SPLIT QUATERNIONS AND INTEGER-VALUED POLYNOMIALS

A. CIGLIOLA, K. A. LOPER, N. WERNER
APRIL 27, 2013

Abstract. The integer split quaternions form a noncommutative algebra over \( \mathbb{Z} \). We describe the prime and maximal spectrum of the integer split quaternions and investigate integer-valued polynomials over this ring. We prove that the set of such polynomials forms a ring, and proceed to study its prime and maximal ideals. In particular we completely classify the primes above 0, we obtain partial characterizations of primes above odd prime integers, and we give sufficient conditions for building maximal ideals above 2.

Keywords: Quaternion, integer-valued polynomial, noncommutative

MSC Primary 16S99, Secondary 13F20, 11R52, 16H05

1. Introduction

Traditionally, integer-valued polynomials have been defined over a commutative integral domain \( D \). Letting \( K \) be the fraction field of \( D \), we define \( \text{Int}(D) = \{ f \in K[x] \mid f(D) \subseteq D \} \), called the ring of integer-valued polynomials over \( D \). The ring \( \text{Int}(D) \) and related constructions have inspired much research in recent decades (see [2]). Recently, several authors have investigated the integer-valued polynomial construction over noncommutative rings and algebras. There is more than one approach to the problem in this instance. Some authors ([3], [4], [5]) begin with a \( D \)-algebra \( A \) and consider polynomials in \( K[x] \) that map elements of \( A \) back to \( A \). The set of such polynomials forms a commutative subring of \( K[x] \), and this ring may be studied in much the same way as \( \text{Int}(D) \).

Another course of action ([3], [8], [9]) is to let noncommutative rings \( A \subseteq B \) take the place of \( D \) and \( K \) in the definition of \( \text{Int}(D) \), yielding the set \( \text{Int}(A) = \{ f \in B[x] \mid f(A) \subseteq A \} \). Under this definition, \( \text{Int}(A) \) consists of polynomials with noncommuting coefficients, and many features (such as closure under multiplication or descriptions of prime ideals) that are trivial to establish for \( \text{Int}(D) \) become more difficult to define and prove. Nevertheless, there are many similarities with the commutative case, although the proofs and methods of analysis are quite different.

In this paper, we will follow the latter approach, and define a noncommutative ring of integer-valued polynomials that act on the split quaternions (sometimes called the paraquaternions), denoted by \( P_{\mathbb{Z}} \), which form a particular quaternion algebra over the integers. In this, there are strong parallels with the work done in [9], which studied integer-valued polynomials over a different algebra, the Lipschitz quaternions, denoted by \( H_{\mathbb{Z}} \). However, because \( P_{\mathbb{Z}} \) contains nilpotent elements and zero divisors while \( H_{\mathbb{Z}} \) does not, the techniques used in this paper are distinct from those in [9]. It is our hope that some of the methods used here will be applicable to the study of integer-valued polynomials over other types of noncommutative rings.
In Section 2, we define our quaternion algebras and discuss properties (such as ideal structure and matrix representations) that will be needed later. In Section 3 we give our conventions for working with polynomials over noncommutative rings, prove that \( \text{Int}(\mathbb{P}_Z) \) has a ring structure, and present a useful localization theorem. In Section 4 we investigate prime and maximal ideals of \( \text{Int}(\mathbb{P}_Z) \). We close with a summary of our results and mention questions for further research.

2. Split Quaternions

In general, a quaternion algebra over \( \mathbb{Z} \) consists of elements of the form \( a + bi + cj + dk \) with \( a, b, c, d \in \mathbb{Z} \) and \( i, j, k \) satisfying the relations \( i^2 = r, j^2 = s, ij = k = -ji \), for some nonzero \( r, s \in \mathbb{Z} \); note that these relations force \( k^2 = -rs \).

**Definition 2.1.** With \( r \) and \( s \) as above, the *Lipschitz quaternions* \( \mathbb{H}_\mathbb{Z} \) are formed by taking \( r = s = -1 \). When we take \( r = -1 \) and \( s = 1 \), we obtain the *split quaternions* \( \mathbb{P}_\mathbb{Z} \). That is

\[
\mathbb{H}_\mathbb{Z} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}, \ i^2 = j^2 = k^2 = -1, \ ij = k = -ji\}
\]

\[
\mathbb{P}_\mathbb{Z} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}, \ i^2 = -1, \ j^2 = k^2 = 1, \ ij = k = -ji\}
\]

More generally, when \( R \) is a commutative ring, we define rings \( \mathbb{H}_R \) and \( \mathbb{P}_R \) by

\[
\mathbb{H}_R = \{a + bi + cj + dk \mid a, b, c, d \in R\}
\]

\[
\mathbb{P}_R = \{a + bi + cj + dk \mid a, b, c, d \in R\}
\]

where the relations on \( i, j, \) and \( k \) are the same as for \( \mathbb{H}_\mathbb{Z} \) and \( \mathbb{P}_\mathbb{Z} \), respectively.

In both \( \mathbb{H}_R \) and \( \mathbb{P}_R \), the elements \( i, j, \) and \( k \) are units, which we refer to as the *quaternion units* or the *basis units*. Both \( \mathbb{H}_R \) and \( \mathbb{P}_R \) are associative rings with identity, but they will not be commutative unless \( R \) has characteristic 2.

While the two rings \( \mathbb{H}_R \) and \( \mathbb{P}_R \) are similar, there are important differences between the two. Our relations on the basis units imply that \( jk = i \) in \( \mathbb{H}_R \), while \( jk = -i \) in \( \mathbb{P}_R \). Thus, the two rings have different multiplications. Moreover, in the case \( R = \mathbb{Z} \), the Lipschitz quaternions 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 \( (1 + j)(1 - j) = 0 \) and \( (i + j)^2 = 0 \).

There is also a representation of \( \mathbb{P}_R \) as a subring of \( M_2(R) \), the ring of 2 \( \times \) 2 matrices with entries in \( R \).

**Proposition 2.2.**

1. Let \( R \) be a commutative ring with identity such that 2 is a unit of \( R \). Then, \( \mathbb{P}_R \cong M_2(R) \) as \( R \)-algebras.

2. Let \( \mathcal{A} \subseteq M_2(\mathbb{Z}) \) be the set \( \mathcal{A} = \{(a_{ij}) \mid a \equiv d, \ b \equiv c \mod 2\} \). Then, \( \mathbb{P}_\mathbb{Z} \cong \mathcal{A} \) as \( \mathbb{Z} \)-algebras.

**Proof.** The result in (1) is well known. One isomorphism \( \phi : \mathbb{P}_R \rightarrow M_2(R) \) is given by defining \( \phi(1) = (1, 0), \ \phi(1) = (-1, 0), \ \phi(j) = (0, 1), \ \phi(k) = (1, 0) \), and then extending linearly over \( R \). For (2), it is clear that \( \phi(\mathbb{P}_\mathbb{Z}) \subseteq \mathcal{A} \). However, this mapping is surjective, since the matrix \( (a \ b) \) will be the image of the split quaternion \( \frac{1}{2}((a + d) + (b - c)i + (b + c)j + (a - d)k) \). Thus, \( \mathbb{P}_\mathbb{Z} \cong \mathcal{A} \). \( \square \)
Note that (1) shows that $P Q \sim M_2(Q)$ and $P F \sim M_2(F)$ when $F$ is a finite field of odd characteristic.

Given $q = a + bi + cj + dk \in P R$, we call $a, b, c$, and $d$ the coefficients of $q$, and $a$ is the real part of $q$. The bar conjugate of $q$ is defined to be $\bar{q} = a - bi - cj - dk$; the norm of $q$ is $N(q) = a^2 + b^2 - c^2 - d^2$ and the trace of $q$ is $T(q) = 2a$. Properties of $q$, $N(q)$ and $T(q)$ are given in the following proposition. All the results can be verified by direct calculation or by an appeal to known properties of general quaternion algebras.

**Proposition 2.3.** Let $R$ be a commutative ring with identity. Let $q, p \in P R$. Then,

1. $\bar{q} = q$
2. $q + p = q + p$
3. $q p = p q$
4. $N(q) = q \bar{q} = \bar{q} q = N(\bar{q})$
5. under the matrix representation $\phi$ in Proposition 2.2, $N(q)$ and $T(q)$ correspond respectively with the determinant and the trace of $\phi(q)$
6. $N(q p) = N(q) N(p)$
7. $q$ is invertible if and only if $N(q)$ is a unit of $R$
8. if $q$ is invertible then $q^{-1} = \frac{1}{N(q)} \bar{q}$.

Using the matrix representation $\phi : P R \to M_2(R)$, we see that $\phi(q)$ (and hence $q$) will be killed by the characteristic polynomial $x^2 - T(q) x + N(q)$ of $\phi(q)$. This leads us to the following definition.

**Definition 2.4.** Given $q \in P R$, we define the minimal polynomial of $q$ to be

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

As we shall see in Section 4 the minimal polynomials of elements of $P Z$ will be important in identifying certain prime and maximal ideals of $\text{Int}(P Z)$.

The rest of this section concerns a classification of the prime and maximal ideals of $P_2$ (unless otherwise noted, all ideals are assumed to be two-sided). Since we are dealing with noncommutative rings, the definition of a prime ideal must be modified. There are several equivalent definitions for a prime ideal in a noncommutative ring (see [3] §10). Among them are the following: an ideal $P$ in a ring $R$ is a prime ideal of $R$ if whenever $a, b \in R$ with $a R b \subseteq P$, then either $a \in P$ or $b \in P$. Equivalently, $P$ is prime if whenever $I$ and $J$ are ideals of $R$ and $I J \subseteq P$, then either $I \subseteq P$ or $J \subseteq P$. Taking either of these as the definition of prime, we can say that $P$ is prime if and only if the zero ideal is prime in the residue ring $R / P$. The definition of a maximal ideal in a noncommutative ring matches the standard commutative definition, and maximal ideals are still prime.

**Lemma 2.5.** Let $I$ be a nonzero ideal of $P Z$. Then, $I$ contains a nonzero integer.

**Proof.** Let $q = a + bi + cj + dk \in I$ be nonzero. Then, one of the coefficients of $q$ must be nonzero. Since $I$ is an ideal, $iq, jq$ and $kq \in I$. Thus, WLOG, we may assume that the real part $a$ of $q$ is nonzero. Furthermore, the following are elements
\(-iqi = a + bi - cj - dk\)
\(jqj = a - bi + cj - dk\)
\(kqk = a - bi - cj + dk\)

Consequently, \(4a = q + -iqi + jqj + kqk \in I\).

**Proposition 2.6.**

1. (0) is a prime ideal of \(\mathbb{P}_R\).
2. Any nonzero prime ideal of \(\mathbb{P}_Z\) contains a prime of \(\mathbb{Z}\).
3. If \(p\) is an odd prime of \(\mathbb{Z}\), then \(p\mathbb{P}_Z\) is a maximal ideal of \(\mathbb{P}_Z\) and is the unique prime ideal of \(\mathbb{P}_Z\) containing \(p\).

**Proof.** 1. Let \(I\) and \(J\) be ideals of \(\mathbb{P}_Z\) such that \(IJ = (0)\). If \(I = (0)\), then we are done. If not, then by Lemma 2.5, \(I\) contains a nonzero integer \(n\). Since \(n\) is central in \(\mathbb{F}_n\), for each \(q \in J\) we have \(nq = 0\), implying that \(q = 0\). Thus, \(J = (0)\) and (0) is prime.

2. Let \(P\) be a nonzero prime ideal of \(\mathbb{P}_Z\). Again using Lemma 2.5, we can find a nonzero \(n \in P \cap Z\). Whenever \(n\) factors as \(n = n_1n_2\), we have \(n_1\mathbb{P}_Zn_2 \subseteq P\), so either \(n_1 \in P\) or \(n_2 \in P\). It follows that \(P\) must contain a prime of \(\mathbb{Z}\).

3. Let \(p\) be an odd prime and let \(P = p\mathbb{P}_Z\). The residue ring \(\mathbb{P}_Z/P \cong \mathbb{F}_p\), where \(\mathbb{F}_p\) is the finite field with \(p\) elements (the isomorphism is given by reducing the coefficients of a split quaternion modulo \(p\)). By Proposition 2.2, \(\mathbb{F}_p \cong F_2(\mathbb{F}_p)\), which is a simple ring. Hence, \(P\) is a maximal ideal of \(\mathbb{P}_Z\). Since any prime ideal of \(\mathbb{P}_Z\) containing \(p\) will contain \(p\mathbb{P}_Z\), \(P\) is the only prime of \(\mathbb{P}_Z\) over \(p\).

To completely classify the prime ideals of \(\mathbb{P}_Z\), it remains to consider prime ideals above 2. As we shall see, \(2\mathbb{P}_Z\) is not prime, but there is a unique prime ideal of \(\mathbb{P}_Z\) containing 2. Key to our work is the observation that since the ring \(\mathbb{P}_Z/2\mathbb{P}_Z\) has characteristic 2, it is commutative.

**Lemma 2.7.** Let \(R = \mathbb{P}_Z/2\mathbb{P}_Z\). Then, \(R\) is a commutative ring with 16 elements, \(R\) has a unique maximal ideal generated by \(1+i\) and \(1+j\), and the residue field of \(R\) is \(\mathbb{F}_2\).

**Proof.** Since \(R \cong \mathbb{F}_2\), we see that \(R\) is commutative and has 16 elements: \(R = \{a + bi + cj + dk \mid a, b, c, d \in \{0, 1\}\}\). Working mod 2, the norm is additive as well as multiplicative (since \((A + B)^2 = A + B\) for all \(A, B \in \mathbb{F}_2\)), so the non-unit elements of \(R\) form a maximal ideal \(M\). There are 8 elements in \(M\), so \(R/M \cong \mathbb{F}_2\). Finally, straightforward calculations show that \(M\) is generated by \(1+i\) and \(1+j\).

Let \(\mathcal{M}\) be the ideal of \(\mathbb{P}_Z\) generated by \(1+i\) and \(1+j\). Borrowing notation from commutative ring theory, we shall also write \(\mathcal{M} = (1+i, 1+j)\). A priori, elements of \(\mathcal{M}\) consist of finite sums of the form \(\sum q_i(1+i)p_i + \sum r_j(1+j)s_j\), where each \(q_i, p_i, r_j, s_j \in \mathbb{P}_Z\). Such an expression is unwieldy to work with, but luckily there is a simpler description available.

**Lemma 2.8.** Let \(q \in \mathcal{M}\). Then, there exist \(p, r \in \mathbb{P}_Z\) such that \(q = p(1+i) + r(1+j)\).

**Proof.** Working in the commutative ring \(\mathbb{P}_Z/2\mathbb{P}_Z\), we have \(q \equiv q_1(1+i) + q_2(1+j)\) for some \(q_1, q_2 \in \mathbb{P}_Z\). Lifting this to \(\mathbb{P}_Z\), we have \(q = q_1(1+i) + q_2(1+j) + 2q_3\) for
some \( q_3 \in \mathbb{P}_2 \). Since \( 2 = (1 - i)(1 + i) \), we get \( q = (q_1 + q_3(1 - i))(1 + i) + q_2(1 + j) \). Taking \( p = q_1 + q_3(1 - i) \) and \( r = q_2 \) yields the result. \( \square \)

We will prove that \( \mathcal{M} \) is maximal and is the only prime ideal of \( \mathbb{P}_2 \) above 2.

**Lemma 2.9.** Let \( P \) be a prime ideal of \( \mathbb{P}_2 \) containing 2. Then, \( P \) must be a maximal ideal.

**Proof.** Since \( \mathbb{P}_2/2\mathbb{P}_2 \) is a finite commutative ring, \( \mathbb{P}_2/P \) must be a finite commutative ring in which \((0)\) is a prime ideal. In other words, \( \mathbb{P}_2/P \) must be a field. Thus, \( P \) must be a maximal ideal of \( \mathbb{P}_2 \). \( \square \)

**Corollary 2.10.** The ideal \( \mathcal{M} = (1 + i, 1 + j) \) of \( \mathbb{P}_2 \) is maximal, and it is the unique prime ideal of \( \mathbb{P}_2 \) above 2.

**Proof.** Given a prime \( P \) of \( \mathbb{P}_2 \) above 2, the image of \( P \) in \( \mathbb{P}_2/2\mathbb{P}_2 \) must be a maximal ideal of \( \mathbb{P}_2/2\mathbb{P}_2 \). By Lemma 2.9, we know that the only maximal ideal of \( \mathbb{P}_2/2\mathbb{P}_2 \) is the ideal generated by \( 1 + i \) and \( 1 + j \). \( \square \)

We now have the complete classification of prime ideals of \( \mathbb{P}_2 \).

**Theorem 2.11.** The prime ideals of \( \mathbb{P}_2 \) are \((0), p\mathbb{P}_2 \) where \( p \) is an odd prime of \( \mathbb{Z} \), and \( \mathcal{M} = (1 + i, 1 + j) \). The primes \( p\mathbb{P}_2 \) and \( \mathcal{M} \) are maximal, \( \mathbb{P}_2/p\mathbb{P}_2 \cong M_2(\mathbb{F}_p) \) and \( \mathbb{P}_2/\mathcal{M} \cong \mathbb{F}_2 \).

3. \( \text{Int}(\mathbb{P}_2) \)

We are now ready to examine the set of integer-valued polynomials over \( \mathbb{P}_2 \). As mentioned in Section 1, when \( D \) is a commutative domain with field of fractions \( K, \text{Int}(D) \) is defined to be \( \text{Int}(D) = \{ f \in K[x] \mid f(D) \subseteq D \} \). Following [8], we will extend this definition to rings that are not necessarily commutative.

We begin by establishing our general conventions regarding polynomials with coefficients from a noncommutative ring. More details can be found in [9] §16, which deals with polynomials over division rings. Given a (possibly noncommutative) ring \( B, B[x] \) denotes the ring of polynomials in one indeterminate with coefficients in \( B \). We assume that the indeterminate \( x \) commutes with all elements of \( B \) and that polynomials are evaluated with \( x \) on the right. Thus, addition and multiplication in the ring \( B[x] \) function just as they do in the commutative case. However, care must be taken when evaluating products of polynomials.

If \( f(x), g(x) \in B[x] \), then \((fg)(x)\) denotes the product of \( f(x) \) and \( g(x) \) in \( B[x] \). So, \((fg)(x)\) always equals \((fg)(x)\). The major difference from the commutative case is that if \( b \in B \), then \((fg)(b)\) need not equal \( f(b)g(b) \). For an easy example, let \( f(x) = x - i \) and \( g(x) = x - j \) in \( \mathbb{P}_2[x] \). Then, their product is \( (fg)(x) = x^2 - (i + j)x + k \). Evaluating \( f, g, \) and \( fg \) at \( i \), we find that \((fg)(i) = i^2 - (i + j)i + k = 2k \) while \((f)(g)(i) = 0(1 - j) = 0 \). Thus, evaluation at an element of \( b \in B \) need no longer define a homomorphism \( B[x] \to B \) (in fact, as shown in [9] §16), we obtain an evaluation homomorphism if and only if \( b \) is in the center of \( B \).

Despite these difficulties, there is a serviceable expression for \((fg)(b)\). If \( f(x) = \sum_{i} a_i x^i \), then we may express \((fg)(x)\) as \((fg)(x) = \sum_{i} a_i g(x)x^i \), and we have \((fg)(b) = \sum_{i} a_i g(b)b^i \). Moreover, if \( g(x) \) is central in \( B[x] \), then for any \( b \in B \) we have \((fg)(b) = f(b)g(b) \), since \((fg)(b) = \sum_{i} a_i g(b)b^i = \sum_{i} a_i b^i g(b) = f(b)g(b) \).

Keeping these conventions in mind, we now define integer-valued polynomials over general rings.
Definition 3.1. Let $A$ and $B$ be rings such that $A \subseteq B$. We define $\text{Int}_B(A) = \{ f \in B[x] \mid f(A) \subseteq A \}$ and call this the set of integer-valued polynomials over $A$ with coefficients in $B$. If $B$ is clear from context, then we will write simply $\text{Int}(A)$. In the case where $D$ is a commutative domain with field of fractions $K$ and $A = \mathbb{P}_D$, then we will take $B = \mathbb{P}_K$, so that $\text{Int}(\mathbb{P}_D) = \{ f \in \mathbb{P}_K[x] \mid f(\mathbb{P}_D) \subseteq \mathbb{P}_D \}$. In particular, we have $\text{Int}(\mathbb{P}_Z) = \{ f \in \mathbb{P}_Q[x] \mid f(\mathbb{P}_Z) \subseteq \mathbb{P}_Z \}$.

It is easy to see that $\text{Int}_B(A)$ is always closed under addition (and is in fact always a left $A$-module). When $A$ and $B$ are commutative, it is also trivial to verify that $\text{Int}_B(A)$ is closed under multiplication, and hence has a ring structure. On the other hand, if $A$ is noncommutative, we have seen that evaluating a product of polynomials can behave in unexpected ways, so it is not clear whether $\text{Int}_B(A)$ is a ring. The following theorem gives a sufficient condition for this to occur.

Theorem 3.2. \cite{[8]} Thm. 1.2] Let $A$ and $B$ be rings such that $A \subseteq B$. Assume that each $a \in A$ may be written as a finite sum $a = \sum c_i u_i$ for some $c_i, u_i \in A$ such that each $u_i$ is a unit in $A$ and each $c_i$ is central in $B$. Then, $\text{Int}_B(A)$ is closed under multiplication and hence is a ring.

When $D$ is a commutative domain, each element of $\mathbb{P}_D$ is expressible in terms of elements of $D$ and the basis units $1, i, j$ and $k$. Thus, we obtain

Corollary 3.3. If $D$ is a commutative domain, then $\text{Int}(\mathbb{P}_D)$ is a ring. In particular, $\text{Int}(\mathbb{P}_Z)$ is a ring.

Having defined $\text{Int}(\mathbb{P}_Z)$ and shown that it is a ring, we will spend the remainder of this paper examining its properties. In Section 4 we will investigate some of the prime and maximal ideals of $\text{Int}(\mathbb{P}_Z)$. Presently, we give a useful theorem regarding localizations of $\text{Int}(\mathbb{P}_Z)$.

By a multiplicative subset of a ring, we mean a set $S$ such that $1 \in S$, $0 \notin S$, and $S$ is closed under multiplication. When $D$ is a commutative Noetherian domain and $S$ is a multiplicative subset of $D$, it is known \cite{[2]} Thm. 1.2.3] that $\text{Int}(D)S^{-1} = \text{Int}(DS^{-1})$. This property also holds for $\text{Int}(\mathbb{P}_Z)$, as long as $S$ consists of integers.

Theorem 3.4. Let $S \subseteq \mathbb{Z}$ be a multiplicative set. Then, $\text{Int}(\mathbb{P}_Z)S^{-1} = \text{Int}(\mathbb{P}_ZS^{-1})$.

Proof. Our proof is an adaptation of \cite{[2]} Thm. 1.2.3], with modifications done to account for the noncommutative rings. First, let $f \in \text{Int}(\mathbb{P}_Z)^{-1}$, and let $\frac{a}{z} \in \mathbb{P}_ZS^{-1}$, where $s \in S$ and $q \in \mathbb{P}_Z$. We use induction on $n = \deg(f)$ to show that $f(\frac{a}{z}) \in \mathbb{P}_ZS^{-1}$.

There is nothing to prove if $n = 0$, so assume that $n > 0$ and that every polynomial in $\text{Int}(\mathbb{P}_Z)^{-1}$ of degree less than $n$ is an element of $\text{Int}(\mathbb{P}_ZS^{-1})$. Let $g(x) = s^n f(x) - f(sx)$. Since $s \in \mathbb{Z}$ is central in $\mathbb{P}_Q$, $f(sx)$ is a polynomial in $\text{Int}(\mathbb{P}_ZS^{-1})$, so $g \in \text{Int}(\mathbb{P}_Z)S^{-1}$. Furthermore, $\deg(g) < n$, so $g \in \text{Int}(\mathbb{P}_ZS^{-1})$. Note that $f(q) \in \mathbb{P}_ZS^{-1}$, so $s^n f(\frac{a}{z}) = g(\frac{a}{z}) + f(q) \in \mathbb{P}_ZS^{-1}$. But, $s$ is a unit in $\mathbb{P}_ZS^{-1}$, so we get $f(\frac{a}{z}) \in \mathbb{P}_ZS^{-1}$. Hence, $f \in \text{Int}(\mathbb{P}_ZS^{-1})$ and $\text{Int}(\mathbb{P}_ZS^{-1}) \subseteq \text{Int}(\mathbb{P}_Z)S^{-1}$.

To prove that $\text{Int}(\mathbb{P}_ZS^{-1}) \subseteq \text{Int}(\mathbb{P}_Z)^{-1}$, let $h \in \text{Int}(\mathbb{P}_ZS^{-1})$, let $M$ be the right $\mathbb{P}_Z$-module generated by the coefficients of $h$, and let $M'$ be the right $\mathbb{P}_Z$-module generated by $(h(q))_{q \in \mathbb{P}_Z}$. Then, $\mathbb{P}_Z$ is Noetherian (as a right module over itself) and $M$ is finitely generated, so $M$ is Noetherian as a right $\mathbb{P}_Z$-module. Since $M' \subseteq M$, $M'$ is also finitely generated. Let $p_1, p_2, \ldots, p_m \in \mathbb{P}_ZS^{-1}$ be generators for $M'$ as a right $\mathbb{P}_Z$-module.
By finding a common denominator, we see that there exists \( u \in S \) such that \( up_i \in \mathbb{P}_Z \) for each \( i \). Then, \( uM' = M'u \subseteq \mathbb{P}_Z \), which gives \( uh \in \text{Int}(\mathbb{P}_Z) \). Thus, \( h \in \text{Int}(\mathbb{P}_Z)S^{-1} \) and \( \text{Int}(\mathbb{P}_Z)S^{-1} \subseteq \text{Int}(\mathbb{P}_Z)S^{-1}. \)

In particular, the previous theorem holds when \( p \) is a prime \( (or p = 0) \) and \( S = \mathbb{Z} \setminus p\mathbb{Z} \). Thus, \( \text{Int}(\mathbb{P}_Z) \) behaves nicely with respect to localization at primes of \( \mathbb{Z} \). Let \( (\mathbb{P}_Z)(p) = \mathbb{P}_{Z(p)} \) be the localization of \( \mathbb{P}_Z \) at \( \mathbb{Z} \setminus p\mathbb{Z} \); note that \( (\mathbb{P}_Z)(0) = \mathbb{P}_Q \). When \( \mathcal{I} \) is an ideal of \( \text{Int}(\mathbb{P}_Z) \) containing \( p \), we let \( \mathcal{I}_p = \{ f(x)/n \in \text{Int}(\mathbb{P}_{Z(p)}) \mid f \in \mathcal{I} \text{ and } n \in \mathbb{Z} \setminus p\mathbb{Z} \} \) be the localization of \( \mathcal{I} \). Then, we have the following.

**Corollary 3.5.** With notation as above, \( \text{Int}(\mathbb{P}_Z)/\mathcal{I} \cong \text{Int}(\mathbb{P}_{Z(p)})/\mathcal{I}_p \)

**Proof.** This is proved just as in the commutative case. Let \( \pi : \text{Int}(\mathbb{P}_Z) \to \text{Int}(\mathbb{P}_Z)/\mathcal{I} \) be the quotient map. By Theorem 3.4, elements of \( \text{Int}(\mathbb{P}_{Z(p)}) \) may be written as \( \frac{f(x)}{n} \), where \( f \in \text{Int}(\mathbb{P}_Z) \) and \( n \in \mathbb{Z} \setminus p\mathbb{Z} \). Using this representation, \( n \) is invertible in \( \text{Int}(\mathbb{P}_Z)/\mathcal{I} \), since \( p \in \mathcal{I} \). So, we define a map \( \text{Int}(\mathbb{P}_{Z(p)}) \to \text{Int}(\mathbb{P}_Z)/\mathcal{I} \) by \( \frac{f(x)}{n} \to n^{-1}\pi(f(x)) \), and this function is a well-defined surjective ring homomorphism with kernel \( \mathcal{I}_p \). \( \square \)

We end this section with a short description of some of the elements of \( \text{Int}(\mathbb{P}_Z) \). Certainly, we have \( \mathbb{P}_Z[x] \subseteq \text{Int}(\mathbb{P}_Z) \), but there are other polynomials in \( \text{Int}(\mathbb{P}_Z) \).

In general, given a polynomial \( f \in \mathbb{P}_Q[x] \), we may write \( f(x) = g(x)/n \) for some \( g \in \mathbb{P}_Z[x] \) and some integer \( n > 0 \). Then, \( f \in \text{Int}(\mathbb{P}_Z) \) if and only if \( g(q) \in \mathbb{P}_Z \) for all \( q \in \mathbb{P}_Z \). Equivalently, \( f \in \text{Int}(\mathbb{P}_Z) \) if and only if \( g \) sends each element of the finite ring \( \mathbb{P}_Z/n\mathbb{P}_Z \) to 0 in \( \mathbb{P}_Z/n\mathbb{P}_Z \). Using these equivalences, one may produce many polynomials in \( \mathbb{P}_Z[x] \setminus \mathbb{P}_Z[x] \). For example, it is easy to verify that \( (1 + i + j + k)(x^2 - x)/2 \in \text{Int}(\mathbb{P}_Z) \). Moreover, it is known (I.1 Thm. 3) that the polynomial \( (x^p^2 - x)(x^p - x) \) kills each matrix in \( \mathbb{M}_2(\mathbb{P}_p) \). Thus, by Theorem 2.11, \( (x^p^2 - x)(x^p - x)/p \in \text{Int}(\mathbb{P}_Z) \) for each odd prime \( p \).

4. **Prime Ideals of \( \text{Int}(\mathbb{P}_Z) \)**

In the commutative case, there are standard ways to find some (but not necessarily all) prime ideals of \( \text{Int}(D) \) (see [2, Chap. V]). Primes above \( (0) \) have the form \( M(x) \cdot K[x] \cap \text{Int}(D) \), where \( M(x) \in K[x] \) is monic and irreducible. When \( P \) is a nonzero prime of \( D \) and \( a \in D \), the set \( \mathcal{P}_{P,a} = \{ f \in \text{Int}(D) \mid f(a) \in P \} \) constitutes a prime of \( \text{Int}(D) \) above \( P \).

For \( \mathbb{P}_Z \), we will attempt similar constructions and look for primes above \( (0) \), \( p\mathbb{P}_Z \) (where \( p \) is an odd prime of \( \mathbb{Z} \)), and \( \mathcal{M} = (1 + i, 1 + j) \). As we shall see, we must adapt our definitions and proofs to accommodate the noncommutative multiplication in \( \mathbb{P}_Z \).

The obvious way to extend the ideals \( \mathcal{P}_{P,a} \) to \( \mathbb{P}_Z \) is to consider sets of the form \( \{ f \in \text{Int}(\mathbb{P}_Z) \mid f(q) \in I \} \), where \( q \in \mathbb{P}_Z \) and \( I \) is an ideal of \( \mathbb{P}_Z \). Unfortunately, this set may fail to be an ideal if \( q \notin \mathbb{Z} \). For example, if \( q = i \) and \( I = (0) \), then the polynomial \( x - i \) is in the above set, but the polynomial \( (x - i)(x - j) = x^2 - (1 + i)j \) \( x + k \) is not, since evaluation at \( i \) yields \( 2k \). However, we obtain an effective definition by expanding the set of elements that must be mapped into \( I \).

**Definition 4.1.** For each \( q = a + bi + cj + dk \in \mathbb{P}_Z \), let \( C(q) = \{ a \pm bi \pm cj \pm dk \} \). Let \( I \) be an ideal of \( \mathbb{P}_Z \). We define \( \mathcal{P}_{I,q} = \{ f \in \text{Int}(\mathbb{P}_Z) \mid f(p) \in I \text{ for all } p \in C(q) \} \). When \( I = (0) \), we let \( \mathcal{P}_{0,q} = \mathcal{P}_{I,q} \), and when \( I = p\mathbb{P}_Z \), we let \( \mathcal{P}_{p,q} = \mathcal{P}_{I,q} \).
Note that if \( q \in \mathbb{Z} \), then \( C(q) = \{ q \} \). Also, for any \( q \in \mathbb{P}_Z \), if \( p \in C(q) \), then \( q \) and \( p \) have the same norm and trace, and hence the same minimal polynomial.

**Proposition 4.2.** Let \( I \) be an ideal of \( \mathbb{P}_Z \) and let \( q \in \mathbb{P}_Z \).

1. If \( I \) is generated by \( n \in \mathbb{Z} \), then \( \mathfrak{I}_{I,q} \) is an ideal of \( \text{Int}(\mathbb{P}_Z) \).
2. If \( I \) is a prime ideal of \( \mathbb{P}_Z \) and \( q \in \mathbb{Z} \), then \( \mathfrak{I}_{I,q} \) is a prime ideal of \( \text{Int}(\mathbb{P}_Z) \).

**Proof.** Given the definition of \( \mathfrak{I}_{I,q} \), (1) may be proved exactly as [2] Thm. 4.5. For (2), having \( q \in \mathbb{Z} \) implies that \((fg)(q) = f(q)g(q)\) for all \( f, g \in \mathbb{P}_Q[x] \). The result now follows easily. □

It remains to consider what happens when \( q \notin \mathbb{Z} \). For this, we will assume that \( I \) is a prime of \( \mathbb{P}_Z \) and will consider three cases: \( I = (0) ; I = p\mathbb{Z} \), \( p \) an odd prime, and lastly primes of \( \text{Int}(\mathbb{P}_Z) \) above \( \mathcal{M} = (1 + \text{i}, 1 + \text{j}) \).

**Primes above 0**

We begin with a negative condition.

**Proposition 4.3.** Let \( q \in \mathbb{P}_Z \). If the minimal polynomial \( m_q(x) \) of \( q \) is reducible, then \( \mathfrak{I}_{0,q} \) is not a prime ideal of \( \text{Int}(\mathbb{P}_Z) \).

**Proof.** The case \( q \in \mathbb{Z} \) gives an irreducible polynomial of degree one. So let \( q \notin \mathbb{Z} \) and \( m_q(x) = (x - A)(x - B) \) with \( A, B \in \mathbb{Z} \). Then by the centrality of \( x - A \) we have that \((x - A)\text{Int}(\mathbb{P}_Z)(x - B) = \text{Int}(\mathbb{P}_Z) \cdot m_q(x) \subseteq \mathfrak{I}_{0,q} \). But neither \( x - A \) nor \( x - B \) is in \( \mathfrak{I}_{0,q} \), so \( \mathfrak{I}_{0,q} \) is not prime. □

In Theorem 4.10 below, we show that the converse of Proposition 4.3 also holds; in other words, \( \mathfrak{I}_{0,q} \) is prime if and only if \( m_q(x) \) is irreducible. We begin with the following general description of \( \mathfrak{I}_{0,q} \).

**Proposition 4.4.** Let \( q \in \mathbb{P}_Z \). Then, \( \mathfrak{I}_{0,q} = m_q(x) \cdot \mathbb{P}_Q[x] \cap \text{Int}(\mathbb{P}_Z) \).

**Proof.** It is clear that polynomials of \( m_q(x) \cdot \mathbb{P}_Q[x] \) vanish at \( q \). So if we select in this set elements from \( \text{Int}(\mathbb{P}_Z) \), then we get elements of \( \mathfrak{I}_{0,q} \).

For the other containment, let \( f(x) \in \mathfrak{I}_{0,q} \). By definition \( f(x) \in \text{Int}(\mathbb{P}_Z) \). Since \( m_q(x) \) is monic, we may divide \( f(x) \) by \( m_q(x) \) to obtain \( f(x) = h(x)m_q(x) + r(x) \), for some \( h(x), r(x) \in \mathbb{P}_Q[x] \). If \( q \in \mathbb{Z} \), then \( m_q(x) \) is a linear polynomial and \( r(x) = p \) is in \( \mathbb{P}_Z \). Then evaluating \( f(x) \) at \( q \) we get \( p = 0 \) and \( f(x) \in m_q(x)\mathbb{P}_Q[x] \). If \( m_q(x) \) is of degree two, suppose that \( r(x) = \gamma x + \delta \), where \( \gamma, \delta \in \mathbb{P}_Q \). If \( q = a + b\text{i} + c\text{j} + d\text{k} \), then one of \( b, c \) and \( d \) is nonzero. Let us consider the case \( b \neq 0 \); the other cases are similar. For all \( p \in C(q) \) we have \( \gamma p + \delta = 0 \), and in particular \( \alpha := \gamma q + \delta = 0 \) and \( \beta := \gamma(a - b\text{i} + c\text{j} + d\text{k}) + \delta = 0 \). It follows that \( \alpha - \beta = 2b\text{i} = 0 \). Since \( \text{i} \) is invertible and \( 2b \) is a nonzero integer, we have \( \gamma = 0 \), and consequently \( \delta = 0 \). Thus, \( f(x) \in m_q(x)\mathbb{P}_Q[x] \) once again. □

In light of this result, we make the following definition.

**Definition 4.5.** For each \( M(x) \in \mathbb{Z}[x] \), we define \( \mathfrak{P}_{M(x)} = M(x) \cdot \mathbb{P}_Q[x] \cap \text{Int}(\mathbb{P}_Z) \).

Because each \( M(x) \) is central in \( \text{Int}(\mathbb{P}_Z) \), it is easy to check that \( \mathfrak{P}_{M(x)} \) forms an ideal of \( \text{Int}(\mathbb{P}_Z) \). As we shall see, \( \mathfrak{P}_{M(x)} \) is a prime ideal when \( M(x) \) is irreducible. To prove this, we will use a generalization of Euclid’s Lemma. We also need to extend the notion of bar conjugate to polynomials.
Definition 4.6. Given \( f(x) \in \mathbb{Q}[x] \), we may view \( f \) as a sum of products of polynomials in \( \mathbb{Q}[x] \) and the basis units: \( f(x) = f_0(x) + f_1(x)i + f_2(x)j + f_3(x)k \), for some uniquely determined \( f_r \in \mathbb{Q}[x] \), \( 0 \leq r \leq 3 \). We define the bar conjugate \( \overline{f}(x) \) of \( f(x) \) to be \( \overline{f}(x) = f_0(x) - f_1(x)i - f_2(x)j - f_3(x)k \). Equivalently, if \( f(x) = \sum_i q_i x^i \), then \( \overline{f}(x) = \sum_i q_i x^i \).

Under this definition, the analogues of Proposition 2.3 parts (1)–(3) hold for polynomials in \( \mathbb{Q}[x] \).

Lemma 4.7. Let \( f(x) \in \mathbb{Q}[x] \) and \( g(x) \in \mathbb{Q}[x] \). Let \( M(x) \in \mathbb{Q}[x] \) be an irreducible polynomial. Assume that \( M(x) \mid f(x)g(x) \) and \( M(x) \nmid f(x) \). Then, \( M(x) \mid g(x) \) in \( \mathbb{Q}[x] \).

Proof. By hypothesis, we have \( f(x)g(x) = M(x)h(x) \) for some \( h(x) \in \mathbb{Q}[x] \). Applying bar conjugation gives \( f(x)\overline{g}(x) = M(x)\overline{h}(x) \), since \( f(x) \) and \( M(x) \) have central coefficients. Thus \( f(x)\overline{g}(x) + \overline{M}(x) = M(x)(h(x) + \overline{h}(x)) \).

Since the last equality involves polynomials with rational coefficients, we must have \( M(x) \mid (g(x) + \overline{g}(x)) \). Using the notation of Definition 4.6, we get \( M(x) \mid 2g_0(x) \), implying that \( M(x) \mid g_0(x) \). Take now the polynomial \( hg(x) = -g_1(x) + g_0(x) \). Arguing as above with \( hg(x) \) instead of \( g(x) \) we obtain that \( M(x) \mid g_1(x) \). Similar steps show that that \( M(x) \mid g_2(x) \) and \( M(x) \mid g_3(x) \). Thus, \( M(x) \mid g(x) \) in \( \mathbb{Q}[x] \). \( \square \)

Theorem 4.8. Let \( M(x) \in \mathbb{Z}[x] \) be irreducible over \( \mathbb{Q} \). Then, \( \mathfrak{P}_{M(x)} \) is a prime ideal of \( \text{Int}(\mathbb{P}_x) \).

Proof. Let \( f(x) \) and \( g(x) \) in \( \text{Int}(\mathbb{P}_x) \) such that \( f(x)\text{Int}(\mathbb{P}_x)g(x) \subseteq \mathfrak{P}_{M(x)} \). If \( M(x) \mid g(x) \) we do not have anything to prove. So assume that \( M(x) \nmid g(x) \). Write \( f(x) = f_0(x) + f_1(x)i + f_2(x)j + f_3(x)k \).

By assumption, for each \( h(x) \in \text{Int}(\mathbb{P}_x) \) the polynomial \( M(x) \) divides the product \( f(x)h(x)g(x) \) over \( \mathbb{P}_x \). In particular \( M(x) \) divides the following polynomials in \( \mathbb{P}_x \): \( f(x)g(x) \), \(-if(x)\overline{g}(x) \), \( jf(x)\overline{g}(x) \), and \( kf(x)\overline{k}(g(x)) \). So, \( M(x) \) divides their sum \( [f(x) - if(x)i + jf(x)j + kf(x)k]g(x) = 4f_0(x)g(x) \), and since we are working over \( \mathbb{P}_x \), \( M(x) \mid f_0(x)g(x) \). By Lemma 4.7, \( M(x) \mid f_0(x) \).

Following the same steps with \( if(x) \) instead of \( f(x) \), we get that \( M(x) \mid f_1(x) \). Similarly, \( M(x) \) divides \( f_2(x) \) and \( f_3(x) \). Thus, \( M(x) \mid f(x) \), and therefore \( \mathfrak{P}_{M(x)} \) is prime.

By the previous theorem, each \( \mathfrak{P}_{M(x)} \) is a prime ideal of \( \text{Int}(\mathbb{P}_x) \) above 0. In fact, every prime of \( \text{Int}(\mathbb{P}_x) \) above 0 has this form.

Theorem 4.9. Let \( \mathfrak{P} \) be a prime ideal of \( \text{Int}(\mathbb{P}_x) \) above 0. Then, \( \mathfrak{P} = \mathfrak{P}_{M(x)} \) for some irreducible \( M(x) \in \mathbb{Z}[x] \).

Proof. By Theorem 3.4 and Corollary 3.5, localizing \( \mathfrak{P} \) at \((0)\) yields a prime \( \mathfrak{P}_0 \) of \( \text{Int}(\mathbb{P}_x)_0 = \text{Int}(\mathbb{P}_x) \cap \mathbb{Q}[x] \). Since \( \mathbb{P}_0 \cong M_2(\mathbb{Q}) \), \( \mathfrak{P}_0 \) is isomorphic to a prime ideal of \( M_2(\mathbb{Q}[x]) \cong M_2(\mathbb{Q}[x]) \). The prime ideals of \( M_2(\mathbb{Q}[x]) \), like \( \mathbb{Q}[x] \), are generated by irreducible polynomials. Thus, \( \mathfrak{P}_0 = M(x) \cdot \mathbb{P}_0[x] \) 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 \( \text{Int}(\mathbb{P}_x) \), we obtain \( \mathfrak{P} = \mathfrak{P}_{M(x)} \cap \text{Int}(\mathbb{P}_x) \). \( \square \)

Combining our previous results, we obtain the following.
Corollary 4.10.

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

2. Let \( q \in \mathbb{P}_\mathbb{Z} \). Then, \( \mathfrak{P}_{0,q} \) is prime if and only if \( m_q(x) \) is irreducible.

3. Let \( q_1, q_2 \in \mathbb{P}_\mathbb{Z} \). Then, \( \mathfrak{P}_{0,q_1} = \mathfrak{P}_{0,q_2} \) if and only if \( m_{q_1}(x) = m_{q_2}(x) \).

We can also describe what occurs with \( \mathfrak{P}_{0,q} \) when \( m_q(x) \) is reducible. For this, we need one more lemma.

Lemma 4.11. Let \( M(x) \neq N(x) \) be monic irreducible polynomials in \( \mathbb{Q}[x] \). Then, \( \mathfrak{P}_{M(x)} \cap \mathfrak{P}_{N(x)} = \mathfrak{P}_{M(x)N(x)} \).

Proof. The inclusion \( \supseteq \) is trivial. For the other inclusion, let \( f(x) \in \mathfrak{P}_{M(x)} \cap \mathfrak{P}_{N(x)} \). Then, \( f(x) = M(x)g(x) = N(x)h(x) \) for some \( g(x), h(x) \in \mathbb{P}_\mathbb{Q}[x] \). By Lemma 4.7, \( M(x) | h(x) \), so \( f(x) \in \mathfrak{P}_{M(x)N(x)} \).

Proposition 4.12. Let \( q \in \mathbb{P}_\mathbb{Z} \) be such that \( m_q(x) = (x-A)(x-B) \) for distinct integers \( A \) and \( B \). Then, \( \mathfrak{P}_{0,q} = \mathfrak{P}_{0,A} \cap \mathfrak{P}_{0,B} \).

Proof. Apply Proposition 4.4 and Lemma 4.11.

Primes above odd primes

Throughout this section, let \( p \) be an odd prime of \( \mathbb{Z} \) and let \( q = a + bi + cj + dk \in \mathbb{P}_\mathbb{Z} \). Let \( Z \) be such that \( \gcd(b,c,d) \) is prime to \( p \). It is likely that results similar to those in this section hold in the case where \( p \mid \gcd(b,c,d) \), but our proofs require that \( p \nmid \gcd(b,c,d) \). As before, we begin with a negative condition.

Proposition 4.13. If \( m_q(x) \in \mathbb{Z}[x] \) is reducible mod \( p \), then \( \mathfrak{P}_{p,q} \) is not a prime ideal of \( \text{Int}(\mathbb{P}_\mathbb{Z}) \).

Proof. Assume that \( m_q(x) \) factors mod \( p \) as \( m_q(x) = (x-A)(x-B) \), with \( A, B \in \mathbb{Z} \). Then, \( (x-A)\text{Int}(\mathbb{P}_\mathbb{Z})(x-B) \subseteq \mathfrak{P}_{p,q} \), but since \( \gcd(b,c,d) \) is prime to \( p \), neither \( x-A \) nor \( x-B \) moves \( q \) into \( p\mathbb{P}_\mathbb{Z} \).

The remainder of the theorems in this section rely on the localization properties proved in Section 3. Let \( R = \mathbb{Z}(p) \). Given an ideal \( \mathfrak{I} \) of \( \text{Int}(\mathbb{P}_\mathbb{Z}) \) containing \( p \), we let \( \mathfrak{I}_p \) be the localization of \( \mathfrak{I} \). Then, we have \( \text{Int}(\mathbb{P}_\mathbb{Z})/\mathfrak{I} \cong \text{Int}(R)/\mathfrak{I}_p \).

Assume that \( m_q(x) \) is irreducible mod \( p \). We will prove that \( \mathfrak{P}_{p,q} \) is a maximal ideal of \( \text{Int}(\mathbb{P}_\mathbb{Z}) \).

Lemma 4.14. Let \( f(x) \in \text{Int}(\mathbb{P}_R) \), and write \( f(x) = h(x)m_q(x) + \gamma x + \delta \), where \( h(x), \gamma x + \delta \in \mathbb{P}_\mathbb{Q}[x] \). Then, \( \gamma, \delta \in \mathbb{P}_R \).

Proof. For each \( p \in C(q) \), we have \( f(p) = \gamma p + \delta \in \mathbb{P}_R \). By making appropriate choices of \( p, p' \in C(q) \) and considering \( f(p) - f(p') \), we can get \( 2b\gamma, 2c\gamma, 2d\gamma \in \mathbb{P}_R \). Since \( 2 \) is invertible in \( R \), we get \( b\gamma, c\gamma, d\gamma \in \mathbb{P}_R \), and then \( \gamma \in \mathbb{P}_R \) since \( \gcd(b,c,d) \) is prime to \( p \).

Recalling our assumption that \( m_q(x) \) is irreducible mod \( p \) (hence irreducible over \( \mathbb{Q} \)), let \( \alpha \) be an algebraic integer that is a root of \( m_q(x) \).

Lemma 4.15. Let \( f(x) \in \text{Int}(\mathbb{P}_R) \). Then, \( f(\alpha) \in \mathbb{P}_{R[\alpha]} \).

Proof. With \( \gamma \) and \( \delta \) as above, we have \( f(\alpha) = \gamma \alpha + \delta \in \mathbb{P}_{R[\alpha]} \).
Let $F = (\mathbb{Z}/p\mathbb{Z})[\alpha] \cong \mathbb{F}_{p^2}$, the finite field with $p^2$ elements. Then, $\mathbb{F}_F \cong M_2(\mathbb{F}_{p^2})$, which is a simple ring. Let $\mathcal{J}_p$ be the localization of $\mathbb{Q}_{p,q}$. We will build a homomorphism from $\text{Int}(\mathbb{P}_f)$ to $\mathbb{P}_F$ with kernel $\mathcal{J}_p$. It follows that $\mathbb{Q}_{p,q}$ is a maximal ideal of $\text{Int}(\mathbb{F}_2)$.

Define $\sigma : \text{Int}(\mathbb{P}_f) \to \mathbb{P}_{R[q]}$ by $\sigma(f) = f(\alpha)$. This map is well-defined by Lemma 4.14 and it is a ring homomorphism because $\alpha$ is central. Let $\pi : \mathbb{P}_{R[q]} \to \mathbb{P}_F$ be the homomorphism given by reduction mod $p$. Then, $\tau = \pi \circ \sigma$ is a surjective ring homomorphism from $\text{Int}(\mathbb{P}_f)$ to $\mathbb{P}_F$. The kernel of $\tau$ is a maximal ideal of $\text{Int}(\mathbb{P}_f)$, and

$$\ker(\tau) = \{ f \in \text{Int}(\mathbb{P}_f) \mid \gamma \alpha + \delta \in p\mathbb{P}_{R[q]} \}, \quad \gamma \text{ and } \delta \text{ as in Lemma 4.14}$$

$$\subseteq \mathcal{J}_p$$

Since $\mathcal{J}_p \neq \text{Int}(\mathbb{P}_f)$, we must have $\mathcal{J}_p = \ker(\tau)$. Thus, $\mathbb{Q}_{p,q}$ is maximal and $\text{Int}(\mathbb{F}_2)/\mathbb{Q}_{p,q} \cong M_2(\mathbb{F}_{p^2})$.

Our findings are summarized in the following theorem.

**Theorem 4.16.** Let $q = a + bi + cj + dk \in \mathbb{F}_2 \setminus \mathbb{Z}$ be such that $\gcd(b, c, d)$ is prime to $p$. Then,

1. $\mathbb{Q}_{p,q}$ is prime if and only if $m_q(x)$ is irreducible mod $p$
2. If $\mathbb{Q}_{p,q}$ is prime, then it is in fact a maximal ideal, and $\text{Int}(\mathbb{F}_2)/\mathbb{Q}_{p,q} \cong M_2(\mathbb{F}_{p^2})$, the field with $p^2$ elements.

**Primes above $\mathcal{M}$**

The final case will consider regards prime ideals of $\text{Int}(\mathbb{F}_2)$ above $\mathcal{M} = (1+i, 1+j)$. In this instance, our analysis is quite different, since $\mathcal{M}$ is not generated by integers. In contrast to what we found with $\mathbb{Q}_{p,q}$, the ideals of $\text{Int}(\mathbb{F}_2)$ that we will discuss are similar to the prime ideals of $\text{Int}(D)$, where $D$ is a commutative domain. This appears to be because the residue ring $\mathbb{P}_Z/\mathcal{M} \cong \mathbb{F}_2$ is commutative.

**Definition 4.17.** For each $q \in \mathbb{F}_2$, we define $\mathcal{M}_q = \{ f \in \text{Int}(\mathbb{F}_2) \mid f(q) \in \mathcal{M} \}$.

Interestingly, the difficulty in working with $\mathcal{M}_q$ 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.

**Theorem 4.18.** Let $q \in \mathbb{F}_2$. Assume that $\text{Int}(\mathbb{F}_2)p \in \mathcal{M}_q$ for all $p \in \mathcal{M}$. Define $\phi : \text{Int}(\mathbb{F}_2) \to \mathbb{P}_Z/\mathcal{M}$ by $\phi(f) = f(q) \bmod \mathcal{M}$. Then, $\phi$ is a surjective homomorphism with kernel $\mathcal{M}_q$, and $\text{Int}(\mathbb{F}_2)/\mathcal{M}_q \cong \mathbb{F}_2$. Consequently, $\mathcal{M}_q$ is a maximal ideal of $\text{Int}(\mathbb{F}_2)$.

**Proof.** It is straightforward to prove that $\phi$ is additive, surjective, and has kernel $\mathcal{M}_q$. For multiplicativity, let $f, g \in \text{Int}(\mathbb{F}_2)$. It suffices to show that $(fg)(q)$ is equivalent mod $\mathcal{M}$ to $f(q)g(q)$.

Let $p = g(q) \in \mathbb{P}_Z$; then, $(fg)(q) = (fp)(q)$. If $p \in \mathcal{M}$, then we are done by assumption. If not, let $r = 1 + p \in \mathcal{M}$. Then, $(fr)(q) = f(q) + (fp)(q)$, and we see that $(fp)(q) \in \mathcal{M}$ if and only if $f(q) \in \mathcal{M}$. In this case, $\phi(g) = 1$ and we have $\phi(fg) = \phi(f)$, so we are done in this case as well. \(\square\)
Thus, to prove that $\mathcal{M}_q$ is a maximal ideal of $\text{Int}(\mathbb{P}_2)$, it suffices to prove that $\text{Int}(\mathbb{P}_2)p \in \mathcal{M}_q$ for each $q \in \mathbb{P}_2$ and $p \in \mathcal{M}$. We do not have proofs that work for arbitrary $q \in \mathbb{P}_2$, but we can establish the result in certain cases, depending on the coefficients of $q$.

We fix some notation concerning generators of $\mathcal{M}$. Throughout the rest of this section, let $\varepsilon = 1 + i$, $\lambda_1 = 1 + j$, $\lambda_2 = 1 + k$, $\lambda_3 = 2 + i + j$, and $\lambda_4 = 2 + i + k$. Observe then that $\mathcal{M} = (\varepsilon, \lambda_1) = (\varepsilon, \lambda_2) = (\varepsilon, \lambda_3) = (\varepsilon, \lambda_4)$. Furthermore, we have the following generalization of Lemma 2.8. The proof is identical to that of Lemma 2.8.

**Lemma 4.19.** Let $q \in \mathcal{M}$. Then, for each $1 \leq i \leq 4$ there exist $p, r \in \mathbb{P}_2$ such that $q = p \varepsilon + r \lambda_i$.

Since $\text{Int}(\mathbb{P}_2)$ is closed under multiplication on the right by elements of $\mathbb{P}_2$, to meet the condition needed in Theorem 4.18 it suffices to show that $\text{Int}(\mathbb{P}_2)\varepsilon$ and some $\text{Int}(\mathbb{P}_2)\lambda_i$ are in $\mathcal{M}_q$. As we shall see, this is not difficult to prove for $\varepsilon$ because $\mathbb{P}_2$ is closed under conjugation by $\varepsilon$. However, $N(\lambda_1) = N(\lambda_2) = 0$, so we do not have a corresponding result for $\lambda_1$ or $\lambda_2$. Nevertheless, we can obtain partial results by working instead with $\lambda_3$ and $\lambda_4$.

**Lemma 4.20.** Let $q = a + bi + cj + dk \in \mathbb{P}_2$. Then,

1. $\varepsilon q \varepsilon^{-1} \in \mathbb{P}_2$
2. if $b \equiv c \pmod{2}$, then $\lambda_3 q \lambda_3^{-1} \in \mathbb{P}_2$
3. if $b \equiv d \pmod{2}$, then $\lambda_4 q \lambda_4^{-1} \in \mathbb{P}_2$

**Proof.** Direct computation shows that

\[
\varepsilon q \varepsilon^{-1} = a + bi - dj + ck
\]
\[
\lambda_3 q \lambda_3^{-1} = a + (-d + \frac{3b-c}{2})i + (-d + \frac{-b+c}{2})j + (-b+c+d)k
\]
\[
\lambda_4 q \lambda_4^{-1} = a + (c + \frac{3b-d}{2})i + (b+c-d)j + (c + \frac{-b+d}{2})k
\]

(If verifying these by hand, it is easiest to first prove them for $q \in \{1, i, j, k\}$ and then extend linearly over $a, b, c, d$ to establish the general result). \hfill \square

**Proposition 4.21.** Let $q = a + bi + cj + dk \in \mathbb{P}_2$ and $h \in \text{Int}(\mathbb{P}_2)$. Then,

1. $he \in \mathcal{M}_q$
2. if $b \equiv c \pmod{2}$, then $h\lambda_3 \in \mathcal{M}_q$
3. if $b \equiv d \pmod{2}$, then $h\lambda_4 \in \mathcal{M}_q$

**Proof.** By Lemma 4.20, $\varepsilon q \varepsilon^{-1} \in \mathbb{P}_2$, so $(h\varepsilon)(q) = h(\varepsilon q \varepsilon^{-1}) \in \mathcal{M}$. If $b \equiv c \pmod{2}$, then $\lambda_3 q \lambda_3^{-1} \in \mathbb{P}_2$, so $(h\lambda_3)(q) = h(\lambda_3 q \lambda_3^{-1}) \lambda_3 \in \mathcal{M}$. Similarly, if $b \equiv d \pmod{2}$, then $(h\lambda_4)(q) \in \mathcal{M}$. \hfill \square

Applying Propositions 4.21 and Theorem 4.18 we obtain the following.

**Corollary 4.22.** Let $q = a + bi + cj + dk \in \mathbb{P}_2$, and assume that either $b \equiv c \pmod{2}$ or $b \equiv d \pmod{2}$. Then, $\mathcal{M}_q$ is a maximal ideal of $\text{Int}(\mathbb{P}_2)$.

It remains to consider the case where $q = a + bi + cj + dk \in \mathbb{P}_2$ and $b \not\equiv c$, $b \not\equiv d \pmod{2}$. This case is more difficult because we were not able to find an appropriate conjugation relation like those in Lemma 4.20. In fact, we suspect that such a conjugation relation may not exist. Nevertheless, we feel that $\mathcal{M}_q$ will once again be a maximal ideal of $\text{Int}(\mathbb{P}_2)$; it is just that the methods used in this paper are not sufficient to prove it.
5. Summary and Open Problems

Here, we summarize the main theorems of this paper, and mention directions for further research. First, we obtained useful results regarding the ring \( \mathbb{P}_Z \) of integer split quaternions.

**Theorem 5.1.**

1. \( \mathbb{P}_Z \) is isomorphic to the subring \( \mathcal{A} = \{ (a, b) \mid a \equiv d, b \equiv c \mod 2 \} \) of \( M_2(\mathbb{Z}) \).
2. The prime ideals of \( \mathbb{P}_Z \) are the trivial ideal \((0)\), the principal ideals \( p\mathbb{P}_Z \) generated by odd prime integers \( p \), and the nonprincipal \( \mathcal{M} = (1 + i, 1 + j) \), which contains \( 2 \). All these ideals, except \((0)\), are maximal.

We next defined the set \( \text{Int}(\mathbb{P}_Z) \) of integer-valued polynomials over \( \mathbb{P}_Z \). Despite the difficulties arising from the noncommutativity of polynomial multiplication, we proved that \( \text{Int}(\mathbb{P}_Z) \) is indeed a ring (Corollary 3.3). Moreover, \( \text{Int}(\mathbb{P}_Z) \) behaves well with localization at sets of integers (Theorem 3.4).

The latter half of the paper focused on ideals of \( \text{Int}(\mathbb{P}_Z) \). For the most part, we cannot use the definition of ideals \( \mathfrak{I}_{I,a} \) common in the commutative setting. However, some ideals can be produced by modifying the definition of \( \mathfrak{I}_{I,a} \) (Definitions 4.1 and 4.17). We finished by investigating the primality and maximality of these ideals.

**Theorem 5.2.** Let \( q = a + bi + cj + dk \in \mathbb{P}_Z \).

1. Every prime ideal of \( \text{Int}(\mathbb{P}_Z) \) above \( (0) \) has the form \( \mathfrak{P}_{M(x)} \) for some irreducible \( M(x) \in \mathbb{Z}[x] \).
2. \( \mathfrak{P}_{0,q} = m_q(x) \cdot \mathbb{Q}[x] \cap \text{Int}(\mathbb{P}_Z) \), and \( \mathfrak{P}_{0,q} \) is prime if and only if \( m_q(x) \) is irreducible over \( \mathbb{Q} \).
3. When \( p \) is an odd prime and \( p \nmid \gcd(b,c,d) \) (implying that \( q \notin \mathbb{Z} \)), then \( \mathfrak{P}_{p,q} \) is prime if and only if \( m_q(x) \) is irreducible mod \( p \). If \( \mathfrak{P}_{p,q} \) is prime, then it is maximal, and \( \text{Int}(\mathbb{P}_Z)/\mathfrak{P}_{p,q} \cong M_2(\mathbb{F}_{p^2}) \).
4. If either \( b \equiv c \mod 2 \) or \( b \equiv d \mod 2 \), then \( \mathfrak{M}_q \) is a maximal ideal of \( \text{Int}(\mathbb{P}_Z) \), and \( \text{Int}(\mathbb{P}_Z)/\mathfrak{M}_q \cong \mathbb{F}_2 \).

Even confining oneself to the ring \( \text{Int}(\mathbb{P}_Z) \) (and saying nothing of integer-valued polynomials over other noncommutative rings!), there are several topics that warrant further research. First, there is the matter of completing the classification of prime and maximal ideals in \( \text{Int}(\mathbb{P}_Z) \). In discussing primes above the nonzero primes of \( \mathbb{P}_Z \), we had to make certain assumptions about the coefficients of \( q \). It is our thought that similar results hold in the cases not considered here, and that perhaps different techniques may lead to more effective proofs. Even so, this need not give a complete classification. In the commutative case, the \( p \)-adic completion of \( \mathbb{Z} \) is used to identify all the primes of \( \text{Int}(\mathbb{Z}) \). So, studying quaternions with \( p \)-adic integer coefficients may be helpful when working with \( \text{Int}(\mathbb{P}_Z) \).

Another avenue for investigation involves localizing \( \text{Int}(\mathbb{P}_Z) \) at sets that are not contained in \( \mathbb{Z} \). Noncommutative localization (discussed in [7, Chap. 4]) has its own difficulties, but could prove to be a powerful tool for studying \( \text{Int}(\mathbb{P}_Z) \) and related structures.

Finally, we recall that it remains an open question whether there exists a noncommutative \( \mathbb{Z} \)-algebra \( A \) such that \( \text{Int}(A) \) (suitably defined) is not a ring. Indeed, this question is unanswered even when \( A \) is a general quaternion algebra over \( \mathbb{Z} \). In
proving that $\text{Int}(\mathbb{P}_Z)$ is a ring, we used Theorem 3.2, which relies on the assumption that elements of $A$ are sums of units times central elements. However, this condition need not be true in a general quaternion algebra, so a new approach is necessary.

References