Integer-valued Polynomials over Quaternion Rings

Nicholas J. Werner

Department of Mathematics, The Ohio State University, 231 West 18th Avenue,
Columbus, OH 43210

Abstract
When $D$ is an integral domain with field of fractions $K$, the ring $\text{Int}(D) = \{f(x) \in K[x] \mid f(D) \subseteq D\}$ of integer-valued polynomials over $D$ has been extensively studied. We will extend the integer-valued polynomial construction to certain noncommutative rings. Specifically, let $i, j, k$ be the standard quaternion units satisfying the relations $i^2 = j^2 = -1$ and $ij = k = -ji$, and define $\mathbb{Z}Q := \{a+bi+cj+dk \mid a, b, c, d \in \mathbb{Z}\}$. Then, $\mathbb{Z}Q$ is a noncommutative ring that lives inside the division ring $\mathbb{Q}Q := \{a+bi+cj+dk \mid a, b, c, d \in \mathbb{Q}\}$.

For any ring $R$ such that $\mathbb{Z}Q \subseteq R \subseteq \mathbb{Q}Q$, we define the set of integer-valued polynomials over $R$ to be $\text{Int}(R) := \{f(x) \in \mathbb{Q}Q[x] \mid f(R) \subseteq R\}$. We will demonstrate that $\text{Int}(R)$ is a ring, discuss how to generate some elements of $\text{Int}(\mathbb{Z}Q)$, prove that $\text{Int}(\mathbb{Z}Q)$ is non-Noetherian, and describe some of the prime ideals of $\text{Int}(\mathbb{Z}Q)$.

1. Introduction and notation

When $D$ is an integral domain with field of fractions $K$, considerable research has been conducted regarding the ring $\text{Int}(D) = \{f(x) \in K[x] \mid f(D) \subseteq D\}$ of integer-valued polynomials over $D$; the book [1] by Cahen and Chabert is an excellent reference for the subject. The purpose of this paper is to extend the integer-valued polynomial construction to a class of noncommutative rings.

All rings under consideration are assumed to have a multiplicative identity, but are not necessarily commutative.
Definition 1.1. Given any ring $S$, we define the $S$-algebra $SQ$ to be $SQ = \{a + bi + cj + dk \mid a, b, c, d \in S\}$, where the symbols $i, j, k$ satisfy the relations $i^2 = j^2 = -1$ and $ij = k = -ji$. We refer to $i, j, k$ as the quaternion units, and we shall call $SQ$ the quaternion ring with coefficients in $S$.

Note that if $\text{char}(S) \neq 2$, then $SQ$ is noncommutative, since $ij \neq ji$. Generally, we will work with $SQ$, where $S$ is either an overring of $\mathbb{Z}$ in $\mathbb{Q}$ or a quotient ring of $\mathbb{Z}$, and our primary focus will be on the quaternion ring $\mathbb{Z}Q := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\}$.

Readers may be familiar with a ring closely associated to $\mathbb{Z}Q$ and usually called the ring of Hurwitz integers, which we define to be $\mathbb{Z}H := \mathbb{Z}Q[\frac{1+i+j+k}{2}]$. The ring $\mathbb{Z}H$ was studied by Adolf Hurwitz in [5], where he determined that, among other interesting properties, $\mathbb{Z}H$ is a principal ideal ring [5, p. 31]. As we shall see, rings that contain the element $1+i+j+k$ in addition to $i, j, k$ play an important role in classifying quaternion rings over $\mathbb{Z}$. This leads to the following definition.

Definition 1.2. Let $\mu = \frac{1+i+j+k}{2}$, which we refer to as the Hurwitz unit. For any ring $S$, we define the $S$-algebra $SH$ to be $SH = SQ[\mu]$.

The notations $SQ$ and $SH$ are meant to be suggestive. The $Q$ in $SQ$ indicates the presence of the quaternion units $i, j, k$, and the $H$ in $SH$ indicates the presence of $i, j, k$ along with the Hurwitz unit $\mu$. By a quaternion ring, we mean a ring of form $SQ$ or $SH$.

Whenever $S$ is an overring of $\mathbb{Z}$ in $\mathbb{Q}$, the quaternion rings $SQ$ and $SH$ lie inside the ring $\mathbb{Q}Q$, and $\mathbb{Q}Q$ itself lives inside the Hamiltonians, the ring of quaternions with coefficients in $\mathbb{R}$, which we denote by $\mathbb{H}$. For any $\alpha = a + bi + cj + dk \in \mathbb{H}$, we refer to $a, b, c, d$ as the coefficients of $\alpha$. In particular, we often call $a$ the constant coefficient of $\alpha$. Furthermore, we define the bar conjugate of $\alpha$ to be $\overline{\alpha} = a - bi - cj - dk$, and define the norm of $\alpha$ to be $N(\alpha) = a^2 + b^2 + c^2 + d^2$. The reason that $\overline{\alpha}$ is not called simply the conjugate of $\alpha$ is because we shall frequently look at quaternions of the form $\omega u^{-1}$, which are the multiplicative conjugates of $\alpha$. Thus, the term conjugate, if left unqualified, can be ambiguous.

Elements $\alpha$ and $\beta$ of $\mathbb{H}$ satisfy the following properties:

\[ N(\alpha\beta) = N(\alpha)N(\beta) \] (i.e., the norm is multiplicative)

\[ \alpha\overline{\alpha} = N(\alpha) = \overline{\alpha}\alpha \]

for all $\alpha \neq 0$, $\alpha^{-1} = \frac{\overline{\alpha}}{N(\alpha)}$. 

2
Note that the above expression for $\alpha^{-1}$ tells us $\mathbb{Q} Q$ is actually a division ring, since for any $\alpha \in \mathbb{Q} Q$ we have $\overline{\alpha} \in \mathbb{Q} Q$ and $N(\alpha) \in \mathbb{Q}$. Also, note that $N(\mu) = 1$, so whenever $\mu$ is in a quaternion ring $R$, its inverse $\mu = \frac{1-i-j-k}{2} = \mu - i - j - k$ is also in $R$. Thus, we are justified in referring to $\mu$ as the Hurwitz unit.

One can verify that for any $\alpha \in \mathbb{H}$ with constant coefficient $a$, we have

$$\alpha^2 = 2aa - N(\alpha).$$

This identity implies that $\alpha$ satisfies a monic quadratic polynomial with real coefficients, namely $x^2 - 2ax + N(\alpha) \in \mathbb{R}[x]$. For any $\alpha \in \mathbb{H}$ with constant coefficient $a$, we define the minimal polynomial of $\alpha$ to be

$$\min_\alpha(x) = \begin{cases} x^2 - 2ax + N(\alpha), & \alpha \notin \mathbb{R} \\ x - a, & \alpha \in \mathbb{R}. \end{cases}$$

A fact that we shall use frequently is the following:

for any $\alpha$ and $\beta$ in $\mathbb{H}$, $\min_\alpha(x) = \min_\beta(x)$ if and only if $\alpha$ and $\beta$ share the same norm and constant coefficient.

2. Integer-valued polynomials

We begin with a definition.

**Definition 2.1.** For any overring $R$ of $\mathbb{Z}Q$ in $\mathbb{Q}Q$, we define the set of integer-valued polynomials over $R$ to be $\text{Int}(R) := \{f(x) \in \mathbb{Q}Q[x] \mid f(R) \subseteq R\}$.

We wish to show that $\text{Int}(R)$ has a ring structure under the usual addition and multiplication of polynomials. In the case where $D$ is a domain with field of fractions $K$, it is straightforward to prove that $\text{Int}(D)$ is a ring, since for any $f, g \in K[x]$ and any $a \in D$ we have $(f+g)(a) = f(a)+g(a)$ and $(fg)(a) = f(a)g(a)$ (here, as elsewhere in this paper, $(fg)(x)$ denotes the product of the polynomials $f(x)$ and $g(x)$). However, if $R$ is a noncommutative ring, $f, g \in R[x]$, and $\alpha \in R$, then it is not true in general that $(fg)(\alpha)$ equals $f(\alpha)g(\alpha)$. Thus, for an overring $R$ of $\mathbb{Z}Q$, it is nontrivial to show that $\text{Int}(R)$ is closed under multiplication. In Theorem 2.3 below, we shall prove that $\text{Int}(R)$ is in fact a ring whenever $R$ is an overring of $\mathbb{Z}Q$, but before doing so we give a classification theorem for overrings of $\mathbb{Z}Q$ in $\mathbb{Q}Q$. This result was known to Hurwitz [5, p. 22] in a slightly different form.
Theorem 2.2. Let $R$ be any overring of $\mathbb{Z}Q$ in $\mathbb{Q}Q$ and let $S = R \cap \mathbb{Q}$. Then, the following hold:

(i) either $R = SQ$ or $R = SH$.

(ii) $R = SQ \iff$ every coefficient of every element of $R$ is in $R$.

(iii) if $R = SH$, then for each $\alpha \in R$ there exist $\alpha' \in SQ$ and $e \in \{0,1\}$ such that $\alpha = \alpha' + e\mu$.

Using this classification theorem, we can prove that $\text{Int}(R)$ has a ring structure.

Theorem 2.3. Let $R$ be any overring of $\mathbb{Z}Q$ in $\mathbb{Q}Q$. Then, $\text{Int}(R)$ is a ring.

Proof. It is easy to see that $\text{Int}(R)$ is an additive subgroup of the polynomial ring $\mathbb{Q}Q[x]$, so it suffices to prove that $\text{Int}(R)$ is closed under multiplication. Toward that end, let $f(x), g(x) \in \text{Int}(R)$, and let $\alpha \in R$. It suffices to show that $(fg)(\alpha) \in R$.

Write $f(x) = \sum_r \alpha_r x^r \in \text{Int}(R)$, where each $\alpha_r \in \mathbb{Q}Q$. Notice that if $u$ is any unit in $R$ and $\beta$ is an arbitrary element of $R$, then

$$(fu)(\beta) = \sum_r \alpha_r u\beta^r = \sum_r \alpha_r (u\beta u^{-1})^r u = f(u\beta u^{-1})u.$$ Since $f \in \text{Int}(R)$, we have $f(u\beta u^{-1})u \in R$. Thus, $fu \in \text{Int}(R)$.

Next, since $g(x) \in \text{Int}(R)$, $g(\alpha) \in R$. Let $S = R \cap \mathbb{Q}$. Then, by Theorem 2.2, $R \subseteq SH$, and $g(\alpha) = a + bi + cj + dk + e\mu$ where $a, b, c, d \in S$ and $e \in \{0,1\}$. Now, we may write the polynomial $(fg)(x)$ as $(fg)(x) = (\sum_r \alpha_r x^r) g(x) = \sum_r \alpha_r g(x) x^r$. We have

$$(fg)(\alpha) = \sum_r \alpha_r g(\alpha) \alpha^r$$

$$= \sum_r \alpha_r (a + bi + cj + dk + e\mu) \alpha^r$$

$$= a \sum_r \alpha_r \alpha^r + b \sum_r \alpha_r i\alpha^r + c \sum_r \alpha_r j\alpha^r$$

$$+ d \sum_r \alpha_r k\alpha^r + e \sum_r \alpha_r \mu\alpha^r$$

$$= af(\alpha) + b(fi)(\alpha) + c(fj)(\alpha) + d(fk)(\alpha) + e(f\mu)(\alpha).$$
We know that $i, j, k \in \mathbb{R}$, so $af(\alpha) + b(fi)(\alpha) + c(fj)(\alpha) + d(fk)(\alpha) \in \mathbb{R}$. If $\mu \in \mathbb{R}$, then $e(f\mu)(\alpha) \in \mathbb{R}$; if $\mu \notin \mathbb{R}$, then $e = 0$ and $g(\alpha) \in SQ$. In either case, we get $(fg)(\alpha) \in \mathbb{R}$ and $fg \in \text{Int}(R)$. Thus $\text{Int}(R)$ is closed under multiplication, and hence is a ring. 

Remark. It is worth noting that the proof of Theorem 2.3 can be extended to other types of rings. For example, let $G$ be any finite group, and let $\mathbb{Z}G$ and $\mathbb{Q}G$ be the standard group rings. If we define $\text{Int}(\mathbb{Z}G) := \{f \in \mathbb{Q}G[x] \mid f(\mathbb{Z}G) \subseteq \mathbb{Z}G\}$, then the steps in the above proof can be used to show that $\text{Int}(\mathbb{Z}G)$ is a ring. The key to the proof is that $\mathbb{Z}G$ can be generated over $\mathbb{Z}$ by a set consisting entirely of units: the elements of $G$. In fact, if we let $Q_8$ denote the quaternion group, then working with the group ring $\mathbb{Z}Q_8$ could yield information about $\mathbb{Z}Q$, since $\mathbb{Z}Q$ is a quotient ring of the group ring $\mathbb{Z}Q_8$. We may also construct integer-valued polynomials over the ring $M_n(\mathbb{Z})$ of $n \times n$ matrices over $\mathbb{Z}$ if we define $\text{Int}(M_n(\mathbb{Z})) := \{f \in M_n(\mathbb{Q})[x] \mid f(M_n(\mathbb{Z})) \subseteq M_n(\mathbb{Z})\}$. We note that in [3], S. Frisch studied a similar structure, the ring of polynomials $\text{Mint}_n(D) = \{f(x) \in K[x] \mid \forall A \in M_n(D), f(A) \in M_n(D)\}$, where $D$ is a domain with field of fractions $K$. More generally, it should be possible to extend the proof of Theorem 2.3 to certain “suitable” $\mathbb{Z}$-algebras that can be generated over $\mathbb{Z}$ by units; however, it is not clear how to describe such a “suitable” algebra, and we will not consider this topic any further for the time being.

Knowing that $\text{Int}(R)$ is a ring for any overring $R$ of $\mathbb{Z}Q$ opens up a multitude of avenues for investigation. Any question that arises in the study of integer-valued polynomials over domains can be considered in the noncommutative case, although definitions, proofs, and oftentimes the statement of such a question must be modified to work in the new setting. Given the scope of the situation, our strategy is to work things out for $\text{Int}(\mathbb{Z}Q)$ and then try to adapt our theorems for overrings of $\mathbb{Z}Q$. In accordance with this plan, the rest of this paper will focus on $\text{Int}(\mathbb{Z}Q)$. In Section 5, we will mention some strategies to extend these results to other rings.

3. Elements of $\text{Int}(\mathbb{Z}Q)$

In this section, we will exhibit some of the elements of $\text{Int}(\mathbb{Z}Q)$, and establish part of a generating set for $\text{Int}(\mathbb{Z}Q)$ over $\mathbb{Z}Q$. Our basic strategy in determining elements of $\text{Int}(\mathbb{Z}Q)$ is as follows. Given $f(x) \in \text{Int}(\mathbb{Z}Q)$, we
may write \( f(x) = \frac{g(x)}{n} \) for some \( g(x) \in \mathbb{Z}Q[x] \) and some \( n \in \mathbb{Z}, n > 0 \). Then, \( g(x) \) is a polynomial in \( \mathbb{Z}Q[x] \) such that \( g(\alpha) \equiv 0 \mod n \) for all \( \alpha \in \mathbb{Z}Q \). Here, to say that \( \beta \in \mathbb{Z}Q \) is equivalent to \( 0 \mod n \) means that \( \beta \) is in the ideal \((n)\) of \( \mathbb{Z}Q \) generated by \( n \), or, equivalently, that each coefficient of \( \beta \) is divisible by \( n \). This leads to the following definition.

**Definition 3.1.** For each \( n > 0 \), let \( I_n = \{ f(x) \in \mathbb{Z}Q[x] \mid f(\alpha) \equiv 0 \mod n \text{ for all } \alpha \in \mathbb{Z}Q \} \).

As described above, there is a correspondence between polynomials in \( \text{Int}(\mathbb{Z}Q) \) and polynomials in \( I_n \): \( f(x) \in \text{Int}(\mathbb{Z}Q) \) can be written as \( \frac{g(x)}{n} \) with \( g(x) \in \mathbb{Z}Q[x] \) and \( n > 0 \) if and only if \( g(x) \in I_n \). If we can determine how to generate the polynomials in each \( I_n \), then we will have a method for generating polynomials in \( \text{Int}(\mathbb{Z}Q) \). So, our focus becomes the study of the sets \( I_n \). Our first result show that \( I_n \) is always an ideal of \( \mathbb{Z}Q[x] \) (throughout this paper, the term *ideal* refers to a two-sided ideal).

**Proposition 3.2.** Let \( n > 0 \). Then, \( I_n \) is an ideal of \( \mathbb{Z}Q[x] \).

**Proof.** It is easy to see that \( I_n \) is closed under addition. Let \( f \in I_n \), let \( g \in \mathbb{Z}Q[x] \), and let \( \alpha \in \mathbb{Z}Q \). We need to show that \( (fg)(\alpha) \) and \( (gf)(\alpha) \) are both equivalent to \( 0 \mod n \). Write \( g(\alpha) = a + bi + cj + dk \). Then, as in Theorem 2.3,

\[
(fg)(\alpha) = af(\alpha) + bf(-i\alpha)i + cf(-j\alpha)j + df(-k\alpha)k
\]

and since \( f \in I_n \), each of \( f(\alpha) \), \( f(-i\alpha) \), \( f(-j\alpha) \), and \( f(-k\alpha) \) is equivalent to \( 0 \mod n \). Hence, \( (fg)(\alpha) \equiv 0 \mod n \).

Next, let \( g(x) = \sum_r \beta_r x^r \). Then, since \( f(\alpha) \equiv 0 \mod n \), we get \( (gf)(\alpha) \equiv \sum_r \beta_r f(\alpha)\alpha^r \equiv 0 \mod n \). Thus, \( fg, gf \in I_n \), and \( I_n \) is in ideal of \( \mathbb{Z}Q[x] \). \( \square \)

Certainly, if \( f \in \mathbb{Z}Q[x] \) and \( n > 0 \), then \( nf \in I_n \). The next proposition shows a way to produce some monic polynomials in \( I_n \).

**Proposition 3.3.** Let \( n > 0 \). Then, \( I_n \) contains a monic polynomial with coefficients in \( \mathbb{Z} \).

**Proof.** Given any \( \alpha \in \mathbb{Z}Q \) with constant coefficient \( a \), the minimal polynomial of \( \alpha \) divides \( x^2 - 2ax + N(\alpha) \in \mathbb{Z}[x] \). Let \( T = \{ x^2 + 2bx + c \in \mathbb{Z}Q[x] \mid b, c \in \{0, 1, \ldots, n - 1\} \} \) and let \( f(x) = \prod_{g(x) \in T} g(x) \). Then, \( f(x) \) is monic and has coefficients in \( \mathbb{Z} \), and since each \( g(x) \in T \) is central in \( \mathbb{Z}Q[x] \) we have
\[ f(\alpha) = \prod_{g(x) \in T} g(\alpha) \] for each \( \alpha \in \mathbb{Z}Q \). Now, for each \( \alpha \in \mathbb{Z}Q \), the reduction of \( \min_\alpha(x) \mod n \) divides some element of \( T \), so \( f(\alpha) \equiv 0 \mod n \). Thus, \( f \in I_n \), as desired.

We have established that \( I_n \) always contains a monic polynomial with coefficients in \( \mathbb{Z} \). So, among all such polynomials in \( I_n \), there must be one of minimal degree. In light of this, we make the following definition.

**Definition 3.4.** For each \( n > 0 \), let \( \phi_n \) be a monic polynomial of minimal degree in \( I_n \cap \mathbb{Z}[x] \).

We make no claims about the uniqueness of any \( \phi_n \); for each \( n \), there will be numerous choices for a \( \phi_n \). However, in the results that follow, no uniqueness will be required. So, the reader may assume at this point that we have fixed \( \phi_n \) for each \( n \). As we will show later, the collection of \( \phi_n \) will help comprise a generating set for \( \text{Int}(\mathbb{Z}Q) \) over \( \mathbb{Z}Q \) (and selecting different polynomials \( \phi_n \) will give different generating sets).

At the present time, we can say little about what \( \phi_n \) is for a general \( n \), but we do have enough information to describe \( \phi_p \) for an odd prime \( p \). We shall do this below, after proving a lemma.

**Lemma 3.5.** Let \( p \) be an odd prime and let \( f(x) \) be a monic quadratic polynomial in \( \mathbb{Z}[x] \). Then, there exists \( \alpha \in \mathbb{Z}Q \) such that

(i) \( f(\alpha) \equiv 0 \mod p \), and

(ii) for all \( a \in \mathbb{Z} \), \( \alpha \not\equiv a \mod p \)

Proof. Let \( f(x) = x^2 + Ax + B \in \mathbb{Z}[x] \). Then, \( A \equiv -2a \mod p \) for some \( a \in \mathbb{Z} \). It suffices to show that we can find \( b, c, d \in \mathbb{Z} \), not all equivalent to 0 mod \( p \), such that \( b^2 + c^2 + d^2 \equiv B - a^2 \mod p \). Then, \( \alpha = a + bi + cj + dk \) will be an element of \( \mathbb{Z}Q \) with the desired properties.

If \( B - a^2 \not\equiv 0 \mod p \), then since every element of the finite field \( \mathbb{Z}/p\mathbb{Z} \) is a sum of two squares, we can find \( b, c \in \mathbb{Z} \) such that \( b^2 + c^2 \equiv B - a^2 \), and at least of \( b \) or \( c \) is necessarily non-zero mod \( p \). If \( B - a^2 \equiv 0 \), then find \( b \) and \( c \) such that \( b^2 + c^2 \equiv -1 \), and take \( d = 1 \). In either case, we have \( \min_\alpha(x) \equiv x^2 + Ax + B \equiv f(x) \), so \( f(\alpha) \equiv 0 \). Furthermore, one of \( b, c, \) or \( d \) is non-zero mod \( p \), so the residue of \( \alpha \mod p \) is not congruent to an integer. Thus, the lemma holds. \( \square \)
Theorem 3.6. Let \( p \) be an odd prime. Then, \((x^{p^2} - x)(x^p - x)\) is a monic polynomial of minimal degree in \( I_p \cap \mathbb{Z}[x] \). Hence, we may take \( \phi_p(x) = (x^{p^2} - x)(x^p - x) \).

Proof. Let \( m(x) \) be any monic quadratic polynomial in \( \mathbb{Z}[x] \). By Lemma 3.5, there exists \( \alpha = a + bi + cj + dk \in \mathbb{Z}Q \) such that \( m(\alpha) \equiv 0 \mod p \) and \( \alpha \) is not congruent to an integer modulo \( p \); the latter condition means that one of \( b, c, \) or \( d \) is not equivalent to 0 mod \( p \). WLOG, assume that \( b \neq 0 \mod p \).

Now, let \( f(x) \in I_p \cap \mathbb{Z}[x] \). We can divide \( f(x) \) by \( m(x) \) to get

\[
  f(x) = g(x)m(x) + sx + t
\]

for some \( g(x), sx + t \in \mathbb{Z}[x] \). Since \( f(x) \in I_p \), we have

\[
  0 \equiv f(\alpha) \equiv sa + t \equiv (sa + t) + sbi + scj + sdk \mod p.
\]

Since \( b \neq 0 \), we must have \( s \equiv 0 \). But, \( sa + t \equiv 0 \), so \( t \equiv 0 \). Thus, \( f(x) \equiv g(x)m(x) \mod p \) and so \( m(x) \) divides \( f(x) \mod p \).

Since \( m(x) \) and \( f(x) \) were arbitrary, we conclude that every polynomial in \( I_p \cap \mathbb{Z}[x] \) is divisible mod \( p \) by every monic quadratic polynomial in \( (\mathbb{Z}/p\mathbb{Z})[x] \).

Thus, for \( \phi_p(x) \) to be a monic polynomial of minimal degree in \( I_p \cap \mathbb{Z}[x] \), the residue of \( \phi_p(x) \) modulo \( p \) must be the least common multiple in \( (\mathbb{Z}/p\mathbb{Z})[x] \) of every monic quadratic polynomial in \( (\mathbb{Z}/p\mathbb{Z})[x] \).

We claim that \((x^{p^2} - x)(x^p - x)\) is the required least common multiple. Indeed, the product of all the monic irreducible polynomials in \( (\mathbb{Z}/p\mathbb{Z})[x] \) of degree 1 or 2 is \( x^{p^2} - x \). To account for all the reducible quadratic polynomials, we must include an additional factor of \( x(x - 1) \cdots (x - (p - 1)) \equiv x^p - x \). So, \((x^{p^2} - x)(x^p - x)\) is the necessary least common multiple. Hence, \( \phi_p(x) \equiv (x^{p^2} - x)(x^p - x) \mod p \) and we may take \( \phi_p(x) = (x^{p^2} - x)(x^p - x) \) in \( I_p \).

Corollary 3.7. For each odd prime \( p \), \( (x^{p^2} - x)(x^p - x) \in \text{Int}(\mathbb{Z}Q) \).

Now that we know some elements of \( \text{Int}(\mathbb{Z}Q) \), we can prove the following.

Theorem 3.8. The ring \( \text{Int}(\mathbb{Z}Q) \) is non-Noetherian.

Proof. Let \( p_1, p_2, \ldots \) be all the (distinct) odd primes in \( \mathbb{Z} \). For each \( t > 0 \), let \( J_t = (\frac{\phi_{p_1}(x)}{p_1}, \frac{\phi_{p_2}(x)}{p_2}, \ldots, \frac{\phi_{p_t}(x)}{p_t}) \) in \( \text{Int}(\mathbb{Z}Q) \). We will show that \( \frac{\phi_{p_{t+1}}(x)}{p_{t+1}} \notin J_t \) for each \( t > 0 \), and this will allow us to produce a strictly increasing chain of ideals in \( \text{Int}(\mathbb{Z}Q) \).

8
Fix $t > 0$ and suppose by way of contradiction that $\frac{\phi_{p_{t+1}}(x)}{p_{t+1}} \in J_t$. Since each $\frac{\phi_{p_r}(x)}{p_r}$ is central in $\text{Int}(\mathbb{Z}Q)$, there exist $\frac{f_1(x)}{n_1}, \frac{f_2(x)}{n_2}, \ldots, \frac{f_t(x)}{n_t} \in \text{Int}(\mathbb{Z}Q)$ such that
\[
\frac{\phi_{p_{t+1}}(x)}{p_{t+1}} = \frac{f_1(x)}{n_1} \frac{\phi_{p_1}(x)}{p_1} + \frac{f_2(x)}{n_2} \frac{\phi_{p_2}(x)}{p_2} + \cdots + \frac{f_t(x)}{n_t} \frac{\phi_{p_t}(x)}{p_t},
\] (1)
and for each $1 \leq r \leq t$, $f_r(x) \in \mathbb{Z}Q[x]$ and $n_r$ is a positive integer. For each $r$, let $\alpha_r$ be the constant coefficient of $f_r(x)$.

We know that $\phi_{p_r}(x) = (x^{p_r^2} - x)(x^{p_r} - x)$ for each $1 \leq r \leq t$, so by equating the coefficients of $x^2$ in (1) we get
\[
\frac{1}{p_{t+1}} = \frac{\alpha_1}{n_1p_1} + \frac{\alpha_2}{n_2p_2} + \cdots + \frac{\alpha_t}{n_tp_t}.
\] (2)

But, for each $r$, $\alpha_r = f_r(0)$ and $\frac{f_r(x)}{n_r} \in \text{Int}(\mathbb{Z}Q)$, so there exists $\beta_r \in \mathbb{Z}Q$ such that $\alpha_r = n_r\beta_r$. So, (2) becomes
\[
\frac{1}{p_{t+1}} = \frac{\beta_1}{p_1} + \frac{\beta_2}{p_2} + \cdots + \frac{\beta_t}{p_t}.
\]

However, this is impossible, as it would imply that $p_{t+1}$ is invertible in $\mathbb{Z}_{(p_{t+1})}Q$ (here, $\mathbb{Z}_{(p_{t+1})}$ is the localization of $\mathbb{Z}$ at the prime ideal $(p_{t+1})$).

Thus, $\frac{\phi_{p_{t+1}}(x)}{p_{t+1}} \notin J_t$.

It now follows that $J_{t+1} \neq J_t$ for all $t > 0$. Hence, $J_1 \subset J_2 \subset J_3 \subset \cdots$ is a strictly increasing chain of ideals in $\text{Int}(\mathbb{Z}Q)$, and therefore $\text{Int}(\mathbb{Z}Q)$ is non-Noetherian. \hfill \square

When $p$ is an odd prime and $e > 1$, $\mathbb{Z}/p^e\mathbb{Z}$ is not a field, so the proof of Theorem 3.6 cannot be extended to $I_{p^e}$. Currently, all we can say about $\phi_{p^e}$ is that $\deg(\phi_{p^e}) \leq e \deg(\phi_p)$, which follows from the fact that $\phi_{p^e} \in I_{p^e}$. For a composite number $n$, we have the following result about $\deg(\phi_n)$.

**Proposition 3.9.** Let $n > 1$. Assume $n$ factors as $n = \ell m$ with $\ell > 1$, $m > 1$, and $\gcd(\ell, m) = 1$. Then $\deg(\phi_n) = \max\{\deg(\phi_\ell), \deg(\phi_m)\}$. In particular, if $n$ has prime factorization $n = p_1^{e_1}p_2^{e_2} \cdots p_t^{e_t}$, then $\deg(\phi_n) = \max_{1 \leq r \leq t} \{\deg(\phi_{p_r^{e_r}})\}$.

**Proof.** Notice that for all $\alpha \in \mathbb{Z}Q$, $\phi_n(\alpha) \equiv 0 \mod \ell$ and $\phi_n(\alpha) \equiv 0 \mod m$, so $\phi_n$ is in both $I_\ell$ and $I_m$. So, $\deg(\phi_n) \geq \deg(\phi_\ell)$ and $\deg(\phi_n) \geq \deg(\phi_m)$. WLOG, assume that $\deg(\phi_\ell) \geq \deg(\phi_m)$. 9
Let \( d = \deg(\phi_\ell) - \deg(\phi_m) \). Since \( \gcd(\ell, m) = 1 \), there exist \( a, b \in \mathbb{Z} \) such that \( a\ell + bm = 1 \). Note that \( \ell \phi_m, m \phi_\ell \in I_n \), so \( a\ell x^d \phi_m + bm \phi_\ell \) is a monic polynomial in \( I_n \cap \mathbb{Z}[x] \) of degree \( \deg(\phi_\ell) \). By the way we defined \( \phi_n \), we must have \( \deg(\phi_n) \leq \deg(\phi_\ell) \). Thus, \( \deg(\phi_n) = \deg(\phi_\ell) \).

Finally, if \( n \) has prime factorization \( n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} \), then the stated result follows from induction on \( t \).

Our goal is to determine generators for \( I_n \) for each \( n > 0 \). Then, the generators for \( I_n \) will give rise to generators for \( \text{Int}(\mathbb{Z}[Q]) \). We will not achieve this goal in the present paper, but we will describe the generators of \( I_n \) when \( n \) is odd (determining generators for \( I_n \) when \( n \) is even is an unresolved issue).

**Theorem 3.10.**

(i) If \( n \) is odd, then \( I_n \) is finitely generated by polynomials with coefficients in \( \mathbb{Z}[x] \).

(ii) If \( p \) is an odd prime, then \( I_p = (\phi_p, p) \).

Before giving the proof, we define some more notation.

**Definition 3.11.** For any \( f(x) = \sum_r (a_r + b_r i + c_r j + d_r k) x^r \in \mathbb{H}[x] \), let

\[
\begin{align*}
  f_1(x) &= \sum_r a_r x^r, \\
  f_1(x) &= \sum_r b_r x^r, \\
  f_j(x) &= \sum_r c_r x^r, \\
  f_k(x) &= \sum_r d_r x^r,
\end{align*}
\]

so that \( f = f_1 + f_1 i + f_j j + f_k k \). We call \( f_1, f_i, f_j, \) and \( f_k \) the component polynomials of \( f \).

**Proof.** (i) The ideal \( I_n \) is finitely generated because \( \mathbb{Z}Q[x] \) is Noetherian. Let \( f \in I_n \). Then, since \( I_n \) is an ideal of \( \mathbb{Z}Q[x] \), we have \( -if_i, -j fj, -k fk \in I_n \). So, \( 4f_1 = f + -if_i + -j fj + -k fk \in I_n \). Now, \( nf_1 \in I_n \) since \( n \in I_n \). Thus, letting \( d = \gcd(4, n) \), we have \( df_1 \in I_n \). Assuming that \( n \) is odd, we get \( f_1 \in I_n \). Similarly, the other component polynomials of \( f \) are in \( I_n \). Hence, a polynomial is in \( I_n \) if and only if its component polynomials are in \( I_n \), and since these component polynomials have coefficients in \( \mathbb{Z} \), we achieve the desired result.

(ii) Assume now that \( n = p \) is an odd prime. Certainly, we have \( (\phi_p, p) \subseteq I_p \). Let \( I = I_p \cap \mathbb{Z}[x] \). By Theorem 3.6, the image of \( I \) in \( (\mathbb{Z}/p\mathbb{Z})[x] \) is principally generated by \( \phi_p \). Let \( f \in I_p \). As in (i), all of the component polynomials
of $f$ are in $I_p$. Upon reduction mod $p$, all of the component polynomials are divisible by $\phi_p$. Hence, in $\mathbb{Z}Q[x]$, all of the component polynomials lie in $(\phi_p, p)$. It follows that $f \in (\phi_p, p)$, and therefore $I_p = (\phi_p, p)$. 

When $n$ is even, we do not have such clean results about $I_n$. As we shall see, the generators we are determining for $I_n$ are related to the maximal ideals of $\mathbb{Z}Q$ above $(n)$. When $n$ is odd, one may show [4, Chap. 3] that the maximal ideals of $\mathbb{Z}Q$ above $(n)$ are principally generated by the prime divisors of $n$ in $\mathbb{Z}$. This ideal structure allows us to give a nice description of the generators for $I_n$ when $n$ is odd. When $n$ is even, $(n)$ lies in the maximal ideal $(1 + i, 1 + j, 1 + k)$ of $\mathbb{Z}Q$, which is neither principally generated nor generated by integers. This additional complexity is reflected in the structure of $I_n$ when $n$ is even. For example, it is not too difficult to show by hand that we may take $\phi_2(x) = x^4 - x^2$ and that $I_2 = (\phi_2(x), (1 + i + j + k)(x^2 - x), 2)$. Thus, $I_2$ is not generated by polynomials in $\mathbb{Z}[x]$. In Corollary 3.15 below, we will establish a generating set for $I_{pe}$ when $p$ is an odd prime, but it is an open problem to give generators for $I_{2e}$.

According to Theorem 3.10, to find generators for $I_n$ when $n$ is odd, it is enough to look at $I_n \cap \mathbb{Z}[x]$. This will be the focus of the next several lemmas and theorems.

Recall that for a commutative ring $R$ and a polynomial $f \in R[x]$, the content of $f$ is the ideal of $R$ generated by the coefficients of $f$. We denote the content of $f$ by $\text{con}(f)$ and say that $f$ has content 1 if $\text{con}(f) = (1)$.

**Lemma 3.12.** Let $n > 0$. If $f \in I_n \cap \mathbb{Z}[x]$ and $\text{con}(f) = (q)$, where $q \in \mathbb{Z}$ is relatively prime to $n$, then there exists $g \in I_n \cap \mathbb{Z}[x]$ such that $\text{con}(g) = (1)$ and $\deg(g) = \deg(f)$.

*Proof.* Assume that $f \in I_n \cap \mathbb{Z}[x]$ has $\text{con}(f) = (q)$ where $q$ and $n$ are relatively prime. Let $f(x) = \sum a_t x^t$. Then, there exists $t \in \{0, 1, \ldots, \deg(f)\}$ such that $a_t$ is relatively prime to $n$. Let $b, c \in \mathbb{Z}$ be such that $ba_t + cn = 1$. Then, since $nx^t \in I_n \cap \mathbb{Z}[x]$, $g = bf + cnx^t$ is the required polynomial. 

**Lemma 3.13.** Let $n > 0$. If $f \in I_n \cap \mathbb{Z}[x]$ and $\text{con}(f) = (1)$, then $\deg(f) \geq \deg(\phi_n)$.

*Proof.* Since $\phi_n \in I_n \cap \mathbb{Z}[x]$ and $\phi_n$ is monic, we have $\text{con}(\phi_n) = (1)$. So, there exist polynomials in $I_n \cap \mathbb{Z}[x]$ of content 1; assume WLOG that $f$ is of minimal degree among all such polynomials. Then, $\deg(f) \leq \deg(\phi_n)$, and to prove the stated theorem it suffices to show that $\deg(f) = \deg(\phi_n)$. 

11
If \( n = 1 \), then there is nothing to prove, since \( I_1 = \mathbb{Z}Q[x] \) and \( \phi_1 = 1 \). So, assume \( n > 1 \). We break the proof into three cases, depending on \( n \).

**Case 1:** \( n = p \) for some prime \( p \).
Consider \( I_p \cap \mathbb{Z}[x] \) as an ideal in \( \mathbb{Z}[x] \), and let \( \pi : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x] \) be the homomorphism given by reduction mod \( p \). Since \( \phi_p \) is of minimal degree among monic polynomials in \( I_p \cap \mathbb{Z}[x] \), \( \pi(I_p \cap \mathbb{Z}[x]) \) is principally generated by \( \pi(\phi_p) \). However, the same could be said of \( f \), since \( f \) is of minimal degree among the content 1 polynomials in \( I_p \cap \mathbb{Z}[x] \). So, we must have \( \deg(\pi(f)) = \deg(\pi(\phi_p)) \).

But, \( \deg(f) \geq \deg(\pi(f)) \) while \( \deg(\pi(\phi_p)) = \deg(\phi_p) \), so \( \deg(f) \geq \deg(\phi_p) \), as required. This proves Case 1.

**Case 2:** \( n = p^e \) for some prime \( p \) and some \( e > 0 \).
We use induction on \( e \). The base case of the induction was covered in Case 1. So, assume that \( e > 1 \) and that the result is true for all powers of \( p \) less than \( p^e \). Suppose by way of contradiction that \( \deg(f) < \deg(\phi_{p^e}) \). Let \( c \) be the leading coefficient of \( f \). Since \( \deg(f) < \deg(\phi_{p^e}) \), \( c \) cannot be relatively prime to \( p^e \); if that were the case, then since \( p^e \in I_{p^e} \cap \mathbb{Z}[x] \), some \( \mathbb{Z} \)-linear combination of \( f \) and \( p^e x^{\deg(f)} \) would be a monic polynomial in \( I_{p^e} \cap \mathbb{Z}[x] \) of degree less than \( \deg(\phi_{p^e}) \). So, we may factor \( c \) as \( c = p^m q \), where \( m > 0 \) and \( p \) does not divide \( q \). Furthermore, if \( m \geq e \), then \( cx^{\deg(f)} \in I_{p^e} \cap \mathbb{Z}[x] \) and so \( f - cx^{\deg(f)} \) is a content 1 polynomial in \( I_{p^e} \cap \mathbb{Z}[x] \) of degree less than \( f \). This contradicts the minimality of \( \deg(f) \). So, \( 0 < m < e \).

Consider \( p^m \phi_{p^e-m} \in I_{p^e} \cap \mathbb{Z}[x] \) and let \( d = \deg(f) - \deg(p^m \phi_{p^e-m}) \). Then, \( cx^d \phi_{p^e-m} = p^m q x^d \phi_{p^e-m} \in I_{p^e} \cap \mathbb{Z}[x] \). Let \( g = f - cx^d \phi_{p^e-m} \in I_{p^e} \cap \mathbb{Z}[x] \). Then, either \( g = 0 \) or \( \deg(g) < \deg(f) \). If \( g = 0 \), then \( \con(g) \subseteq (c) \), which is a contradiction. So, \( \deg(g) < \deg(f) \). By the minimality of \( \deg(f) \), \( g \) cannot have content 1.

We claim that \( \con(g) \subseteq (p) \). If not, by Lemma 3.12, there exists a content 1 polynomial in \( I_{p^e} \cap \mathbb{Z}[x] \) of degree less than \( \deg(f) \). This is impossible, so we must have \( \con(g) \subseteq (p) \).

Since \( f = cx^d \phi_{p^e-m} + g \), having \( \con(g) \subseteq (p) \) forces \( \con(f) \subseteq (p) \), which is yet another contradiction. We arrive at a contradiction no matter what we do, so we must conclude that \( \deg(f) = \deg(\phi_{p^e}) \). This completes the induction on \( e \) and proves Case 2.

**Case 3:** \( n \) has prime factorization \( n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} \), where the \( p_r \) (\( 1 \leq r \leq t \)) are distinct primes and each \( e_r > 0 \).
Let \( p \) and \( e \) be such that \( \phi_{pe} \) has maximal degree among all the \( \phi_{pe} \). Then, by Proposition 3.9, \( \deg(\phi_{ne}) = \deg(\phi_{pe}) \). Now, \( f \in I_{pe} \cap \mathbb{Z}[x] \), so by Case 2 we have \( \deg(f) \geq \deg(\phi_{pe}) \). Thus, the lemma holds in this case as well.

There are no more cases to consider, so the proof is complete. \( \square \)

Our next two results give an explicit generating set for \( I_{pe} \) when \( p \) is an odd prime.

**Theorem 3.14.** Let \( n > 1 \). Assume that \( n \) is odd, and that \( p_1, p_2, \ldots, p_t \) are all the odd primes dividing \( n \). Then, \( I_n = (\phi_n, n) + p_1 I_{n/p_1} + p_2 I_{n/p_2} + \cdots + p_t I_{n/p_t} \).

**Proof.** Let \( I = (\phi_n, n) + p_1 I_{n/p_1} + p_2 I_{n/p_2} + \cdots + p_t I_{n/p_t} \). Then, \( I_n \supseteq I \), so we just need the other inclusion. Let \( f \in I_n \). As shown in Theorem 3.10, all the component polynomial of \( f \) are in \( I_n \), so it suffices to show that these component polynomials are in \( I \).

Let \( g \) be an arbitrary component polynomial of \( f \). Since \( \phi_n \) is monic, we may divide \( g \) by \( \phi_n \) in \( \mathbb{Z}[x] \) to get \( g = q\phi_n + h \), where \( q, h \in \mathbb{Z}[x] \) and either \( h = 0 \) or \( \deg(h) < \deg(\phi_n) \). If \( h = 0 \), then \( g \in (\phi_n) \) and we are done.

So, assume that \( \deg(h) < \deg(\phi_n) \). Then, \( \text{con}(h) \neq (1) \) by Lemma 3.13, and by Lemma 3.12, \( \text{con}(h) \) must be contained in \( (p) \) for some \( p \in \{p_1, p_2, \ldots, p_t\} \). In that case, \( h \in pI_{n/p} \subseteq I \), so \( g = q\phi_n + h \in I \), and we are done. \( \square \)

**Corollary 3.15.** For any odd prime \( p \) and any \( e > 0 \), we have \( I_{pe} = (\phi_{pe}, p\phi_{pe-1}, p^2\phi_{pe-2}, \ldots, p^{e-1}\phi_p, p) \).

**Proof.** Use the previous theorem and induction on \( e \). \( \square \)

**Corollary 3.16.** Let \( f(x) \in \text{Int}(\mathbb{Z}Q) \) and assume that \( f(x) = \frac{g(x)}{pe} \), where \( g(x) \in \mathbb{Z}Q[x] \), \( p \) is an odd prime, and \( e > 0 \). Then, there exist \( g_0(x), g_1(x), \ldots, g_e(x) \in \mathbb{Z}Q[x] \) such that

\[
 f(x) = g_e(x)\frac{\phi_{pe}(x)}{pe} + g_{e-1}(x)\frac{\phi_{pe-1}(x)}{pe-1} + \cdots + g_1(x)\frac{\phi_{p}(x)}{p} + g_0(x).
\]

**Proof.** Since \( g(x) \in I_{pe} \) and the generators for \( I_{pe} \) given in Corollary 3.15 are central in \( \mathbb{Z}Q[x] \), we have

\[
 g(x) = g_e(x)\phi_{pe}(x) + pg_{e-1}(x)\phi_{pe-1}(x) + \cdots + p^{e-1}g_1(x)\phi_p(x) + p^e g_0(x)
\]

for some \( g_0(x), g_1(x), \ldots, g_e(x) \in \mathbb{Z}Q[x] \). The stated result follows upon division by \( p^e \). \( \square \)
4. Prime ideals

In this section, we will begin to describe the prime ideals of \( \text{Int}(\mathbb{Z}Q) \). Because we are working in a noncommutative setting, the usual definition for a prime ideal over a commutative ring no longer holds the same utility. Instead, we extend this definition to a noncommutative ring in the following way.

**Definition 4.1.** A proper ideal \( P \) in a ring \( R \) is called a prime ideal if whenever \( x, y \in R \) with \( xRy \subseteq P \), then either \( x \in P \) or \( y \in P \).

There are several equivalent characterizations of a prime ideal in a noncommutative ring, but the above definition seems to be the easiest one with which to work. The other characterizations are summarized in §10 of [6]. Note that when \( R \) is commutative, this definition for a prime ideal reduces to the customary one.

Given a prime ideal \( P \) in an integral domain \( D \) and an element \( \alpha \in D \), the set \( P_{\alpha} := \{ f \in \text{Int}(D) \mid f(\alpha) \in P \} \) constitutes a prime ideal of \( \text{Int}(D) \). It turns out that these sets can be extended to \( \text{Int}(\mathbb{Z}Q) \), although we need to modify the definition.

**Definition 4.2.** Given \( \alpha \in \mathbb{Z}Q \), we denote the (multiplicative) conjugacy class of \( \alpha \) in \( \mathbb{Z}Q \) by \( \text{Conj}(\alpha) = \{ u\alpha u^{-1} \mid u \in \mathbb{Z}Q \text{ is a unit} \} \). Since the unit group of \( \mathbb{Z}Q \) is \( (\mathbb{Z}Q)^\times = \{ \pm1, \pm i, \pm j, \pm k \} \), for any \( \alpha \in \mathbb{Z}Q \) we have \( \text{Conj}(\alpha) = \{ \alpha, -i\alpha i, -j\alpha j, -k\alpha k \} \).

The following fact regarding multiplicative conjugacy in \( \mathbb{Z}Q \) will be used several times and is worth pointing out: if \( \beta \in \text{Conj}(\alpha) \), then \( \alpha \) and \( \beta \) share the same norm and constant coefficient, and thus have the same minimal polynomial. However, the converse is not true, since, for example, \( i \) and \( j \) have the same minimal polynomial, but are not conjugate in \( \mathbb{Z}Q \).

**Definition 4.3.** Given an ideal \( J \) of \( \mathbb{Z}Q \) and \( \alpha \in \mathbb{Z}Q \), we define \( \mathfrak{p}_{J,\alpha} := \{ f \in \text{Int}(\mathbb{Z}Q) \mid f(\beta) \in J \text{ for all } \beta \in \text{Conj}(\alpha) \} \). If the ideal \( J \) is generated by the integer \( n \), then we shall write \( \mathfrak{p}_{n,\alpha} \) for \( \mathfrak{p}_{J,\alpha} \).

If the ring \( R \) is an integral domain, \( \alpha \in R \), and \( P \) is a prime ideal of \( R \), then the definition of \( \mathfrak{p}_{P,\alpha} \) reduces to \( \{ f \in \text{Int}(R) \mid f(\alpha) \in P \} \), which, as mentioned above, is a prime ideal of \( \text{Int}(R) \). Our next major goal is to determine to what extent this carries over to quaternion rings, i.e. we want
to answer the question: if \( \alpha \in \mathbb{Z}Q \) and \( P \) is a prime ideal of \( \mathbb{Z}Q \), then when is the set \( \mathfrak{P}_{P,\alpha} \) a prime ideal of \( \text{Int}(\mathbb{Z}Q) \)? In this paper, we will deal only with the case \( P = (n) \), where \( n \in \mathbb{Z} \).

In what follows, we will sometimes need to work in quotient rings of \( \mathbb{Z}Q \), i.e. rings of the form \( \mathbb{Z}Q/J \), where \( J \) is an ideal of \( \mathbb{Z}Q \). Of particular importance will be quotient rings of the form \( \mathbb{Z}Q/(n) \), where \( n \in \mathbb{Z} \). If \( J \) is any non-zero ideal of \( \mathbb{Z}Q \), then \( N(\alpha) = \alpha\overline{\alpha} \) is in \( J \) for any \( \alpha \in J \), so \( J \) always contains a non-zero integral ideal \( (n) \) and hence \( \mathbb{Z}Q/J \) is a quotient of the ring \( \mathbb{Z}Q/(n) \).

For any \( n \in \mathbb{Z} \), we define \( (\mathbb{Z}/n\mathbb{Z})q = \{ a+bi+cj+dk \mid a,b,c,d \in \mathbb{Z}/n\mathbb{Z} \} \).
Then, we have \( (\mathbb{Z}/n\mathbb{Z})q \cong \mathbb{Z}Q/(n) \); in particular, \( \mathbb{Z}Q/(n) \) is finite when \( n \neq 0 \). Combining this with the remarks in the previous paragraph, we see that any proper quotient ring of \( \mathbb{Z}Q \) is a quotient of \( (\mathbb{Z}/n\mathbb{Z})q \) for some \( n \), and hence is a finite ring.

We shall tend to write \( \mathbb{Z}Q/(n) \) when discussing the quotient ring of \( \mathbb{Z}Q \) modulo \( (n) \), but we shall always assume elements of this ring have the form \( a+bi+cj+dk \) where \( a,b,c,d \in \mathbb{Z}/n\mathbb{Z} \), and we shall view \( \mathbb{Z}/n\mathbb{Z} \) as a subring of \( \mathbb{Z}Q/(n) \). The following theorem gives some information about \( \mathbb{Z}Q/(p) \) when \( p \) is an odd prime.

**Theorem 4.4.** Let \( F \) be a field of odd characteristic. Then, \( FQ \cong M_2(F) \), the ring of \( 2 \times 2 \) matrices over \( F \). In particular, when \( p \) is an odd prime, \( \mathbb{Z}Q/(p) \) is isomorphic to \( M_2(F_p) \), where \( F_p \) is the finite field with \( p \) elements.

**Proof.** A proof that \( \mathbb{Z}Q/(p) \cong M_2(F_p) \) is outlined in Chapter 3 of [4], but the proof is easily adapted to work over any field of odd characteristic \( p \). \( \square \)

In Chapter 3 of [4], we learn that the prime ideals of \( \mathbb{Z}Q \) are \( (0) \), \( (1+i) \), \( (1+j) \), and \( (p) \), where \( p \) is an odd prime of \( \mathbb{Z} \). The next result shows that if \( P \neq (1+i,1+j) \), then \( \mathfrak{P}_{P,\alpha} \) is at least an ideal of \( \text{Int}(\mathbb{Z}Q) \).

**Theorem 4.5.** Let \( \alpha \in \mathbb{Z}Q \) and \( n \in \mathbb{Z} \). Then, \( \mathfrak{P}_{n,\alpha} \) is an ideal of \( \text{Int}(\mathbb{Z}Q) \), and when \( n \neq 0 \), \( \text{Int}(\mathbb{Z}Q)/\mathfrak{P}_{n,\alpha} \) is a finite ring.

**Proof.** Since \( (f+g)(\gamma) = f(\gamma)+g(\gamma) \) for any \( f,g \in \text{Int}(\mathbb{Z}Q) \) and any \( \gamma \in \mathbb{Z}Q \), we see that \( \mathfrak{P}_{n,\alpha} \) is closed under addition.

Now, fix \( f(x) = \sum_r \alpha_r x^r \in \mathfrak{P}_{n,\alpha} \), and let \( g(x) \in \text{Int}(\mathbb{Z}Q) \). Let \( \beta \in \text{Conj}(\alpha) \). Then, there exist \( s,t,u,v \in \mathbb{Z} \) such that \( g(\beta) = s + ti + uj + vk \).
We have, as in Theorem 2.3,

\[
(fg)(\beta) = sf(\beta) + tf(-i\beta i) + uf(-j\beta j)j + vf(-k\beta k)k.
\]
Since $\beta \in \text{Conj}(\alpha)$, so are $-i\beta, -j\beta, \text{and} -k\beta$. Since $f \in \mathfrak{P}_{n,\alpha}$, each of $f(\beta), f(-i\beta), f(-j\beta)$, and $f(-k\beta)$ is in $(n)$. So, $(fg)(\beta) \in (n)$ and hence $fg \in \mathfrak{P}_{n,\alpha}$.

To prove the first assertion in our theorem, it remains to show that $gf \in \mathfrak{P}_{n,\alpha}$. Writing $f(\beta) = a + bi + cj + dk$ for some integers $a, b, c,$ and $d$, we get

$$(gf)(\beta) = ag(\beta) + bg(-i\beta)i + cg(-j\beta)j + dg(-k\beta)k.$$ 

The fact that $f(\beta) \in (n)$ means that $a, b, c,$ and $d$ are all in $(n)$. Since $g \in \text{Int}(\mathbb{Z}Q)$, it follows that $(gf)(\beta) \in (n)$, and hence $gf \in \mathfrak{P}_{n,\alpha}$. Thus, $\mathfrak{P}_{n,\alpha}$ is an ideal of $\text{Int}(\mathbb{Z}Q)$.

Next, let $\mathcal{R} = \text{Int}(\mathbb{Z}Q)/\mathfrak{P}_{n,\alpha}$, and assume that $n \neq 0$. Since $n \in \mathfrak{P}_{n,\alpha}$, $\mathcal{R}$ contains a subring isomorphic to $\mathbb{Z}Q/(n)$. For every $F \in \text{Int}(\mathbb{Z}Q)$, we define a map

$$F^* : \text{Conj}(\alpha) \to \mathbb{Z}Q/(n)$$

$$\beta \mapsto F(\beta) \text{ mod } n.$$ 

Then, for all $F, G \in \text{Int}(\mathbb{Z}Q)$,

$$F^* = G^* \iff F(\beta) - G(\beta) \equiv 0 \text{ mod } n \text{ for all } \beta \in \text{Conj}(\alpha)$$

$$\iff F - G \in \mathfrak{P}_{n,\alpha}$$

$$\iff F \equiv G \text{ in } \mathcal{R}.$$ 

These equivalences show that for any $F \in \text{Int}(\mathbb{Z}Q)$, the residue of $F$ modulo $\mathfrak{P}_{n,\alpha}$ is determined by the associated map $F^*$. Thus, the number of possible residues in $\mathcal{R}$ is bounded by the number of possible maps from $\text{Conj}(\alpha)$ to $\mathbb{Z}Q/(n)$. Since both $\text{Conj}(\alpha)$ and $\mathbb{Z}Q/(n)$ are finite sets, there are only finitely many maps between them. Therefore, we conclude that $\mathcal{R} = \text{Int}(\mathbb{Z}Q)/\mathfrak{P}_{n,\alpha}$ is a finite ring. $\square$

The preceding result also holds when $P = (1 + i, 1 + j)$, but since $P$ is not principal in this case, the proof given does not apply. Our subsequent theorems focus on $P = (p)$ with $p$ an odd prime, so we will not explore the case where $P = (1 + i, 1 + j)$ in this paper.

When $n$ is composite, it is straightforward to show that $\mathfrak{P}_{n,\alpha}$ is not a prime ideal of $\text{Int}(\mathbb{Z}Q)$ for any $\alpha \in \mathbb{Z}Q$ (if $n$ factors as $n = \ell m$, one need only consider the set $\ell \text{ Int}(\mathbb{Z}Q) m \subseteq \mathfrak{P}_{n,\alpha}$). It is also true that $\mathfrak{P}_{2,\alpha}$ is never a prime of $\text{Int}(\mathbb{Z}Q)$ (in this case, it would suffice to show that $(1 + i)\text{Int}(\mathbb{Z}Q)(1 - i)$ is
contained in $\mathfrak{P}_{2,\alpha}$). Neither of these results should be surprising, since $(n)$ is not a prime ideal of $\mathbb{Z}Q$ when $n = 2$ or $n$ is composite. The question remains whether $\mathfrak{P}_{n,\alpha}$ is prime if $(n)$ is prime. Under certain conditions on $\alpha$, we will prove that $\mathfrak{P}_{p,\alpha}$ is in fact a prime ideal of $\text{Int}(\mathbb{Z}Q)$ when $p$ is an odd prime. The case $p = 0$ is true without restrictions on $\alpha$, as we show in the next proposition.

**Proposition 4.6.** Let $\alpha \in \mathbb{Z}Q$. Then $\mathfrak{P}_{0,\alpha}$ is a prime ideal of $\text{Int}(\mathbb{Z}Q)$.

*Proof.* Let $f, g \in \text{Int}(\mathbb{Z}Q)$ and assume that $f \text{Int}(\mathbb{Z}Q) g \subseteq \mathfrak{P}_{0,\alpha}$. If $g \in \mathfrak{P}_{0,\alpha}$, then there is nothing to prove. So, assume $g \notin \mathfrak{P}_{0,\alpha}$. Then, there exists $\beta \in \text{Conj}(\alpha)$ such that $g(\beta) \notin (0)$, i.e. such that $N(g(\beta))$ is a non-zero integer.

Let $u$ be any unit in $\mathbb{Z}Q$. Then, the constant polynomial $\overline{ug(\beta)}$ is an element of $\text{Int}(\mathbb{Z}Q)$. Let $f(x) = \sum_{r} \alpha_r x^r$. Since $f \text{Int}(\mathbb{Z}Q) g \subseteq \mathfrak{P}_{0,\alpha}$, we have

$$0 = (f \overline{ug(\beta)}g)(\beta)$$

$$= \sum_{r} \alpha_r (\overline{ug(\beta)}g)(\beta)\beta^r$$

$$= \sum_{r} \alpha_r u\overline{g(\beta)}g(\beta)\beta^r$$

$$= \sum_{r} \alpha_r uN(g(\beta))\beta^r$$

$$= N(g(\beta))\sum_{r} \alpha_r u\beta^r$$

$$= N(g(\beta))(f(\beta))$$

$$= N(g(\beta))(f(\beta))\overline{u\beta u^{-1}}u.$$ 

We know that $N(g(\beta)) \neq 0$, so we must have $f(\overline{u\beta u^{-1}})u = 0$. Since $u$ is a unit, this implies that $f(\overline{u\beta u^{-1}}) = 0$. But $u$ was an arbitrary unit, so $f(\gamma) = 0$ for all $\gamma \in \text{Conj}(\alpha)$. Thus, $f \in \mathfrak{P}_{0,\alpha}$ and therefore $\mathfrak{P}_{0,\alpha}$ is a prime ideal. \qed

When $p$ is an odd prime, not every $\mathfrak{P}_{p,\alpha}$ ideal is prime; it depends on $\alpha$. Furthermore, showing that $\mathfrak{P}_{p,\alpha}$ is prime is more difficult, and requires knowledge of the generators of $\text{Int}(\mathbb{Z}Q)$ that was derived in §3. Before proceeding, we need two results from number theory regarding integers that can be represented as sums of three squares. Both theorems are due to Gauss,
and a thorough treatment in terms of quadratic forms is given in Chapter 5 of [2]. The first theorem is the well-known condition under which an integer can be written as a sum of three squares.

**Theorem 4.7.** Let \( N \in \mathbb{Z} \) be positive, and write \( N = 4^m u \), where \( m \geq 0 \) and \( 4 \nmid u \). Then, there exist \( y, z, w \in \mathbb{Z} \) such that \( N = y^2 + z^2 + w^2 \) if and only if \( u \neq 7 \mod 8 \).

The second result is a weakened form of Theorem 8.7 in Chapter 5 of [2].

**Theorem 4.8.** Let \( u \) be a positive integer. If \( u \equiv 1, 2, 3, 5, \) or \( 6 \mod 8 \), then there exist \( y, z, w \in \mathbb{Z} \) such that \( u = y^2 + z^2 + w^2 \) and gcd\((y, z, w) = 1\). Using these, we can prove the following lemma.

**Lemma 4.9.** Let \( p \) be an odd prime, \( r > 0 \), and \( \alpha \in \mathbb{Z}Q \). Divide \( \phi_{p^r}(x) \) by \( \min_{\alpha}(x) \) to get \( \phi_{p^r}(x) = q(x) \min_{\alpha}(x) + CX + D \) for some \( q(x) \), \( CX + D \in \mathbb{Z}[x] \). Then, \( p^r \mid C \) and \( p^r \mid D \).

**Proof.** Write \( \alpha = a + bi + cj + dk \). Then, \( \phi_{p^r}(\alpha) = C\alpha + D = (Ca + D) + Cbi + Ccj + Cdk \). Since \( \frac{\phi_{p^r}(x)}{p^r} \in \text{Int}(\mathbb{Z}Q) \), we have \( \frac{\phi_{p^r}(\alpha)}{p^r} \in \mathbb{Z}Q \). So, \( p^r \) divides all of \( Ca + D, Cb, Cc, \) and \( Cd \).

Assume first that \( \alpha \in \mathbb{Z} \). Then, \( \min_{\alpha}(x) \) is linear, so \( C = 0 \) and \( p^r \mid D \), as required. So, assume that \( \alpha \notin \mathbb{Z} \).

If \( \alpha \equiv a \mod p \), then either \( p \nmid b, p \nmid c, \) or \( p \nmid d \). WLOG, assume that \( p \nmid b \). Then, the condition \( p^r \mid Cb \) forces \( p^r \mid C \). Since \( p^r \mid Ca + D \), we also get \( p^r \mid D \), so we are done if \( \alpha \equiv a \mod p \).

Assume now that \( \alpha \equiv a \mod p \). Let \( N = b^2 + c^2 + d^2 \). Since \( \alpha \notin \mathbb{Z}, N > 0 \). So, we may write \( N = 4^\ell u \), where \( \ell \geq 0, u > 0 \), and \( 4 \nmid u \). Since \( N \) is a sum of three squares, Theorem 4.7 shows that \( u \neq 7 \mod 8 \). Since \( 4 \nmid u \), we see that \( u \equiv 1, 2, 3, 5, \) or \( 6 \mod 8 \). Thus, by Theorem 4.8 there exist \( y, z, w \in \mathbb{Z} \) such that \( u = y^2 + z^2 + w^2 \) and gcd\((y, z, w) = 1\).

So,

\[
N = 4^\ell u = 2^{2\ell}(y^2 + z^2 + w^2) = (2^\ell y)^2 + (2^\ell z)^2 + (2^\ell w)^2.
\]

Let \( \beta = a + 2^\ell yi + 2^\ell zj + 2^\ell wk \in \mathbb{Z}Q \). Then, \( \beta \) and \( \alpha \) share the same constant coefficient and \( N(\alpha) = a^2 + N = N(\beta) \). So, \( \min_{\beta}(x) = \min_{\alpha}(x) \) and consequently \( \phi_{p^r}(\beta) = C\beta + D \). Hence,

\[
\frac{\phi_{p^r}(\beta)}{p^r} = \frac{Ca + D}{p^r} + \frac{2^\ell Cy}{p^r} i + \frac{2^\ell Cz}{p^r} j + \frac{2^\ell Cw}{p^r} k
\]

18
and this is an element of $\mathbb{Z}Q$. Since $\gcd(y, z, w) = 1$, either $p \nmid y, p \nmid z$, or $p \nmid w$, and $p$ cannot divide $2^k$ because $p$ is odd. Proceeding as in the case where $\alpha \not\equiv a \mod p$ now gives $p^r \mid C$ and $p^r \mid D$. This completes the proof of the lemma.

We can now restart our discussion of prime ideals in $\text{Int}(\mathbb{Z}Q)$.

**Theorem 4.10.** Let $p$ be an odd prime and let $\alpha \in \mathbb{Z}Q$. Let $T = \{a + bi + cj + dk \in \mathbb{Z}Q \mid a, b, c, d \in \{0, 1, \ldots, p - 1\}\}$ and let $L = \{\alpha_1 x + \alpha_0 \in \mathbb{Z}Q[x] \mid \alpha_1, \alpha_0 \in T\}$. Then, $L$ represents a complete (though not necessarily irredundant) set of residues in $\text{Int}(\mathbb{Z}Q)/\mathfrak{P}_{p, \alpha}$.

**Proof.** Let $\mathcal{R} = \text{Int}(\mathbb{Z}Q)/\mathfrak{P}_{p, \alpha}$ and let $\pi : \text{Int}(\mathbb{Z}Q) \to \mathcal{R}$ be the quotient map. We know that $L \subseteq \text{Int}(\mathbb{Z}Q)$. We wish to show that $\pi(L) = \mathcal{R}$.

Note that $(\min_{\alpha}(x), p) \subseteq \mathfrak{P}_{p, \alpha}$. This means that whenever $f \in \mathbb{Z}Q[x]$, there exist $g \in \mathbb{Z}Q[x]$ and $h \in L$ such that $f(x) \equiv g(x) \min_{\alpha}(x) + h(x) \mod p$. It follows that $\pi(f) \in \pi(L)$.

Next, assume that $f(x)$ is a generic element of $\text{Int}(\mathbb{Z}Q)$. Then, there exist $F(x) \in \mathbb{Z}Q[x]$ and $n > 0$ such that $f(x) = F(x)_n$. Write $n = p^r q$, where $e \geq 0$ and $\gcd(p, q) = 1$. Then, $q$ is invertible mod $p$, so $\pi(F(x)_n) = \pi(q)^{-1} \pi(F(x))_e$. Thus, it suffices to show that $\pi(F(x))_e$ lies in $\pi(L)$.

If $e = 0$, then we are done. So, assume that $e > 1$. Since $F(x) \in \text{Int}(\mathbb{Z}Q)$, by Corollary 3.16, there exist $g_0, g_1, \ldots, g_e \in \mathbb{Z}Q[x]$ such that

$$F(x) = g_e(x) \frac{\phi_{p^e}(x)}{p^e} + g_{e-1}(x) \frac{\phi_{p^{e-1}}(x)}{p^{e-1}} + \cdots + g_1(x) \frac{\phi_{p^1}(x)}{p} + g_0(x)$$

where each $\phi_{p^r}(x) \in \text{Int}(\mathbb{Z}Q)$. Thus, it suffices to show that for every $r > 0$, $\frac{\phi_{p^r}(x)}{p^r}$ can be represented mod $\mathfrak{P}_{p, \alpha}$ by a residue in $L$.

So, let $r > 0$, and let $\phi(x) = \frac{\phi_{p^r}(x)}{p^r} \in \text{Int}(\mathbb{Z}Q)$. Since $\phi_{p^r}(x) \in \mathbb{Z}[x]$, we may divide $\phi_{p^r}(x)$ by $\min_{\alpha}(x)$ to get $\phi_{p^r}(x) = q_0(x) \min_{\alpha}(x) + Cx + D$ for some $q_0(x), Cx + D \in \mathbb{Z}[x]$. By Lemma 4.9, we have $p^r \mid C$ and $p^r \mid D$. Let $C', D' \in \mathbb{Z}$ be such that $C = p^r C'$ and $D = p^r D'$; then, $\phi(\alpha) = C' \alpha + D'$. Let $\psi(x) = C'x + D' \in \mathbb{Z}Q[x]$. Then, because both $\phi$ and $\psi$ have rational coefficients, we have, for any unit $u \in \mathbb{Z}Q$,

$$\phi(u \alpha u^{-1}) = u \phi(\alpha) u^{-1} = u \psi(\alpha) u^{-1} = \psi(u \alpha u^{-1})$$.
Thus, \( \phi(\beta) = \psi(\beta) \) for all \( \beta \in \text{Conj}(\alpha) \).

Recall that in the proof of Theorem 4.5, we introduced the following notation: for every \( \tau \in \text{Int}(\mathbb{Z}Q) \), let \( \tau^* : \text{Conj}(\alpha) \to \mathbb{Z}Q/(p) \) be the map defined by \( \tau^*(\beta) = \tau(\beta) \mod p \) for any \( \beta \in \text{Conj}(\alpha) \). In that same proof, we showed that for any \( \tau, \sigma \in \text{Int}(\mathbb{Z}Q) \), we have \( \tau^* = \sigma^* \) if and only if \( \tau \) and \( \sigma \) are equivalent modulo \( \mathfrak{P}_{p,\alpha} \). Phrased in these terms, (1) indicates that \( \phi^* = \psi^* \), and consequently \( \phi \equiv \psi \) in \( \mathcal{R} \). But, \( \psi \in \mathbb{Z}Q[x] \) and hence is equivalent to an element of \( L \). Therefore, \( \pi(\phi) \in \pi(L) \), and \( L \) represents a complete set of residues in \( \mathcal{R} \).

\[ \square \]

**Theorem 4.11.** Let \( \mathcal{R} = \text{Int}(\mathbb{Z}Q)/\mathfrak{P}_{p,\alpha} \), where \( p \) is an odd prime \( \alpha \in \mathbb{Z}Q \). Let \( m(x) \) be a monic polynomial in \( \mathbb{Z}[x] \) of minimal positive degree such that \( m(\alpha) \in (p) \). Then, \( \mathcal{R} \) is a simple ring if and only if \( m(x) \) is irreducible mod \( p \).

**Proof.** (\( \Rightarrow \)) We prove the contrapositive. Assume that \( m(x) \) is reducible mod \( p \). Then, there exist non-constant, monic \( f, g \in \mathbb{Z}[x] \) such that \( m \equiv fg \mod p \). Since \( m(\alpha) \in (p) \), the minimality of \( \deg(m(x)) \) implies that \( f(\alpha) \notin (p) \) and \( g(\alpha) \notin (p) \). So, the residues of \( f \) and \( g \) are non-zero in \( \mathcal{R} \), but \( fg \equiv m \equiv 0 \) in \( \mathcal{R} \). Thus, the residue of \( f \) in \( \mathcal{R} \) is a central, non-zero zero divisor. It follows that the ideal of \( \mathcal{R} \) generated by the residue of \( f \) is a proper, non-zero ideal of \( \mathcal{R} \). Thus, \( \mathcal{R} \) is not simple.

(\( \Leftarrow \)) Assume that \( m(x) \) is irreducible mod \( p \). If \( m(x) \) is linear, then by Theorem 4.10, the set \( T = \{a + bi + cj + dk \mid a, b, c, d \in \{0, 1, \ldots, p - 1\}\} \) represents a complete set of residues in \( \mathcal{R} \). So, \( \mathcal{R} \) is a non-zero quotient ring of \( \mathbb{Z}Q/(p) \); however, \( (p) \) is a maximal ideal of \( \mathbb{Z}Q \), so \( \mathbb{Z}Q/(p) \) is a simple ring. Thus, \( \mathcal{R} \cong \mathbb{Z}Q/(p) \) is a simple ring (and in fact, appealing to Theorem 4.4 shows that \( \mathcal{R} \cong M_2(\mathbb{F}_p) \)).

So, assume that \( \deg(m(x)) > 1 \). Then, \( \alpha \notin \mathbb{Z} \), so we know that \( \min_{\alpha}(x) \) is a monic quadratic polynomial in \( \mathfrak{P}_{p,\alpha} \). Let \( J \) be the ideal of \( \mathbb{Z}[x] \) generated by \( p \) and \( m(x) \). In Int(\( \mathbb{Z}Q \)), both \( m(x) \) and \( p \) are contained in \( \mathfrak{P}_{p,\alpha} \), so the ring \( \mathcal{R} \) contains a subring isomorphic to \( \mathbb{Z}[x]/J \cong \mathbb{F}_p^2 \). Adjoining the quaternion units to this copy of \( \mathbb{F}_p^2 \) shows that \( \mathcal{R} \) contains a subring \( \mathcal{S} \) isomorphic to \( \mathbb{F}_p^2 Q \). However, \( |\mathbb{F}_p^2 Q| = p^8 \), and by Theorem 4.10, \( |\mathcal{R}| \leq p^8 \). Thus, we must have equality between \( \mathcal{R} \) and \( \mathcal{S} \), and hence \( \mathcal{R} \cong \mathbb{F}_p^2 Q \). Furthermore, another application of Theorem 4.4 shows that \( \mathcal{R} \cong M_2(\mathbb{F}_p^2) \).

20
The known results about maximal ideals of $\text{Int}(\mathbb{ZQ})$ are summarized in the following theorem.

**Theorem 4.12.** Let $\mathcal{R} = \text{Int}(\mathbb{ZQ})/\mathfrak{p}_p$, where $p$ is an odd prime and $\alpha \in \mathbb{ZQ}$. Let $m(x)$ be a monic polynomial in $\mathbb{Z}[x]$ of minimal positive degree such that $m(\alpha) \in (p)$. Then, $\deg(m(x)) \leq 2$, and

(i) $\mathfrak{p}_{p,\alpha}$ is a maximal ideal of $\text{Int}(\mathbb{ZQ})$ if and only if $m(x)$ is irreducible mod $p$.

(ii) if $m(x)$ is linear, then $\mathfrak{p}_{p,\alpha}$ is a maximal ideal of $\text{Int}(\mathbb{ZQ})$ and $\mathcal{R} \cong \mathbb{ZQ}/(p) \cong M_2(\mathbb{F}_p)$.

(iii) if $m(x)$ is quadratic and irreducible mod $p$, then $\mathfrak{p}_{p,\alpha}$ is a maximal ideal of $\text{Int}(\mathbb{ZQ})$ and $\mathcal{R} \cong \mathbb{ZQ}/M \cong M_2(\mathbb{F}_p^2)$.

(iv) if $m(x)$ is quadratic and reducible mod $p$, then $\mathfrak{p}_{p,\alpha}$ is not a prime ideal of $\text{Int}(\mathbb{ZQ})$. However, if $x - A$ represents an irreducible factor of $m(x)$ mod $p$, then $\mathfrak{m} := (\mathfrak{p}_{p,\alpha}, x - A)$ is a maximal ideal of $\text{Int}(\mathbb{ZQ})$, and $\text{Int}(\mathbb{ZQ})/\mathfrak{m} \cong \mathbb{ZQ}/(p) \cong M_2(\mathbb{F}_p)$.

**Proof.** Parts (i), (ii), and (iii) were all shown in Theorem 4.11.

(iv) Since $m(x)$ is reducible mod $p$, there exist integers $a$ and $b$ such that $m_\alpha(x) \equiv (x - a)(x - b)$ mod $p$, and $(\beta - a)(\beta - b) \in (p)$ in $\mathbb{ZQ}$ for all $\beta \in \text{Conj}(\alpha)$. Consider $(x - a)\text{Int}(\mathbb{ZQ})(x - b)$. We wish to show that this set of polynomials lies in $\mathfrak{p}_{p,\alpha}$. Toward that end, let $h(x) \in \text{Int}(\mathbb{ZQ})$ and let $H(x) = (x - a)h(x)(x - b)$. We have, for any $\beta \in \text{Conj}(\alpha)$,

$$H(x) = h(x)x^2 - ah(x)x - bh(x)x + abh(x) \quad \text{and}$$

$$H(\beta) = h(\beta)\beta^2 - ah(\beta)\beta - bh(\beta)\beta + abh(\beta)$$

$$= h(\beta)(\beta - a)(\beta - b) \in (p).$$

Since $h$ was an arbitrary element of $\text{Int}(\mathbb{ZQ})$, we have $(x - a)\text{Int}(\mathbb{ZQ})(x - b) \subseteq \mathfrak{p}_{p,\alpha}$. However, neither $x - a$ nor $x - b$ is in $\mathfrak{p}_{p,\alpha}$ because $m(x)$ is not linear. Therefore, $\mathfrak{p}_{p,\alpha}$ cannot be a prime ideal.

Assuming that $m(x)$ is quadratic and that $x - A$ is an irreducible factor of $m(x)$ mod $p$, the proof of the forward implication of Theorem 4.11 shows
that the residue of $x - A$ in $\mathcal{R}$ generates a non-zero, proper ideal $\mathcal{I}$ of $\mathcal{R}$. Taking into account Theorem 4.10, we see that $\operatorname{Int}(\mathbb{Z}Q)/\mathfrak{M} \cong \mathcal{R}/\mathcal{I}$ is a non-zero ring that can be completely represented by residues in $\mathbb{Z}Q/(p)$. Since $\mathbb{Z}Q/(p)$ is simple, we must have $\operatorname{Int}(\mathbb{Z}Q)/\mathfrak{M} \cong \mathbb{Z}Q/(p) \cong M_2(\mathbb{F}_p)$. □

5. Generalizing Sections 3 and 4

The techniques used in Sections 3 and 4 to produce elements and prime ideals in $\operatorname{Int}(\mathbb{Z}Q)$ can be applied to other rings of integer-valued polynomials. However, doing so often requires a different approach or alternate definitions.

One way to extend the results in Section 3 is to reformulate the theorems in terms of quotient rings of $\mathbb{Z}Q$. To do this, instead of working with $I_n$, one would let $R = \mathbb{Z}Q/(n)$ and consider

$$\{f(x) \in R[x] \mid f(\alpha) \equiv 0 \text{ in } R \text{ for all } \alpha \in R\}.$$

The advantage to this approach is that theorems proven for $\mathbb{Z}Q/(n)$ will hold for any ring with quotient rings isomorphic to $\mathbb{Z}Q/(n)$. For example, it is known that for any odd prime $p$, $\mathbb{Z}Q/(p) \cong \mathbb{Z}H/(p) \cong M_2(\mathbb{F}_p)$. Hence, both $\operatorname{Int}(\mathbb{Z}H)$ and $\operatorname{Int}(M_2(\mathbb{Z}))$ contain $(x^2-x)(x^2-x)$ for each odd prime $p$, and consequently Theorem 3.8 shows that both $\operatorname{Int}(\mathbb{Z}H)$ and $\operatorname{Int}(M_2(\mathbb{Z}))$ are non-Noetherian.

Theorems similar to those of Section 4 will hold for other quaternion rings if we modify the definition of $\mathfrak{P}_{P,\alpha}$. For $\mathbb{Z}Q$, we defined $\mathfrak{P}_{P,\alpha} = \{f \in \operatorname{Int}(\mathbb{Z}Q) \mid f(\beta) \in P \text{ for all } \beta \in \text{Conj}(\alpha)\}$. The problem with using this definition for a general quaternion ring comes from $\text{Conj}(\alpha)$. For $\alpha \in \mathbb{Z}Q$, $\text{Conj}(\alpha)$ is always finite, since $(\mathbb{Z}Q)^\times$ is finite. However, in an arbitrary overring $R$ of $\mathbb{Z}Q$, the conjugacy class of $\alpha \in R$ may be infinite. The way to extend $\mathfrak{P}_{P,\alpha}$ to an overring $R$ of $\mathbb{Z}Q$ is let $S = R \cap \mathbb{Q}$ and define

$$\mathfrak{P}_{P,\alpha} := \{f(x) \in \operatorname{Int}(R) \mid f(\beta \alpha \beta^{-1}) \in P \text{ for all } \beta \in (\mathbb{Z}Q)^\times\} \text{ if } R = SQ,$$

and

$$\mathfrak{P}_{P,\alpha} := \{f(x) \in \operatorname{Int}(R) \mid f(\beta \alpha \beta^{-1}) \in P \text{ for all } \beta \in (\mathbb{Z}H)^\times\} \text{ if } R \neq SQ.$$

Here, $(\mathbb{Z}Q)^\times = \{\pm 1, \pm i, \pm j, \pm k\}$ and $(\mathbb{Z}H)^\times$ is the unit group of the ring of Hurwitz integers, which is generated by $i, j, \text{ and } \mu$ and consists of 24 elements.
6. Summary and open questions

We have shown that $\text{Int}(R)$ is a ring for any overring $R$ of $\mathbb{Z}Q$, and we have determined some of the elements and prime ideals of $\text{Int}(\mathbb{Z}Q)$. However, there are still many open questions regarding integer-valued polynomials over quaternion rings. Among them:

- How can we describe a complete generating set for $\text{Int}(\mathbb{Z}Q)$? A related question is, what are the generators for $I_{2^n}$?
- The prime ideals of $\text{Int}(\mathbb{Z})$ can be classified by using $p$-adic numbers (see Chapter V of [1]). Will a similar strategy work for $\text{Int}(\mathbb{Z}Q)$?
- The ring $\text{Int}(\mathbb{Z})$ is a well-known example of a Prüfer domain. Does $\text{Int}(\mathbb{Z}Q)$ have any Prüfer-like qualities?

Acknowledgement

The author would like to thank the reviewer for the many detailed suggestions that were given during the completion of this paper.

References