int}(\mathbb{P}_{\mathbb{Z}})$. Thus, $h(x) \in \operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1}$ and $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}}S^{-1}) \subseteq \operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1}$. **QED**

Similarly it is proven that

$$S^{-1}\operatorname{Int}(\mathbb{P}_{\mathbb{Z}}) = \operatorname{Int}(S^{-1}\mathbb{P}_{\mathbb{Z}}).$$

This easily follows since S is central. In particular the previous proposition holds when $S = \mathbb{Z} \setminus p\mathbb{Z}$ or $S = \mathbb{Z}^*$.

Corollary 3.3.2. *If we take $S = \mathbb{Z} \setminus p\mathbb{Z}$, we have*

$$\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1} = \operatorname{Int}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$$

and for $S = \mathbb{Z}^*$, we have

$$\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1} = \mathrm{Int}(\mathbb{P}_{\mathbb{Q}}) = \mathbb{P}_{\mathbb{Q}}[x].$$

Proof. It follows by Propositions 2.2.5, 2.2.4 and 3.3.1 **QED**

Moreover, if we take a polynomial $g(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ then, by taking a common denominator, $g(x) = \frac{f(x)}{n}$, for some $f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ and $n \in \mathbb{Z} \setminus p\mathbb{Z}$ (it is enough to take a common denominator between the coefficients of $g(x)$).

Proposition 3.3.3. *Let p be a prime integer. Then*

$$\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})_{(p)} = \mathrm{Int}(\mathbb{P}_{\mathbb{Z}_{(p)}}) = \left\{ \frac{f(x)}{n} \;\middle|\; f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}),\ n \in \mathbb{Z} \setminus p\mathbb{Z} \right\}.$$

Proof. From Propositions 2.2.5 and 3.3.1. **QED**

Analogously, when $\mathcal{I}$ is an ideal of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ such that $\mathcal{I} \cap \mathbb{Z} = p\mathbb{Z}$, we can define the localization of $\mathcal{I}$ at p as the set

$$\mathcal{I}_{(p)} \overset{\text{def}}{=} \left\{ \frac{f(x)}{n} \;\middle|\; f(x) \in \mathcal{I},\ n \in \mathbb{Z} \setminus p\mathbb{Z} \right\}.$$

It turns out that $\mathcal{I}_{(p)}$ is an ideal of $\mathrm{Int}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$.

Theorem 3.3.4. *Let p be a prime integer and $\mathcal{I}$ an ideal of* $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ *such that $\mathcal{I} \cap \mathbb{Z} = p\mathbb{Z}$. Then*

$$\frac{\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})}{\mathcal{I}} \simeq \frac{\mathrm{Int}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)}{\mathcal{I}_{(p)}}.$$

Proof. We prove this in the same way as in the commutative case. Let $\pi : \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) \to \frac{\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})}{\mathcal{I}}$ be the quotient homomorphism associated to $\mathcal{I}$. Define a function $\Pi : \mathrm{Int}(\mathbb{P}_{\mathbb{Z}_{(p)}}) \to \frac{\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})}{\mathcal{I}}$ by $\Pi(\frac{f(x)}{n}) = n^{-1}\pi(f(x))$. Here, $f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ and $n \in \mathbb{Z} \setminus p\mathbb{Z}$, using the representation as in Proposition 3.3.3. Since p is contained in $\mathcal{I}$, we can use a Bézout identity to show that n is invertible in the quotient ring $\frac{\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})}{\mathcal{I}}$. Then Π is a well defined ring homomorphism with kernel $\mathcal{I}_{(p)}$. To see this, take two polynomials $\frac{f(x)}{n}$, $\frac{g(x)}{m} \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}_{(p)}})$. Then $\Pi\left(\frac{f(x)}{n} + \frac{g(x)}{m}\right) = (mn)^{-1}\left(\pi(mf(x) + ng(x)\right) = n^{-1}\pi(f(x)) + m^{-1}\pi(g(x)) = \Pi\left(\frac{f(x)}{n}\right) + \Pi\left(\frac{g(x)}{m}\right)$. As regards the multiplication, we have: $\Pi\left(\frac{f(x)}{n}\cdot\frac{g(x)}{m}\right) = (mn)^{-1}\left(\pi(f(x)g(x)\right) = n^{-1}\pi(f(x)) \cdot m^{-1}\pi(g(x)) = \Pi\left(\frac{f(x)}{n}\right)\cdot\Pi\left(\frac{g(x)}{m}\right)$. Let us now calculate $\ker(\Pi)$. Take $f(x) \in \mathcal{I}_{(p)}$. Then $f(x) = \frac{g(x)}{n}$, for some $g(x) \in \mathcal{I}$ and $n \in \mathbb{Z} \setminus p\mathbb{Z}$. So $\Pi\left(f(x)\right) = n^{-1}\pi(g(x)) = 0$, since $\pi(g(x)) = 0$. Let now $\frac{f(x)}{n} \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ such that $\Pi(\frac{f(x)}{n}) = 0$. Then $n^{-1}\pi(f(x)) = 0$, so $f(x) \in \ker(\pi)$. Thus $f(x) \in \mathcal{I}$ and $\frac{f(x)}{n} \in \mathcal{I}_{(p)}$. Moreover Π is surjective since π is. The isomorphism contained in the thesis, follows applying the theorem of isomorphism to Π. **QED**

3.4 Some ideals of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$

The obvious way to extend the ideals $\mathfrak{P}_{\mathscr{I},\mathrm{q}}$ to $\mathbb{P}_{\mathbb{Z}}$ is to consider sets used in [4] of the form $\{f \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) \mid f(\mathrm{q}) \in \mathscr{I}\}$, where $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$ and $\mathscr{I}$ is an ideal of $\mathbb{P}_{\mathbb{Z}}$. Unfortunately, this set may fail to be an ideal if $\mathrm{q} \notin \mathbb{Z}$. For example, if $\mathrm{q} = \mathbf{i}$ and $\mathscr{I} = (0)$, then the polynomial $x - \mathbf{i}$ is in the above set, but the polynomial $(x - \mathbf{i})(x - \mathbf{j}) = x^2 - (\mathbf{i} + \mathbf{j})x + \mathbf{k}$ is not, since evaluation at $\mathbf{i}$ yields $2\mathbf{k}$. However, we obtain an effective definition by expanding the set of elements that must be mapped into $\mathscr{I}$.

Let $\mathscr{I}$ be an ideal of $\mathbb{P}_{\mathbb{Z}}$ and $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$. If we define the set $\mathfrak{P}_{\mathscr{I},\mathrm{q}}$ as the analogue in Definition 3.2.1 for $\mathbb{H}_{\mathbb{Z}}$:

$$\mathfrak{P}_{\mathscr{I},\mathrm{q}} = \{\, f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) \mid f(\mathrm{p}) \in \mathscr{I},\ \forall\, \mathrm{p} \in \mathrm{Co}_{\mathbb{P}_{\mathbb{Z}}}(\mathrm{q}) \,\},$$

we are not able in general to prove that it is an ideal of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ for any $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$

(if q is central then $\mathfrak{P}_{\mathscr{I},\mathrm{q}}$ is an ideal).

More precisely, in our setting, in order to prove that $\mathfrak{P}_{\mathscr{I},\mathrm{q}}$ is an ideal, we need to deal not only with multiplicative conjugates of q ($\mathrm{Co}_{\mathbb{P}_{\mathbb{Z}}}(\mathrm{q})$), but more generally with some of the split quaternions that have the same minimal polynomial of q, as it is clear from the proof of Proposition 3.4.13 and Theorem 3.4.40. We will call them the algebraic conjugates of q.

We give the following definitions.

Definition 3.4.1. Let $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$. We define the *algebraic conjugacy class* of q to be the set

$$\mathrm{C}(\mathrm{q}) = \{\, a \pm b\,\mathbf{i} \pm c\,\mathbf{j} \pm d\,\mathbf{k} \,\}\,.$$

It is easy to see that $\mathrm{C}(a) = \{\, a \,\}$, for all $a \in \mathbb{Z}$. Moreover, given $\mathrm{q} \notin \mathbb{Z}$ and taken any $\mathrm{p} \in \mathrm{C}(\mathrm{q})$, then $m_{\mathrm{q}}(x) = m_{\mathrm{p}}(x)$ (according to Definition 1.4.16 of minimal polynomial).

Definition 3.4.2. Let $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$ and let $\mathscr{I}$ be an ideal of $\mathbb{P}_{\mathbb{Z}}$. We define the set

$$\mathfrak{P}_{\mathscr{I},\mathrm{q}} \overset{\text{def}}{=} \{\, f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) \mid f(\mathrm{p}) \in \mathscr{I},\ \ \forall\, \mathrm{p} \in \mathrm{C}(\mathrm{q}) \,\}\,.$$

When $\mathscr{I} = (0)$, we let

$$\mathfrak{P}_{0,\mathrm{q}} \overset{\text{def}}{=} \mathfrak{P}_{\mathscr{I},\mathrm{q}}$$

and when $\mathscr{I} = n\mathbb{P}_{\mathbb{Z}}$, for an integer $n \in \mathbb{Z}$, we let

$$\mathfrak{P}_{n,\mathrm{q}} \overset{\text{def}}{=} \mathfrak{P}_{\mathscr{I},\mathrm{q}}.$$

Now we analyze some properties of the subsets $\mathfrak{P}_{\mathscr{I},\mathrm{q}}$ of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ defined above in Definition 3.4.2 and compare them with their analogous in $\mathbb{H}_{\mathbb{Z}}$ (Section 3.2).

In Section 1.6 we saw that the prime ideals of $\mathbb{P}_{\mathbb{Z}}$ are (0), the ideals $p\mathbb{P}_{\mathbb{Z}}$, for odd prime integers p, and the nonprincipal ideal $\mathscr{M} = (1 + \mathbf{i}, 1 + \mathbf{j})$ above $2\mathbb{P}_{\mathbb{Z}}$. Among these, the maximal ones are the ideals $p\mathbb{P}_{\mathbb{Z}}$, for odd prime integers p and $\mathscr{M}$.

We will see that $\mathfrak{P}_{\mathscr{I},\mathrm{q}}$ is an ideal when $\mathscr{I} = n\mathbb{P}_{\mathbb{Z}}$, for some $n \in \mathbb{Z}$, and $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$ (cf. 3.4.3). Moreover the residue ring $\frac{\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})}{\mathfrak{P}_{n,\mathrm{q}}}$ is finite (see Propositions 3.4.4 and 3.4.9). Lastly we show that $\mathfrak{P}_{\mathscr{P},a}$ is a prime ideal of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$, for each prime ideal $\mathscr{P}$ of $\mathbb{P}_{\mathbb{Z}}$ and $a \in \mathbb{Z}$ (cf. 3.4.11).

In the next result we consider the sets $\mathfrak{P}_{\mathscr{I},\mathrm{q}}$ where $\mathscr{I}$ is generated by a central element and show that these are ideals.

Proposition 3.4.3. *Let $n \in \mathbb{Z}$ and $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$. Then $\mathfrak{P}_{n,\mathrm{q}}$ is an ideal of* $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$.

Proof. The proof is similar to [22, theorem 6.2.3]. **QED**

In general, we are not able to prove Proposition 3.4.3 when $\mathscr{I}$ is any ideal of $\mathbb{P}_{\mathbb{Z}}$. For the case of the unique non principal prime ideal of $\mathbb{P}_{\mathbb{Z}}$, $\mathscr{I} = \mathscr{M}$, we will need to slightly correct Definition 3.4.2.

In Proposition 3.2.2 it is stated that the quotient ring of $\mathrm{Int}(\mathbb{H}_{\mathbb{Z}})$ over $\mathfrak{P}_{n,\alpha}$ is a finite ring. We are able to prove the same result for $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ (conf. Propositions 3.4.4 and 3.4.9).

If the split quaternion q is an integer, then the result is immediate and we can give a complete description of its elements.

Proposition 3.4.4. *Let $n \in \mathbb{Z}$, $n \neq 0$, and $\mathrm{q} \in \mathbb{Z}$. Then the residue ring $\frac{\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})}{\mathfrak{P}_{n,\mathrm{q}}} \simeq \mathbb{P}_{\mathbb{Z}_n}$. In particular it is a finite ring.*

Proof. Let us consider the evaluation map at q, $\varphi_{\mathrm{q}} : \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) \to \mathbb{P}_{\mathbb{Z}}$, $f(x) \mapsto f(\mathrm{q})$ and the reduction modulo n, $\Pi : \mathbb{P}_{\mathbb{Z}} \to \mathbb{P}_{\mathbb{Z}_n}$, $\mathrm{q} \mapsto \mathrm{q}$ (mod. n). Since

$\mathrm{q} \in \mathbb{Z}$, φ_{q} is a ring homomorphism. Then it is straightforward to see that $\Pi \circ \varphi_{\mathrm{q}}$ is a surjective ring homomorphism. Its kernel is the set

$$\ker(\Pi \circ \varphi_{\mathrm{q}}) = \{\, f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) \mid f(\mathrm{q}) \equiv 0 \pmod{n} \,\}\,.$$

Since q is a central element, this set is exactly the ideal $\mathfrak{P}_{n,\mathrm{q}}$. Thesis follows by the ring homomorphism theorem. **QED**

If $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}} \smallsetminus \mathbb{Z}$, we need the following lemmas.

Lemma 3.4.5. *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}} \smallsetminus \mathbb{Z}$*. Then there exists* $\mathrm{q}_1 \in \mathrm{C}(\mathrm{q})$ *such that* $\mathrm{q} - \mathrm{q}_1 \neq 0$ *and* $\mathrm{q} - \mathrm{q}_1 \in 2\mathbb{P}_{\mathbb{Z}}$*.*

Proof. Assume that $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$. Since $\mathrm{q} \notin \mathbb{Z}$, one among b, c, d is nonzero. Simply take q_1 to be either $a - b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$, $a + b\,\mathbf{i} - c\,\mathbf{j} + d\,\mathbf{k}$ or $a + b\,\mathbf{i} + c\,\mathbf{j} - d\,\mathbf{k}$. **QED**

Lemma 3.4.6. *Let* $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}} \smallsetminus \mathbb{Z}$ *and let* $m_{\mathrm{q}}(x)$ *be its minimal polynomial. Take* $f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ *and let* $\alpha_1 x + \alpha_0$*, for some* $\alpha_1, \alpha_0 \in \mathbb{P}_{\mathbb{Q}}$*, be the remainder of the division of* $f(x)$ *by* $m_{\mathrm{q}}(x)$*. Then* $2b\alpha_1$*,* $2c\alpha_1$ *and* $2d\alpha_1$ *belong to* $\mathbb{P}_{\mathbb{Z}}$*.*

Proof. First of all we notice that every element of $m_{\mathrm{q}}(x)\mathbb{P}_{\mathbb{Q}}[x]$ (and of $\mathbb{P}_{\mathbb{Q}}[x]m_{\mathrm{q}}(x)$) vanishes at q. Since $\mathrm{q} \notin \mathbb{Z}$, at least one of b, c and d is nonzero. To avoid trivial cases, suppose that $b \neq 0$. Take $\mathrm{q}_1 = a - b\,\mathbf{i} - c\,\mathbf{j} - d\,\mathbf{k}$. Then $f(\mathrm{q}) - f(\mathrm{q}_1) = 2b\alpha_1\,\mathbf{i} \in \mathbb{P}_{\mathbb{Z}}$. The conclusion follows since $\mathbf{i}$ is a unit of $\mathbb{P}_{\mathbb{Z}}$, thus $2b\alpha_1 \in \mathbb{P}_{\mathbb{Z}}$ as well. Similarly if $c \neq 0$ or $d \neq 0$. **QED**

Lemma 3.4.7. *Let* $n \in \mathbb{Z}$*,* $n \neq 0$*, and* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}} \smallsetminus \mathbb{Z}$*. For each* $f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ *define the map*

$$\begin{aligned} f^* : \mathrm{C}(\mathrm{q}) &\longrightarrow \mathbb{P}_{\mathbb{Z}_n} \\ \mathrm{p} &\longmapsto f(\mathrm{p}) \pmod{n} \end{aligned}$$

Let $f(x), g(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$*. Then* $f(x) \equiv g(x) \pmod{\mathfrak{P}_{n,\mathrm{q}}}$ *if and only if* $f^* = g^*$*.*

Proof.

$$\begin{aligned} f^* = g^* &\iff f^*(\mathrm{p}) = g^*(\mathrm{p}), \text{ for all } \mathrm{p} \in \mathrm{C}(\mathrm{q}) \\ &\iff f(\mathrm{p}) \equiv g(\mathrm{p}) \ (\mathrm{mod.}\ n), \text{ for all } \mathrm{p} \in \mathrm{C}(\mathrm{q}) \\ &\iff n \mid (f(\mathrm{p}) - g(\mathrm{p})), \text{ for all } \mathrm{p} \in \mathrm{C}(\mathrm{q}) \\ &\iff f(x) - g(x) \in \mathfrak{P}_{n,\mathrm{q}}. \end{aligned}$$

QED

The following result is obvious when the polynomial involved is an element of $\mathbb{P}_{\mathbb{Z}}[x]$. The significance of the result is that it also holds when the polynomial is in $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) \setminus \mathbb{P}_{\mathbb{Z}}[x]$.

Lemma 3.4.8. *Let* $n \in \mathbb{Z}$*,* $n \neq 0$ *and let* $\mathscr{I} = n\mathbb{P}_{\mathbb{Z}}$*. Let* $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$*, with* $b \neq 0$ *(equivalently for* $c \neq 0$ *or* $d \neq 0$*). Take* $f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$*. Assume that* $\mathrm{q}_1, \mathrm{q}_2 \in \mathrm{C}(\mathrm{q})$ *and* $\mathrm{q}_1 \equiv \mathrm{q}_2 \ (\mathrm{mod.}\ 2bn)$*. Then* $f^*(\mathrm{q}_1) = f^*(\mathrm{q}_2)$*.*

Proof. Write $\mathrm{q}_1 = \mathrm{q}_2 + 2bn\gamma$, for some $\gamma \in \mathbb{P}_{\mathbb{Z}}$. Let $m_{\mathrm{q}}(x)$ be the minimal polynomial of q and let $f(x) \equiv \alpha_1 x + \alpha_0 \ (\mathrm{mod.}\ m_{\mathrm{q}}(x))$, for some $\alpha_1, \alpha_0 \in \mathbb{P}_{\mathbb{Q}}$ as in Lemma 3.4.6. Then:

$$\begin{aligned} f(\mathrm{q}_1) &= \alpha_1 \mathrm{q}_1 + \alpha_0 \\ &= \alpha_1(\mathrm{q}_2 + 2bn\gamma) + \alpha_0 \\ &= \alpha_1 \mathrm{q}_2 + \alpha_0 + 2bn\alpha_1\gamma \\ &= f(\mathrm{q}_2) + 2bn\alpha_1\gamma. \end{aligned}$$

This leads us to the conclusion that $f^*(\mathrm{q}_1) = f^*(\mathrm{q}_2)$. **QED**

Proposition 3.4.9. *Let $n \in \mathbb{Z}$, $n \neq 0$, and $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}} \smallsetminus \mathbb{Z}$. Then the residue ring $\frac{\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})}{\mathfrak{P}_{n,\mathrm{q}}}$ is finite.*

Proof. Let $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$ and take $b \neq 0$ (similarly for cases $c \neq 0$ and $d \neq 0$). Let $\overline{A}$ be a set of residue representatives for $\mathrm{C}(\mathrm{q})$ modulo $2bn$. Then $\overline{A} \subseteq \mathbb{P}_{\mathbb{Z}_{2bn}}$ is finite. Now, for each $\mathrm{q}_1 \in \mathrm{C}(\mathrm{q})$, there exists $\mathrm{q}_2 \in \overline{A}$ such that $\mathrm{q}_1 \equiv \mathrm{q}_2 \pmod{2bn}$. By Lemma 3.4.8, for any $f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$, $f^*(\mathrm{q}_1) = f^*(\mathrm{q}_2)$. So the values of f^* are determined entirely by the values f^* takes on the finite set $\overline{A}$. Thus the number of all possible f^* maps is bounded above by $|\mathbb{P}_{\mathbb{Z}_{2bn}}|^{|\overline{A}|} \leqslant (2bn)^{4(2bn)^4}$. By the correspondence between f^* maps and residues in $\frac{\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})}{\mathfrak{P}_{n,\mathrm{q}}}$ (Lemma 3.4.7), we see that the residue ring is also finite. **QED**

Proposition 3.4.10. *Let $n \in \mathbb{Z}$, $n \neq 0$, $\mathscr{I} = n\mathbb{P}_{\mathbb{Z}}$ and $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$. If $\mathfrak{P}_{n,\mathrm{q}}$ is a prime ideal of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$, then $\mathscr{I}$ is a prime ideal of $\mathbb{P}_{\mathbb{Z}}$.*

Proof. Given the definition of $\mathfrak{P}_{\mathscr{I},\mathrm{q}}$, the statement can be proved exactly as [22, Theorem 4.5]. **QED**

The following result is useful for classifying the ideals $\mathfrak{P}_{\mathscr{P},a}$, where $\mathscr{P}$ is a prime ideal of $\mathbb{P}_{\mathbb{Z}}$ and a is an integer.

Proposition 3.4.11. *Let $\mathscr{P}$ be a prime ideal of $\mathbb{P}_{\mathbb{Z}}$. Then for all $a \in \mathbb{Z}$ the set $\mathfrak{P}_{\mathscr{P},a}$ is a prime ideal of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$.*

Proof. Having $a \in \mathbb{Z}$ implies that $(fg)(a) = f(a)g(a)$, for all $f(x), g(x) \in \mathbb{P}_{\mathbb{Q}}[x]$. The result now follows easily. **QED**

3.4.1 Primes of $\mathrm{Int}(\mathbb{P}_\mathbb{Z})$ above (0)

In this section we give a full description of the prime ideals of $\mathrm{Int}(\mathbb{P}_\mathbb{Z})$ above (0), see Theorem 3.4.22.

We start with this interesting fact.

Proposition 3.4.12. *Let* $\mathrm{q} \in \mathbb{P}_\mathbb{Z}$*. If* $m_\mathrm{q}(x) \in \mathbb{Z}[x]$ *is a reducible polynomial, then* $\mathfrak{P}_{0,\mathrm{q}}$ *is not a prime ideal of* $\mathrm{Int}(\mathbb{P}_\mathbb{Z})$*.*

Proof. The case $\mathrm{q} \in \mathbb{Z}$ gives an irreducible polynomial of degree one. So let $\mathrm{q} \notin \mathbb{Z}$ and $m_\mathrm{q}(x) = (x - A)(x - B)$. Then by the centrality of $x - A$ we have that $(x - A)\,\mathrm{Int}(\mathbb{P}_\mathbb{Z})(x - B) = \mathrm{Int}(\mathbb{P}_\mathbb{Z}) \cdot m_\mathrm{q}(x) \subseteq \mathfrak{P}_{0,\mathrm{q}}$. But $(x - A) \notin \mathfrak{P}_{0,\mathrm{q}}$ nor $(x - B) \notin \mathfrak{P}_{0,\mathrm{q}}$. **QED**

It is worth spending few words on the previous result. In fact it does not have an analogue for $\mathbb{H}_\mathbb{Z}$ because the minimal polynomial of an integer quaternion is always irreducible over $\mathbb{Q}$, as we pointed out after Definition 1.4.16. Moreover, in [22] Werner found that for all $\alpha \in \mathbb{H}_\mathbb{Z}$, $\mathfrak{P}_{(0),\alpha}$ is a prime ideal of $\mathrm{Int}(\mathbb{H}_\mathbb{Z})$ (see Proposition 3.2.3 we recalled).

We begin with the following general description of $\mathfrak{P}_{0,\mathrm{q}}$.

Theorem 3.4.13. *With the above notation, given* $\mathrm{q} \in \mathbb{P}_\mathbb{Z}$*, we have that*

$$\mathfrak{P}_{0,\,\mathrm{q}} = m_\mathrm{q}(x) \cdot \mathbb{P}_\mathbb{Q}[x] \cap \mathrm{Int}(\mathbb{P}_\mathbb{Z}).$$

Proof. It is clear that polynomials of $m_\mathrm{q}(x) \cdot \mathbb{P}_\mathbb{Q}[x]$ vanish at all p's in C(q). So if we select in this set elements from $\mathrm{Int}(\mathbb{P}_\mathbb{Z})$ obviously we get elements of $\mathfrak{P}_{0,\,\mathrm{q}}$.

For the converse we initially observe that $\mathrm{Int}(\mathbb{P}_\mathbb{Z}) \cdot m_\mathrm{q}(x) \subseteq \mathfrak{P}_{0,\,\mathrm{q}}$. This fact joined to the previous part does not ensure that $\mathfrak{P}_{0,\,\mathrm{q}}$ is a principal ideal in

$\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. Let us now take $f(x) \in \mathfrak{P}_{0,\mathrm{q}}$. By definition $f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. Suppose that dividing $f(x)$ by $m_{\mathrm{q}}(x)$ we obtain $f(x) = q(x)m_{\mathrm{q}}(x) + r(x)$, for some $q(x), r(x) \in \mathbb{P}_{\mathbb{Q}}[x]$. If $\mathrm{q} \in \mathbb{Z}$, then $m_{\mathrm{q}}(x)$ is a linear polynomial and $r(x) = \mathrm{p} \in \mathbb{P}_{\mathbb{Z}}$. Then evaluating $f(x)$ at q we get $\mathrm{p} = 0$ and $f(x) \in m_{\mathrm{q}}(x)\mathbb{P}_{\mathbb{Q}}[x]$. If $m_{\mathrm{q}}(x)$ is of degree two, suppose that $r(x) = \gamma x + \delta$, where $\gamma, \delta \in \mathbb{P}_{\mathbb{Q}}$. If $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$, one of b, c and d is nonzero. Let us consider the case $b \neq 0$; the other cases are similar. For all $\mathrm{p} \in \mathrm{C}(\mathrm{q})$ we have that $\gamma\mathrm{p} + \delta = 0$, and in particular $\alpha \overset{\mathrm{def}}{=} \gamma\overline{\mathrm{q}} + \delta = 0$ and $\beta \overset{\mathrm{def}}{=} \gamma(a + b\,\mathbf{i} - c\,\mathbf{j} - d\,\mathbf{k}) + \delta = 0$. It follows that $\beta - \alpha = 2b\gamma\,\mathbf{i} = 0$. Since $\mathbf{i}$ is invertible and $2b$ is a nonzero integer, we have $\gamma = 0$, and consequently $\delta = 0$. This ends our proof. **QED**

In Theorem 3.4.19 below, we show that the converse of Theorem 3.4.12 also holds; in other words, $\mathfrak{P}_{0,\mathrm{q}}$ is prime if and only if $m_{\mathrm{q}}(x)$ is irreducible.

Corollary 3.4.14. *Let* $\mathrm{q}_1,\ \mathrm{q}_2 \in \mathbb{P}_{\mathbb{Z}}$ *with the same minimal polynomial, call it* $m(x)$. *Then*

$$\mathfrak{P}_{0,\mathrm{q}_1} = \mathfrak{P}_{0,\mathrm{q}_2}.$$

Proof. By Proposition 3.4.13 we know that $\mathfrak{P}_{0,\mathrm{q}_1} = m(x) \cdot \mathbb{P}_{\mathbb{Q}}[x] \cap \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) = \mathfrak{P}_{0,\mathrm{q}_2}$. **QED**

In light of Proposition 3.4.13, we give the following definition.

Definition 3.4.15. Let $M(x) \in \mathbb{Z}[x]$. We define

$$\mathfrak{P}_{M(x)} \overset{\mathrm{def}}{=} M(x) \cdot \mathbb{P}_{\mathbb{Q}}[x] \cap \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}).$$

The following property of $\mathfrak{P}_{M(x)}$ is the same as in the commutative case (cf. [4]).

Theorem 3.4.16. *Let $M(x) \in \mathbb{Z}[x]$. Then the set*

$$\mathfrak{P}_{M(x)} = M(x) \cdot \mathbb{P}_{\mathbb{Q}}[x] \cap \operatorname{Int}(\mathbb{P}_{\mathbb{Z}})$$

is an ideal of $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})$. *Moreover, if $M(x)$ is an irreducible polynomial over $\mathbb{Q}$, then $\mathfrak{P}_{M(x)}$ is a prime ideal.*

Proof. Since $M(x)$ is a central polynomial, it is easy to see that $\mathfrak{P}_{M(x)}$ is an ideal of $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})$. To prove that it is prime, take $f(x)$ and $g(x)$ in $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})$ such that $f(x)\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})g(x) \subseteq \mathfrak{P}_{M(x)}$. We must have that $f(x) \in \mathfrak{P}_{M(x)}$ or $g(x) \in \mathfrak{P}_{M(x)}$. If $M(x) \mid g(x)$ we do not have anything to prove. Suppose that $M(x) \nmid g(x)$, we will show that necessarily, $M(x) \mid f(x)$. For convenience write $f(x) = f_0(x) + f_1(x)\,\mathbf{i} + f_2(x)\,\mathbf{j} + f_3(x)\,\mathbf{k}$. Since by assumption $f(x)\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})g(x) \subseteq \mathfrak{P}_{M(x)}$, then $M(x)$ divides the product $f(x)r(x)g(x)$, for all $r(x) \in \operatorname{Int}(\mathbb{P}_{\mathbb{Z}})$. In particular $M(x)$ divides the polynomials $f(x)g(x)$, $-\mathbf{i}f(x)\,\mathbf{i}g(x)$, $\mathbf{j}f(x)\,\mathbf{j}g(x)$, $\mathbf{k}f(x)\,\mathbf{k}g(x)$ in $\mathbb{P}_{\mathbb{Q}}[x]$. Thus $M(x)$ divides their sum $[f(x) - \mathbf{i}f(x)\,\mathbf{i} + \mathbf{j}f(x)\,\mathbf{j} + \mathbf{k}f(x)\,\mathbf{k}]\,g(x)$. After Lemma 1.6.5, we state that the polynomial contained in the square brakets is $4f_0(x)$ and that $M(x) \mid f_0(x)g(x)$. Now applying the Euclid's Lemma 3.1.11, we have that $M(x) \mid f_0(x)$. We obtain that $M(x) \mid f_1(x)$, working with the polynomial $f(x)\,\mathbf{i}$ replacing $f(x)$. In fact $(f(x)\,\mathbf{i})\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})g(x) \subseteq \mathfrak{P}_{M(x)}$ and the polynomial $f(x)\,\mathbf{i}$ has $f_1(x)$ as real part. In the same we obtain that $M(x) \mid f_2(x)$ and that $M(x) \mid f_3(x)$, working on $f(x)\,\mathbf{j}$ and $f(x)\,\mathbf{k}$ respectively. Finally $M(x) \mid f(x)$, as we wanted. **QED**

Proposition 3.4.17. *Let $M(x)$ and $N(x)$ be two nonassociate irreducible polynomials of* $\mathbb{Q}[x]$. *Then*

$$\mathfrak{P}_{M(x)} \cap \mathfrak{P}_{N(x)} = \mathfrak{P}_{M(x)N(x)}.$$

Proof. Let $f(x) \in \mathfrak{P}_{M(x)} \cap \mathfrak{P}_{N(x)}$. Then $f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$, $f(x) = M(x)g(x)$ and $f(x) = N(x)h(x)$, for some $g(x), h(x) \in \mathbb{P}_{\mathbb{Q}}[x]$. Since $M(x)$ is an irreducible polynomials, by Euclid's Lemma 3.1.11, $M(x) \mid h(x)$ in $\mathbb{P}_{\mathbb{Q}}[x]$. Then $f(x) \in \mathfrak{P}_{M(x)N(x)}$. The other inclusion is somewhat trivial. **QED**

Proposition 3.4.18. *Let $M(x)$ and $N(x)$ be two polynomials of $\mathbb{Q}[x]$ such that $M(x) \mid N(x)$. Then*

$$\mathfrak{P}_{N(x)} \subseteq \mathfrak{P}_{M(x)}.$$

Moreover we have the equality if and only if $M(x)$ and $N(x)$ are associates over $\mathbb{Q}$.

Proof. This statement is an immediate consequence of the divisibility properties. **QED**

We are ready for the first main result of this section.

Theorem 3.4.19. *Let $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$ and let $m_{\mathrm{q}}(x) \in \mathbb{Z}[x]$ be its minimal polynomial. Then $\mathfrak{P}_{0,\mathrm{q}}$ is a prime ideal of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ if and only if $m_{\mathrm{q}}(x)$ is an irreducible polynomial.*

Proof. If $\mathrm{q} \in \mathbb{Z}$ then we use Proposition 3.4.11. Moreover $m_{\mathrm{q}}(x)$ is a linear polynomial with integer coefficients. Otherwise, by Proposition 3.4.13, we have that $\mathfrak{P}_{0,\mathrm{q}} = \mathfrak{P}_{m_{\mathrm{q}}(x)}$. If $m_{\mathrm{q}}(x)$ is irreducible, the thesis follows applying Theorem 3.4.16. If not, we are in the case of Proposition 3.4.12. **QED**

Notice that the previous proposition has an analogue for quaternions (see [21, Proposition 6.2.5]). However, the proof is completely different. In fact Werner uses the fact that $\mathbb{H}_{\mathbb{Q}}$ is a skew field. Because of the existence of zero-divisors in $\mathbb{P}_{\mathbb{Q}}$, we could not use this argument.

Proposition 3.4.20. *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$ *such that* $m_{\mathrm{q}}(x) = (x - A)(x - B)$*, for some* $A \neq B \in \mathbb{Z}$*. Then*

$$\mathfrak{P}_{0,\,\mathrm{q}} = \mathfrak{P}_{0,\,A} \cap \mathfrak{P}_{0,\,B}.$$

Proof. By Proposition 3.4.13 we know that $\mathfrak{P}_{0,\,\mathrm{q}} = \mathfrak{P}_{m_{\mathrm{q}}(x)}$, $\mathfrak{P}_{0,\,A} = \mathfrak{P}_{x-A}$ and $\mathfrak{P}_{0,\,B} = \mathfrak{P}_{x-B}$. Thus the thesis is equivalent to $\mathfrak{P}_{m_{\mathrm{q}}(x)} = \mathfrak{P}_{x-A} \cap \mathfrak{P}_{x-B}$. This is true thanks to Proposition 3.4.17. **QED**

By Theorem 3.4.16, each $\mathfrak{P}_{M(x)}$, for an irreducible $M(x) \in \mathbb{Z}[x]$ is a prime ideal of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ above 0. In fact, every prime of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ above 0 has this form.

Proposition 3.4.21. *Let* $\mathfrak{P}$ *be a prime ideal of* $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ *above* 0*. Then,* $\mathfrak{P} = \mathfrak{P}_{M(x)}$ *for some irreducible* $M(x) \in \mathbb{Z}[x]$*.*

Proof. By Propositions 3.3.1 and 3.3.4, localizing $\mathfrak{P}$ at (0) yields a prime $\mathfrak{P}_0$ of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})_{(0)} = \mathrm{Int}(\mathbb{P}_{\mathbb{Q}}) = \mathbb{P}_{\mathbb{Q}}[x]$. Since $\mathbb{P}_{\mathbb{Q}} \simeq \mathcal{M}_2(\mathbb{Q})$, $\mathfrak{P}_0$ is isomorphic to a prime ideal of $\mathcal{M}_2(\mathbb{Q})[x] \simeq \mathcal{M}_2(\mathbb{Q}[x])$. The prime ideals of $\mathcal{M}_2(\mathbb{Q}[x])$, like $\mathbb{Q}[x]$, are generated by irreducible polynomials. Thus, $\mathfrak{P}_0 = M(x) \cdot \mathbb{P}_{\mathbb{Q}}[x]$ for some irreducible $M(x) \in \mathbb{Q}[x]$, and by clearing denominators we may assume that $M(x) \in \mathbb{Z}[x]$. Contracting $\mathfrak{P}_0$ back to $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$, we obtain $\mathfrak{P} = M(x) \cdot \mathbb{P}_{\mathbb{Q}}[x] \cap \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. **QED**

Combining our previous results, we obtain the following.

Theorem 3.4.22. *The prime ideals of* $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ *above* (0) *are precisely those of the form* $\mathfrak{P}_{M(x)}$ *with* $M(x) \in \mathbb{Z}[x]$ *irreducible.*

Proof. From Propositions 3.4.16 and 3.4.21. **QED**

3.4.2 Primes of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ above odd primes p

Throughout this section we suppose that p is an odd prime integer and we attempt to describe the primes of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ over $p\mathbb{P}_{\mathbb{Z}}$. In this case we do not get so complete results as for the uppers to (0); nevertheless we obtain several interesting theorems (see Theorems 3.4.40 and 3.4.33).

We will call the following technical results *reduction lemmas*.

Lemma 3.4.23 (First reduction Lemma)**.** *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$ *and* $A \in \mathbb{Z}$. *Then* $\mathfrak{P}_{p,\mathrm{q}} \subseteq \mathfrak{P}_{p,A}$ *if and only if* $\mathfrak{P}_{p,\mathrm{q}-a} \subseteq \mathfrak{P}_{p,A-a}$*, for all* $a \in \mathbb{Z}$.

Proof. Let be given the inclusion $\mathfrak{P}_{p,\mathrm{q}} \subseteq \mathfrak{P}_{p,A}$. Take a polynomial $f(x) \in \mathfrak{P}_{p,\mathrm{q}-a}$, we want to show that $f(x) \in \mathfrak{P}_{p,A-a}$. We remark that

$$\mathrm{C}(\mathrm{q}-a) = \mathrm{C}(\mathrm{q}) - a.$$

This means that for all $\mathrm{q}_1 \in \mathrm{C}(\mathrm{q}-a)$ there exists a $\mathrm{q}_2 \in \mathrm{C}(\mathrm{q})$ such that $\mathrm{q}_1 = \mathrm{q}_2 - a$, as an easy calculation can prove. Define the polynomial $g(x) \overset{\mathrm{def}}{=} f(x-a)$. Then for all $\mathrm{p} \in \mathrm{C}(\mathrm{q})$, $g(\mathrm{p}) = f(\mathrm{p}-a) \in p\mathbb{P}_{\mathbb{Z}}$. So $g(x) \in \mathfrak{P}_{p,\mathrm{q}} \subseteq \mathfrak{P}_{p,A}$. Finally, $f(A-a) = g(A) \in p\mathbb{P}_{\mathbb{Z}}$, as wanted. The reverse implication follows by taking $a = 0$. **QED**

It is true somewhat similar for multiplication.

Lemma 3.4.24 (Second reduction Lemma)**.** *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$ *and* $A \in \mathbb{Z}$. *If* $\mathfrak{P}_{p,\mathrm{q}} \subseteq \mathfrak{P}_{p,A}$ *then* $\mathfrak{P}_{p,n\mathrm{q}} \subseteq \mathfrak{P}_{p,nA}$*, for all* $n \in \mathbb{Z}$.

Proof. We are going to repeat previous proof, excepted some necessary small modifications. Let be given the inclusion $\mathfrak{P}_{p,\mathrm{q}} \subseteq \mathfrak{P}_{p,A}$. Take a polynomial $f(x) \in \mathfrak{P}_{p,n\mathrm{q}}$, we want to show that $f(x) \in \mathfrak{P}_{p,nA}$. We remark that

$$\mathrm{C}(n\mathrm{q}) = n\,\mathrm{C}(\mathrm{q}).$$

This means that for all $\mathrm{q}_1 \in \mathrm{C}(n\mathrm{q})$ there exists a $\mathrm{q}_2 \in \mathrm{C}(\mathrm{q})$ such that $\mathrm{q}_1 = n\mathrm{q}_2$, as an easy calculation can prove. Define the polynomial $g(x) \overset{\text{def}}{=} f(nx)$. Then for all $\mathrm{p} \in \mathrm{C}(\mathrm{q})$, $g(\mathrm{p}) = f(n\mathrm{p}) \in p\mathbb{P}_{\mathbb{Z}}$. So $g(x) \in \mathfrak{P}_{p,\mathrm{q}} \subseteq \mathfrak{P}_{p,A}$. Finally, $f(nA) = g(A) \in p\mathbb{P}_{\mathbb{Z}}$, as wanted. **QED**

Here follows a preliminary result about the ideals $\mathfrak{P}_{p,\mathrm{q}}$ for some particular $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$.

Proposition 3.4.25. *Let* $\mathrm{q} = b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$*,* $\mathrm{q} \neq 0$ *and* $\gcd(b, c, d) = 1$*. Suppose that* $(x - A) \mid m_{\mathrm{q}}(x)$*, for some* $A \in \mathbb{Z}$*. Then*

$$\mathfrak{P}_{p,\mathrm{q}} \subseteq \mathfrak{P}_{p,A}.$$

Proof. Let $f \in \mathfrak{P}_{p,\mathrm{q}}$. Suppose that dividing $f(x)$ by $m_{\mathrm{q}}(x)$ we obtain $f(x) = g(x)m_{\mathrm{q}}(x) + \gamma x + \delta$, for some $g(x)$ and $\gamma x + \delta$ in $\mathbb{P}_{\mathbb{Q}}[x]$. Our thesis is equivalent to $\gamma A + \delta \in p\mathbb{P}_{\mathbb{Z}}$. Since $-\mathrm{q} \in \mathrm{C}(\mathrm{q})$, then $-\gamma\mathrm{q} + \delta$ and $\gamma\mathrm{q} + \delta$ are both element of $p\mathbb{P}_{\mathbb{Z}}$. So $2\delta \in p\mathbb{P}_{\mathbb{Z}}$. In particular for all $r \in \mathbb{P}_{\mathbb{Z}}$ we have that $r2\delta = 2r\delta \in p\mathbb{P}_{\mathbb{Z}}$, that is to say $2\mathbb{P}_{\mathbb{Z}}\delta \subseteq p\mathbb{P}_{\mathbb{Z}}$. By the primality of $p\mathbb{P}_{\mathbb{Z}}$ we get $\delta \in p\mathbb{P}_{\mathbb{Z}}$. We also know that $\gamma(\pm b\,\mathbf{i} \pm c\,\mathbf{j} \pm d\,\mathbf{k}) + \delta \in p\mathbb{P}_{\mathbb{Z}}$ so taking wisely sign combinations we get that $2\gamma b$, $2\gamma c$, $2\gamma d \in p\mathbb{P}_{\mathbb{Z}}$. By our hypothesis we can write $\lambda b + \mu c + \nu d = 1$, for some $\lambda, \mu, \nu \in \mathbb{Z}$. So $2\gamma = \lambda 2\gamma b + \mu 2\gamma c + \nu 2\gamma d \in p\mathbb{P}_{\mathbb{Z}}$. As for δ we conclude that $\gamma \in p\mathbb{P}_{\mathbb{Z}}$. **QED**

Immediately we have:

Corollary 3.4.26. *Let* $\mathrm{q} = b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$*, with* $\mathrm{q} \neq 0$ *and* $\gcd(b, c, d) = 1$*. Let* $m_{\mathrm{q}}(x) = (x - A)(x - B)$*. Then*

$$\mathfrak{P}_{p,\mathrm{q}} \subseteq \mathfrak{P}_{p,A} \cap \mathfrak{P}_{p,B}.$$

Proof. It follows by Proposition 3.4.25. **QED**

We want now to apply Proposition 3.4.25 to all integer split quaternions. This is immediately done, if we notice that to every split quaternion we can associate to a primitive integer split quaternion with zero real part.

Definition 3.4.27. Let be given $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$. Call $g = \gcd(b, c, d)$. We define the *reduced* split quaternion associated to q, the split quaternion

$$\mathrm{q}^{red} = \frac{1}{g}(\mathrm{q} - a).$$

It is easy to see that given $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$, then q^{red} is a primitive integer split quaternion with zero real part. We say that q is *reduced* if $\mathrm{q}^{red} = \mathrm{q}$.

It is necessary to relate $m_{\mathrm{q}}(x)$ with $m_{\mathrm{q}^{red}}(x)$.

Proposition 3.4.28 (Third reduction Lemma)**.** *Let be given* $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$ *and let* q^{red} *be the reduced split quaternion associated to* q*. Let* $g = \gcd(b, c, d)$*.*

(i) $m_{\mathrm{q}}(x)$ *is the square of a linear polynomial if and only if* $m_{\mathrm{q}^{red}}(x)$ *is.*

(ii) $m_{\mathrm{q}}(x)$ *is reducible if and only if* $m_{\mathrm{q}^{red}}(x)$ *is.*

(iii) If $(x - A) \mid m_{\mathrm{q}}(x)$ *then* $(x - A') \mid m_{\mathrm{q}^{red}}(x)$*, where* $A = a + gA'$*.*

Proof. It is easy to calculate that the discriminant of $m_{\mathrm{q}}(x)$ is $\Delta = -4(b^2 - c^2 - d^2)$ and the discriminant of $m_{\mathrm{q}^{red}}(x)$ is $\Delta' = -\frac{4}{g^2}(b^2 - c^2 - d^2)$. Since $\Delta = g^2\Delta'$, (i), (ii) and (iii) follows immediately. **QED**

Thanks to the reduction lemmas, it is possible to extend Proposition 3.4.25 and Corollary 3.4.26 to the general case.

Proposition 3.4.29. *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}} \setminus \mathbb{Z}$*. Let* $(x - A) \mid m_{\mathrm{q}}(x)$*, for some* $A \in \mathbb{Z}$*. Then*

$$\mathfrak{P}_{p,\mathrm{q}} \subseteq \mathfrak{P}_{p,A}.$$

Proof. Let $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$, $g = \gcd(b, c, d)$ and let q^{red} be the reduced of q. Thanks to third reduction lemma , we know that $(x - A') \mid m_{\mathrm{q}^{red}}(x)$, where $A = a + gA'$. By Proposition 3.4.25, we have that $\mathfrak{P}_{p,\,\mathrm{q}^{red}} \subseteq \mathfrak{P}_{p,\,A'}$. By the second reduction lemma we have that $\mathfrak{P}_{p,\,g\mathrm{q}^{red}} \subseteq \mathfrak{P}_{p,\,gA'}$ and finally, by the first reduction lemma, $\mathfrak{P}_{p,\,a+g\mathrm{q}^{red}} \subseteq \mathfrak{P}_{p,\,a+gA'}$. The last inclusion is our thesis. **QED**

It immediately follows this fact.

Corollary 3.4.30. *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$. *Let* $m_{\mathrm{q}}(x) = (x - A)(x - B)$. *Then*

$$\mathfrak{P}_{p,\,\mathrm{q}} \subseteq \mathfrak{P}_{p,\,A} \cap \mathfrak{P}_{p,\,B}.$$

Proof. By Proposition 3.4.29. **QED**

We ask now when the containment stated in Corollary 3.4.30 is an equality.

Proposition 3.4.31. *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$. *Let* $m_{\mathrm{q}}(x) = (x - A)(x - B)$, *for some* $A, B \in \mathbb{Z}$ *such that* $A \not\equiv B \pmod{p}$. *Then*

$$\mathfrak{P}_{p,\,\mathrm{q}} \supseteq \mathfrak{P}_{p,\,A} \cap \mathfrak{P}_{p,\,B}.$$

Proof. Take $f(x) \in \mathfrak{P}_{p,\,A} \cap \mathfrak{P}_{p,\,B}$. Suppose that dividing $f(x)$ by $m_{\mathrm{q}}(x)$ we obtain $f(x) = m_{\mathrm{q}}(x)g(x) + \gamma x + \delta$, for some $g(x)$, $\gamma x + \delta \in \mathbb{P}_{\mathbb{Q}}[x]$. By hypothesis $A\gamma + \delta \in p\mathbb{P}_{\mathbb{Z}}$ and $B\gamma + \delta \in p\mathbb{P}_{\mathbb{Z}}$. Thus $A(B\gamma + \delta) - B(A\gamma + \delta) = (A - B)\delta \in p\mathbb{P}_{\mathbb{Z}}$. This implies that $(A - B)\mathbb{P}_{\mathbb{Z}}\delta \subseteq p\mathbb{P}_{\mathbb{Z}}$. By the primality of $p\mathbb{P}_{\mathbb{Z}}$, then $\delta \in p\mathbb{P}_{\mathbb{Z}}$. Similarly, $(A - B)\gamma \in p\mathbb{P}_{\mathbb{Z}}$ says that $\gamma \in p\mathbb{P}_{\mathbb{Z}}$. Finally, for each $\mathrm{p} \in \mathrm{C}(\mathrm{q})$, $f(\mathrm{p}) \in p\mathbb{P}_{\mathbb{Z}}$, as wanted. **QED**

Remark 3.4.32. In the previous proposition the hypothesis that $A \not\equiv B \pmod{p}$ is necessary. Take for instance a (odd) prime p, $p\mathbb{P}_\mathbb{Z}$ and $\mathrm{q} = \mathbf{i} + \mathbf{j} + p\mathbf{k}$. Then $m_\mathrm{q}(x) = (x-p)(x+p)$ and $\mathfrak{P}_{p,\mathrm{q}} \subseteq \mathfrak{P}_{p,p} \cap \mathfrak{P}_{p,-p}$. Consider now the integer-valued polynomial $f(x) = (x^2 - p^2) + x$. It is clear that $f(p) \in p\mathbb{P}_\mathbb{Z}$, $f(-p) \in p\mathbb{P}_\mathbb{Z}$ but $f(\mathrm{q}) = \mathrm{q} \notin p\mathbb{P}_\mathbb{Z}$.

Combining Proposition 3.4.30 and Proposition 3.4.31 we obtain the following fact.

Theorem 3.4.33. *Let* $\mathrm{q} \in \mathbb{P}_\mathbb{Z}$. *Let* $m_\mathrm{q}(x) = (x-A)(x-B)$. *Then*

$$\mathfrak{P}_{p,\mathrm{q}} \subseteq \mathfrak{P}_{p,A} \cap \mathfrak{P}_{p,B}.$$

Moreover, if $A \not\equiv B \pmod{p}$ *then*

$$\mathfrak{P}_{p,\mathrm{q}} = \mathfrak{P}_{p,A} \cap \mathfrak{P}_{p,B}.$$

Here follows the analogue of Proposition 3.4.12.

Proposition 3.4.34. *Let* $\mathrm{q} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{P}_\mathbb{Z}$ *such that* $\gcd(b,c,d)$ *is prime to* p. *If* $m_\mathrm{q}(x) \in \mathbb{Z}[x]$ *is reducible modulo* p*, then* $\mathfrak{P}_{p,\mathrm{q}}$ *is not a prime ideal of* $\mathrm{Int}(\mathbb{P}_\mathbb{Z})$.

Proof. We have that $\mathrm{q} \in \mathbb{P}_\mathbb{Z} \setminus \mathbb{Z}$. Assume that $m_\mathrm{q}(x)$ factors modulo p as $m_\mathrm{q}(x) = (x-A)(x-B) + pf(x)$, with $A, B \in \mathbb{Z}$ and $f(x) \in \mathbb{Z}[x]$. Then, $(x-A)\,\mathrm{Int}(\mathbb{P}_\mathbb{Z})(x-B) \subseteq \mathfrak{P}_{p,\mathrm{q}}$. For seeing this take a $g(x) \in \mathrm{Int}(\mathbb{P}_\mathbb{Z})$. Then, for any $\mathrm{p} \in \mathrm{C}(\mathrm{q})$, we have that $(\mathrm{p}-A)g(\mathrm{p})(\mathrm{p}-B) = (\mathrm{p}-A)(\mathrm{p}-B)g(\mathrm{p}) = m_\mathrm{q}(\mathrm{p})g(\mathrm{p}) - pg(\mathrm{p}) \in p\mathbb{P}_\mathbb{Z}$. But, since $\gcd(b,c,d)$ is prime to p, neither $x-A$ nor $x-B$ moves q into $p\mathbb{P}_\mathbb{Z}$. **QED**

Corollary 3.4.35. *Let* $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$ *such that* $\gcd(b,c,d)$ *is prime to* p*. Suppose that* $m_{\mathrm{q}}(x)$ *is reducible in* $\mathbb{Z}[x]$*. Then* $\mathfrak{P}_{p,\mathrm{q}}$ *is not a prime ideal of* $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$*.*

Proof. If $m_{\mathrm{q}}(x)$ factors in $\mathbb{Z}[x]$, then it factors modulo p. Thus apply Proposition 3.4.34. **QED**

We will prove at the end of this section that if $m_{\mathrm{q}}(x)$ is irreducible, then $\mathfrak{P}_{p,\mathrm{q}}$ is a maximal ideal in $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. For showing this we need some more results about localization at prime integers. Moreover we will introduce split quaternions with coefficients over quadratic extensions of $\mathbb{Q}$.

Lemma 3.4.36. *Let* $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$ *such that* $p \nmid \gcd(b,c,d)$*. Let* $f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ *and write* $f(x) = h(x)m_{\mathrm{q}}(x) + \gamma x + \delta$*, where* $h(x), \gamma x + \delta \in \mathbb{P}_{\mathbb{Q}}[x]$*. Then* $\gamma, \delta \in \mathbb{P}_{\mathbb{Z}_{(p)}}$*.*

Proof. Arguing as in Lemma 3.4.6, we get $2b\gamma$, $2c\gamma$, $2d\gamma \in \mathbb{P}_{\mathbb{Z}_{(p)}}$. Since 2 is invertible in $\mathbb{Z}_{(p)}$, we get $b\gamma$, $c\gamma$, $d\gamma \in \mathbb{P}_{\mathbb{Z}_{(p)}}$. Since $\gcd(b,c,d)$ is prime to p, then $\gamma \in \mathbb{P}_{\mathbb{Z}_{(p)}}$ and $\delta \in \mathbb{P}_{\mathbb{Z}_{(p)}}$. **QED**

Proposition 3.4.37. *Let* p *be an odd prime number and* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}} \setminus \mathbb{Z}$ *such that* $m_{\mathrm{q}}(x)$ *is irreducible modulo* p*. Let* α *be an algebraic integer which is a root of* $m_{\mathrm{q}}(x)$*. Then the rings* $\mathbb{P}_{\mathbb{Z}_{(p)}}[\alpha]$ *and* $\mathbb{P}_{\mathbb{Z}_{(p)}[\alpha]}$ *are isomorphic.*

Proof. Such an α can be found since $m_{\mathrm{q}}(x)$ is irreducible modulo p so it is irreducible over $\mathbb{Q}$. The isomorphism between the two rings can be proven as in Theorem 3.1.6. **QED**

Lemma 3.4.38. *Let* $f(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}_{(p)}})$*. Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}} \setminus \mathbb{Z}$ *and let* $m_{\mathrm{q}}(x)$ *be irreducible modulo* p*. Let* α *be an algebraic integer which is a root of* $m_{\mathrm{q}}(x)$*. Then* $f(\alpha) \in \mathbb{P}_{\mathbb{Z}_{(p)}[\alpha]}$*.*

Proof. With γ and δ as in Lemma 3.4.36, we obtain that $f(\alpha) = \gamma\alpha + \delta \in \mathbb{P}_{\mathbb{Z}_{(p)}[\alpha]}$. **QED**

Remark 3.4.39. Under the hypothesis we worked with until now, since $m_{\mathrm{q}}(x) \in \mathbb{Z}[x]$ is a quadratic polynomial irreducible modulo p, then $F \overset{\text{def}}{=} \frac{\mathbb{Z}}{p\mathbb{Z}}[\alpha] \simeq \mathbb{F}_{p^2}$, the finite field with p^2 elements. Then $\mathbb{P}_F \simeq \mathcal{M}_2(\mathbb{F}_{p^2})$, which is a simple ring.

We are now ready for our main result.

Theorem 3.4.40. *Let* $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$ *such that* $p \not| \gcd(b, c, d)$. *Then*

(i) $\mathfrak{P}_{p,\mathrm{q}}$ *is a prime ideal if and only if* $m_q(x)$ *is irreducible modulo p.*

(ii) If $\mathfrak{P}_{p,\mathrm{q}}$ *is prime, then it is a maximal ideal. Moreover* $\frac{\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})}{\mathfrak{P}_{p,\mathrm{q}}} \simeq \mathcal{M}_2(\mathbb{F}_{p^2})$.

Proof. Let $\mathcal{I}$ be the localization at p of the ideal $\mathfrak{P}_{p,\mathrm{q}}$. Suppose first that $m_{\mathrm{q}}(x)$ is irreducible modulo p. Let α be a root of $m_{\mathrm{q}}(x)$. Define the map $\sigma : \mathrm{Int}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right) \to \mathbb{P}_{\mathbb{Z}_{(p)}[\alpha]}$ by $\sigma(f(x)) = f(\alpha)$. This map is well-defined by Lemma 3.4.38 and it is a ring homomorphism since α is central over $\mathbb{P}_{\mathbb{Z}_{(p)}[\alpha]}$. It is surjective. A fraction $\frac{a}{b} \in \mathbb{Z}_{(p)}[\alpha]$ can be sent in an element of $\mathbb{F}_{p^2}$ in a natural way by taking the reduction modulo p of a and b^{-1}. This can be done since $p \not| b$. Thus it makes sense to consider the homomorphism $\pi : \mathbb{P}_{\mathbb{Z}_{(p)}[\alpha]} \to \mathbb{P}_{\mathbb{F}_{p^2}}$ given by the reduction modulo p. π also is surjective. Then the map $\tau \overset{\text{def}}{=} \pi \circ \sigma : \mathrm{Int}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right) \to \mathbb{P}_{\mathbb{F}_{p^2}}$ is a surjective ring homomorphism. Since $\mathbb{P}_{\mathbb{F}_{p^2}}$ is a simple ring, then $\ker(\tau)$ is a maximal ideal of $\mathrm{Int}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$. Take $f(x) \in \ker(\tau)$. Then $f(\alpha) = \gamma\alpha + \delta \in p\mathbb{P}_{\mathbb{Z}_{(p)}[\alpha]}$, where γ, δ are as in Lemma 3.4.36. This happens if and only if γ and δ are in $p\mathbb{P}_{\mathbb{Z}_{(p)}}$. Thus for each

$\mathrm{p} \in C(\mathrm{q})$, we have that $f(\mathrm{p}) = \gamma \mathrm{p} + \delta \in p\mathbb{P}_{\mathbb{Z}_{(p)}}$. This means that $f(x) \in \mathcal{I}$. Since $1 \notin \mathcal{I}$ and $\ker(\tau)$ is a maximal ideal, then $\ker(\tau) = \mathcal{I}$. By the first isomorphism theorem for τ, we get $\frac{\mathrm{Int}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)}{\mathcal{I}} \simeq \mathbb{P}_{\mathbb{F}_{p^2}}$. Moreover, by Theorem 3.3.4, $\frac{\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})}{\mathfrak{P}_{\mathscr{I},\mathrm{q}}} \simeq \frac{\mathrm{Int}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)}{\mathcal{I}} \simeq \mathbb{P}_{\mathbb{F}_{p^2}}$. This implies that $\mathfrak{P}_{\mathscr{I},\mathrm{q}}$ is a maximal (and prime) ideal and proves (ii). If $m_{\mathrm{q}}(x)$ is reducible, we are in the hypothesis of Proposition 3.4.35; then $\mathfrak{P}_{\mathscr{I},\mathrm{q}}$ is not a prime ideal. **QED**

3.4.3 Some ideals of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ above $\mathscr{M} = (1 + \mathbf{i}, 1 + \mathbf{j})$

The final case we will consider regards prime ideals of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ above $\mathscr{M} = (1 + \mathbf{i}, 1 + \mathbf{j})$. In this instance, our analysis is quite different, since $\mathscr{M}$ is not generated by integers. In contrast to what we found with $\mathfrak{P}_{p,\mathrm{q}}$, the ideals of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ that we will discuss are similar to the prime ideals of $\mathrm{Int}(D)$, where D is a commutative domain. This appears to be because the residue ring $\frac{\mathbb{P}_{\mathbb{Z}}}{\mathscr{M}} \simeq \mathbb{F}_2$ is commutative.

Definition 3.4.41. For each $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$, we define

$$\mathfrak{M}_{\mathrm{q}} = \{f \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) \mid f(\mathrm{q}) \in \mathscr{M}\}.$$

Interestingly, the difficulty in working with $\mathfrak{M}_{\mathrm{q}}$ is not in showing that the set forms a maximal or prime ideal, but in showing that it forms an ideal at all.

We begin by stating a sufficient condition for this to occur.

Proposition 3.4.42. *Let* $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$. *Assume that* $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})\mathrm{p} \in \mathfrak{M}_{\mathrm{q}}$ *for all* $\mathrm{p} \in \mathscr{M}$. *Define* $\phi : \mathrm{Int}(\mathbb{P}_{\mathbb{Z}}) \to \frac{\mathbb{P}_{\mathbb{Z}}}{\mathscr{M}}$ *by* $\phi(f) = f(\mathrm{q})$ *modulo* $\mathscr{M}$. *Then,* ϕ *is a surjective homomorphism with kernel* $\mathfrak{M}_{\mathrm{q}}$, *and* $\frac{Int(\mathbb{P}_{\mathbb{Z}})}{\mathfrak{M}_{\mathrm{q}}} \simeq \mathbb{F}_2$. *Consequently,* $\mathfrak{M}_{\mathrm{q}}$ *is a maximal ideal of* $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$.

Proof. It is straightforward to prove that ϕ is additive, surjective, and has kernel $\mathfrak{M}_{\mathrm{q}}$. For multiplicativity, let $f, g \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. It suffices to show that $(fg)(\mathrm{q})$ is equivalent mod $\mathscr{M}$ to $f(\mathrm{q})g(\mathrm{q})$.

Let $\mathrm{p} = g(\mathrm{q}) \in \mathbb{P}_{\mathbb{Z}}$. Then $(fg)(\mathrm{q}) = (f\mathrm{p})(\mathrm{q})$. If $\mathrm{p} \in \mathscr{M}$, then we are done by assumption. If not, let $\mathrm{r} = 1 + \mathrm{p} \in \mathscr{M}$. Then, $(f\mathrm{r})(\mathrm{q}) = f(\mathrm{q}) + (f\mathrm{p})(\mathrm{q})$, and we see that $(f\mathrm{p})(\mathrm{q}) \in \mathscr{M}$ if and only if $f(\mathrm{q}) \in \mathscr{M}$. In this case, $\phi(g) = 1$ and we have $\phi(fg) = \phi(f)$, so we are done in this case as well. **QED**

Thus, to prove that $\mathfrak{M}_{\mathrm{q}}$ is a maximal ideal of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$, it suffices to prove that $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})\mathrm{p} \in \mathfrak{M}_{\mathrm{q}}$ for each $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$ and $\mathrm{p} \in \mathscr{M}$. We do not have proofs that work for arbitrary $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$, but we can establish the result in certain cases, depending on the coefficients of q.

We fix some notation concerning generators of $\mathscr{M}$. Throughout the rest of this section, let $\varepsilon = 1 + \mathbf{i}$, $\lambda_1 = 1 + \mathbf{j}$, $\lambda_2 = 1 + \mathbf{k}$, $\lambda_3 = 2 + \mathbf{i} + \mathbf{j}$, and $\lambda_4 = 2 + \mathbf{i} + \mathbf{k}$. Observe then that $\mathscr{M} = (\varepsilon, \lambda_1) = (\varepsilon, \lambda_2) = (\varepsilon, \lambda_3) = (\varepsilon, \lambda_4)$. Furthermore, we have the following generalization of Lemma 1.6.18. The proof is identical to that of Lemma 1.6.18.

Proposition 3.4.43. *Let* $\mathrm{q} \in \mathscr{M}$. *Then, for each* $1 \le i \le 4$ *there exist* $\mathrm{p}, \mathrm{r} \in \mathbb{P}_{\mathbb{Z}}$ *such that* $\mathrm{q} = \mathrm{p}\varepsilon + \mathrm{r}\lambda_i$.

Since $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ is closed under multiplication on the right by elements of $\mathbb{P}_{\mathbb{Z}}$, to meet the condition needed in Theorem 3.4.42 it suffices to show that $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})\varepsilon$ and some $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})\lambda_i$ are in $\mathfrak{M}_{\mathrm{q}}$. As we shall see, this is not difficult to prove for ε because $\mathbb{P}_{\mathbb{Z}}$ is closed under conjugation by ε. However, $N(\lambda_1) = N(\lambda_2) = 0$, so we do not have a corresponding result for λ_1 or λ_2. Nevertheless, we can obtain partial results by working instead with λ_3 and λ_4.

Proposition 3.4.44. *Let* $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$*. Then,*

(i) $\varepsilon \mathrm{q} \varepsilon^{-1} \in \mathbb{P}_{\mathbb{Z}}$

(ii) if $b \equiv c$ (mod. 2)*, then* $\lambda_3 \mathrm{q} \lambda_3^{-1} \in \mathbb{P}_{\mathbb{Z}}$

(iii) if $b \equiv d$ (mod. 2)*, then* $\lambda_4 \mathrm{q} \lambda_4^{-1} \in \mathbb{P}_{\mathbb{Z}}$

Proof. Direct computation shows that

$$\begin{aligned} \varepsilon \mathrm{q} \varepsilon^{-1} &= a + b\,\mathbf{i} - d\,\mathbf{j} + c\,\mathbf{k} \\ \lambda_3 \mathrm{q} \lambda_3^{-1} &= a + \left(-d + \tfrac{3b-c}{2}\right)\mathbf{i} + \left(-d + \tfrac{b+c}{2}\right)\mathbf{j} + \left(-b + c + d\right)\mathbf{k} \\ \lambda_4 \mathrm{q} \lambda_4^{-1} &= a + \left(c + \tfrac{3b-d}{2}\right)\mathbf{i} + \left(b + c - d\right)\mathbf{j} + \left(c + \tfrac{b+d}{2}\right)\mathbf{k} \end{aligned}$$

(If verifying these by hand, it is easiest to first prove them for $\mathrm{q} \in \{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ and then extend linearly over a, b, c, d to establish the general result). **QED**

Proposition 3.4.45. *Let* $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$ *and* $h(x) \in \mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$*. Then,*

(i) $h\varepsilon \in \mathfrak{M}_{\mathrm{q}}$

(ii) if $b \equiv c$ (mod. 2)*, then* $h\lambda_3 \in \mathfrak{M}_{\mathrm{q}}$

(iii) if $b \equiv d$ (mod. 2)*, then* $h\lambda_4 \in \mathfrak{M}_{\mathrm{q}}$

Proof. By Lemma 3.4.44, $\varepsilon \mathrm{q} \varepsilon^{-1} \in \mathbb{P}_{\mathbb{Z}}$, so $(h\varepsilon)(\mathrm{q}) = h(\varepsilon \mathrm{q} \varepsilon^{-1})\varepsilon \in \mathscr{M}$. If $b \equiv c$ (mod. 2), then $\lambda_3 \mathrm{q} \lambda_3^{-1} \in \mathbb{P}_{\mathbb{Z}}$, so $(h\lambda_3)(\mathrm{q}) = h(\lambda_3 \mathrm{q} \lambda_3^{-1})\lambda_3 \in \mathscr{M}$. Similarly, if $b \equiv d$ (mod. 2), then $(h\lambda_4)(\mathrm{q}) \in \mathscr{M}$. **QED**

Applying Propositions 3.4.45 and Theorem 3.4.42 we obtain the following.

Proposition 3.4.46. *Let* $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$*, and assume that either* $b \equiv c$ (mod. 2) *or* $b \equiv d$ (mod. 2)*. Then,* $\mathfrak{M}_{\mathrm{q}}$ *is a maximal ideal of* $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$*.*

It remains to consider the case where $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$ and $b \not\equiv c$, $b \not\equiv d \bmod 2$. This case is more difficult because we were not able to find an appropriate conjugation relation like those in Lemma 3.4.44. In fact, we suspect that such a conjugation relation may not exist. Nevertheless, we feel that $\mathfrak{M}_{\mathrm{q}}$ will once again be a maximal ideal of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$; it is just that the methods used in this paper are not sufficient to prove it.

Chapter 4

Localization properties of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$

4.1 Localization of integer-valued polynomials

In this chapter we will analyze some localization properties of the ring $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. When D is a commutative noetherian domain, $\mathrm{Int}(D)$ behaves well with respect to the localization at a multiplicative subset of D. In fact, taken a multiplicatively closed subset S of D, containing 1 but not 0, then $S^{-1}\,\mathrm{Int}(D) = \mathrm{Int}(S^{-1}D)$, see [4, Theorem I.2.3].

In his Ph.D. thesis, Werner shows that somewhat similar is true for quaternion rings. His result states:

Theorem 4.1.1. [22, theorem 3.3.2] *Let R be an overring of $\mathbb{H}_{\mathbb{Z}}$ in $\mathbb{H}_{\mathbb{Q}}$ and let S be a multiplicative subset of $\mathbb{Z}$. Then $S^{-1}\,\mathrm{Int}(R) = \mathrm{Int}(S^{-1}R)$.*

We will see that also for split quaternions the localization at a multiplicative subset commutes with the formation of integer-valued polynomials. In what follows we prove a statement true not only for $\mathbb{H}_R$ and $\mathbb{P}_R$, but more in general that is true for any right noetherian ring R and a right denominator set $S \subseteq R$.

Theorem 4.1.2. *Let R be a right noetherian ring that admits total ring of fractions $\mathcal{Q}(R)$. Let S be a right denominator set of R without zero-divisors. Suppose that*

$$\operatorname{Int}(R) = \{\, f(x) \in \mathcal{Q}(R)[x] \mid f(R) \subseteq R \,\},$$

$$\operatorname{Int}(RS^{-1}) = \left\{\, f(x) \in \mathcal{Q}(R)[x] \;\middle|\; f(RS^{-1}) \subseteq RS^{-1} \,\right\}$$

and $\operatorname{Int}(R)S^{-1}$ *are rings. Then*

$$\operatorname{Int}(R)S^{-1} = \operatorname{Int}(RS^{-1}).$$

Proof. Since we are working with noncommutative rings, it is not obvious that $\operatorname{Int}(R)$, $\operatorname{Int}(RS^{-1})$ and $\operatorname{Int}(R)S^{-1}$ are rings. For this reason we assume this property as hypothesis. We first show that $\operatorname{Int}(R)S^{-1} \subseteq \operatorname{Int}(RS^{-1})$. Let $f(x) \in \operatorname{Int}(R)S^{-1}$ and let $\mathrm{p} \in RS^{-1}$. Then there exist $F(x) \in \operatorname{Int}(R)$ and $s \in S$ such that $f(x) = F(x)s^{-1}$. Furthermore, there exist $\mathrm{q} \in R$ and $s \in S$ such that $\mathrm{p} = \mathrm{q}s^{-1}$. We want to show that $f(\mathrm{p}) \in RS^{-1}$. We proceed by induction on the degree n of $f(x)$. If $n = 0$, $f(x)$ is constant and there is nothing to prove. Assume now that $n > 0$ and that all polynomials in $\operatorname{Int}(R)S^{-1}$ of degree less than n are elements of $\operatorname{Int}(RS^{-1})$. Define the polynomial

$$g(x) \overset{\text{def}}{=} f(x)s^n - f(xs).$$

Since $s \in S$, $f(xs)$ is a polynomial of $\operatorname{Int}(R)S^{-1}$, so $g(x) \in \operatorname{Int}(R)s^{-1}$. Moreover $\deg(g(x)) < \deg(f(x))$, thus, by induction, $g(x) \in \operatorname{Int}(RS^{-1})$. Now, $f(x)s^n = g(x) + f(xs)$, so $f(\mathrm{p})s^n = g(\mathrm{p}) + f(\mathrm{q}) = g(\mathrm{p}) + F(\mathrm{q})s^{-1} \in RS^{-1}$. Now, being s invertible in the ring RS^{-1}, we conclude that $f(\mathrm{p}) \in RS^{-1}$.

For the reverse inclusion, let $f(x) = \sum_{r=0}^{n} \mathrm{q}_r x^r \in \mathrm{Int}(RS^{-1})$. Let

$$M = \mathrm{q}_0\, R + \mathrm{q}_1\, R + \cdots + \mathrm{q}_n\, R$$

be the right R-module generated by the coefficients of $f(x)$. Since R is noetherian as a right R-module over itself and M is finitely generated, M is noetherian as a right R-module (see [14, Proposition 1.21]). Let now N be the right R-module generated by the set $\{\, f(\mathrm{q}) \mid \mathrm{q} \in R \,\}$. Then $N \subseteq M$ and M is noetherian, so N is finitely generated as a right R-module (see [14, Proposition 1.20]). Let $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_m$ be its generators. Since by hypothesis, $f(x) \in \mathrm{Int}(RS^{-1})$, then $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_m \in RS^{-1}$. As we told in general in Section 2.1.2, since S is a denominator set, we can find a common denominator for the p_l's. So there exists an $s \in S$ such that $\mathrm{p}_l s \in R$, for all $1 \leqslant l \leqslant m$. In this way we get that $\mathrm{p}s \in R$, for all $\mathrm{p} \in N$ and in particular $f(\mathrm{p})s \in R$, for all $\mathrm{p} \in R$. Then the polynomial $f(x)s$ belongs to $\mathrm{Int}(R)$, that is to say $f(x) \in \mathrm{Int}(R)S^{-1}$. This ends our proof. **QED**

We are not able to prove the left analogous of Theorem 4.1.2. In fact it is not possible to adapt the entire proof given above. We can just prove only the first part, thus obtaining the following weaker result.

Proposition 4.1.3. *Let R be a left noetherian ring that admits total ring of fractions $\mathcal{Q}(R)$. Let S be a left denominator set of R without zero-divisors. Suppose that*

$$\mathrm{Int}(R) = \{\, f(x) \in \mathcal{Q}(R)[x] \mid f(R) \subseteq R \,\},$$

$$\mathrm{Int}(S^{-1}R) = \left\{\, f(x) \in \mathcal{Q}(R)[x] \;\middle|\; f(S^{-1}R) \subseteq S^{-1}R \,\right\}$$

and $S^{-1}\,\mathrm{Int}(R)$ are rings. Then

$$S^{-1}\,\mathrm{Int}(R) \subseteq \mathrm{Int}(S^{-1}R).$$

Proof. We must adapt the proof of Theorem 4.1.2. Let $f(x) \in S^{-1}\operatorname{Int}(R)$ and let $\mathrm{p} \in S^{-1}R$. Then there exist $F(x) \in \operatorname{Int}(R)$ and $s \in S$ such that $f(x) = s^{-1}F(x)$. Furthermore, there exist $\mathrm{q} \in R$ and $s \in S$ such that $\mathrm{p} = s^{-1}\mathrm{q}$. We want to show that $f(\mathrm{p}) \in S^{-1}R$. We proceed by induction on the degree n of $f(x)$. If $n = 0$, $f(x)$ is constant and there is nothing to prove. Assume now that $n > 0$ and that all polynomials in $S^{-1}\operatorname{Int}(R)$ of degree less than n are elements of $\operatorname{Int}(S^{-1}R)$. Define the polynomial

$$g(x) \overset{\text{def}}{=} s^n f(x) - f(sx).$$

Since $s \in S$, $f(sx)$ is a polynomial of $S^{-1}\operatorname{Int}(R)$, so $g(x) \in s^{-1}\operatorname{Int}(R)$. Moreover $\deg(g(x)) < \deg(f(x))$, thus, by induction, $g(x) \in \operatorname{Int}(S^{-1}R)$. Now, $s^n f(x) = g(x) + f(sx)$, so $s^n f(\mathrm{p}) = g(\mathrm{p}) + f(\mathrm{q}) = g(\mathrm{p}) + s^{-1}F(\mathrm{q}) \in S^{-1}R$. Now, being s invertible in the ring $S^{-1}R$, we conclude that $f(\mathrm{p}) \in S^{-1}R$. **QED**

We cannot adapt the proof of Theorem 4.1.2 for proving the reverse inclusion $S^{-1}\operatorname{Int}(R) \subseteq \operatorname{Int}(S^{-1}R)$, since we fixed the right notation $R[x]$ for writing the polynomials (*i.e.* the indeterminate x is written on the right of the coefficients). This will not be an obstacle for our investigations, since we will focuse on central denominator sets.

If the denominator set is central we obviously obtain the following result.

Proposition 4.1.4. *Let R be a noetherian ring. Suppose that R admits total ring of fractions $\mathcal{Q}(R)$ and suppose that*

$$\operatorname{Int}(R) = \{\, f(x) \in \mathcal{Q}(R)[x] \mid f(R) \subseteq R \,\}$$

is a ring. Let S be a central multiplicative subset of R that does not contain zero-divisors and such that $\operatorname{Int}(RS^{-1})$ *is a ring. Then we have the following* *ring equalities:*

$$S^{-1}\operatorname{Int}(R) = \operatorname{Int}(S^{-1}R) = \operatorname{Int}(RS^{-1}) = \operatorname{Int}(R)S^{-1}.$$

We immediately apply Theorems 4.1.2, 4.1.3 and 4.1.4 to $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})$. We saw in Chapter 2 that $\mathbb{Z}^*$ and $\mathbb{Z} \smallsetminus p\mathbb{Z}$, for a prime integer p, are central denominator sets of $\mathbb{P}_{\mathbb{Z}}$. Moreover, the set of non zero-divisors $\mathcal{R}(\mathbb{P}_{\mathbb{Z}})$ and $\mathscr{C}(Q)$, for a maximal ideal Q of $\mathbb{P}_{\mathbb{Z}}$, are denominator sets of $\mathbb{P}_{\mathbb{Z}}$. Then we saw that

$$\mathcal{Q}(\mathbb{P}_{\mathbb{Z}}) = \mathbb{P}_{\mathbb{Z}}\mathcal{R}(\mathbb{P}_{\mathbb{Z}})^{-1} = \mathbb{P}_{\mathbb{Z}}(\mathbb{Z}^*)^{-1} = \mathbb{P}_{\mathbb{Q}},$$

if p is an odd prime integer

$$\mathbb{P}_{\mathbb{Z}}\,(\mathbb{Z} \smallsetminus p\mathbb{Z})^{-1} = \mathbb{P}_{\mathbb{Z}}\,\mathscr{C}(p\mathbb{P}_{\mathbb{Z}})^{-1} = \mathbb{P}_{\mathbb{Z}_{(p)}}$$

and, for $p = 2$ we have

$$\mathbb{P}_{\mathbb{Z}}\,(\mathbb{Z} \smallsetminus 2\mathbb{Z})^{-1} = \mathbb{P}_{\mathbb{Z}}\,\mathscr{C}(\mathscr{M})^{-1} = \mathbb{P}_{\mathbb{Z}_{(2)}},$$

where $\mathscr{M} = (1 + \mathbf{i}, 1 + \mathbf{j})$, the maximal ideal of $\mathbb{P}_{\mathbb{Z}}$ over 2.

It is easy to prove the following statement.

Proposition 4.1.5. *With the above notation and definitions, let S be one of the denominator sets of $\mathbb{P}_{\mathbb{Z}}$ listed previously.*

(i) If $S = \mathcal{R}(\mathbb{P}_{\mathbb{Z}})$ or $S = \mathbb{Z}^*$, then

$$\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1} = \mathbb{P}_{\mathbb{Q}}[x].$$

(ii) If p is an odd prime integer and $S = \mathbb{Z} \smallsetminus p\mathbb{Z}$ or $S = \mathscr{C}(p\mathbb{P}_{\mathbb{Z}})$, then

$$\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1} = \operatorname{Int}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right).$$

(iii) If $S = \mathbb{Z} \smallsetminus 2\mathbb{Z}$ or $S = \mathscr{C}(\mathscr{M})$, then

$$\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1} = \operatorname{Int}\left(\mathbb{P}_{\mathbb{Z}_{(2)}}\right).$$

Proof. It is an immediate consequence of Theorem 4.1.2. **QED**

If the denominator set is central, we can also build the left localization with respect to S. We obtain the following fact as a corollary of Theorem 4.1.4. We proved it directly in Section 3.3.

Proposition 4.1.6. *Fix the above notation and definitions.*

(i) If $S = \mathbb{Z}^*$, then

$$S^{-1}\operatorname{Int}(\mathbb{P}_{\mathbb{Z}}) = \operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1} = \mathbb{P}_{\mathbb{Q}}[x].$$

(ii) If p is a prime integer and $S = \mathbb{Z} \smallsetminus p\mathbb{Z}$, then

$$S^{-1}\operatorname{Int}(\mathbb{P}_{\mathbb{Z}}) = \operatorname{Int}(\mathbb{P}_{\mathbb{Z}})S^{-1} = \operatorname{Int}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right).$$

Proof. A direct proof is in Proposition 3.3.1. It follows also by Proposition 4.1.4. **QED**

Let us now analyze some properties of these localization rings.

First of all we prove the following

Proposition 4.1.7. *With the above hypothesis and notation, we have that*

$$\bigcap_{\substack{p \text{ prime} \\ \text{integer}}} \mathbb{P}_{\mathbb{Z}_{(p)}} = \mathbb{P}_{\mathbb{Z}}.$$

Proof. The inclusion '$\supseteq$' is obvious since for every prime p, $\mathbb{P}_{\mathbb{Z}} \subseteq \mathbb{P}_{\mathbb{Z}_{(p)}}$. For the reverse inclusion, take an element $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}$ of the intersection. Then a, b, c, $d \in \bigcap_p \mathbb{Z}_{(p)} = \mathbb{Z}$ and so $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}}$. **QED**

Here we prove the analogous for integer-valued polynomials ring.

Proposition 4.1.8. *With the above hypothesis and notation, we have that*

$$\operatorname{Int}(\mathbb{P}_{\mathbb{Z}}) = \bigcap_{\substack{p \text{ prime} \\ \text{integer}}} \operatorname{Int}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right).$$

Proof. For all primes p, let Q_p be the maximal ideal of $\mathbb{P}_{\mathbb{Z}}$ above p. We have that $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}}) \subseteq (\operatorname{Int}(\mathbb{P}_{\mathbb{Z}}))\mathscr{C}(Q_p)^{-1} = \operatorname{Int}(\mathbb{P}_{\mathbb{Z}_{(p)}})$. **QED**

The matrix representation (1.5) we introduced in Section 1.3.1 will help us in studying the spectrum of $\operatorname{Int}(\mathbb{P}_{\mathbb{Z}})$, passing through a result proved by S. Frisch about integer-valued polynomials over matrix rings in [9]. We introduce the following:

Notation 4.1.9. Let D be a commutative domain and let K be its field of fractions. Then

$$\operatorname{Int}_D(\mathcal{M}_n(D)) \overset{\text{def}}{=} \{\, f(x) \in K[x] \mid \forall A \in \mathcal{M}_n(D) : f(A) \in \mathcal{M}_n(D) \,\}$$

and

$$\operatorname{Int}_D[\mathcal{M}_n(D)] \overset{\text{def}}{=} \{\, f(x) \in \mathcal{M}_n(K)[x] \mid \forall A \in \mathcal{M}_n(D) : f(A) \in \mathcal{M}_n(D) \,\}.$$

Proposition 4.1.10. [9, Theorems 7.2-3] *Let D be a commutative domain and let K be its field of fractions. Then*

$$\operatorname{Int}_D[\mathcal{M}_n(D)] = \mathcal{M}_n(\operatorname{Int}_D(\mathcal{M}_n(D))).$$

Moreover:

(i) The ideals of $\operatorname{Int}_D[\mathcal{M}_n(D)]$ *are in* $1-1$ *correspondence with the sets of the form* $\mathcal{M}_n(\mathscr{I})$*, where* $\mathscr{I}$ *is an ideal of* $\operatorname{Int}_D(\mathcal{M}_n(D))$*.*

(ii) *The prime ideals of* $\mathrm{Int}_D[\mathcal{M}_n(D)]$ *are in* $1-1$ *correspondence with the sets of the form* $\mathcal{M}_n(\mathscr{P})$*, where* $\mathscr{P}$ *is a prime ideal of* $\mathrm{Int}_D(\mathcal{M}_n(D))$.

(iii) *The maximal ideals of* $\mathrm{Int}_D[\mathcal{M}_n(D)]$ *are in* $1–1$ *correspondence with the sets of the form* $\mathcal{M}_n(\mathscr{M})$*, where* $\mathscr{M}$ *is a maximal ideal of* $\mathrm{Int}_D(\mathcal{M}_n(D))$.

Proof. See [9, theorem 7.2] and [9, theorem 7.3]. The remaining part follows from Proposition K. **QED**

We need another little of notation. In order to not make confusion in using the previous result, we will use the following

Notation 4.1.11. We will indicate

$$\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right) \overset{\text{def}}{=} \left\{ f(x) \in \mathbb{Q}[x] \;\middle|\; f(\mathbb{P}_{\mathbb{Z}_{(p)}}) \subseteq \mathbb{P}_{\mathbb{Z}_{(p)}} \right\}$$

and

$$\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}(\mathbb{P}_{\mathbb{Z}_{(p)}}) \overset{\text{def}}{=} \left\{ f(x) \in \mathbb{P}_{\mathbb{Q}}[x] \;\middle|\; f(\mathbb{P}_{\mathbb{Z}_{(p)}}) \in \mathbb{P}_{\mathbb{Z}_{(p)}} \right\}.$$

The first one of these two sets is a ring: since it is a subset of $\mathbb{Q}[x]$ this can be seen using the polynomial evaluation. For the second one we can use Theorem 3.1.3. In particular $\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$ is what we called $\mathrm{Int}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$ above, since $\mathcal{Q}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right) = \mathbb{P}_{\mathbb{Q}}$. To avoid confusion we explicit the set of coefficients using the subscript.

We can state the following:

Theorem 4.1.12. *Let* p *be an odd prime integer. Then*

$$\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}(\mathbb{P}_{\mathbb{Z}_{(p)}}) \simeq \mathcal{M}_2\left(\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)\right). \tag{4.1}$$

Proof. We recall by (1.5) that $\mathbb{P}_{\mathbb{Z}_{(p)}} \simeq \mathcal{M}_2(\mathbb{Z}_{(p)})$, for every odd prime integer p, since 2 is invertible in $\mathbb{Z}_{(p)}$. We conclude by Proposition 4.1.10. **QED**

Combining Theorem 4.1.12 and Proposition 4.1.10 we get the following corollary.

Corollary 4.1.13. *With the above hypothesis and notation, fixed an odd prime integer p, there is a one-to-one order preserving correspondence between prime ideals of* $\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}(\mathbb{P}_{\mathbb{Z}})$ *above $p\mathbb{Z}$ and prime ideals of* $\mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ *above $p\mathbb{Z}$.*

By the previous corollary, the investigation of prime ideals of $\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}(\mathbb{P}_{\mathbb{Z}})$ containing an odd prime integer p is equivalent to the analogue investigation in the ring $\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$, which is a commutative subring of $\mathbb{Q}[x]$.

4.2 The ideal $p\,\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$

Let p be a prime integer. We aim to prove that the ideal $p\,\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$ is not a prime ideal of $\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$. We start with an important isomorphisms.

Proposition 4.2.1. *Let p be a prime integer. Let us consider the application* $\varphi : \mathbb{P}_{\mathbb{Z}_{(p)}} \to \mathbb{P}_{\mathbb{Z}_p}$ *such that for all* $\mathrm{q} = \frac{a}{a'} + \frac{b}{b'}\mathbf{i} + \frac{c}{c'}\mathbf{j} + \frac{d}{d'}\mathbf{k} \in \mathbb{P}_{\mathbb{Z}_{(p)}}$, *we have*

$$\varphi(\mathrm{q}) = \frac{\overline{a}}{\overline{a'}} + \frac{\overline{b}}{\overline{b'}}\mathbf{i} + \frac{\overline{c}}{\overline{c'}}\mathbf{j} + \frac{\overline{d}}{\overline{d'}}\mathbf{k},$$

where the overline means we are taking the residue modulo p. Then φ is a surjective ring homomorphism.

Proof. Given any $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}_{(p)}}$, then the denominators of its coefficients are not zero modulo p: it makes sense to consider the application φ. Since $\frac{\mathbb{Z}_{(p)}}{p\mathbb{Z}_{(p)}} \simeq \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)_{(p)} \simeq \mathbb{Z}_p$, it is easy to see that φ preserves addition and multiplication. Obviously φ is surjective. **QED**

Proposition 4.2.2. *Let p be a prime integer. Then*

$$\frac{\mathbb{P}_{\mathbb{Z}_{(p)}}}{p\mathbb{P}_{\mathbb{Z}_{(p)}}} \simeq \mathbb{P}_{\mathbb{Z}_p}.$$

Proof. Consider the ring homomorphism φ of Proposition 4.2.1. Take now a split quaternion $\mathrm{q} = \frac{a}{a'} + \frac{b}{b'}\mathbf{i} + \frac{c}{c'}\mathbf{j} + \frac{d}{d'} \in \ker\varphi$. Then $\frac{\overline{a}}{\overline{a'}} = \frac{\overline{b}}{\overline{b'}} = \frac{\overline{c}}{\overline{c'}} = \frac{\overline{d}}{\overline{d'}} = \overline{0}$ in $\mathbb{Z}_p$. This means that $p \mid a, b, c, d$ and therefore $\ker\varphi \subseteq p\mathbb{P}_{\mathbb{Z}_{(p)}}$. The other inclusion is straightforward. The thesis follows by the first isomorphism theorem. **QED**

Here follows a technical result about φ and the polynomial evaluation.

Lemma 4.2.3. *Let p be a prime integer. Let $f(x) = \sum_{t=0}^{n} \mathrm{p}_t\, x^t \in \mathbb{Z}_{(p)}[x]$ and call $\overline{f}(x) = \sum_{t=0}^{n} \varphi(\mathrm{p}_t)\, x^t \in \mathbb{Z}_p[x]$. Let $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}_{(p)}}$. Then we have that $\varphi(f(\mathrm{q})) = \overline{f}(\varphi(\mathrm{q}))$.*

Proof. It is an immediate consequence of Proposition 4.2.1. **QED**

Proposition 4.2.4. *Let p be a prime integer and let φ be as in Proposition 4.2.1. Let $f(x) \in \mathbb{Z}[x]$ and let $\overline{f}(x) \in \mathbb{Z}_p[x]$ be the polynomial obtained from $f(x)$ reducing its coefficients modulo p. Let $n > 1$ be an integer such that $n = p^{\alpha}m$ and $p \nmid m$. Then $\frac{1}{n}f(x) \in \mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ if and only if $f(\mathrm{q}) \in p^{\alpha}\mathbb{P}_{\mathbb{Z}_{(p)}}$, for all $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}_{(p)}}$. In particular if $\alpha = 1$, then $\frac{1}{n}f(x) \in \mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ if and only if $\overline{f}(\mathrm{q}) = \overline{0}$ in $\mathbb{P}_{\mathbb{Z}_p}$, for all $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}_p}$.*

Proof. Let us prove the first part. Take a split quaternion $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}_{(p)}}$. If $\frac{1}{n}f(x) \in \mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$, then $\frac{1}{n}f(\mathrm{q}) \in \mathbb{P}_{\mathbb{Z}_{(p)}}$. This means that the numerator of every coefficient of $f(\mathrm{q})$ must contain the factor p^{α} so that it can be deleted from the denominator of $\frac{1}{n}$. Therefore $f(\mathrm{q}) \in p^{\alpha}\mathbb{P}_{\mathbb{Z}_{(p)}}$. The reverse implication is obvious.

Let us show the second part, where $n = pm$ for some integer m not divisible by p. Recall that for any $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}_{(p)}}$ $\varphi(f(\mathrm{q})) = \overline{f}(\varphi(\mathrm{q}))$, using the notation of Lemma 4.2.3. Take a split quaternion $\mathrm{q}' \in \mathbb{P}_{\mathbb{Z}_p}$. Since φ is surjective, there exists a $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}_{(p)}}$ such that $\varphi(\mathrm{q}) = \mathrm{q}'$. Then $\overline{f}(\mathrm{q}') = \overline{f}(\varphi(\mathrm{q})) = \varphi(f(\mathrm{q})) = \overline{0}$, being $f(\mathrm{q}) \in p\mathbb{P}_{\mathbb{Z}_{(p)}}$ for the first part. Take now $\mathrm{q} \in \mathbb{P}_{\mathbb{Z}_{(p)}}$. Since $\overline{f}(\varphi(\mathrm{q})) = \overline{0}$, then $\varphi(f(\mathrm{q})) = \overline{0}$ in $\mathbb{P}_{\mathbb{Z}_p}$. Then $f(\mathrm{q}) \in \ker\varphi = p\mathbb{P}_{\mathbb{Z}_{(p)}}$, as wanted.

QED

Lemma 4.2.5. *Let R be a commutative domain. Take a split quaternion $\mathrm{q} \in \mathbb{P}_R \smallsetminus R$. Let $m_q(x) \in R[x]$ be its minimal polynomial over R. If a polynomial $f(x) \in R[x]$ is such that $f(\mathrm{q}) = 0$, then $m_{\mathrm{q}}(x) \mid f(x)$ in $R[x]$.*

Proof. Since $m_{\mathrm{q}}(x)$ is a monic polynomial, we can divide $f(x)$ by $m_{\mathrm{q}}(x)$ obtaining

$$f(x) = g(x)m_{\mathrm{q}}(x) + r(x), \tag{4.2}$$

for some $g(x)$ and $r(x)$ polynomials of $R[x]$. In particular $r(x) = ax + b$ is a linear polynomial, being $m_{\mathrm{q}}(x)$ of degree two. Since $R[x] \subseteq \mathcal{Z}(\mathbb{P}_R[x])$, we can evaluate the polynomial relation (4.2) in q. We get: $0 = f(\mathrm{q}) = g(\mathrm{q})\cdot 0 + a\mathrm{q} + b$. Since R is a domain and $\mathrm{q} \notin R$, necessarily $a = b = 0$. **QED**

The lemma above is not true if the polynomial $f(x) \in \mathbb{P}_R[x]$ has imaginary coefficients. For example consider the split quaternion $\mathbf{i} \in \mathbb{P}_{\mathbb{Z}}$. Take the polynomial $f(x) = x^3 + \mathbf{i}x^2 + (\mathbf{i} + 1)x + \mathbf{i} + 1$. It results that $f(\mathbf{i}) = 0$. If we divide $f(x)$ by $x^2 + 1$ we obtain $f(x) = (x^2 + 1)(x + \mathbf{i}) + \mathbf{i}x + 1$, where the remainder is nonzero.

Corollary 4.2.6. *Let p be a prime integer. Let $f(x) \in \mathbb{Z}[x]$ and let $\overline{f}(x) \in \mathbb{Z}_p[x]$ be the polynomial obtained from $f(x)$ reducing its coefficients modulo p.*

Let $n > 1$ be an integer such that $n = pm$ and $p \nmid m$. Then $\frac{1}{n}f(x) \in \mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ if and only if $\overline{f}(x)$ is divisible by all the minimal polynomials of the elements of $\mathbb{P}_{\mathbb{Z}_p}$.

Proof. It is an immediate consequence of Proposition 4.2.4 and Lemma 4.2.5.

QED

Example 4.2.7. The polynomial

$$\Phi_p(x) = \frac{1}{p}(x^p - x)(x^{p^2} - x)$$

in an element of $\mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$. After Proposition 4.2.4, it is sufficient to show that $f(x) = (x^p - x)(x^{p^2} - x) \in \mathbb{Z}_p[x]$ vanishes over all elements of $\mathbb{P}_{\mathbb{Z}_p}$. Observe that every monic and irreducible polynomial of $\mathbb{Z}_p[x]$ of degree one or two is a factor of $f(x)$. In particular the linear polynomials are raised to the second power. This means that the minimal polynomial of every split quaternion of $\mathbb{P}_{\mathbb{Z}_p}$ is a factor of $f(x)$.

In particular we can show that every monic and quadratic polynomial of $\mathbb{Z}_p[x]$ is the minimal polynomial for some element of $\mathbb{P}_{\mathbb{Z}_p}$. The proof is *mutatis mutandis* the same as the proof of [22, lemma 4.2.2]. This means that the polynomial $\Phi_p(x)$ of the previous example does not contain any irredundant factor.

Proposition 4.2.8. *The following proper inclusions are given:*

$$\mathbb{Z}_{(p)}[x] \subsetneq \mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right) \subsetneq \mathrm{Int}(\mathbb{Z}_{(p)}).$$

Proof. The first inclusion is straightforward since $\mathbb{Z}_{(p)} \subseteq \mathbb{P}_{\mathbb{Z}_{(p)}}$. For seeing that it is proper, use the polynomial $\Phi_p(x)$ of the Example 4.2.7. For the second inclusion take a polynomial $f(x) \in \mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$. If $a \in \mathbb{Z}_{(p)}$, then $f(a) \in \mathbb{Q}$ since $f(x) \in \mathbb{Q}[x]$. Moreover $f(a) \in \mathbb{P}_{\mathbb{Z}_{(p)}}$ by hypothesis. Finally $f(a) \in \mathbb{Q} \cap \mathbb{P}_{\mathbb{Z}_{(p)}} = \mathbb{Z}_{(p)}$. A counterexample for the reverse inclusion is the polynomial $f(x) = \frac{x(x-1)(x-2)\ldots(x-p+1)}{p}$. For $p = 2$ we work by hands using $\mathrm{q} = \mathbf{i}$. For odd primes we use Corollary 4.2.6: $pf(x)$ is not divisible by x^2+1, the minimal polynomial of $\mathrm{q} = \mathbf{i}$. **QED**

We are ready for the most important result of this section.

Proposition 4.2.9. *The ideal* $p\,\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$ *is not a prime ideal of* $\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$.

Proof. Let us consider the polynomials:

$$\begin{aligned} F(x) &= \frac{1}{p}(x^p - x)^2\left(x^{p^2} - x\right)^2 \in \mathbb{Q}[x], \\ f(x) &= (x^p - x)^2 \in \mathbb{Z}[x], \\ g(x) &= \frac{1}{p}\left(x^{p^2} - x\right)^2 \in \mathbb{Q}[x]. \end{aligned}$$

We start showing that these three polynomials are elements of $\mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$. For $f(x)$ it is trivially seen since $\mathbb{Z}[x] \subseteq \mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$. For $F(x)$ and $g(x)$ observe that the polynomial $\Phi_p(x)$, introduced in Example 4.2.7, divides both $F(x)$ and $g(x)$ in $\mathbb{Z}[x]$. Moreover we have that $F(x) \in p\,\mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ but $f(x) \notin p\,\mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ and $g(x) \notin p\,\mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$. In fact it results that $\frac{1}{p}F(x) = (\Phi_p(x))^2 \in \mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$. As regards $f(x)$, using Corollary 4.2.6, we have that $\overline{f}(x)$ is not divisible by any quadratic irreducible polynomial over $\mathbb{Z}_p$. Lastly we prove that $\frac{1}{p}g(x) = \frac{1}{p^2}\left(x^{p^2} - x\right)^2 \notin \mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$. For $p = 2$, it is easily seen that $\frac{1}{2}g(\mathbf{i}) = -\frac{\mathbf{i}}{2} \notin \mathbb{P}_{\mathbb{Z}_{(2)}}$. If p is odd then we use the split quaternion $\mathrm{q} = \mathbf{i} + (p-1)\,\mathbf{k}$. By some trivial calculations, we have that $\mathrm{q}^2 = p^2 - 2p$. Moreover if we raise q to an even power greater than 2, we obtain an integer divisible by p^2. Since $\frac{1}{p}g(x)$ is a central polynomial, we can evaluate it in q even if it is factorized. Thus we get, for some $m \in \mathbb{Z}$:

$$\frac{1}{p}g(\mathrm{q}) = \frac{(\mathrm{q}^{p^2} - \mathrm{q})^2}{p^2} = \frac{\mathrm{q}^{2p^2} + \mathrm{q}^2 - 2\mathrm{q}^{p^2+1}}{p^2} = m + \frac{p-2}{p} \notin \mathbb{P}_{\mathbb{Z}_{(p)}}.$$

We can conclude that $p\,\mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ is not a prime ideal of $\mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$. **QED**

4.3 Some properties of $\mathrm{Spec}\left(\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)\right)$

Given $\mathbb{Q}(\theta)$ a finite degree extension of $\mathbb{Q}$, we indicate by $\mathcal{A}_\theta$ the ring of algebraic integers of $\mathbb{Q}(\theta)$. Taken a positive $n \in \mathbb{N}$, the set of all algebraic integers of degree at most n over $\mathbb{Q}$ is

$$\mathcal{A}_n \overset{\text{def}}{=} \bigcup_{[\mathbb{Q}(\theta):\mathbb{Q}]\leqslant n} \mathcal{A}_\theta.$$

In [18] Loper and Werner define the set of integer-valued polynomials over $\mathcal{A}_n$ with rational coefficients to be the set:

$$\mathrm{Int}(\mathcal{A}_n) \overset{\text{def}}{=} \bigcap_{\theta\in\mathcal{A}_n} \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_\theta).$$

They also show that $\mathrm{Int}(\mathcal{A}_n)$ can be seen as the set of all polynomials with rational coefficients that map $\mathcal{A}_n$ into $\mathcal{A}_n$.

Here follow some important properties of this ring.

Proposition 4.3.1. [18, Theorem 3.9] *For all positive integer n, the ring* $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$ *is a Prüfer domain.*

Proposition 4.3.2. [18, Theorem 4.6] *For all positive integer n, the integral closure of the ring* $\mathrm{Int}_{\mathbb{Q}}(\mathcal{M}_n(\mathbb{Z}))$ *is* $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_n)$.

Since by Theorem 1.3.1 split quaternions can be embedded into 2 × 2 matrices rings, we will focuse in the following on the set $\mathcal{A}_2$.

We have the following result that join the ring $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_2)$ with the set $\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$.

Theorem 4.3.3. *Let p be a prime odd integer. Then* $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_2)_{(p)}$ *is the integral closure of* $\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$ *in* $\mathbb{Q}[x]$.

Proof. Using 4.3.2 for $n = 2$ and recalling that the localization at prime integers preserves the integral closure, we have that:

$$\begin{aligned}\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_2)_{(p)} &= \overline{\mathrm{Int}_{\mathbb{Q}}(\mathcal{M}_2(\mathbb{Z}))}_{(p)} = \overline{\mathrm{Int}_{\mathbb{Q}}(\mathcal{M}_2(\mathbb{Z}))_{(p)}} = \\ &= \overline{\mathrm{Int}_{\mathbb{Q}}(\mathcal{M}_2(\mathbb{Z})_{(p)})} = \overline{\mathrm{Int}_{\mathbb{Q}}\left(\mathcal{M}_2(\mathbb{Z}_{(p)})\right)} = \overline{\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)}.\end{aligned}$$

QED

Now, from the spectrum of the ring $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_2)_{(p)}$ we can obtain interesting information on the spectrum of $\overline{\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)}$ (using the well-known theorems of going-up, going-down and lying over). From Theorem 4.1.12 it is possible to transfer results about $\mathrm{Spec}\left(\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)\right)$ to $\mathrm{Spec}\left(\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)\right)$.

From now on we suppose that p is an odd prime integer. Call for simplicity $B = \mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_2)_{(p)}$. We will first calculate the Krull dimension of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ starting from the fact that

$$\dim\left(\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)\right) = \dim(B),$$

since B is the integral closure of the ring $\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$.

We use the notion of *valuative dimension.* For further references see [10, Chapter 30] about dimension theory. We recall that the valuative dimension of an integral commutative domain D is defined as

$$\dim_v(D) = \sup\left\{\dim(V) \mid V \text{ is a valuation overring of } D\right\}.$$

If D is a Prüfer domain, then $\dim(D) = \dim_v(D)$. Moreover if $A \subseteq D$ is a ring extension with the same quotient field, then $\dim_v(D) \leqslant \dim_v(A)$.

In [18] it is shown that $\mathrm{Int}_{\mathbb{Q}}(\mathcal{A}_2)$ is a Prüfer ring. It follows that B is also Prüfer (as being a localization of a Prüfer domain) and so $\dim(B) = \dim_v(B)$.

Since $\mathbb{Z}[x] \subseteq B$, then

$$1 \leqslant \dim_v(B) \leqslant \dim_v(\mathbb{Z}[x]) = 2$$

and

$$1 \leqslant \dim\left(\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)\right) \leqslant 2.$$

We can explicitly describe a chain of prime ideals of length 2 in $\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)$, so showing that $\dim\left(\mathrm{Int}_{\mathbb{Q}}\left(\mathbb{P}_{\mathbb{Z}_{(p)}}\right)\right) = 2$.

Take in fact an integer split quaternion $\mathrm{q} = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k} \in \mathbb{P}_{\mathbb{Z}}$ such that $p \nmid \gcd(b, c, d)$ and the minimal polynomial of q $m_{\mathrm{q}}(x) \in \mathbb{Z}[x]$ is irreducible modulo p. Then the ideal $\mathfrak{P}_{p,\mathrm{q}}$ is a prime ideal of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$. Since $m_{\mathrm{q}}(x)$ is irreducible modulo p, then it is also irreducible in $\mathbb{Q}[x]$. Thus the ideal $\mathfrak{P}_{0,\mathrm{q}}$ is a prime ideal too. Finally, it is obvious that $\mathfrak{P}_{0,\mathrm{q}} \subseteq \mathfrak{P}_{p,\mathrm{q}}$. This inclusion between prime ideals is preserved when localizing at $\mathbb{Z} \setminus p\mathbb{Z}$, thus $\dim(\mathrm{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})) = 2$. This fact, together with the correspondence given by Corollary 4.1.13, establishes that the height of a prime ideal of $\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}(\mathbb{P}_{\mathbb{Z}})$ containing p is at most 2. In the following, we will show something more. Exactly we will see that such ideals are always maximal and so there are no containment relations between primes of $\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}(\mathbb{P}_{\mathbb{Z}})$ containing an odd prime integer p. This replicates the same pattern of $\mathrm{Spec}(\mathrm{Int}(\mathbb{Z}))$ ([4, Proposition V.2.7]).

We start from an investigation on $\mathrm{Spec}(B)$ and then we will transfer these results to $\mathrm{Int}_{\mathbb{P}_{\mathbb{Q}}}(\mathbb{P}_{\mathbb{Z}})$.

Theorem 4.3.4. *With the above hypothesis and notation, fixed an odd prime integer p, the prime ideals of B above p are all maximal.*

Proof. Let Q be a prime ideal of B such that $Q \cap \mathbb{Z} = (p)$. Then, by [17, Corollary 3.3], there exist a valuation overring V of B and a prime ideal P of $V \cap \mathbb{Q}[x]$ such that

$$B_Q = (V \cap \mathbb{Q}[x])_P.$$

Moreover the domain V is *minimal* over B in the sense of [17, Theorem 2.8 and Notation 2.9] and it is a *limit* since B is a Prüfer domain ([17, Theorem 4.2]).

Since Q contains p, the same holds for the ideal P. Then $B_Q = (V \cap \mathbb{Q}[x])_P$ is a valuation overring of $V \cap \mathbb{Q}[x]$ containing p as nonunit. It follows that it is exactly V, since all the other valuation overrings of $V \cap \mathbb{Q}[x]$ are overrings of $\mathbb{Q}[x]$ in which p is invertible.

We claim that Q is maximal. If not, there exists $Q' \in \operatorname{Spec}(B)$ with $Q \subsetneq Q'$. Then $p \in Q'$ and applying again the results of [17] used for Q, we get that $B_{Q'} = (V' \cap \mathbb{Q}[x])_{P'} = V'$, where V' is a minimal, limit valuation overring of B containing p as nonunit. But $B_{Q'} \subsetneq B_Q$, thus $V' \subseteq V$. The only possible valuation overring of a limit domain is an overring of $\mathbb{Q}[x]$ by [17, §1].

Thus we get a contradiction when assuming that Q is nonmaximal. **QED**

Corollary 4.3.5. *The prime ideals of* $\operatorname{Int}_{\mathbb{P}_{\mathbb{Q}}}(\mathbb{P}_{\mathbb{Z}})$ *above an odd prime integer p are all maximal.*

Proof. From Theorem 4.3.4 we have that the prime ideals of B above an odd prime integer p are all maximal and this property transfers to $\operatorname{Int}_{\mathbb{Q}}(\mathbb{P}_{\mathbb{Z}_{(p)}})$ for the going up theorem between a domain and its integral closure. At this point it is sufficient to apply Corollary 4.1.13. **QED**

As regards the prime and maximal ideals of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ that contains the prime $p = 2$ so far we do not have results as for the case p odd prime. We have seen some examples of such ideals but we are not able to completely classify them. For working with odd prime integers we used the matrix representation which turned out to be useless in the case $p = 2$. Our studies show that the properties of $\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})$ are similar to the ones of $\mathrm{Int}(\mathbb{Z})$: we also conjecture that $\dim(\mathrm{Int}(\mathbb{P}_{\mathbb{Z}})) = 2$.

Bibliography

[1] M.F. Atiyah, I.G. MacDonald, *Introduction to commutative Algebra*, Westview Press, Boulder, CO, 1969.

[2] V. Bargmann, *Representations of the Lorentz Group*, Annals of Mathematics **48** (1947), 568–640.

[3] J.V. Brawley, L. Carlitz, *Scalar polynomial functions on the $n \times n$ matrices over a finite field*, Linear Algebra and Appl. **10** (1975) 199–217.

[4] P.J. Cahen, J.L. Chabert, *Integer-valued polynomials*, Amer. Math. Soc. Surveys and monographs, Providence, 1997.

[5] A. Cigliola, A.K. Loper, N.J. Werner, *Split quaternions and integer-valued polynomials*, Comm. Alg., (2014, *to appear*).

[6] J. Cokle, *On Systems of Algebra involving more than one Imaginary and on equations of the fifth degree* , Philosophical Magazine, (series 3) **35** (1849), 434–437.

[7] S. Evrard, Y. Fares, K. Johnson, *Integer-valued polynomials on lower triangular integer matrices*, Monatsh. Math. **170** (2013), no. 2, 147–160.

[8] S. Frisch, *Integer-valued polynomials on algebras: a survey*, CIRM, Troisième Rencontre Internationale sur les Polynômes à Valeurs Entières (2010), 27–32.

[9] S. Frisch, *Integer-valued polynomials on algebras*, J. Algebra, **373** (2013), 414–425.

[10] R. Gilmer, *Multiplicative ideal theory*, Marcel Dekker, Inc., New York, 1972.

[11] A.W. Goldie, *Localization in noncommutative noetherian rings*, J. Algebra, **5** (1967), 89–105.

[12] K.R. Goodearl, R.B. Warfield Jr., *An introduction to noncommutative noetherian rings*, Cambridge University Press, 2004.

[13] S. Ivanov, S. Zamkovoy, *Parahermitian and paraquaternionic manifolds*, Differential Geometry and its Applications (2005), **23**, 205–234.

[14] T.Y. Lam, *A first course in noncommutative ring theory*, Springer, 2001.

[15] T.Y. Lam, *Lectures on modules and rings*, Springer, 1999.

[16] T.Y. Lam, *Introduction to Quadratic Forms over Fields*, Graduate Studies in Mathematics **67**, American Mathematical Society, 2005.

[17] K.A. Loper, F. Tartarone, *A classification of the integrally closed rings of polynomials containing $Z[X]$*, J. Commut. Algebra **1** (2009), no. 1, 91–157.

[18] K.A. Loper, N.J. Werner, *Generalized rings of integer-valued polynomials*, J. Num. Theory, **132** (2012), 2481–2490.

[19] M. Özdemir, A.A. Ergin, *Rotations with timelike quaternions in Minkowski 3-space*, Journal of Geometry and Physics **56** (2006), 322–336.

[20] B.A. Rosenfeld, *A History of Non-Euclidean Geometry*, Springer-Verlag (1988)

[21] N.J. Werner, *Integer-valued polynomials over quaternion rings*, Ph.D. Thesis, The Ohio State University, 2010.

[22] N.J. Werner, *Integer-valued polynomials over quaternion rings*, J. of Algebra, **324** (2010),1754–1769.

[23] N.J. Werner, *Integer-valued polynomials over matrix rings*, Comm. Algebra, **40** (2012), 4717–4726.

Acknowledgments

I wish to express my sincere gratitude to my advisor, Prof. Francesca Tartarone, for her helpful suggestions, for her wise guidance and for her patience.

I feel also grateful to Prof. K. Alan Loper for his encouragement and collaboration.

I thank Prof. Valentina Barucci, Prof. Sophie Frisch and Prof. Marco Fontana for accepting to be members of my defense committee.

I also express my gratitude to Dr. Carmelo Antonio Finocchiaro and to Dr. Nicholas J. Werner for their continuous advice and useful suggestions.

I acknowledge Prof. Stefania Gabelli, Prof. Florida Girolami and Dr. Alice Fabbri for the support they gave me during my studies.

Finally, I thank my friends, the Ph.D. students, the professors and the students of the Math Department of Roma Tre.