INTEGRAL-VALUED POLYNOMIALS OVER QUATERNION RINGS

DISSERTATION

Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in the Graduate School of The Ohio State University

By

Nicholas J. Werner, B.A., M.S.

Graduate Program in Mathematics

* * * * *

The Ohio State University

2010

Dissertation Committee:
Professor K. Alan Loper, Advisor
Professor S. Tariq Rizvi
Professor Daniel Shapiro
© Copyright by

Nicholas J. Werner

2010
ABSTRACT

When \( D \) is an integral domain with field of fractions \( K \), one may define the ring \( \text{Int}(D) \) of integer-valued polynomials over \( D \) to be \( \text{Int}(D) = \{ f(x) \in K[x] \mid f(a) \in D \text{ for all } a \in D \} \). The goal of this dissertation is to extend the integer-valued polynomial construction to certain noncommutative rings. Specifically, for any ring \( R \), we define the \( R \)-algebra \( RQ \) to be \( RQ = \{ a + bi + cj + dk \mid a, b, c, d \in R \} \), where \( i, j, \) and \( k \) are the standard quaternion units satisfying the relations \( i^2 = j^2 = -1 \) and \( ij = k = -ji \). When this is done with the integers \( \mathbb{Z} \), we obtain a noncommutative ring \( \mathbb{Z}Q \); when this is done with the rational numbers \( \mathbb{Q} \), we obtain a division ring \( \mathbb{Q}Q \) that contains \( \mathbb{Z}Q \). Our main focus will be on the construction and study of integer-valued polynomials over a ring \( R \) such that \( \mathbb{Z}Q \subseteq R \subseteq \mathbb{Q}Q \). For such an \( R \), we define \( \text{Int}(R) := \{ f(x) \in \mathbb{Q}Q[x] \mid f(\alpha) \in R \text{ for all } \alpha \in R \} \). In this treatise, we will prove that \( \text{Int}(R) \) always has a ring structure and will investigate elements, generating sets, and prime ideals of \( \text{Int}(R) \). The final chapter examines the idea of integer-valued polynomials on subsets of rings. Throughout, particular attention will be paid to the ring \( \text{Int}(\mathbb{Z}Q) \).
For my mother, whose support and encouragement were always incomparable.
ACKNOWLEDGMENTS

Most grateful thanks are extended to my advisor, Alan Loper, for proposing this project in the first place, and for his many helpful comments and suggestions during its completion. I would also like to thank the members of my dissertation committee, Tariq Rizvi and Daniel Shapiro, for taking the time to evaluate my work.

Lastly, I want to thank all the friends I have made in the math department during my time here. In particular, I would like to express my appreciation to Liz, Jenn, Jason, Eric, and Matt. Without all the fun times and diversions I’ve had with you, it is unlikely that I would have maintained my sanity long enough to finish this dissertation. Congratulations, guys. Your names are now officially attached to a thesis.
VITA

2004 ........................................... B.A. in Mathematics,  
                                  The College of New Jersey
2006 ........................................... M.S. in Mathematics,  
                                  The Ohio State University
2004-2009 ................................. VIGRE Graduate Fellow,  
                                  The Ohio State University
2009-Present ............................... Graduate Teaching Associate,  
                                  The Ohio State University

FIELDS OF STUDY

Major Field: Mathematics

Specialization: Algebra and Ring Theory
TABLE OF CONTENTS

Abstract ..................................................... ii
Dedication .................................................. iii
Acknowledgments ........................................... iv
Vita .............................................................. v

Chapters:

1. Introduction ............................................... 1
   1.1 Motivation ............................................. 1
   1.2 Notation and Conventions: Quaternions .................. 3
   1.3 Notation and Conventions: Polynomials .................. 7
   1.4 When is a Quaternion Ring a Matrix Ring? .......... 10

2. Properties of Overrings ................................. 14
   2.1 Basic Properties ...................................... 14
   2.2 Classifying Overrings of $\mathbb{Z}Q$ .................. 17
   2.3 A Useful Theorem ..................................... 22

3. Rings of Integer-Valued Polynomials ................... 25
   3.1 Proving $\text{Int}(R)$ Is a Ring ....................... 25
   3.2 The Trouble with Bar Conjugation in $\text{Int}(\mathbb{Z}H)$ . 30
   3.3 Localization Properties .............................. 31
CHAPTER 1

INTRODUCTION

1.1 Motivation

The set of integer-valued polynomials is defined to be $\text{Int}(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] \mid f(a) \in \mathbb{Z} \text{ for all } a \in \mathbb{Z}\}$. It is not difficult to prove that $\text{Int}(\mathbb{Z})$ is closed under the addition and multiplication of polynomials, and thus we may speak of the ring of integer-valued polynomials. Furthermore, this construction easily extends to an integral domain $D$ with field of fractions $K$ by defining $\text{Int}(D) = \{f(x) \in K[x] \mid f(a) \in D \text{ for all } a \in D\}$, called the ring of integer-valued polynomials over $D$. In this more general context, integer-valued polynomials have inspired considerable research in recent decades; the book [2] by Cahen and Chabert is an excellent reference for the subject. However, one need look no further than $\text{Int}(\mathbb{Z})$ to find interesting results. For instance, it is easy to see that $\mathbb{Z}[x] \subseteq \text{Int}(\mathbb{Z}) \subseteq \mathbb{Q}[x]$, but no element of $\mathbb{Q} - \mathbb{Z}$ can lie in $\text{Int}(\mathbb{Z})$, so $\text{Int}(\mathbb{Z}) \neq \mathbb{Q}[x]$. On the other hand, the polynomial $\frac{x(x-1)}{2}$ is integer-valued without having integer coefficients, so $\mathbb{Z}[x] \neq \text{Int}(\mathbb{Z})$. Thus, $\text{Int}(\mathbb{Z})$ is a ring that lies properly between $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. Other notable properties of $\text{Int}(\mathbb{Z})$ include the following (proofs may be found in the indicated chapter of [2]):
• for each $n \geq 0$, the binomial polynomial \( \binom{x}{n} = \frac{x(x-1)\cdots(x-(n-1))}{n!} \) lies in \( \text{Int}(\mathbb{Z}) \) (Chapter I of [2]).

• the collection \( \{ \binom{x}{n} \}_{n \geq 0} \) of all the binomial polynomials forms a basis for \( \text{Int}(\mathbb{Z}) \) as a \( \mathbb{Z} \)-module (Chapter I of [2]).

• the ring \( \text{Int}(\mathbb{Z}) \) is non-Noetherian (Chapter VI of [2]), i.e. there exist ideals of \( \text{Int}(\mathbb{Z}) \) that are not finitely generated.

• for each prime number \( p \) of \( \mathbb{Z} \), there is a one-to-one correspondence between the maximal ideals of \( \text{Int}(\mathbb{Z}) \) containing \( p \) and elements of the ring \( \mathbb{Z}_p \) of \( p \)-adic integers (Chapter V of [2]).

• for each subset \( S \subseteq \mathbb{Z} \), the set \( \text{Int}(S, \mathbb{Z}) = \{ f(x) \in \mathbb{Q}[x] \mid f(a) \in \mathbb{Z} \text{ for all } a \in S \} \) is closed under addition and multiplication of polynomials, and hence is a ring (Chapter I of [2]).

The purpose of this treatise is to extend the integer-valued polynomial construction to a class of noncommutative rings (these rings, which we call quaternion rings, will be introduced in the next section). Our overriding strategy in this endeavour is to use what is known about \( \text{Int}(\mathbb{Z}) \) as a roadmap and a source of inspiration. Most of the problems we will investigate regarding integer-valued polynomials over quaternion rings are fairly basic and are reminiscent of the properties of \( \text{Int}(\mathbb{Z}) \) listed above. Among the issues we want to resolve are: do these sets of polynomials have a ring structure? Assuming that they do, what sorts of polynomials lie in these rings? What can we say about generators and prime ideals? Are the rings we get non-Noetherian?
And what happens when we consider integer-valued polynomials on subsets of quaternion rings? We will not completely answer all of these questions, although for each of them we will give some resolution, at least in special cases. If nothing else, we have posed enough questions to encourage further research.

1.2 Notation and Conventions: Quaternions

All rings under consideration are assumed to have a multiplicative identity, but are not necessarily commutative. By an integral domain, we mean a commutative ring with unity that has no non-zero zero divisors.

Given any ring $R$, we define the $R$-algebra $RQ$ to be

$$RQ = \{a + bi + cj + dk \mid a, b, c, d \in R\},$$

where the symbols $i, j, k$ satisfy the relations $i^2 = j^2 = −1$ and $ij = k = −ji$. We refer to $i, j,$ and $k$ as the quaternion units, and we shall call $RQ$ the quaternion ring with coefficients in $R$. Note that if char($R$) $\neq 2$, then $RQ$ is noncommutative, since $ij \neq ji$. Generally, we will work with $RQ$, where $R$ 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

$$\mathbb{Z}Q := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\}.$$

An element of $\mathbb{Z}Q$ is sometimes called a Lipschitz quaternion. Readers may be familiar with a ring closely associated to $\mathbb{Z}Q$ and usually called the Hurwitz integers or Hurwitz quaternions. Specifically, let $\mu = \frac{1+i+j+k}{2}$ (which we refer to as the Hurwitz unit) and define the Hurwitz integers to be

$$\mathbb{Z}H := \mathbb{Z}Q[\mu].$$
The ring $ZH$ was studied by Adolf Hurwitz in [5], where he determined that, among other interesting properties, $ZH$ is a principal ideal ring. As we shall see, the Hurwitz unit plays an important role in classifying quaternion rings over $Z$, and so, given any ring $R$, we define the $R$-algebra $RH$ to be $RH = RQ[\mu]$. By a quaternion ring, we mean a ring of form $RQ$ or $RH$. The notations $RQ$ and $RH$ are meant to be suggestive. The $Q$ in $RQ$ indicates the presence of the quaternion units $i,j,$ and $k$, and the $H$ in $RH$ indicates the presence of $i,j,$ and $k$ along with the Hurwitz unit $\mu$.

Whenever $R$ is an overring of $Z$ in $Q$, the quaternion rings $RQ$ and $RH$ lie inside the ring $QQ$, and $QQ$ itself lives inside the Hamiltonians, the ring of quaternions with coefficients in $R$, which we denote by $H$. At this point, we need to point out a slight conflict of notation. The quaternion unit $i$ that we presume to be part of the algebra $RQ$ is distinct from the complex square root of $-1$ found in $C$. In our notation, the ring $H$ of Hamiltonian quaternions may be written as $H = RQ$. However, while $H$ contains infinitely many subrings isomorphic to the complex numbers $C$, the $C$-algebra denoted by $CQ$ is different than $H$. This notational conflict will not be a problem in this text, because the ring $R$ as found in $RQ$ will usually be a quotient ring of $Z$ or an overring of $Z$ in $Q$.

For any $\alpha = a + bi + cj + dk \in H$, we refer to $a,b,c,$ and $d$ 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 $\overline{\alpha} = a - bi - cj - dk$. We say that a subset $S$ of $H$ is closed under bar conjugation if $\overline{\alpha} \in S$ for all $\alpha \in S$. The reason that $\overline{\alpha}$ is not called simply the conjugate of $\alpha$ is because we shall frequently look at quaternions of the form $u\alpha u^{-1}$, which are the multiplicative conjugates of $\alpha$. Thus, the term conjugate,
if left unqualified, can be ambiguous. In this text, we will always qualify the term to avoid confusion.

Another tool that is useful in dealing with quaternions is the norm. The **norm** of \( \alpha = a + bi + cj + dk \in \mathbb{H} \) is denoted by \( N(\alpha) \) and is defined to be the real number

\[
N(\alpha) = a^2 + b^2 + c^2 + d^2 .
\]

Elements \( \alpha \) and \( \beta \) of \( \mathbb{H} \) satisfy the following properties related to bar conjugation and the norm (these can be verified by direct calculation):

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

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

\[
N(\alpha) = 0 \text{ if and only if } \alpha = 0
\]

\[
\text{for all } \alpha \neq 0, \quad \alpha^{-1} = \frac{\overline{\alpha}}{N(\alpha)}
\]

\[
\overline{\alpha \beta} = \overline{\beta} \overline{\alpha} .
\]

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

Note that \( i^{-1} = -i \), \( j^{-1} = -j \), and \( k^{-1} = -k \). Then, for any \( \alpha = a + bi + cj + dk \in \mathbb{H} \), we have

\[
-i(a + bi + cj + dk)i = a + bi - cj - dk
\]

\[
-j(a + bi + cj + dk)j = a - bi + cj - dk
\]

\[
-k(a + bi + cj + dk)k = a - bi - cj + dk ;
\]
thus, multiplicative conjugation by \( i, j, \) or \( k \) does nothing except negate some of the coefficients of \( \alpha \). Similarly, multiplicative conjugation by \( \mu \) merely permutes the coefficients of \( i, j, \) and \( k \):

\[
\mu(a + bi + cj + dk)\mu^{-1} = a + di + bj + ck.
\]

These relations will come up often in proofs and computations in the succeeding chapters, so it is recommended that the reader be familiar with them, or at least remember that they are given here.

One can verify that for any \( \alpha \in \mathbb{H} \),

\[
\alpha^2 = 2a\alpha - N(\alpha)
\]

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

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

It is straightforward to prove that for each \( \alpha \in \mathbb{H} \), the minimal polynomial of \( \alpha \) is unique, i.e. if \( f(x) \) is any monic polynomial in \( \mathbb{R}[x] \) with \( \deg(f) = \deg(\min_{\alpha}(x)) \), then \( f(\alpha) = 0 \) if and only if \( f(x) = \min_{\alpha}(x) \). An easily verifiable 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.

Lastly, we explain the terminology we will use regarding ideals. Throughout this text, the term ideal refers to a two-sided ideal. If we have need to consider left or
right ideals, we will refer to them as such. As far as notation, given $\alpha \in R$, we let $R\alpha$ denote the left ideal of $R$ generated by $\alpha$, and likewise $\alpha R$ denotes the right ideal generated by $\alpha$. We use $(\alpha)$ to denote the two-sided ideal of $R$ generated by $\alpha$. Note that if $R$ is noncommutative, then $(\alpha)$ contains not only triples $\beta\alpha\gamma$ with $\beta, \gamma \in R$ (in general, the set of all such triples will not be closed under addition), but also finite sums of the form $\beta_1\alpha_1\gamma_1 + \beta_2\alpha_2\gamma_2 + \cdots + \beta_n\alpha_n\gamma_n$. Finally, if $S$ is some subset of $R$, then $(S)$ is the two-sided ideal of $R$ generated by $S$; in particular, for $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$, we have $(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha_1) + (\alpha_2) + \cdots + (\alpha_n)$.

1.3 Notation and Conventions: Polynomials

Most of the rest of this text will deal with polynomials that have quaternion coefficients, which means that we will be working with polynomials in noncommuting coefficients. Since one most often meets polynomials whose coefficients lie in commutative rings, some remarks are in order about the similarities and differences between the two cases (a detailed treatment of polynomials over division rings is given in §16 of [6]).

Assume for now that $R$ is a noncommutative ring. We can form the polynomial ring $R[x]$ just as in the commutative case. First, we define addition and multiplication of monomials. For any $\alpha, \beta \in R$, we take

$$\alpha x^n + \beta x^n = (\alpha + \beta)x^n \quad \text{and} \quad \alpha x^n \cdot \beta x^m = \alpha \beta x^{n+m}$$

Addition for arbitrary polynomials is performed componentwise (as usual) and multiplication is carried out by expanding products via the distributive laws and then
grouping terms with the same powers of $x$ (also as usual). Note that when multiplying, the indeterminant $x$ always commutes with the coefficients. Thus, on the level of $R[x]$, nothing is amiss when we assume that $R$ is noncommutative.

The big difference in dealing with polynomials over noncommutative rings has to do with evaluating products of polynomials. If $f(x)$ and $g(x)$ are polynomials with coefficients in a ring $R$ (whether commutative or noncommutative), then we let $(fg)(x)$ denote the product of the polynomials $f(x)$ and $g(x)$ in $R[x]$. That is,

$$(fg)(x) = f(x)g(x).$$

Now, if $S$ is a commutative ring, then evaluating polynomials in $S[x]$ at $a \in S$ defines a ring homomorphism from $S[x]$ to $S$. Explicitly, if $a \in S$, then the function $E_a : S[x] \rightarrow S$ defined by $E_a(f) = f(a)$ is a ring homomorphism. Put slightly differently,

if $f(x), g(x) \in S[x]$ and $a \in S$, then $(fg)(a) = f(a)g(a)$.

However, this sort of relationship may not hold if we are working over a noncommutative ring. Consider the following example with polynomials in $\mathbb{Z}Q[x]$. Let $f(x) = x - i$ and $g(x) = x - j$. Then, $(fg)(x) = f(x)g(x) = x^2 - (i + j)x + k$ and

$$(fg)(i) = i^2 - (i + j)i + k = 2k, \text{ but}$$

$$f(i)g(i) = (i - i)(i - j) = 0.$$  

Thus,

$$(fg)(i) \neq f(i)g(i).$$

and evaluation does not give a homomorphism in this case. In fact, if $R$ is a noncommutative ring and $\alpha \in R$, the function $E_\alpha : R[x] \rightarrow R$ defined by $E_\alpha(f) = f(\alpha)$ is a ring homomorphism if and only if $\alpha$ lies in the center of $R$. 
The important thing to take away from this discussion is that evaluating a product of polynomials in noncommuting coefficients may be counterintuitive and must be dealt with carefully. In general, it is legal to evaluate a product \((fg)(x)\) if the product is written in such a way that all the indeterminants are “on the right.” For example, suppose that \(f(x) = \sum r \alpha_r x^r\) (throughout this text, we use \(r\) as the index of summation in polynomials). Then, one way to write \((fg)(x)\) would be

\[
(fg)(x) = \sum_r \alpha_r g(x) x^r. \tag{1.3.1}
\]

It is then true that

\[
(fg)(\alpha) = \sum_r \alpha_r g(\alpha) \alpha^r
\]

(in particular, this equation means that if \(g(\alpha) = 0\), then \((fg)(\alpha) = 0\), a fact that will occasionally come in handy). Usually, we will evaluate products of polynomials by using formula (1.3.1) or something similar.

Because of the nature of the problems we are considering, the evaluation issue described above will be lurking behind the scenes in all of the major theorems in this manuscript. Recall that for an integral domain \(D\) with field of fractions \(K\), we define \(\text{Int}(D) = \{f(x) \in K[x] \mid f(a) \in D \text{ for all } a \in D\}\). If \(R\) is an overring of \(\mathbb{Z}Q\) in \(\mathbb{Q}Q\), then \(R\) is not an integral domain, since \(R\) is not commutative. However, the fact that \(R \subset \mathbb{Q}Q\) and \(\mathbb{Q}Q\) is a division ring means that \(R\) has no zero divisors. So, despite being noncommutative, overrings of \(\mathbb{Z}Q\) make fair substitutes for integral domains. Accordingly, the definition of the set of integer-valued polynomial over a quaternion ring is similar to the above definition for \(\text{Int}(D)\). For any overring \(R\) of \(\mathbb{Z}Q\) in \(\mathbb{Q}Q\), we define the set of integer-valued polynomials over \(R\) to be

\[
\text{Int}(R) = \{f(x) \in \mathbb{Q}Q[x] \mid f(\alpha) \in R \text{ for all } \alpha \in R\}.
\]
Notice that at this point, we refer to \( \text{Int}(R) \) only as a set. It is not hard to see that \( \text{Int}(R) \) is closed under addition, but it is non-trivial to prove that \( \text{Int}(R) \) is closed under multiplication (see Theorem 3.1.1). The reason such a proof is difficult is that the polynomials in \( \text{Int}(R) \) have noncommuting coefficients and are defined entirely in terms of evaluation; but, as elucidated above, evaluating the product of two such polynomials may lead to unexpected behavior. Once again, because we are working over noncommutative rings, care must be taken when doing something that would be easy in a commutative setting.

### 1.4 When is a Quaternion Ring a Matrix Ring?

Given a commutative ring \( R \), the quaternion ring \( RQ \) is sometimes isomorphic to \( M_2(R) \), the ring of \( 2 \times 2 \) matrices over \( R \). Knowing when this occurs will occasionally be useful in the chapters that follow, so this section is devoted to giving examples of rings \( R \) with this property.

The theorems in this section are not new results. However, the author could not find proofs in the available literature. So, for the sake of completeness, proofs are provided here.

Sufficient conditions under which \( RQ \cong M_2(R) \) are given in by the following theorem.

**Theorem 1.4.1.** Let \( R \) be a commutative ring such that

(i) there exist \( A, B \in R \) such that \( A^2 + B^2 = -1 \), and

(ii) \( 2 \) is a unit in \( R \).

Then, the \( R \)-algebra \( RQ \) is isomorphic to \( M_2(R) \), the ring of \( 2 \times 2 \) matrices over \( R \).
Proof. We extend a construction given in Chapter 3 of [4] that covers the case $R = \mathbb{F}_p$, where $p$ is an odd prime.

Given that $A^2 + B^2 = -1$, construct an $R$-module homomorphism $\phi : RQ \to M_2(R)$ by defining

$$
\phi(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \phi(i) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \phi(j) = \begin{bmatrix} A & B \\ B & -A \end{bmatrix}, \quad \phi(k) = \begin{bmatrix} B & -A \\ -A & B \end{bmatrix},
$$

and extending linearly over $R$. It is easy to check that $(\phi(i))^2 = (\phi(j))^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ and $\phi(i)\phi(j) = \phi(k) = -\phi(i)\phi(j)$, so $\phi$ respects multiplication and thus is a ring homomorphism.

**Claim 1: $\phi$ is injective**

**Proof of Claim:** Let $a + bi + cj + dk \in \text{Kern}(\phi)$. Then,

$$
\begin{bmatrix}
  a + cA + dB \\
  -b + cB - dA
\end{bmatrix}
= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},
$$

so $a + cA + dB$ and $a - cA - dB$ are both $0$ in $R$. This gives $2a = 0$, and since $2$ is a unit in $R$, we have $a = 0$. Similarly, $b = 0$. So, we have

$$
\begin{bmatrix}
  cA + dB \\
  cB - dA
\end{bmatrix}
= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.
$$

(∗)

Then,

$$
0 = B(cA + dB)
= (cB)A + dB^2
= dA^2 + dB^2, \quad \text{using (∗)}
= -d,
$$

11
so \( d = 0 \). Similarly, we can show that \( c = 0 \) by considering \( A(cA + dB) \). Thus, \( \text{Kern}(\phi) = \{0\} \) and \( \phi \) is injective. This proves Claim 1.

**Claim 2: \( \phi \) is surjective**

*Proof of Claim:* Note that

\[
\phi\left(\frac{1}{2}(1 - Aj - Bk)\right) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \phi\left(\frac{1}{2}(1 + Aj + Bk)\right) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},
\]

\[
\phi\left(\frac{1}{2}(i - Bj + Ak)\right) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \text{ and } \phi\left(-\frac{1}{2}(i + Bj - Ak)\right) = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.
\]

Since the matrices \( \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \) and \( \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \) generate \( M_2(R) \) over \( R \), we have \( \text{Im}(\phi) = M_2(R) \). Thus, \( \phi \) is surjective. This proves Claim 2.

We have shown that \( \phi \) is bijective, so \( \phi : RQ \rightarrow M_2(R) \) is an isomorphism. \( \square \)

We point out that the previous result does not conflict with the theorem that \( \mathbb{H} \) is isomorphic to a proper subring of \( M_2(\mathbb{C}) \) (see [6] §1). The reason for this, as mentioned in Section 1.2, is that the quaternion unit \( i \) found in an \( R \)-algebra \( RQ \) is different than the complex square root of \(-1\) found in \( \mathbb{C} \). Thus, while we may view \( \mathbb{C} \) as a subring of \( \mathbb{H} \) in multiple ways (the obvious example would be to use \{\( a + bi \mid a, b \in \mathbb{R} \)\}), the \( \mathbb{C} \)-algebra denoted by \( \mathbb{C}Q \) is (by the above theorem) isomorphic to \( M_2(\mathbb{C}) \) and not to \( \mathbb{H} \). In any case, we will not employ this representation of \( \mathbb{H} \) as a ring of complex matrices, so the difficulty mentioned here, while possibly confusing, will not be an issue in the rest of this text.

**Corollary 1.4.2.** The following rings satisfy the conditions of Theorem 1.4.1:

(i) any field \( F \) of odd characteristic; in particular, the finite field \( \mathbb{F}_q \), where \( q \) is a power of an odd prime.
(ii) \( \mathbb{Z}/n\mathbb{Z} \), where \( n \) is any odd integer greater than 1.

(iii) \( \mathbb{Q}_p \), the field of \( p \)-adic numbers, where \( p \) is an odd prime.

Thus, if \( R \) is any of the rings listed above, then \( RQ \cong M_2(R) \).

Proof. (i) Let \( F \) be a field of odd characteristic \( p \). Then, 2 is invertible in \( F \). Also, \( F \) contains a copy of \( \mathbb{F}_p \), the finite field with \( p \) elements. Since every element in a finite field is the sum of two squares, there exist \( A, B \in \mathbb{F}_p \subseteq F \) such that \( A^2 + B^2 = -1 \), so the conditions of Theorem 1.4.1 are met.

(ii) Let \( R = \mathbb{Z}/n\mathbb{Z} \). Then, 2 is a unit in \( R \) because \( \text{char}(R) \) is odd. Assume that \( n \) has prime factorization \( n = p_1^{e_1}p_2^{e_2} \cdots p_t^{e_t} \). Then, for each \( 1 \leq \ell \leq t \), there exist \( x_\ell, y_\ell \in \mathbb{Z}/p_\ell\mathbb{Z} \) such that \( x_\ell^2 + y_\ell^2 \equiv -1 \mod p_\ell \). For each \( 1 \leq \ell \leq t \), we can apply Hensel’s Lemma (see Chapter 10 of [1]) to the polynomial \( x^2 + y_\ell^2 + 1 \in (\mathbb{Z}/p_\ell^{e_\ell}\mathbb{Z})[x] \) to obtain elements \( z_\ell, w_\ell \in \mathbb{Z}/p_\ell^{e_\ell}\mathbb{Z} \) such that \( z_\ell^2 + w_\ell^2 \equiv -1 \mod p_\ell^{e_\ell} \). The existence of the required \( A \) and \( B \) in \( R \) now follows from the Chinese Remainder Theorem.

(iii) The rational numbers are contained in \( \mathbb{Q}_p \), so 2 is invertible in \( \mathbb{Q}_p \). As in part (ii), the necessary \( A \) and \( B \) can be obtained via Hensel’s Lemma (applied this time to the ring \( \mathbb{Z}_p \) of \( p \)-adic integers, which has maximal ideal \( p\mathbb{Z}_p \) with quotient field \( \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p \)). \( \Box \)
CHAPTER 2

PROPERTIES OF OVERRINGS

2.1 Basic Properties

We begin by proving some results concerning general overrings of \( \mathbb{Z}Q \) in \( \mathbb{Q}Q \). The results of this chapter, in particular Theorem 2.2.3, were known to Hurwitz [5] in a slightly different form.

The first lemma is elementary but will be extremely useful in the discussion to follow.

**Lemma 2.1.1.** Let \( S \) be any overring of \( \mathbb{Z} \) in \( \mathbb{Q} \), and let \( \frac{x}{y} \in S \) with \( x \) and \( y \) relatively prime. Then, \( \frac{1}{y} \in S \).

**Proof.** Since \( x \) and \( y \) are relatively prime, \( x \) is invertible mod \( y \). So, there exists \( m \in \mathbb{Z} \) such that \( xm \equiv 1 \mod y \). Then, \( \frac{xm}{y} = k + \frac{1}{y} \) for some \( k \in \mathbb{Z} \), which gives \( \frac{1}{y} \in S \). \( \square \)

In particular, we see that Lemma 2.1.1 holds for any overring \( R \) of \( \mathbb{Z}Q \) in \( \mathbb{Q}Q \), since the ring \( S = R \cap \mathbb{Q} \) is an overring of \( \mathbb{Z} \) in \( \mathbb{Q} \).

**Theorem 2.1.2.** Let \( R \) be an overring of \( \mathbb{Z}Q \) in \( \mathbb{Q}Q \), and let \( a \) be a coefficient of a element of \( R \). If \( a \notin R \), then \( a = \frac{x}{zy} \) for relatively prime odd integers \( x \) and \( y \).
Proof. We prove the contrapositive. Assume that $a$ is a coefficient of $\alpha \in R$. By multiplying $\alpha$ by $\pm i, \pm j,$ or $\pm k$, we may assume that $a$ is the constant coefficient of $\alpha$. Furthermore, since $4a = \alpha - i\alpha - j\alpha - k\alpha$, we see that $4a \in R$ regardless of the value of $a$.

Write $a = \frac{x}{2^ny}$ where $n \geq 0$, $y$ is odd, and $x$ is relatively prime to $2^n y$. We have three cases to consider.

Case 1: $n = 0$

In this case, $a = \frac{x}{y}$ and $4a = \frac{4x}{y} = 4a \in R$. Since $x$ is invertible mod $y$ and $y$ is odd, $4x$ is also invertible mod $y$. Thus, $\frac{1}{y} \in R$ by Lemma 2.1.1 and hence $a = x(\frac{1}{y}) \in R$.

Note that Case 1 covers any instance in which $x$ is even, so for the remaining Cases we may assume that $x$ is odd.

Case 2: $n > 2$

In this case, $a = \frac{x}{2^ny}$ and $4a = \frac{x}{2^{n-2}y} \in R$. By Lemma 2.1.1, $\frac{1}{2^{n-2}y} \in R$. Then, $2^{n-2}(\frac{1}{2^{n-2}y}) = \frac{1}{y} \in R$ and $y(\frac{1}{2^{n-2}y}) = \frac{1}{2^{n-2}} \in R$. Since $\frac{1}{2^{n-2}} \in R$, so is $\frac{1}{2} = 2^{n-3}(\frac{1}{2^{n-2}})$.

This means that $\frac{1}{2^n} = (\frac{1}{2})^n \in R$, and finally $a = \frac{x}{2^ny} = x(\frac{1}{2^n})(\frac{1}{y}) \in R$.

Case 3: $n = 2$

In this case, $a = \frac{x}{4y}$ with $x$ odd. We know that $\frac{x}{y} = 4a \in R$, so we can get $\frac{1}{y} \in R$.

Thus, it suffices to show that $\frac{1}{4} \in R$.

By multiplying $\alpha$ by odd integers, we can clear all the odd numbers from the denominators of the coefficients of $\alpha$. So, WLOG we may assume that $\alpha = a + bi + \ldots$. 

15
\[ cj + dk \] where \( a = \frac{x}{4} \), \( x \) is odd and \( b, c, d \) are rational numbers whose denominators are all powers of 2 and whose numerators are all odd.

If any of the denominators of \( b, c, \) or \( d \) equals \( 2^n \) with \( n > 2 \), then as in Case 2 we have \( \frac{1}{2} \in R \), and hence \( \frac{1}{4} = (\frac{1}{2})^2 \in R \). So, we may assume that each of the denominators of \( b, c, \) and \( d \) is 1, 2, or 4. Furthermore, by subtracting integer multiples of 1, \( i, j, \) and \( k \) from \( \alpha \), we may assume that \( a, b, c, \) and \( d \) all lie in the interval \((-\frac{1}{2}, \frac{1}{2}]\).

Finally, by multiplying \( \alpha \) by \(-1\) we may guarantee that \( a > 0 \). Thus, WLOG we may assume that \( \alpha = \frac{1}{4} + bi + cj + dk \) with \( b, c, d \in \{0, \frac{1}{2}, \pm \frac{1}{4}\} \).

Recall that for any \( \gamma \in \mathbb{H} \) with constant coefficient \( \gamma_0 \), we have \( \gamma^2 = 2\gamma_0 - N(\gamma) \).
Using this, we see that if any of \( b, c, \) or \( d \) equals \( \pm \frac{1}{4} \), then \( \alpha^2 = 2(\frac{1}{4})\alpha - N(\alpha) = \frac{1}{2}\alpha - N(\alpha) \) has a coefficient equal to \( \pm \frac{1}{8} \), and in this instance we are done by the argument of the preceding paragraph. If all of \( b, c, \) and \( d \) are equal to 0 or \( \frac{1}{2} \), then \( N(\alpha) = \frac{k}{16} \) where \( k \) is odd. This means that \( \alpha^2 \) has constant coefficient equal to \( \frac{1}{8} - \frac{k}{16} = \frac{2-k}{16} \). Since \( 2-k \) is odd, we can get \( \frac{1}{16} \in R \) by Lemma 2.1.1, so \( \frac{1}{4} = 4(\frac{1}{16}) \in R \), and once again we can get \( a \in R \).

In each case, we see that \( a \in R \). This completes the proof.

Note that the converse of Theorem 2.1.2 does not hold: if an overring \( R \) contains an element with a coefficient \( a \) equal to \( \frac{x}{2y} \) with \( x \) and \( y \) odd and relatively prime, then \( a \) may or may not be in \( R \). For example, \( \frac{1+i+j+k}{2} \) is in both \( \mathbb{Z}[\frac{1}{2}]Q \) and \( \mathbb{Z}H \), but \( \frac{1}{2} \in \mathbb{Z}[\frac{1}{2}]Q \) and \( \frac{1}{2} \notin \mathbb{Z}H \). However, the following results are always true regardless of the overring.

**Corollary 2.1.3.** Let \( R \) be any overring of \( \mathbb{Z}Q \) in \( QQ \). For any \( \alpha = a + bi + cj + dk \in R \), we have \( 2a, 2b, 2c, 2d \in R \).
Proof. The only case left to consider is if \( \alpha \) has a coefficient equal to \( \frac{x}{y} \) with \( x \) and \( y \) odd and relatively prime. But in this case, \( \frac{x}{y} \) is a coefficient of \( 2\alpha \in R \), so \( 2\left(\frac{x}{y}\right) = \frac{x}{y} \in R \).

\[ \square \]

**Corollary 2.1.4.** Let \( R \) be any overring of \( \mathbb{Z}Q \) in \( \mathbb{Q}Q \). Then, \( R \) is closed under bar conjugation.

*Proof.* Let \( \alpha = a + bi + cj + dk \in R \). Then, \( \overline{\alpha} = \alpha - 2bi - 2cj - 2dk \in R \).

**Corollary 2.1.5.** Let \( R \) be any overring of \( \mathbb{Z}Q \) in \( \mathbb{Q}Q \). Then, for any \( \alpha \in R \), \( N(\alpha) \in R \).

*Proof.* Let \( \alpha = a + bi + cj + dk \in R \). Then, \( \alpha^2 = 2a\alpha - N(\alpha) \), and both \( 2a\alpha \) and \( \alpha^2 \) are in \( R \), so \( N(\alpha) \in R \).

\[ \square \]

### 2.2 Classifying Overrings of \( \mathbb{Z}Q \)

We can now prove that overrings of \( \mathbb{Z}Q \) are closely related to overrings of \( \mathbb{Z} \). We begin with two lemmas.

**Lemma 2.2.1.** Let \( R \) be an overring of \( \mathbb{Z}Q \) in \( \mathbb{Q}Q \). Assume that there exists \( \alpha \in R \) such that some coefficient of \( \alpha \) is not in \( R \). Then, no coefficient of \( \alpha \) lies in \( R \).

*Proof.* Suppose by way of contradiction that some coefficient of \( \alpha \) is in \( R \), and write \( \alpha = a + bi + cj + dk \). We have three cases to consider, and we will derive a contradiction in each case.

**Case 1:** Exactly three coefficients of \( \alpha \) are in \( R \)

In this case, by multiplying \( \alpha \) by \( \pm i, \pm j, \) or \( \pm k \), we may assume that the constant coefficient \( a \) is the coefficient not in \( R \). But then, \( a = \alpha - bi - cj - dk \in R \), which is
Case 2: Exactly two coefficients of $\alpha$ are in $R$

In this case, assume WLOG that $a, b \notin R$, and subtract $cj$ and $dk$ from $\alpha$. So, we may assume $\alpha = a + bi$. By Theorem 2.1.2, we must have $a = \frac{x_1}{2y_1}$ and $b = \frac{x_2}{2y_2}$ with $x_\ell$ and $y_\ell$ ($\ell = 1, 2$) odd and relatively prime. By Corollary 2.1.3, $\frac{x_1}{y_1}$ and $\frac{x_2}{y_2}$ (and hence $\frac{1}{y_1}$ and $\frac{1}{y_2}$) are in $R$, but $\frac{1}{2} \notin R$ because $a \notin R$.

Consider

$$ N(\alpha) = a^2 + b^2 = \frac{x_1^2}{4y_1^2} + \frac{x_2^2}{4y_2^2} = \frac{x_1^2 y_2^2 + x_2^2 y_1^2}{4y_1^2 y_2^2}. $$

Since each of $x_1, x_2, y_1,$ and $y_2$ is odd, the square of each of these integers is congruent to 1 mod 4. So, $x_1^2 y_2^2 + x_2^2 y_1^2 \equiv 2 \mod 4$ and we may write $x_1^2 y_2^2 + x_2^2 y_1^2 = 2m$ for some odd integer $m$. This gives

$$ N(\alpha) = \frac{x_1^2 y_2^2 + x_2^2 y_1^2}{4y_1^2 y_2^2} = \frac{2m}{4y_1^2 y_2^2} = \frac{m}{2y_1^2 y_2^2}. $$

Now, since $m$ is odd, there exists $n \in \mathbb{Z}$ with $m + 2n = y_1^2 y_2^2$. So,

$$ N(\alpha) + \frac{n}{y_1^2 y_2^2} = \frac{m}{2y_1^2 y_2^2} + \frac{n}{y_1^2 y_2^2} = \frac{m + 2n}{2y_1^2 y_2^2} = \frac{1}{2}. $$

By Corollary 2.1.5, $N(\alpha) \in R$, and we know $\frac{1}{y_1}, \frac{1}{y_2} \in R$. Thus, the above equation implies that $\frac{1}{2} \in R$, which is a contradiction.

Case 3: Exactly one coefficient of $\alpha$ is in $R$.

In this case, assume WLOG that $a, b, c \notin R$ and subtract $dk$ from $\alpha$. So, we may assume $\alpha = a + bi + cj$. As in Case 2, we write $a = \frac{x_1}{2y_1}, b = \frac{x_2}{2y_2}$, and $c = \frac{x_3}{2y_3}$, and again $\frac{1}{2} \notin R$. We compute

$$ N(\alpha) = \frac{x_1^2 y_2^2 y_3^2 + x_2^2 y_1^2 y_3^2 + x_3^2 y_1^2 y_2^2}{4y_1^2 y_2^2 y_3^2} = \frac{m}{4n}. $$
for some odd integers $m$ and $n$. Multiplying $N(\alpha)$ by $n$ gives $\frac{m}{4} \in R$, so $\frac{1}{4} \in R$ by Lemma 2.1.1. However, this implies $\frac{1}{2} \in R$, which is again a contradiction.

We arrive at a contradiction in each case, so we conclude that no coefficient of $\alpha$ is in $R$. \hfill \Box

Recall that our convention is to let $\mu = \frac{1+i+j+k}{2}.$

**Lemma 2.2.2.** Let $R$ be an overring of $\mathbb{Z}Q$ in $\mathbb{Q}Q$. Assume that there exists $\alpha \in R$ such that some coefficient of $\alpha$ is not in $R$. Then,

(i) $\mu \in R$.

(ii) there exists $\alpha' \in R$ such that $\alpha = \mu + \alpha'$ and each coefficient of $\alpha'$ is in $R$.

**Proof.** We prove (i) and (ii) together. By Lemma 2.2.1 and Theorem 2.1.2, we may write $\alpha = \frac{x_1}{2y_1} + \frac{x_2}{2y_2}i + \frac{x_3}{2y_3}j + \frac{x_4}{2y_4}k$ with $x_\ell$ and $y_\ell$ odd for all $1 \leq \ell \leq 4$ and with each $\frac{1}{y_\ell} \in R$. Since each $x_\ell$ is odd, for each $\ell$ there exists $m_\ell \in \mathbb{Z}$ such that $x_\ell + 2m_\ell = y_\ell$. Then, $\frac{m_\ell}{y_\ell} \in R$ for each $\ell$ and

$$\alpha + \frac{m_1}{y_1} + \frac{m_2}{y_2}i + \frac{m_3}{y_3}j + \frac{m_4}{y_4}k = \frac{x_1 + 2m_1}{2y_1} + \frac{x_2 + 2m_2}{2y_2}i + \frac{x_3 + 2m_3}{2y_3}j + \frac{x_4 + 2m_4}{2y_4}k$$

$$= \frac{1 + i + j + k}{2}$$

is also in $R$, proving (i). Taking $\alpha' = -(\frac{m_1}{y_1} + \frac{m_2}{y_2}i + \frac{m_3}{y_3}j + \frac{m_4}{y_4}k)$ proves (ii). \hfill \Box

**Theorem 2.2.3.** Let $R$ be any overring of $\mathbb{Z}Q$ in $\mathbb{Q}Q$ and let $S = R \cap Q$. Then, the following hold:

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

19
(ii) either $R = SQ$ or $R = SH$.

(iii) if $R = SH$, then every $\alpha \in R$ may be written as $\alpha = \alpha' + e\mu$, where $\alpha' \in SQ$ and $e$ is either $0$ or $1$.

Proof. First, note that $SQ = \{\alpha \in R \mid \text{every coefficient of } \alpha \text{ is in } R\}$. Let $T = \{q \in \mathbb{Q} \mid q \text{ is a coefficient of some } \alpha \in R\}$. Then, (i) is the claim that $R = SQ \iff T \subseteq R$. Also, $T$ is a $\mathbb{Z}$-module, and if we close $T$ under multiplication we get the ring $\mathbb{Z}[T]$. Note the following relationships that exist between $R, S, T$:

\[
S = T \cap R \quad \quad (*)
\]

\[
SQ \subseteq R \text{ and } R \subseteq \mathbb{Z}[T]Q. \quad \quad (**)\]

Now, assume first that $R = SQ$. Then, $T \subseteq R$, because $R = (R \cap \mathbb{Q})Q = \{q_0 + q_1i + q_2j + q_3k \mid q_0, q_1, q_2, q_3 \in R \cap \mathbb{Q}\}$. Conversely, assume that $T \subseteq R$, so that $T = T \cap R$. By $(*)$, we get $S = T$ and consequently $SQ = \mathbb{Z}[T]Q$. Then, $(**)$ implies that $R = SQ$. Thus, (i) holds, and we may confine ourselves to the case where $S \subset T$.

Assume that $S$ is strictly contained in $T$. Then, there exists $\alpha \in R$ such that at least one coefficient of $\alpha$ is not in $R$. By Lemma 2.2.2, $\mu \in R$, and there exists $\alpha' \in SQ$ such that $\alpha = \mu + \alpha'$. Thus, $\alpha \in SH$.

Now, since $\mu \in R$ and $S \subseteq R$, we have $SH \subseteq R$. Let $\beta \in R$. If all the coefficients of $\beta$ are in $R$, then $\beta \in SQ \subseteq SH$. If some coefficient of $\beta$ is not in $R$, then the previous paragraph shows that $\beta \in SH$. In either case, $\beta \in SH$, so $R \subseteq SH$ and therefore $R = SH$.

Part (iii) is essentially a restatement of Lemma 2.2.2. Given $\alpha \in R = SH$, if $\alpha \in SQ$, then take $e = 0$; if $\alpha \notin SQ$, then apply Lemma 2.2.2 part (ii) and take $e = 1$. \qed
Applying Theorem 2.2.3 to \( ZH \) gives us the following corollary.

**Corollary 2.2.4.**

(i) For each \( \alpha \in ZH \), either all the coefficients of \( \alpha \) are integers (in which case \( \alpha \in ZQ \)), or all the coefficients of \( \alpha \) are half-integers (in which case \( \alpha \in ZH - ZQ \)).

More explicitly, given \( \alpha = a + bi + cj + dk \in ZH \), either \( a, b, c, d \in Z \), or \( a, b, c, d \in Z + \frac{1}{2} = \{ \frac{u}{2} \mid u \text{ is an odd integer} \} \).

(ii) The unit group of \( ZH \) has order 24, and consists of the eight units in \((ZQ)\times = \{\pm 1, \pm i, \pm j, \pm k\}\) and the sixteen elements in \( \{\frac{u_1 + u_2i + u_3j + u_4k}{2} \mid u_1, u_2, u_3, u_4 \in \{\pm 1\}\} \). Explicitly,

\[
(ZH)\times = \{\pm 1, \pm i, \pm j, \pm k, \pm \mu, \pm i\mu, \\
\pm j\mu, \pm k\mu, \pm \mu^2, \pm i\mu^2, \pm j\mu^2, \pm k\mu^2k\}.
\]

**Proof.** (i) Let \( \alpha \in ZH \), and write \( \alpha \) in the form \( \alpha = x + yi + zj + wk + e\mu \), where \( x, y, z, w, e \in ZH \cap Q = Z \) and \( e \in \{0, 1\} \). If \( e = 0 \), then \( \alpha \in ZQ \); if \( e = 1 \), then \( \alpha = \frac{(2x+1)+(2y+1)i+(2z+1)j+(2w+1)k}{2} \in Z + \frac{1}{2} \).

(ii) If \( \alpha \in (ZH)\times \), then the inverse of \( \alpha \) is \( \alpha^{-1} = \frac{\bar{\alpha}}{N(\alpha)} \), and \( \bar{\alpha}^{-1} = \alpha^{-1} \in ZH \), so \( N(\alpha) = \alpha\bar{\alpha} \) is a unit in \( ZH \). Since \( ZH \cap Q = Z \), we see that \( \alpha \in (ZH)\times \) if and only if \( N(\alpha) = 1 \). So, let \( \alpha \in (ZH)\times \), and write \( \alpha = a + bi + cj + dk + e\mu \), where \( a, b, c, d \in Z \) and \( e \in \{0, 1\} \). If \( e = 0 \), then \( \alpha \in (ZQ)\times \), which equals \( \{\pm 1, \pm i, \pm j, \pm k\} \). If \( e = 1 \), then \( \alpha \in ZH - ZQ \), so \( \alpha = \frac{u_1 + u_2i + u_3j + u_4k}{2} \) for some odd integers \( u_1, u_2, u_3 \) and \( u_4 \). Since \( N(\alpha) = 1 \), we must have \( u_1^2 + u_2^2 + u_3^2 + u_4^2 = 4 \), implying that \( u_1, u_2, u_3, u_4 \in \{\pm 1\} \). Finally, using the fact that \( \mu = \frac{1+i+j+k}{2} \) and \( \mu^2 = \frac{-1+i+j+k}{2} \), it
is not hard to see that
\[(\mathbb{Z}H)^\times = \{\pm 1, \pm i, \pm j, \pm k, \pm \mu, \pm i\mu i, \pm j\mu j, \pm k\mu k, \pm \mu^2, \pm i\mu^2 i, \pm j\mu^2 j, \pm k\mu^2 k\}.
\]

2.3 A Useful Theorem

The next result gives a way of expressing powers of elements of overrings of $\mathbb{Z}Q$ that will come in handy in our later work.

**Theorem 2.3.1.** Let $R$ be any overring of $\mathbb{Z}Q$ in $\mathbb{Q}Q$, let $S = R \cap \mathbb{Q}$, and let $\alpha \in R$. Assume that $\beta \in R$ is such that $\alpha$ and $\beta$ have the same constant coefficient and $N(\beta) = N(\alpha)$. Then,

(i) For all $n \geq 0$, there exist $C_n, D_n \in S$ such that $\alpha^n = C_n \alpha + D_n$. Furthermore, $\beta^n = C_n \beta + D_n$.

(ii) If $f(x) \in S[x]$, then there exist $C, D \in S$ such that $f(\alpha) = C\alpha + D$. Furthermore, $f(\beta) = C\beta + D$.

(iii) If $f(x) \in R[x]$, then there exist $\gamma, \delta \in R$ such that $f(\alpha) = \gamma \alpha + \delta$. Furthermore, $f(\beta) = \gamma \beta + \delta$.

**Proof.** (i) We will use induction on $n$ and the fact that $\alpha^2 = 2a\alpha - N(\alpha)$, where $a$ is the constant coefficient of $\alpha$. 

\[\square\]
For the base case of the induction, we have $\alpha^0 = 1$, so $C_0 = 0$ and $D_0 = 1$. So, assume that $n \geq 0$ and $\alpha^n = C_n \alpha + D_n$ for some $C_n, D_n \in R \cap \mathbb{Q}$. Then,

$$
\alpha^{n+1} = C_n \alpha^2 + D_n \alpha \\
= C_n (2a\alpha - N(\alpha)) + D_n \alpha \\
= (2aC_n + D_n)\alpha - C_n N(\alpha).
$$

So, we can take

$$
C_{n+1} = 2aC_n + D_n \\
D_{n+1} = -C_n N(\alpha).
$$

By assumption, $C_n, D_n \in R \cap \mathbb{Q}$, and $2a, N(\alpha) \in R \cap \mathbb{Q}$ by Corollaries 2.1.3 and 2.1.5, so $C_{n+1}, D_{n+1} \in R \cap \mathbb{Q}$.

The second assertion follows because $C_n$ and $D_n$ were defined in terms of the constant coefficient of $\alpha$ and $N(\alpha)$.

(ii) Assume that $f(x) = \sum_r a_r x^r$, where each $a_r \in S$. Then,

$$
f(\alpha) = \sum_r a_r \alpha^r \\
= \sum_r a_r(C_r \alpha + D_r) \quad \text{for some } C_r, D_r \in S, \text{ by part (i)} \\
= C\alpha + D, \quad \text{where } C = \sum_r a_r C_r \in S \text{ and } D = \sum_r a_r D_r \in S.
$$

As above, the second assertion is true because $\alpha$ and $\beta$ have the same norm and constant coefficient.

(iii) This is essentially the same as the proof of (ii). 

\[\square\]
Remark. We proved the above theorem by using the relation $\alpha^2 = 2a\alpha - N(\alpha)$, but we could also have proven parts (ii) and (iii) by using $\min_\alpha(x)$. Since $\min_\alpha(x)$ is monic, we may divide $f(x) \in R[x]$ by $\min_\alpha(x)$ to get $f(x) = q(x) \min_\alpha(x) + \gamma x + \delta$ for some $q(x), \gamma x + \delta \in R[x]$. Then, $f(\alpha) = \gamma \alpha + \delta$, and we get $f(\beta) = \gamma \beta + \delta$ because $\alpha$ and $\beta$ have the same minimal polynomial.
CHAPTER 3

RINGS OF INTEGER-VALUED POLYNOMIALS

3.1 Proving Int$(R)$ Is a Ring

Recall that for any overring $R$ of $\mathbb{Z}$ in $\mathbb{Q}$, we define $\text{Int}(R) = \{ f(x) \in \mathbb{Q}[x] \mid f(\alpha) \in R \text{ for all } \alpha \in R \}$. The first theorem of this chapter proves that $\text{Int}(R)$ is a ring for any overring $R$ of $\mathbb{Z}$ in $\mathbb{Q}$.

Theorem 3.1.1. Let $R$ be any overring of $\mathbb{Z}$ in $\mathbb{Q}$. 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 $\mathbb{Q}[x]$, 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 $(fg)(\alpha)$ is in $R$.

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

\[
(fu)(\beta) = \sum r \alpha_r u\beta^r
= \sum r \alpha_r u\beta^r u^{-1}u
= \sum r \alpha_r (u\beta u^{-1})^r u
= f(u\beta u^{-1})u.
\]
Since \( f \in \text{Int}(R) \) and \( u \in R \), 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 2.2.3, \( R \subset SH \), 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

\[
(fg)(\alpha) = \sum_r \alpha_r g(\alpha) \alpha^r
= \sum_r \alpha_r (a + bi + cj + dk + e\mu) \alpha^r
= \sum_r \alpha_r (a\alpha^r + b\alpha^r + c\alpha^r + d\alpha^r + e\mu\alpha^r)
= a \sum_r \alpha_r \alpha^r + b \sum_r \alpha_r i\alpha^r + c \sum_r \alpha_r j\alpha^r
+ d \sum_r \alpha_r k\alpha^r + e \sum_r \alpha_r \mu\alpha^r
= af(\alpha) + b(fi)(\alpha) + c(fj)(\alpha) + d(fk)(\alpha) + e(f\mu)(\alpha).
\]

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

It is worth noting that the technique in the proof of Theorem 3.1.1 extends to different kinds 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 \( \text{Int}(\mathbb{Z}G) := \{ f \in \mathbb{Q}G[x] \mid f(\alpha) \in \mathbb{Z}G \text{ for all } \alpha \in \mathbb{Z}G \} \), 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 \( G \). A similar construction works over matrix rings if we define \( \text{Int}(M_n(\mathbb{Z})) := \{ f \in M_n(\mathbb{Q})[x] \mid f(A) \in M_n(\mathbb{Z}) \text{ for all } A \in M_n(\mathbb{Z}) \} \).
Furthermore, since reducing either $ZG$ or $M_n(Z)$ modulo an integer greater than 1 yields a finite quotient ring, the theorems in Chapter 4 can be used to construct elements of $\text{Int}(ZG)$ or $\text{Int}(M_n(Z))$.

More generally, the proof of Theorem 3.1.1 and the techniques of Chapter 4 should work as long as we have suitable algebras over $\mathbb{Z}$ and $\mathbb{Q}$ that have bases of units and as long as we have properly defined what an integer-valued polynomial means for such algebras (of course, we would need to determine exactly what “suitable” and “properly defined” mean). We shall not delve any further into this particular topic, but it definitely warrants future research.

Recall that for $\alpha = a + bi + cj + dk \in \mathbb{H}$, the bar conjugate of $\alpha$ is defined to be $\overline{\alpha} = a - bi - cj - dk$. We have a similar definition for polynomials in $\mathbb{H}[x]$. Given $f(x) = \sum_r \alpha_r x^r$ with coefficients in $\mathbb{H}$, define the bar conjugate polynomial $\overline{f}$ to be $\overline{f}(x) = \sum_r \overline{\alpha}_r x^r$. A subset $S \subseteq \mathbb{H}[x]$ is said to be closed under bar conjugation if $\overline{f} \in S$ for all $f \in S$. The rest of this section is devoted to showing that if $R = SQ$ for some overring $S$ of $\mathbb{Z}$ in $\mathbb{Q}$, then $\text{Int}(R)$ is closed under bar conjugation. Proving this is straightforward, if a bit technical. It turns out that when $R = SH$, $\text{Int}(R)$ is also closed under bar conjugation, but in this case the proof requires some of the techniques used in Chapters 4 and 5. In light of this, we delay the proof that $\text{Int}(SH)$ is closed under bar conjugation until Chapter 5.

**Lemma 3.1.2.** Let $\alpha, \beta \in \mathbb{H}$. Then,

$$\overline{\alpha \beta} = \frac{1}{2} \left( \alpha \overline{\beta} + \overline{\alpha \beta} \right) + \frac{1}{2} \left( \alpha(-i\overline{\beta}i) + \overline{\alpha(-i\overline{\beta}i)} \right) i$$

$$+ \frac{1}{2} \left( \alpha(-j\overline{\beta}j) + \overline{\alpha(-j\overline{\beta}j)} \right) j + \frac{1}{2} \left( \alpha(-k\overline{\beta}k) + \overline{\alpha(-k\overline{\beta}k)} \right) k$$
Proof. Before diving into the proof, it is useful to consider what this lemma actually says. The expression $\frac{1}{2} (\alpha \overline{\beta} + \overline{\alpha \beta})$ represents the constant coefficient of $\alpha \overline{\beta}$, so the lemma is indicating that $\alpha \overline{\beta}$ and $\overline{\alpha \beta}$ have the same constant coefficient. Similarly, $\frac{1}{2} (\alpha (-i \overline{\beta}i) + \overline{\alpha (-i \overline{\beta}i)}i)$ equals the constant coefficient of $\alpha (-i \overline{\beta}i)$, which is the negative of the coefficient of $i$ in $\alpha (-i \overline{\beta}i)$. Thus, the lemma says that coefficient of $i$ in $\overline{\alpha \beta}$ is the negative of the coefficient of $i$ in $\alpha (-i \overline{\beta}i)$. Analogous statements hold for $j$ and $k$.

Now, let $\alpha = a + bi + cj + dk$ and $\beta = x + yi + zj + wk$. Then,

$$\overline{\alpha \beta} = (a - bi - cj - dk)(x + yi + zj + wk)$$

$$= (ax + by + cz + dk) + (ay - bx - cw + dz)i$$

$$+ (az + bw - cx - dy)j + (aw - bz + cy - dx)k.$$  

We have $\overline{\beta} = x - yi - zj - wk$, and one may compute that the constant coefficient of $\overline{\alpha \beta}$ equals $ax + by + cz + dk$. So,

$$ax + by + cz + dk = \frac{1}{2} \left( \alpha \overline{\beta} + \overline{\alpha \beta} \right).$$

Next, since $-i \overline{\beta}i = x - yi + zj + wk$, computation shows that the coefficient of $i$ in $\alpha (-i \overline{\beta}i)$ equals $-ay + bx + cw - dz$. So, the constant coefficient of $\alpha (-i \overline{\beta}i)$ is $-(-ay + bx + cw - dz) = ay - bx - cw + dz$, and thus

$$(ay - bx - cw + dz)i = \frac{1}{2} \left( \alpha (-i \overline{\beta}i) + \overline{\alpha (-i \overline{\beta}i)}i \right) i.$$  

Arguing in a similar manner, one can show that

$$(az + bw - cx - dy)j = \frac{1}{2} \left( \alpha (-j \overline{\beta}j) + \overline{\alpha (-j \overline{\beta}j)}j \right) j$$

$$(aw - bz + cy - dx)k = \frac{1}{2} \left( \alpha (-k \overline{\beta}k)k + \overline{\alpha (-k \overline{\beta}k)k} \right) k,$$

which proves the lemma. \qed
The next lemma presents a polynomial analogue of Lemma 3.1.2.

**Lemma 3.1.3.** Let \( f(x) \in \mathbb{H}[x] \) and \( \beta \in \mathbb{H} \). Then,

\[
\overline{f(\beta)} = \frac{1}{2} \left( f(\overline{\beta}) + f(\overline{\beta}) \right) + \frac{1}{2} \left( f(-i\overline{\beta}i) + f(-i\overline{\beta}i) \right) i + \frac{1}{2} \left( f(-j\overline{\beta}j) + f(-j\overline{\beta}j) \right) j + \frac{1}{2} \left( f(-k\overline{\beta}k) + f(-k\overline{\beta}k) \right) k
\]

*Proof.* Note that taking the bar conjugate in \( \mathbb{H}[x] \) is additive: if \( g, h \in \mathbb{H}[x] \), then \( \overline{g + h} = \overline{g} + \overline{h} \). Thus, it suffices to prove the lemma for monomials. Assume that \( f(x) = \alpha x^r \in \mathbb{H}[x] \). By Lemma 3.1.2, we have

\[
\overline{f(\beta)} = \overline{\alpha \beta^r} = \frac{1}{2} \left( \overline{\alpha \beta^r} + \overline{\alpha \beta^r} \right) + \frac{1}{2} \left( \overline{\alpha(-i\overline{\beta}i)} + \overline{\alpha(-i\overline{\beta}i)} \right) i + \frac{1}{2} \left( \overline{\alpha(-j\overline{\beta}j)} + \overline{\alpha(-j\overline{\beta}j)} \right) j + \frac{1}{2} \left( \overline{\alpha(-k\overline{\beta}k)} + \overline{\alpha(-k\overline{\beta}k)} \right) k.
\]

We always have \( \overline{\beta^r} = (\overline{\beta})^r \), so

\[
\frac{1}{2} \left( \overline{\alpha \beta^r} + \overline{\alpha \beta^r} \right) = \frac{1}{2} \left( \overline{\alpha \beta^r} + \overline{\alpha \beta^r} \right) = \frac{1}{2} \left( f(\overline{\beta}) + f(\overline{\beta}) \right).
\]

Next, consider the coefficient of \( i \) in the above expression for \( \overline{f(\beta)} \). Since \( i \) is invertible with inverse \(-i\), we get \( -i\overline{\beta}i = (-i\beta i)^r \). So,

\[
\frac{1}{2} \left( \overline{\alpha(-i\overline{\beta}i)} + \overline{\alpha(-i\overline{\beta}i)} \right) = \frac{1}{2} \left( \overline{\left( \alpha(-i\beta i)^r \right)} i + \overline{\left( \alpha(-i\beta i)^r \right)} i \right) = \frac{1}{2} \left( f(-i\overline{\beta}i) + f(-i\overline{\beta}i) \right).
\]

Analogous results hold for \( j \) and \( k \), from which we conclude the desired result. \(\square\)

**Proposition 3.1.4.** Let \( R \) be an overring of \( \mathbb{Z}Q \) in \( \mathbb{Q}Q \) such that \( R = SQ \) for some overring \( S \) of \( \mathbb{Z} \) in \( \mathbb{Q} \). Then, \( \text{Int}(R) \) is closed under bar conjugation.
Proof. Let \( f(x) = \sum \alpha_r x^r \in \text{Int}(R) \). By Lemma 3.1.3, for each \( \beta \in R \) we have

\[
\overline{f}(\beta) = \frac{1}{2} \left( f(\beta) + \overline{f(\beta)} \right) + \frac{1}{2} \left( f(-i\beta)i + \overline{f(-i\beta)i} \right) i \\
+ \frac{1}{2} \left( f(-j\beta j)j + \overline{f(-j\beta j)j} \right) j + \frac{1}{2} \left( f(-k\beta k)k + \overline{f(-k\beta k)k} \right) k.
\]

Now, \( f(\beta) \in R \) and \( \frac{1}{2}(f(\beta) + \overline{f(\beta)}) \) equals the constant coefficient of \( f(\beta) \). Since \( R = SQ \), Theorem 2.2.3 part (i) tells us that every coefficient of every element of \( R \) is in \( R \); thus, \( \frac{1}{2}(f(\beta) + \overline{f(\beta)}) \in R \). Similarly, the other coefficients in the above expression for \( \overline{f}(\beta) \) are in \( R \). Thus, \( \overline{f}(\beta) \in R \) and \( \overline{f}(x) \in \text{Int}(R) \).

\[\square\]

### 3.2 The Trouble with Bar Conjugation in \( \text{Int}(\mathbb{Z}H) \)

We would like to be able to extend Proposition 3.1.4 to all overrings of \( \mathbb{Z}Q \) in \( \mathbb{Q}Q \). The difficulty with accomplishing this latter goal comes from the expression

\[
\overline{f}(\beta) = \frac{1}{2} \left( f(\beta) + \overline{f(\beta)} \right) + \frac{1}{2} \left( f(-i\beta)i + \overline{f(-i\beta)i} \right) i \\
+ \frac{1}{2} \left( f(-j\beta j)j + \overline{f(-j\beta j)j} \right) j + \frac{1}{2} \left( f(-k\beta k)k + \overline{f(-k\beta k)k} \right) k.
\]  

(3.2.1)

In the proof of Proposition 3.1.4, we showed that \( \overline{f}(\beta) \in R \) by arguing that each coefficient of \( \overline{f}(\beta) \) in (3.2.1) lies in \( R \), which relied on Theorem 2.2.3 part (i). However, this last result does not apply to arbitrary overrings of \( \mathbb{Z}Q \). For example, let \( f \in \text{Int}(\mathbb{Z}H) \) and \( \beta \in \mathbb{Z}H \), and consider \( \frac{1}{2}(f(\beta) + \overline{f(\beta)}) \) as in (3.2.1). By assumption, \( f(\beta) \) is in \( \mathbb{Z}H \), and \( \frac{1}{2}(f(\beta) + \overline{f(\beta)}) \) is simply the constant coefficient of \( f(\beta) \). Every coefficient of every element of \( \mathbb{Z}H \) lies in either \( \mathbb{Z} \) or \( \mathbb{Z} + \frac{1}{2} \), so \( \frac{1}{2}(f(\beta) + \overline{f(\beta)}) \) is either an integer or a half-integer. Similarly, the other coefficients in (3.2.1) all lie in either \( \mathbb{Z} \) or \( \mathbb{Z} + \frac{1}{2} \). This is good; it means that we will not get anything bizarre or unexpected in (3.2.1). The problem is that for any element \( \alpha \in \mathbb{Z}H \) either every coefficient of \( \alpha \)
lies in \( \mathbb{Z} \), or every coefficient of \( \alpha \) lies in \( \mathbb{Z} + \frac{1}{2} \), and a priori the coefficients in (3.2.1) have nothing to do with one another. For example, if

\[
\frac{1}{2} \left( f(\overline{\beta}) + f(\overline{\beta}) \right) = \frac{3}{2}
\]

and

\[
\frac{1}{2} \left( f(-i\overline{\beta}i) + f(-i\overline{\beta}i) \right) = 3,
\]

then we would be forced to conclude that \( \overline{f} \notin \text{Int}(\mathbb{Z}H) \), since \( \overline{f}(\beta) \notin \mathbb{Z}H \).

We will show in Chapter 5 (Theorem 5.2.4) that \( \text{Int}(\mathbb{Z}H) \) is in fact closed under \( \overline{\cdot} \) conjugation, so the situation just described cannot occur. However, the proof of Theorem 5.2.4 is attained only after an extensive study of the quotient rings of \( \mathbb{Z}H \). Thus, while the result of Proposition 3.1.4 is true when \( R = \mathbb{Z}H \), the proof given in this chapter is not applicable.

### 3.3 Localization Properties

When \( D \) is a (commutative) Noetherian domain, the formation of integer-valued polynomials over \( D \) behaves well with respect to localization, as the following theorem illustrates.

**Theorem 3.3.1.** Let \( D \) be a (commutative) Noetherian domain and let \( S \) be a multiplicatively closed subset of \( D \) that does not contain 0. Then, \( S^{-1}\text{Int}(D) = \text{Int}(S^{-1}D) \).

**Proof.** This is Theorem I.2.3 in [2]. \( \Box \)

It turns out that we can get similar behavior with quaternion rings if the subset \( S \) consists of integers.

**Theorem 3.3.2.** Let \( R \) be an overring of \( \mathbb{Z}Q \) in \( QQ \), and let \( T \) be a multiplicatively closed subset of \( \mathbb{Z} \) that does not contain 0. Then, \( T^{-1}\text{Int}(R) = \text{Int}(T^{-1}R) \).
Proof. The proof is essentially the same as the proof of Theorem 1.2.3 in [2], except that some minor modifications are necessary because $R$ is noncommutative.

First, we show that $T^{-1}\text{Int}(R) \subseteq \text{Int}(T^{-1}R)$. Let $f(x) \in T^{-1}\text{Int}(R)$, and let $\frac{\alpha}{t} \in T^{-1}R$, where $\alpha \in R$ and $t \in T$. We need to show that $f\left(\frac{\alpha}{t}\right) \in T^{-1}R$. To do so, we use induction on the degree of $f$. Let $n = \deg(f)$. If $n = 0$, then $f$ is a constant and there is nothing to prove. So, assume $n > 0$ and that every polynomial in $T^{-1}\text{Int}(R)$ of degree less than $n$ is an element of $\text{Int}(T^{-1}R)$. Let $g(x) = t^n f(x) - f(tx)$.

Since $t \in \mathbb{Z}$, $f(tx)$ is a polynomial in $T^{-1}\text{Int}(R)$, so $g(x) \in T^{-1}\text{Int}(R)$. Furthermore, $\deg(g) < \deg(f)$, so by induction $g(x) \in \text{Int}(T^{-1}R)$. Now, $t^n f(x) = g(x) - f(tx)$, so

$$t^n f\left(\frac{\alpha}{t}\right) = g\left(\frac{\alpha}{t}\right) - f(\alpha).$$

Consider the right-hand side of this equation. We have $g\left(\frac{\alpha}{t}\right) \in T^{-1}R$ since $g(x) \in \text{Int}(T^{-1}R)$, and $f(x) \in T^{-1}\text{Int}(R)$, so $f(x) = \frac{F(x)}{t}$ for some $F(x) \in \text{Int}(R)$ and some $t' \in T$; hence, $f(\alpha) = \frac{F(\alpha)}{t'} \in T^{-1}R$. So, $t^n f\left(\frac{\alpha}{t}\right) \in T^{-1}R$. But, $t$ is a unit in $T^{-1}R$, so $f\left(\frac{\alpha}{t}\right) \in T^{-1}R$ and $f(x) \in \text{Int}(T^{-1}R)$. This shows that $T^{-1}\text{Int}(R) \subseteq \text{Int}(T^{-1}R)$.

For the reverse inclusion, let $h(x) = \sum_{r=0}^{d} \alpha_r x^r \in \text{Int}(T^{-1}R)$. Let $C = \alpha_0 R + \alpha_1 R + \cdots + \alpha_d R$ be the right $R$-module generated by the coefficients of $h$. Since $R$ is Noetherian as a right $R$-module over itself and $C$ is finitely generated, $C$ is Noetherian as a right $R$-module (this follows from Proposition 1.4 in Chapter X of [7]). Let $M$ be the right $R$-module generated by $\{h(\beta)\}_{\beta \in R}$. Then, $M \subseteq C$ and $C$ is Noetherian, so $M$ is finitely generated as a right $R$-module. Let $\gamma_1, \gamma_2, \ldots, \gamma_m$ be the generators for $M$ as a right $R$-module.

Now, since $h(x) \in \text{Int}(T^{-1}R)$, $M$ is contained in $T^{-1}R$. So, $\gamma_1, \gamma_2, \ldots, \gamma_m \in T^{-1}R$, and by finding a common denominator, we see that there exists $u \in T$ such that $u \gamma_\ell \in R$ for each $1 \leq \ell \leq m$. Thus, for each $\gamma \in M$, $u \gamma \in R$. In particular, we
have $uh(\beta) \in R$ for all $\beta \in R$. Hence, $uh(x) \in \text{Int}(R)$ and $h(x) \in T^{-1}\text{Int}(R)$, as required.

When combined with Theorem 2.2.3, the previous theorem says, in effect, that to prove something is true for $\text{Int}(R)$ with $R$ an overring of $\mathbb{Z}Q$ in $\mathbb{Q}Q$, it suffices to consider what happens for $\text{Int}(\mathbb{Z}Q)$ and $\text{Int}(\mathbb{Z}H)$. Assume that $R$ is an overring of $\mathbb{Z}Q$ in $\mathbb{Q}Q$. Then, by Theorem 2.2.3, we know that $R = SQ$ or $R = SH$, where $S$ is an overring of $\mathbb{Z}$ in $\mathbb{Q}$. Now, by taking $T$ to be the set of integers that are invertible in $S$, it is straightforward to check that $T$ is multiplicatively closed and $S = T^{-1}\mathbb{Z}$. So, Theorem 3.3.2 tells us that to study $\text{Int}(R)$ it is enough to consider $T^{-1}\text{Int}(\mathbb{Z}Q)$ and $T^{-1}\text{Int}(\mathbb{Z}H)$. Most of the rest of this text will focus on topics (such as generating sets and prime ideals) that behave well under localization at subsets of $\mathbb{Z}$. So, it is no loss to stop considering general overrings of $\mathbb{Z}Q$ and instead focus on $\mathbb{Z}Q$ and $\mathbb{Z}H$, and we will follow this tactic in the chapters to follow.
CHAPTER 4

MUFFINS AND GENERATING SETS (I)

4.1 What Are Muffins, and Why Do We Care?

The major goal in this chapter is to establish a generating set for Int($\mathbb{Z}Q$) over $\mathbb{Z}Q$. That is, we wish to describe a collection $\mathcal{P}$ of polynomials in Int($\mathbb{Z}Q$) such that Int($\mathbb{Z}Q$) = $\mathbb{Z}Q[\mathcal{P}]$. Furthermore, we would like these generators to be “nice” in the sense that all the polynomials in $\mathcal{P}$ have a standard form or satisfy similar properties. Currently, we do not have such a generating set, although we can classify many of the polynomials in Int($\mathbb{Z}Q$) (see Corollary 4.3.10).

In Chapter 5, we will describe a full generating set (in the sense of the previous paragraph) for Int($\mathbb{Z}H$). As we shall see, the reason we will have more success with Int($\mathbb{Z}H$) is because $\mathbb{Z}H$ is a principal ideal ring, a property that makes the ideal structure of $\mathbb{Z}H$ less complicated than the ideal structure of $\mathbb{Z}Q$. However, the present chapter lays all of the groundwork for the theorems of Chapter 5, and in fact most of the results proven here will carry over to Int($\mathbb{Z}H$), sometimes without change and other times with minor modifications.

Our basic strategy in this chapter is to replace calculations in the infinite ring Int($\mathbb{Z}Q$) with calculations in quotient rings of $\mathbb{Z}Q$, which (with the exception of $\mathbb{Z}Q$
itself) are all finite rings. In fact, the idea of working in quotient rings of \( \mathbb{Z}Q \) and later \( \mathbb{Z}H \) will be a recurring theme for the remainder of this manuscript. The first result of this chapter shows why this technique is applicable to the study of integer-valued polynomials.

**Correspondence 4.1.1.**

(i) Let \( f(x) \in \text{Int}(\mathbb{Z}Q) \). Then, there exist \( g(x) \in \mathbb{Z}Q[x] \) and an integer \( n > 0 \) such that \( f(x) = \frac{g(x)}{n} \).

(ii) Let \( g(x) \in \mathbb{Z}Q[x] \) and let \( n > 0 \). Then, \( \frac{g(x)}{n} \in \text{Int}(\mathbb{Z}Q) \) if and only if \( g(\alpha) \equiv 0 \) in \( \mathbb{Z}Q/(n) \) for all \( \alpha \in \mathbb{Z}Q/(n) \) (here, \( (n) \) is the ideal of \( \mathbb{Z}Q \) generated by \( n \)).

**Proof.** (i) Essentially, we just need to find a common denominator for the coefficients of \( f(x) \). Write \( f(x) = \sum_r \alpha_r x^r \), where each \( \alpha_r \in \mathbb{Q}Q \). Now, for \( \alpha \in \mathbb{Q}Q \) we may write

\[
\alpha = \frac{a_1}{n_1} + \frac{a_2}{n_2} + \frac{a_3}{n_3} + \frac{a_4}{n_4}
\]

for some \( q_\ell, n_\ell \in \mathbb{Z}, 1 \leq \ell \leq 4 \). But, by finding a common denominator \( d \in \mathbb{Z} \) for the \( \frac{q_\ell}{n_\ell} \), we can write \( \alpha = \frac{a'}{d} \) for some \( a' \in \mathbb{Z}Q \). Applying this to each coefficient of \( f(x) \), we have \( f(x) = \sum_r \frac{a'_r}{d} x^r \), where each \( d_r \in \mathbb{Z} \) and each \( a'_r \in \mathbb{Z}Q \). Letting \( n \) be the least common multiple of the \( d_r \), we may write \( f(x) = \sum_r \frac{\beta_r}{n} x^r \) for some \( \beta_r \in \mathbb{Z}Q \). Thus, taking \( g(x) = \sum_r \beta_r x^r \in \mathbb{Z}Q[x] \), we have \( f(x) = \frac{g(x)}{n} \), as required.

(ii) (\( \Rightarrow \)) Let \( f(x) = \frac{g(x)}{n} \) and assume that \( \frac{g(x)}{n} \in \text{Int}(\mathbb{Z}Q) \). Since \( f(\alpha) \in \mathbb{Z}Q \) for all \( \alpha \in \mathbb{Z}Q \), \( n \) divides \( g(\alpha) \) for all \( \alpha \in \mathbb{Z}Q \). This means that \( g(\alpha) \equiv 0 \) in \( \mathbb{Z}Q/(n) \) for any residue \( \alpha \in \mathbb{Z}Q/(n) \).
(⇐) Assume that \( g(x) \in \mathbb{Z}Q[x] \) and \( n > 0 \) are such that \( g(\alpha) \equiv 0 \) in \( \mathbb{Z}Q/(n) \) for all \( \alpha \in \mathbb{Z}Q/(n) \). Let \( \beta \in \mathbb{Z}Q \), and let \( \beta' \) represent the residue of \( \beta \) in \( \mathbb{Z}Q/(n) \). Then, \( g(\beta) \equiv g(\beta') \equiv 0 \) in \( \mathbb{Z}Q/(n) \), so \( g(\beta) \in (n) \) in \( \mathbb{Z}Q \). Since \( \beta \in \mathbb{Z}Q \) was arbitrary, we conclude that \( \frac{g(x)}{n} \in \text{Int}(\mathbb{Z}Q) \).

The preceding theorem gives us two powerful methods for dealing with \( \text{Int}(\mathbb{Z}Q) \). First, given \( f(x) = \frac{g(x)}{n} \in \mathbb{Q}Q[x] \) with \( g(x) \in \mathbb{Z}Q[x] \) and \( n > 0 \), to show that \( f(x) \in \text{Int}(\mathbb{Z}Q) \) it suffices to check the values of \( f(x) \) on a finite set: the set of representatives for the residues in \( \mathbb{Z}Q/(n) \). Second, if we know that \( f(x) = \frac{g(x)}{n} \in \text{Int}(\mathbb{Z}Q) \), then \( g(x) \mod n \) (the polynomial resulting from reducing each coefficient of \( g(x) \) modulo the integer \( n \)) is a polynomial in \( \mathbb{Z}Q/(n) \) \([x]\) that sends each element of \( \mathbb{Z}Q/(n) \) to 0 in \( \mathbb{Z}Q/(n) \). If we can classify each such \( g(x) \) for each integer \( n > 1 \), then we will be able to establish a generating set for \( \text{Int}(\mathbb{Z}Q) \).

In light of these observations, it makes sense to study quotient rings of \( \mathbb{Z}Q \), i.e. rings of the form \( \mathbb{Z}Q/I \), where \( I \) is an ideal of \( \mathbb{Z}Q \). If \( R \) is such a quotient ring and \( f \in R[x] \), then we frequently abuse our notation and consider \( f \) to be a polynomial in \( \mathbb{Z}Q[x] \). Furthermore, if \( I \) is an ideal of \( R \), then we may also reduce the coefficients of \( f \) modulo \( I \) to get \( f \) in \( (R/I) [x] \); we refer to this polynomial as \( f \mod I \). In general, the ring from which a polynomial takes its coefficients should be clear from context.

As mentioned above, it will be helpful to look for polynomials in quotient rings of \( \mathbb{Z}Q \) that kill each element of the ring. This inspires the following definition.

**Definition 4.1.2.** For any ring \( R \), let \( \text{Muff}(R) = \{ f(x) \in R[x] \mid f(\alpha) = 0 \text{ for all } \alpha \in R \} \), called (for want of a better term) the muffin of \( R \).

In terms of this definition, Correspondence 4.1.1 can be rephrased as follows:
• $f(x) \in \text{Int}(\mathbb{Z}Q)$ can be written as $\frac{g(x)}{n}$ with $g(x) \in \mathbb{Z}Q[x]$ and $n > 0$ if and only if $g(x) \mod n \in \text{Muff}(\mathbb{Z}Q/(n))$.

• if $g(x) \in \text{Muff}(\mathbb{Z}Q/(n))$, then $\frac{g(x)}{n} \in \text{Int}(\mathbb{Z}Q)$.

If $R$ is an infinite ring, then there is no guarantee that $\text{Muff}(R) \neq \{0\}$. For our purposes, we shall focus on finite quotient rings of $\mathbb{Z}Q$, and (as shown below in Proposition 4.1.5) if $R$ is such a ring, then $\text{Muff}(R)$ always contains non-trivial elements.

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 $n \neq 0$. 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 $\mathbb{Z}Q/(n)$. More generally, if $R$ is a finite quotient ring of $\mathbb{Z}Q$ and $n$ is the characteristic of $R$, then we may view $\mathbb{Z}/n\mathbb{Z}$ as a subring of $R$.

If $I$ is any non-zero ideal of $\mathbb{Z}Q$, then $N(\alpha) = \alpha \bar{\alpha}$ is in $I$ for any $\alpha \in I$, so $I$ always contains a non-zero integral ideal $(n)$ and hence $\mathbb{Z}Q/I$ is a quotient of the finite ring $\mathbb{Z}Q/(n)$. In general, we will be obtaining information about $\text{Muff}(\mathbb{Z}Q/I)$ where $I$ is a proper, non-zero ideal of $\mathbb{Z}Q$. In the case where $I = (n)$ for some $n > 0$, we let $\text{Muff}(n) = \text{Muff}(\mathbb{Z}Q/I)$. Note that $\text{Muff}(1) = \{0\}$.

Before long, we shall be delving into a protracted discussion on muffins, but we first describe some notation considering ideals and quotient rings of $\mathbb{Z}Q$.

When $n \in \mathbb{Z}$, we will usually denote the ideal of $\mathbb{Z}Q$ generated by $n$ as $(n)$, and we may write “$(n)$ in $\mathbb{Z}Q$.” If, instead, we wish to work with the ideal $I$ generated by $n$ in a quotient ring $R$ of $\mathbb{Z}Q$, then we will normally write $I = nR$ or $I = Rn$; this is
done to avoid confusion about the ring in which $I$ resides. Since $n \in \mathbb{Z}$, the left ideal $Rn$, the right ideal $nR$, and the two-sided ideal $(n)$ are all the same in $R$, so there is no loss of information with this notation. If $\alpha$ is not central in $R$, then $\alpha R$, $R \alpha$, and $(\alpha)$ might all be different, so when considering the ideal generated by $\alpha$, we will tend to write “$(\alpha)$ in $R$” or “$(\alpha)$ in $\mathbb{Z}Q$” if the ring in which the ideal resides might not be clear from context.

As discussed in Chapter 6, the definition of a prime ideal in a noncommutative ring is different than the definition in a commutative ring. However, the definition of a maximal ideal remains unchanged. For any ring $R$, let $\text{Max}(R)$ denote the collection of maximal ideals of $R$. Then, one can show (see [4], Chapter 3) that $\text{Max}(\mathbb{Z}Q) = \{(1 + i, 1 + j)\} \cup \{(p) \mid p \text{ is an odd prime}\}$. Given this, the following proposition is not surprising.

**Proposition 4.1.3.** Let $R$ be any quotient ring of $\mathbb{Z}Q$. Let $n = \text{char}(R)$. Let $I = (1 + i, 1 + j)$ in $R$. Then,

(i) $\text{Max}(R) \subseteq \{I\} \cup \{pR \mid p \text{ is an odd prime}\}$.

(ii) if $n$ is odd, then $\text{Max}(R) = \{pR \mid p \text{ is an odd prime and } p \text{ divides } n\}$.

(iii) if $n$ is even, then $\text{Max}(R) = \{I\} \cup \{pR \mid p \text{ is an odd prime and } p \text{ divides } n\}$.

**Proof.** (i) Since $R$ is a quotient of $\mathbb{Z}Q$, each maximal ideal of $R$ is the image of some ideal in $\text{Max}(\mathbb{Z}Q)$ under the quotient map $\mathbb{Z}Q \to R$. Thus, $\text{Max}(R) \subseteq \{I\} \cup \{pR \mid p \text{ is an odd prime }\}$.

(ii) Assume $n$ is odd. Then, both $1 + i$ and $1 + j$ are invertible in $R$ (because they have norm 2), so $(1 + i, 1 + j)$ in $R$ equals $R$. For an odd prime $p$, we have $pR \neq R$ if
and only if \( p \mid n \). Furthermore, if \( p \mid n \), then \( pR \) is a maximal ideal of \( R \) because \((p)\) is a maximal ideal in \( \mathbb{Z}Q \).

(iii) This is the same as (ii), except that \((1 + i, 1 + j)\) in \( R \) is a proper ideal of \( R \) because \( 1 + i \) and \( 1 + j \) are not invertible in \( R \). \( \blacksquare \)

We now proceed to the first substantial result about muffins, which shows that \( \text{Muff}(R) \) is always an ideal of \( R[x] \).

**Proposition 4.1.4.** Let \( R \) be a finite, non-zero quotient ring of \( \mathbb{Z}Q \). Then, \( \text{Muff}(R) \) is an ideal of \( R[x] \).

**Proof.** This is similar to the proof of Theorem 3.1.1. It is easy to see that \( \text{Muff}(R) \) is closed under addition. Let \( f \in \text{Muff}(R) \), let \( g \in R[x] \), and let \( \alpha \in R \). It suffices to show that \((fg)(\alpha)\) and \((gf)(\alpha)\) are both 0. Write \( g(\alpha) \equiv a + bi + cj + dk \). Then, as in Theorem 3.1.1,

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

and since \( f \in \text{Muff}(R) \), each of \( f(\alpha) \), \( f(-i\alpha i) \), \( f(-j\alpha j) \), and \( f(-k\alpha k) \) is 0. Hence, \((fg)(\alpha) \equiv 0 \). Let \( g(x) = \sum_r \beta_r x^r \), where each \( \beta_r \in R \). Then,

\[
(gf)(\alpha) \equiv \sum_r \beta_r f(\alpha) \alpha^r \equiv 0.
\]

Thus, \( fg, gf \in \text{Muff}(R) \), and \( \text{Muff}(R) \) is in ideal of \( R[x] \). \( \blacksquare \)

As mentioned above, \( \text{Muff}(R) \) is non-zero for any non-zero finite ring \( R \). When \( I \) is a proper, non-zero ideal of \( \mathbb{Z}Q \) and \( R = \mathbb{Z}Q/I \), we can explicitly describe some of the elements in \( \text{Muff}(R) \).
Proposition 4.1.5. Let $R$ be a finite, non-zero quotient ring of $\mathbb{Z}Q$, and let $n = \text{char}(R)$. Then, $\text{Muff}(R)$ contains a monic polynomial with coefficients in $\mathbb{Z}/n\mathbb{Z}$.

Proof. Given any $\alpha \equiv a + bi + cj + dk \in R$, we know that $\alpha^2 \equiv 2aa - N(\alpha)$. This means that $\alpha$ is a root of the polynomial $x^2 - 2ax + N(\alpha)$ in $(\mathbb{Z}/n\mathbb{Z})[x]$. Let $S = \{x^2 + bx + c \in R[x] \mid b, c \in \mathbb{Z}/n\mathbb{Z}\}$ and let $f(x) = \prod_{g(x) \in S} g(x)$. Then, $f(x)$ is monic and has coefficients in $\mathbb{Z}/n\mathbb{Z}$, and since each $g(x) \in S$ is central in $R[x]$ we have $f(\alpha) \equiv \prod_{g(x) \in S} g(\alpha) \equiv 0$ for all $\alpha \in R$. Thus, $f \in \text{Muff}(R)$, as desired. \qed

4.2 The Polynomials $\phi_R$

With $R$ and $n$ as in the preceding proposition, we have established that $\text{Muff}(R)$ always contains a monic polynomial with coefficients in $\mathbb{Z}/n\mathbb{Z}$. So, we may pick such a monic polynomial in $\text{Muff}(R)$ of least degree, and we denote this polynomial by $\phi_R$. When $R = \mathbb{Z}Q/(n)$, we let $\phi_n = \phi_R$; when necessary (as in Corollaries 4.3.8 and 4.3.10), we take $\phi_1 = x$. We make no claims about the uniqueness of any $\phi_R$; in most cases, there could be numerous choices for a $\phi_R$. However, in the results that follow, no uniqueness will be required. So, the reader may assume at this point that we have fixed $\phi_R$ for each finite, non-zero quotient ring $R$ of $\mathbb{Z}Q$. As we will show later, the collection of $\phi_R$ will help comprise a generating set for $\text{Int}(\mathbb{Z}Q)$ over $\mathbb{Z}Q$ (and selecting different polynomials $\phi_R$ will give different generating sets). At this point, the most important thing to recognize about $\phi_n$ is that for each $n > 1$, $\frac{\phi_n}{n} \in \text{Int}(\mathbb{Z}Q)$.

At the present time, we can say little about what $\phi_R$ is for a general quotient ring $R$ of $\mathbb{Z}Q$, but we do have enough tools to determine $\phi_p$ for an odd prime $p$. We shall
do this below, after proving a proposition and a lemma. The proposition gives some basic information about elements of $\mathbb{Z}Q/(p)$ when $p$ is an odd prime.

**Proposition 4.2.1.** Let $p$ be an odd prime. Let $\alpha \in \mathbb{Z}Q/(p)$, and let $a$ be the constant coefficient of $\alpha$. Then,

(i) $\alpha$ is a unit $\iff N(\alpha) \not\equiv 0$.

(ii) $\alpha$ is nilpotent $\iff N(\alpha) \equiv 0$ and $a \equiv 0$.

(iii) $\alpha$ is a non-nilpotent zero divisor $\iff N(\alpha) \equiv 0$ and $a \not\equiv 0$.

(iv) if $\alpha$ is nilpotent, then $\alpha^2 \equiv 0$.

(v) for all $\beta \in \mathbb{Z}Q/(2)$, either $\beta^2 \equiv 0$ or $\beta^2 \equiv 1$; hence, $\mathbb{Z}Q/(2)$ has no non-nilpotent zero divisors.

**Proof.**

(i) Assume $N(\alpha) \not\equiv 0$. Then, $N(\alpha)$ is invertible mod $p$ and $N(\alpha)^{p-1} \equiv 1$. Since $\alpha$ and $\bar{\alpha}$ commute and $\alpha\bar{\alpha} \equiv N(\alpha)$, we have $\alpha(\alpha^{p-2}\bar{\alpha}^{p-1}) \equiv N(\alpha)^{p-1} \equiv 1$ and $\alpha$ is a unit.

Conversely, if $N(\alpha) \equiv 0$, then $a\bar{\alpha} \equiv 0$, so $\alpha$ is a zero divisor and hence cannot be a unit.

(ii) If $N(\alpha) \equiv 0$ and $a \equiv 0$, then $\alpha^2 \equiv 2a\alpha - N(\alpha) \equiv 0$ and $\alpha$ is nilpotent.

Conversely, assume $\alpha^n \equiv 0$ for some $n > 0$. Then, $\alpha$ is not a unit, so $N(\alpha) \equiv 0$. Since $\alpha^2 \equiv 2a\alpha$, a quick induction shows that $\alpha^m \equiv (2a)^{m-1}\alpha$ for all $m > 0$. So, $0 \equiv \alpha^n \equiv (2a)^{n-1}\alpha$.

Let $\alpha \equiv a + bi + cj + dk$. If $\alpha \equiv a$, then since $\alpha$ is nilpotent and $\mathbb{Z}/p\mathbb{Z}$ is a field, we must have $a \equiv 0$. If $\alpha \not\equiv a$, then one of $b$, $c$, or $d$ is not equivalent to 0. WLOG,
assume that \( b \neq 0 \). Then, the fact that \( 0 \equiv (2a)^{n-1}\alpha \) means that \((2a)^{n-1}b \equiv 0 \). This forces \((2a)^{n-1} \equiv 0 \), and consequently \( a \equiv 0 \), as required.

(iii) This follows from (i), (ii), and the fact that every non-unit in a finite ring is a zero divisor.

(iv) This follows from (ii) and the fact that \( \alpha^2 = 2a\alpha - N(\alpha) \).

(v) Let \( \beta \in (\mathbb{Z}/(2)\mathbb{Z})Q \) with constant coefficient \( x \). Then, \( \beta^2 \equiv 2x\beta - N(\beta) \equiv N(\beta) \) and \( N(\beta) \) is either 0 or 1. Thus, every element of \((\mathbb{Z}/(2)\mathbb{Z})Q\) is either a unit or is nilpotent.

Remark. It turns out that when \( p \) is an odd prime, \( \mathbb{Z}Q/(p) \) is isomorphic to \( M_2(\mathbb{F}_p) \), the ring of \( 2 \times 2 \) matrices over the field of order \( p \) (see Corollary 1.4.2). So, Proposition 4.2.1 could have been formulated and proven in terms of matrices. However, this representation will not be particularly useful in the discussion to follow, so we do not emphasize it. Also, \( \mathbb{Z}Q/(2) \) is not isomorphic to \( M_2(\mathbb{F}_2) \) because, among other reasons, \( M_2(\mathbb{F}_2) \) contains matrices that are neither units nor nilpotent.

Recall that any \( \alpha \in \mathbb{Z}Q \) satisfies a polynomial with integer coefficients, called the minimal polynomial of \( \alpha \) and denoted by \( \min_{\alpha}(x) \).

Lemma 4.2.2. Let \( p \) be an odd prime, and let \( R = \mathbb{Z}Q/(p) \). Then, every monic quadratic polynomial in \((\mathbb{Z}/p\mathbb{Z})[x]\) is the minimal polynomial of some \( \alpha \in R - \mathbb{Z}/p\mathbb{Z} \).

Proof. Let \( x^2 + Ax + B \in (\mathbb{Z}/p\mathbb{Z})[x] \). Then, \( A \equiv -2a \) for some \( a \in \mathbb{Z}/p\mathbb{Z} \). It suffices to show that we can find \( b, c, d \in \mathbb{Z}/p\mathbb{Z} \), not all zero, such that \( b^2 + c^2 + d^2 \equiv B - a^2 \). Then, \( \alpha \equiv a + bi + cj + dk \) will be an element of \( R - \mathbb{Z}/p\mathbb{Z} \) with the desired minimal
polynomial. If \( B - a^2 \neq 0 \), then since every element of a finite field is a sum of two squares, we can find \( b, c \in \mathbb{Z}/p\mathbb{Z} \) such that \( b^2 + c^2 \equiv B - a^2 \), and at least one of \( b \) or \( c \) is necessarily non-zero. 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 \( \min_{\alpha}(x) = x^2 + Ax + B \), as required.

**Theorem 4.2.3.** Let \( p \) be an odd prime. Then, \( \phi_p(x) = (x^{p^2} - x)(x^p - x) \) is the unique monic polynomial of minimal degree in \( \text{Muff}(p) \cap (\mathbb{Z}/p\mathbb{Z})[x] \).

**Proof.** Let \( R = \mathbb{Z}Q/(p) \) and let \( f(x) \) be any polynomial in \( \text{Muff}(p) \cap (\mathbb{Z}/p\mathbb{Z})[x] \). Then, \( f(x) \) kills \( 0, 1, \ldots, p - 1 \), so \( \deg(f) \geq p > 2 \). So, for any \( \alpha \in R - \mathbb{Z}/p\mathbb{Z} \), we may write

\[
f(x) = g(x)\min_{\alpha}(x) + sx + t,
\]

where \( g(x), sx + t \in (\mathbb{Z}/p\mathbb{Z})[x] \). Then, \( f(\alpha) \equiv s\alpha + t \equiv 0 \) and \( f(\bar{\alpha}) \equiv s\bar{\alpha} + t \equiv 0 \). Thus, \( s\alpha + t \equiv s\bar{\alpha} + t \) and \( s\alpha \equiv s\bar{\alpha} \). Since \( s \in \mathbb{Z}/p\mathbb{Z} \), we have either \( s \equiv 0 \) or \( \alpha \equiv \bar{\alpha} \). We assumed that \( \alpha \notin \mathbb{Z}/p\mathbb{Z} \), so \( \alpha \neq \bar{\alpha} \). Hence, \( s \equiv 0 \). Since \( s\alpha + t \equiv 0 \), we also have \( t \equiv 0 \). So,

\[
f(x) = g(x)\min_{\alpha}(x).
\]

Since \( \alpha \) was an arbitrary element of \( R - \mathbb{Z}/p\mathbb{Z} \), this means that every possible minimal polynomial over \( \mathbb{Z}Q/(p) \) must divide \( f(x) \). By Lemma 4.2.2, we conclude that every monic quadratic polynomial in \( (\mathbb{Z}/p\mathbb{Z})[x] \) divides \( f(x) \). Thus, for \( \phi_p \) to be a monic polynomial in \( \text{Muff}(p) \cap (\mathbb{Z}/p\mathbb{Z})[x] \) of minimal degree, \( \phi_p \) must be the least common multiple in \( (\mathbb{Z}/p\mathbb{Z})[x] \) of every monic quadratic polynomial in \( (\mathbb{Z}/p\mathbb{Z})[x] \).

It is a standard result in the theory of finite fields that the product of all irreducible polynomials in \( (\mathbb{Z}/p\mathbb{Z})[x] \) of degree 2 or less is equal to \( x^{p^2} - x \). Thus, \( x^{p^2} - x \) accounts for all the irreducible quadratics in the least common multiple we desire. To handle
the reducible quadratics, we note that a reducible quadratic must factor into a product of two linear polynomials. To deal with any such factorization, we need to multiply $x^p^2 - x$ by $x(x - 1) \cdots (x - (p - 1)) = x^p - x$. Hence, $(x^p^2 - x)(x^p - x)$ is the least common multiple we seek, so we take $\phi_p(x) = (x^p^2 - x)(x^p - x)$. Finally, $\phi_p$ is unique because all of the calculations in this paragraph took place over the field $\mathbb{Z}/p\mathbb{Z}$.

**Corollary 4.2.4.** For each odd prime $p$, the polynomial $\frac{\phi_p(x)}{p} = \frac{(x^{p^2} - x)(x^p - x)}{p}$ is an element of $\text{Int}(\mathbb{Z}Q)$.

**Proof.** This follows from Correspondence 4.1.1. \qed

Now that we know that the polynomials $\frac{(x^{p^2} - x)(x^p - x)}{p}$ are in $\text{Int}(\mathbb{Z}Q)$, we have enough information to prove that $\text{Int}(\mathbb{Z}Q)$ is non-Noetherian. The proof is given in Section 4.4 at the end of this chapter.

### 4.3 From Muffins to Generating Sets

Before proceeding to the next result on muffins, we give a couple pieces of notation.

We define the *annihilator* of an ideal $I$ in a ring $R$ to be $\text{Ann}_R(I) = \{\alpha \in R \mid \alpha I = I \alpha = (0)\}$. If it is clear from context what ring we are working in, we write simply $\text{Ann}(I)$. Given any $\alpha \in R$, we define $\text{Ann}(\alpha)$ to be the annihilator of the ideal generated by $\alpha$, i.e. $\text{Ann}(\alpha) = \text{Ann}(\langle \alpha \rangle)$.

**Definition 4.3.1.** Let $I$ be an ideal in a ring $R$, and let $\pi : R \to R/I$ be the quotient map. We define

$$\widehat{\text{Muff}}(R/I) = \pi^{-1}(\text{Muff}(R/I)) = \{f(x) \in R[x] \mid f(\alpha) \in I \text{ for all } \alpha \in R\}.$$ 

In other words, $\widehat{\text{Muff}}(R/I)$ is the inverse image of $\text{Muff}(R/I)$ in $R[x]$. 

44
Theorem 4.3.2. Let $R$ be a finite, non-zero quotient ring of $\mathbb{Z}Q$ and let $n = \text{char}(R)$. Then,

(i) for any ideal $I$ of $R$, $\text{Muff}(R) \mod I \subseteq \text{Muff}(R/I)$.

(ii) for any $\gamma \in R$ and any ideal $I$ of $R$ such that $I \subseteq \text{Ann}(\gamma)$, we have $\gamma \text{Muff}(R/I) \subseteq \text{Muff}(R)$. In particular, if $n$ factors as $n = \ell m$ for integers $\ell > 1$ and $m > 1$, then $\ell \text{Muff}(R/mR) \subseteq \text{Muff}(R)$.

(iii) Assume that $\gamma$ is central in $R$. If $f \in \text{Muff}(R)$ and $f = \gamma g$ for some $g \in R[x]$, then $f \in \gamma \text{Muff}(R/\text{Ann}(\gamma))$.

(iv) for any ideal $I$ of $R$, $\deg(\phi_R) \geq \deg(\phi_{R/I})$.

(v) Assume $n$ factors as $n = \ell m$ with $\ell > 1$, $m > 1$, and $\gcd(\ell, m) = 1$. Then $\deg(\phi_R) = \max\{\deg(\phi_{R/\ell R}), \deg(\phi_{R/mR})\}$. In particular, if $n$ has prime factorization $n = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$, then $\deg(\phi_R) = \max_{1 \leq r \leq t}\{\deg(\phi_{R/p_r R})\}$.

Proof. (i) Let $g \in \text{Muff}(R)$. Then, $g(\alpha) \equiv 0$ in $R$, so the reduction of $g$ mod $I$ kills every residue in $R/I$. Thus, $g \mod I \in \text{Muff}(R/I)$ and $\text{Muff}(R) \mod I \subseteq \text{Muff}(R/I)$.

(ii) Let $\gamma f \in \gamma \text{Muff}(R/I)$, and let $\alpha \in R$. Then, reducing both $f$ and $\alpha$ mod $I$, we have $f(\alpha) \equiv 0$. So, $f(\alpha) \in I$ in $R$, and hence $\gamma f(\alpha) \equiv 0$ in $R$. This gives $\gamma f \in \text{Muff}(R)$ and $\gamma \text{Muff}(R/I) \subseteq \text{Muff}(R)$. The second assertion is true because $\ell m \equiv 0$, and so $mR \subseteq \text{Ann}(\ell)$.

(iii) Assume that $f \in \text{Muff}(R)$ and $f = \gamma g$ for some $g \in R[x]$. Then, for any $\alpha \in R, \gamma g(\alpha) \equiv 0$. Since $\gamma$ is central in $R$, this is enough to conclude that
\( g(\alpha) \in \text{Ann}(\gamma) \). Thus, \( g \mod \text{Ann}(\gamma) \in \text{Muff}(R/\text{Ann}(\gamma)) \) and \( f \in \gamma\text{Muff}(R/\text{Ann}(\gamma)) \).

(iv) By (i), \( \phi_R \mod I \) is a monic polynomial in \( \text{Muff}(R/I) \), and \( \deg(\phi_R) = \deg(\phi_R \mod I) \geq \deg(\phi_R/I) \).

(v) Assume that \( \gcd(\ell, m) = 1 \). Let \( \psi = \phi_{R/\ell R} \) and \( \tau = \phi_{R/m R} \). WLOG, assume that \( \deg(\psi) = \max\{\deg(\psi), \deg(\tau)\} \). By (iv), \( \deg(\phi_R) \geq \deg(\psi) \).

Now, let \( d = \deg(\psi) - \deg(\tau) \). Since \( \gcd(\ell, m) = 1 \), there exist \( a, b \in \mathbb{Z} \) such that \( a\ell + bm = 1 \). By (ii), both \( \ell \tau \) and \( m \psi \) are in \( \text{Muff}(R) \), so \( a\ell x^d \tau + bm \psi \) equals a monic polynomial in \( \text{Muff}(R) \) of degree \( \deg(\psi) \). By the way we defined \( \phi_R \), we must have \( \deg(\phi_R) \leq \deg(\psi) \). Thus, \( \deg(\phi_R) = \deg(\psi) = \max\{\deg(\phi_{R/\ell R}), \deg(\phi_{R/m R})\} \).

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 ultimate goal is to determine generators for the muffin ideal of any finite quotient ring of \( \mathbb{Z}Q \). Then, the generators for \( \text{Muff}(n) \) will give rise to generators for \( \text{Int}(\mathbb{Z}Q) \). It turns out that the nicest cases occur when the characteristic of the quotient ring is odd.

**Theorem 4.3.3.** Let \( R \) be a finite, non-zero quotient ring of \( \mathbb{Z}Q \) of characteristic \( n \).

(i) If \( n \) is odd, then \( \text{Muff}(R) \) is finitely generated by polynomials with coefficients in \( \mathbb{Z}/n\mathbb{Z} \).

(ii) If \( n = p \) for some odd prime \( p \), then \( \text{Muff}(R) = (\phi_R) \). In particular, \( \text{Muff}(p) = (\phi_p) \).

Before giving the proof, we define some more notation.
Definition 4.3.4. For any \( f(x) = \sum_r (a_r + b_r i + c_r j + d_r k) x^r \in \mathbb{H}[x] \), let

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

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

Proof. (i) The ideal \( \text{Muff}(R) \) is finitely generated because \( R[x] \) is Noetherian. Let \( f \) be any polynomial in \( \text{Muff}(R) \). Then, since \( \text{Muff}(R) \) is an ideal of \( R[x] \), we have

\[-ifi, -jfj, -kfk \in \text{Muff}(R)\].

So, \( 4f_1 = f - ifi - jfj - kfk \in \text{Muff}(R) \). Assume \( n \) is odd. Then, 4 is invertible in \( R \), so \( f_1 \in \text{Muff}(R) \). Similarly, the other component polynomials of \( f \) are in \( \text{Muff}(R) \). Hence, a polynomial is in \( \text{Muff}(R) \) if and only if its component polynomials are in \( \text{Muff}(R) \), and since these component polynomials have coefficients in \( \mathbb{Z}/n\mathbb{Z} \), we achieve the stated result.

(ii) Assume now that \( n = p \) is an odd prime. Certainly, we have \( (\phi_R) \subseteq \text{Muff}(R) \). Let \( I = \text{Muff}(R) \cap (\mathbb{Z}/p\mathbb{Z})[x] \); then \( \phi_R \in I \). Since \( \mathbb{Z}/p\mathbb{Z} \) is a field, \( I \) is generated by a polynomial of minimal degree in \( I \), i.e. by \( \phi_R \). Now, let \( f \in \text{Muff}(R) \), and let \( f_1, f_i, f_j, \) and \( f_k \) be the component polynomials of \( f \). As in part (i), each of these component polynomials is in \( \text{Muff}(R) \). But, \( f_1, f_i, f_j, \) and \( f_k \) all have coefficients in \( \mathbb{Z}/p\mathbb{Z} \), so \( f_1, f_i, f_j, f_k \in I \). So, \( \phi_R \) divides each component polynomial; hence, \( \phi_R \) divides \( f \). It follows that \( \text{Muff}(R) \subseteq (\phi_R) \) in \( R[x] \), and therefore \( \text{Muff}(R) = (\phi_R) \). □

For a quotient ring \( R \) of \( \mathbb{Z}Q \) of even characteristic, we do not have such nice results. As we shall see, the generators we are determining for \( \text{Muff}(R) \) are related to the ideals of \( R \). When \( n = \text{char}(R) \) is odd, the same steps used in the proof
of Theorem 4.3.3 part (i) can be used to show that every ideal of \( R \) is generated by an element of \( \mathbb{Z}/n\mathbb{Z} \), and this ideal structure will allow us to fairly easily derive generators for \( \text{Muff}(R) \). When \( n \) is even, the ideal structure of \( R \) is more complicated, and this complexity is reflected in the muffin ideal of \( R \). The odd case is dealt with shortly in Theorem 4.3.7. At present time, we do not have a complete proof for the even case, although a plan of attack is outlined at the end of this section.

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 adopt the same definition for a noncommutative ring. Explicitly, given \( f(x) = \sum_{r=0}^{m} \alpha_r x^r \in R[x] \), we define the *content* of \( f \) to be the ideal \((\alpha_0, \alpha_1, \ldots, \alpha_m)\). We denote the content of \( f \) by \( \text{con}(f) \), and we say that \( f \) has content 1 if \( \text{con}(f) = (1) \).

**Lemma 4.3.5.** Let \( R \) be a finite, non-zero quotient ring of \( \mathbb{Z}Q \), and let \( n = \text{char}(R) \). If \( f \in \text{Muff}(R) \cap (\mathbb{Z}/n\mathbb{Z})[x] \) and \( \text{con}(f) = (1) \), then \( \deg(f) \geq \deg(\phi_R) \).

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

From here, we break the proof into three cases, depending on \( n \).

**Case 1: \( n = p \) for some prime \( p \)**

If \( p \) is odd, then the lemma holds by Theorem 4.3.3 part (ii). If \( p = 2 \), then \( \text{Muff}(R) \cap (\mathbb{Z}/2\mathbb{Z})[x] = \{ g \in (\mathbb{Z}/2\mathbb{Z})[x] \mid g(\alpha) = 0 \text{ for all } \alpha \in R \} \), which is an ideal in \((\mathbb{Z}/2\mathbb{Z})[x]\). Since \((\mathbb{Z}/2\mathbb{Z})[x]\) is a PID, we have \( \text{Muff}(R) \cap (\mathbb{Z}/2\mathbb{Z})[x] = (\phi_R) \), so
the lemma holds when \( n = 2 \). This completes Case 1.

**Case 2:** \( n = p^e \) for some prime \( p \) and some \( e > 0 \)

We use induction on \( e \). The base case was handled 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 \( \deg(f) < \deg(\phi_R) \). Let \( c \) be the leading coefficient of \( f \). Since \( \deg(f) < \deg(\phi_R) \), \( c \) cannot be a unit in \( \mathbb{Z}/n\mathbb{Z} \); if that were the case, then \( c^{-1}f \) would be a monic polynomial in \( \text{Muff}(R) \cap (\mathbb{Z}/n\mathbb{Z})[x] \) of degree less than \( \deg(\phi_R) \). So, \( p \) divides \( c \); let \( m \in \{1, 2, \ldots, e - 1\} \) be such that \( p^m \) is the highest power of \( p \) dividing \( c \). Let \( \psi = \phi_{R/p^{e-m}R} \). Then, by Theorem 4.3.2 part (ii), \( p^m\psi \in \text{Muff}(R) \), and by Theorem 4.3.2 part (iv) we have \( \deg(p^m\psi) = \deg(\psi) \leq \deg(\phi_R) \). If \( \deg(f) < \deg(\psi) \), then \( f \mod p^{e-m}R \) is a content 1 polynomial in \( \text{Muff}(R/p^{e-m}R) \cap (\mathbb{Z}/p^{e-m}\mathbb{Z})[x] \) of degree less than \( \deg(\psi) \), which contradicts the inductive hypothesis. So, \( \deg(f) \geq \deg(\psi) = \deg(p^m\psi) \).

Since \( p^m \) is the highest power of \( p \) dividing \( c \) and we are assuming that \( n = p^e \), there exists \( y \in \mathbb{Z}/n\mathbb{Z} \) such that \( c \equiv yp^m \). Let \( d = \deg(f) - \deg(p^m\psi) \). Then, we may write \( f = x^dyp^m\psi + g \), where \( g \in (\mathbb{Z}/n\mathbb{Z})[x] \) is either 0 or \( \deg(g) < \deg(f) \). If \( g = 0 \), then \( \text{con}(f) \subseteq (p) \), which is a contradiction. So, \( \deg(g) < \deg(f) \), and \( g \in \text{Muff}(R) \) because \( f, p^m\psi \in \text{Muff}(R) \). We cannot have \( \text{con}(g) = (1) \) because it would contradict the minimality of \( \deg(f) \), so we must have \( \text{con}(g) \subseteq (p) \). But then, \( g = ph \) for some \( h \in (\mathbb{Z}/n\mathbb{Z})[x] \), and we have \( f = yx^d p^m\psi + g = p(x^dyp^{m-1}\psi + h) \), which yields \( \text{con}(f) \subseteq (p) \). Thus, we arrive at a contradiction no matter what we do, so we conclude that \( \deg(f) = \deg(\phi_R) \). This 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 $\phi_{p^e}$ has maximal degree among all the $\phi_{p_i^{e_i}}$. Then, by Theorem 4.3.2 part (v), $\deg(\phi_R) = \deg(\phi_{R/p^eR})$. Now, $f \mod p^eR$ is in $\text{Muff}(R/p^eR) \cap (\mathbb{Z}/p^e\mathbb{Z})[x]$, so by Case 2 we have $\deg(f) \geq \deg(\phi_{R/p^eR}) = \deg(\phi_R)$. Thus, the lemma holds in this case as well.

There are no more cases, so the proof is complete.

\[\Box\]

**Theorem 4.3.6.** Let $R$ be a finite, non-zero quotient ring of $\mathbb{Z}Q$, and let $n = \text{char}(R)$.

Assume that $n$ is odd. If $f \in \text{Muff}(R)$ and $\text{con}(f) = 1$, then $\deg(f) \geq \deg(\phi_R)$.

**Proof.** Let $f$ be a content 1 polynomial in $\text{Muff}(R)$. Since $R$ is finite and non-zero, $n > 1$. Let $n$ factor as $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, where the $p_r$ $(1 \leq r \leq t)$ are distinct odd primes and each $e_r > 0$. By Theorem 4.3.2 part (v), we have $\deg(\phi_R) = \max_{1 \leq r \leq t} \{\deg(\phi_{R/p_i^{e_i}R})\}$.

Let $p$ and $e$ be such that $\phi_{R/p^eR}$ has maximal degree among all the $\phi_{R/p_i^{e_i}R}$. Then, $\deg(\phi_R) = \deg(\phi_{R/p^eR})$, so it suffices to show that $\deg(f) \geq \deg(\phi_{R/p^eR})$.

Consider the component polynomials $f_1$, $f_i$, $f_j$, and $f_k$ of $f$. Since $n$ is odd, these component polynomials are all elements of $\text{Muff}(R)$. Furthermore, $\text{con}(f) \subseteq \text{con}(f_1) + \text{con}(f_i) + \text{con}(f_j) + \text{con}(f_k)$. Since $\text{con}(f) = (1)$, this means that at least one of the component polynomials has content not contained in the maximal ideal $pR$ of $R$ (if not, then $\text{con}(f) \subseteq pR$, a contradiction). WLOG, assume that $\text{con}(f_1) \not\subseteq pR$.

Then, in $R/p^eR$, we must have

$$\text{con}(f_1 \mod p^eR) = R/p^eR.$$
Since $f_1 \mod p^e R$ lies in Muff($R/p^e R$) and has coefficients in $\mathbb{Z}/p^e \mathbb{Z}$, by Lemma 4.3.5 we have

$$\deg(f_1 \mod p^e R) \geq \deg(\phi_{R/p^e R}).$$

Thus,

$$\deg(f) \geq \deg(f_1) \geq \deg(f_1 \mod p^e R) \geq \deg(\phi_{R/p^e R})$$

and therefore $\deg(f) \geq \deg(\phi_R)$. \hfill \Box

Our next few results give an explicit generating set for Muff($n$) when $n$ is odd.

**Theorem 4.3.7.** Let $R$ be a finite, non-zero quotient ring of $\mathbb{Z}Q$, and let $n = \text{char}(R)$. Assume that $n$ is odd and that $p_1, \ldots, p_t$ are all the primes dividing $n$. Then, $\text{Muff}(R) = (\phi_n, p_1 \widetilde{\text{Muff}}(R/\text{Ann}(p_1)), \ldots, p_t \widetilde{\text{Muff}}(R/\text{Ann}(p_t)))$.

**Proof.** Let $I = (\phi_n, p_1 \widetilde{\text{Muff}}(R/\text{Ann}(p_1)), \ldots, p_t \widetilde{\text{Muff}}(R/\text{Ann}(p_t)))$. By Theorem 4.3.2 part (ii), we have $\text{Muff}(R) \supseteq I$, so we just need the other inclusion. Let $f \in \text{Muff}(R)$. Since $\phi_R$ is monic, there exist $g, h \in R[x]$ such that $f = g\phi_R + h$, where either $h = 0$ or $\deg(h) < \deg(\phi_R)$. If $h = 0$, then $f \in (\phi_R)$ and we are done. So, assume $\deg(h) < \deg(\phi_R)$. It suffices to show that $h \in (p_1 \widetilde{\text{Muff}}(R/\text{Ann}(p_1)), \ldots, p_t \widetilde{\text{Muff}}(R/\text{Ann}(p_t)))$. Since $\deg(h) < \deg(\phi_R)$, Theorem 4.3.6 tells us that $\text{con}(h) \neq (1)$. By Proposition 4.1.3, there exists a prime divisor $p_\ell$ of $n$ such that $\text{con}(h) \subseteq p_\ell R$. Then, $h \in p_\ell \widetilde{\text{Muff}}(R/\text{Ann}(p_\ell))$, so $\text{Muff}(R) \subseteq I$ and we are done. \hfill \Box

**Remark.** With $R$ and $n$ as in the theorem, we know via Theorem 4.3.3 that $\text{Muff}(R)$ is generated by polynomials in $(\mathbb{Z}/n\mathbb{Z})[x]$, so we could have proven Theorem 4.3.7 using only Lemma 4.3.5.

**Corollary 4.3.8.** Let $n > 1$ be odd. Then, $\text{Muff}(n) = \{m\phi_{\frac{n}{m}} \mid m \text{ divides } n\}$. 51
Proof. For each $n > 1$, let $I_n = \{m\phi_n \mid m \text{ divides } n\}$. The fact that $\text{Muff}(n) \supseteq I_n$ follows from Theorem 4.3.2 part (ii). To get the other inclusion, we will apply Theorem 4.3.7. Let $n$ have prime factorization $n = p_1^{e_1}p_2^{e_2} \cdots p_t^{e_t}$, and let $E = e_1 + e_2 + \cdots + e_t$. We will use induction on $E$. The base case, $E = 1$, holds by Theorem 4.3.3. Assume that $E > 1$ and that the result holds for any odd integer with prime factorization $q_1^{f_1}q_2^{f_2} \cdots q_s^{f_s}$ such that $f_1 + f_2 + \cdots + f_s < E$.

By Theorem 4.3.7, we have $\text{Muff}(n) = (\phi_n, p_1\widetilde{\text{Muff}}(\frac{n}{p_1}), \ldots, p_t\widetilde{\text{Muff}}(\frac{n}{p_t}))$. By induction, for each $1 \leq \ell \leq t$ we have $p_\ell\widetilde{\text{Muff}}(\frac{n}{p_\ell}) = p_\ell I_{n/p_\ell}$. Each divisor of $\frac{n}{p_\ell}$ is a divisor of $n$, so $p_\ell I_{n/p_\ell} \subseteq I_n$, and the stated corollary now follows. 

\begin{corollary}
For any odd prime $p$ and any $e > 0$, we have $\text{Muff}(p^e) = (\phi_p, p\phi_{p^{-1}}, p^2\phi_{p^{-2}}, \ldots, p^{e-1}\phi_p)$.
\end{corollary}

\begin{proof}
This follows from Corollary 4.3.8.
\end{proof}

Translating our results back to $\text{Int}(\mathbb{Z}Q)$, we achieve the following interesting corollary.

\begin{corollary}
\begin{enumerate}
\item Let $p$ be an odd prime and let
\[ R_p = \left\{ f(x) \in \text{Int}(\mathbb{Z}Q) \mid f(x) = \frac{g(x)}{p^e} \text{ for some } g(x) \in \mathbb{Z}Q[x] \text{ and } e \geq 0 \right\} . \]
Then, $R_p$ is a ring and $R_p = \mathbb{Z}Q\left[\left\{ \frac{\phi_p}{p^e} \right\}_{\ell \geq 0} \right]$ (recall that our convention is to take $\phi_1 = x$).
\item Let
\[ R = \left\{ f(x) \in \text{Int}(\mathbb{Z}Q) \mid f(x) = \frac{g(x)}{n} \text{ for some } g(x) \in \mathbb{Z}Q[x] \text{ and some odd } n \right\} , \]
\end{enumerate}
\end{corollary}
and let
\[ \mathcal{P} = \left\{ \frac{\phi_p^\ell}{p^\ell} \mid p \text{ is an odd prime and } \ell \geq 0 \right\}, \]

where we again take \( \phi_1 = x \). Then, \( \mathcal{R} \) is a ring and \( \mathcal{R} = \mathbb{Z}Q[\mathcal{P}] \). In particular, \( \mathcal{R} \) can be generated over \( \mathbb{Z}Q \) by monic polynomials with rational coefficients.

**Proof.** (i) It easy to verify that \( \mathcal{R}_p \) is closed under addition and multiplication. So, \( \mathcal{R}_p \) is a subring of \( \text{Int}(\mathbb{Z}Q) \), and it suffices to establish the claim about the generators \( \frac{\phi_p^\ell}{p^\ell} \). Let \( f(x) = \frac{g(x)}{p^e} \in \mathcal{R}_p \), where \( g(x) \in \mathbb{Z}Q[x] \) and \( e \geq 0 \). If \( e = 0 \), then \( f(x) \in \mathbb{Z}Q[x] = \mathbb{Z}Q[\phi_1] \) and we are done. So, assume that \( e > 0 \). Since \( f(x) \in \text{Int}(\mathbb{Z}Q) \), \( g(x) \mod p^e \) lies in \( \text{Muff}(p^e) \). By Corollary 4.3.9 there exist polynomials \( g_0, g_1, \ldots, g_{e-1} \in (\mathbb{Z}Q/(p^e))[x] \) such that
\[
g(x) \equiv g_0(x)\phi_{p^e}(x) + pg_1(x)\phi_{p^{e-1}}(x) + \cdots + p^{e-1}g_{e-1}\phi_p(x) \mod p^e.
\]
So, in \( \mathbb{Z}Q[x] \), we may write
\[
g(x) = g_0(x)\phi_{p^e}(x) + pg_1(x)\phi_{p^{e-1}}(x) + \cdots + p^{e-1}g_{e-1}\phi_p(x) + p^eg_e(x)
\]
for some \( g_e(x) \in \mathbb{Z}Q[x] \). Hence, we can express \( f(x) = \frac{g(x)}{p^e} \) as
\[
\frac{g(x)}{p^e} = g_0(x)\frac{\phi_{p^e}(x)}{p^e} + g_1(x)\frac{\phi_{p^{e-1}}(x)}{p^{e-1}} + \cdots + g_{e-1}\frac{\phi_p(x)}{p} + g_e(x).
\]
Thus, \( f(x) \) can be generated over \( \mathbb{Z}Q \) by \( \left\{ \frac{\phi_p^\ell(x)}{p^\ell} \right\}_{0 \leq \ell \leq e} \). It follows that all the polynomials in \( \mathcal{R}_p \) can be generated by \( \left\{ \frac{\phi_p^\ell(x)}{p^\ell} \right\}_{\ell \geq 0} \), i.e. \( \mathcal{R}_p = \mathbb{Z}Q\left[ \left\{ \frac{\phi_p^\ell(x)}{p^\ell} \right\}_{\ell \geq 0} \right] \).

(ii) As in part (i), it is straightforward to check that \( \mathcal{R} \) is a subring of \( \text{Int}(\mathbb{Z}Q) \). Let \( f(x) = \frac{g(x)}{n} \in \mathcal{R} \). If \( n = 1 \), then \( f(x) \in \mathbb{Z}Q[x] \) and we are done. So, assume that \( n > 1 \) and has prime factorization \( n = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t} \). We use induction on \( t \) to show that \( f(x) \) can be generated over \( \mathbb{Z}Q \) by polynomials in \( \mathcal{P} \). If \( t = 1 \), then we are
done by part (i), since \( f(x) \in \mathcal{R}_{p_1} \) and each polynomial \( \frac{\phi_{p_1}}{p_1} \in \mathcal{P} \). So, assume that \( t > 1 \) and that the result holds whenever \( n \) has less than \( t \) distinct prime factors. For convenience, let \( p = p_1, e = e_1 \), and \( q = p_2^{e_2} \cdots p_t^{e_t} \). Then, \( n = p^e q \). Since \( p^e \) and \( q \) are relatively prime, there exist \( a, b \in \mathbb{Z} \) such that \( ap^e + bq = 1 \). Hence,

\[
\frac{g(x)}{n} = \frac{ag(x)}{q} + b \frac{g(x)}{p^e}.
\]

Since \( \frac{g(x)}{q} = p^e f(x) \in \mathcal{R} \) and \( \frac{g(x)}{p^e} = q f(x) \in \mathcal{R} \), the inductive hypothesis holds for both \( \frac{g(x)}{q} \) and \( \frac{g(x)}{p^e} \). Since both of these polynomials can be generated over \( \mathbb{Z}Q \) by polynomials from \( \mathcal{P} \), so can \( f(x) \). Thus, the desired result holds.

\[ \square \]

At this point, all of our firm results end, and we move into the realm of conjecture. Other than a few examples, we cannot prove much about Muff\((R)\) when \( R \) has even characteristic. By applying a brute force approach and using some of the theorems we have already proven, one can compute generators for Muff\((n)\) for small even values of \( n \):

\[
\begin{align*}
\text{Muff}(2) &= (x^2(x^2 + 1), (1 + i)(1 + j)(x^2 + x)), \\
\text{Muff}(6) &= ((x^3 - x)(x^9 - x), 3x^2(x^2 + 1), 3(1 + i + j + k)(x^2 + x)), \text{ and} \\
\text{Muff}(4) &= (x^4(x^2 + 1)^2, (1 + i)(x^6 + x^5 + x^4 + 3x^3 + 2x), \\
& \hspace{1cm} (1 + j)(x^6 + x^5 + x^4 + 3x^3 + 2x), 2x^2(x^2 + 1), \\
& \hspace{1cm} 2(1 + i)(1 + j)(x^2 + x)).
\end{align*}
\]

At present, the best conjecture about the generators for Muff\((R)\) when \( n = \text{char}(R) \) is even is that

\[
\text{Muff}(R) = \left( \phi_R, (1 + i)\widetilde{\text{Muff}}(R/\text{Ann}(1 + i)), (1 + j)\widetilde{\text{Muff}}(R/\text{Ann}(1 + j)), \\
p_1\widetilde{\text{Muff}}(R/\text{Ann}(p_1)), \ldots, p_t\widetilde{\text{Muff}}(R/\text{Ann}(p_t)) \right),
\]

(4.3.11)
where $p_1, \ldots, p_t$ are all the odd primes dividing $n$. In general, the ideals $\text{Ann}(1+i)$ and $\text{Ann}(1+j)$ are not generated by integers, so the quotient rings $R/\text{Ann}(1+i)$ and $R/\text{Ann}(1+j)$ can be quite messy. However, there does not seem to be a way around dealing with them, which explains why we have tried to consider all quotient rings of $\mathbb{Z}Q$ rather than just those of the form $\mathbb{Z}Q/(n)$.

While we do not have proofs for the proposed decomposition of $\text{Muff}(R)$, we do have a plan of attack. We would like

1) to be able to extend Theorem 4.3.6 to rings of even characteristic, and

2) to prove that if $f \in \text{Muff}(R)$ and $\text{con}(f) \subseteq (1+i, 1+j)$, then $f$ is contained in the ideal generated by $(1+i)\widetilde{\text{Muff}}(R/\text{Ann}(1+i))$ and $(1+j)\widetilde{\text{Muff}}(R/\text{Ann}(1+j))$.

If both of these conjectures are true, then we can prove (4.3.11) the same way we proved Theorem 4.3.7. So far, no counterexamples have been found to disprove either 1) or 2).

Finally, there is one other thing to note about the generators given above for $\text{Muff}(2), \text{Muff}(4),$ and $\text{Muff}(6)$. All these generators have the form $\gamma f$, where $\gamma \in \mathbb{Z}Q/(n)$ and $f \in (\mathbb{Z}/n\mathbb{Z})[x]$. Assuming that (4.3.11) is true, we can prove that any finite quotient ring $R$ of $\mathbb{Z}Q$ is generated by polynomials of the form $\gamma f$. A corollary of this is that $\text{Int}(\mathbb{Z}Q)$ is generated over $\mathbb{Z}Q$ by polynomials of the form $\frac{\gamma f}{n}$, where $\gamma \in \mathbb{Z}Q, n \in \mathbb{Z},$ and $f \in \mathbb{Z}[x]$.

### 4.4 A Proof that $\text{Int}(\mathbb{Z}Q)$ is Non-Noetherian

**Theorem 4.4.1.** The ring $\text{Int}(\mathbb{Z}Q)$ is non-Noetherian.
Proof. By Corollary 4.2.4, for each odd prime \( p \) the polynomial \( \frac{\phi_p(x)}{p} = \frac{(x^{p^2} - x)(x^p - x)}{p} \) is in \( \text{Int}(\mathbb{Z}Q) \). Let \( p_1, p_2, \ldots \) be all the (distinct) odd primes in \( \mathbb{Z} \). For each \( n > 0 \), let \( I_n = (\phi_{p_1}(x), \phi_{p_2}(x), \ldots, \phi_{p_n}(x)) \) in \( \text{Int}(\mathbb{Z}Q) \). We will show that \( \frac{\phi_{p_{n+1}}(x)}{p_{n+1}} \notin I_n \) for each \( n > 0 \), and this will allow us to produce a strictly increasing chain of ideals in \( \text{Int}(\mathbb{Z}Q) \). Fix \( n > 0 \) and suppose by way of contradiction that \( \frac{\phi_{p_{n+1}}(x)}{p_{n+1}} \in I_n \). Since each \( \frac{\phi_{p_\ell}(x)}{p_\ell} \) is central in \( \text{Int}(\mathbb{Z}Q) \) (because each \( \frac{\phi_{p_\ell}(x)}{p_\ell} \) has rational coefficients), there exist \( \frac{f_1(x)}{m_1}, \frac{f_2(x)}{m_2}, \ldots, \frac{f_n(x)}{m_n} \in \text{Int}(\mathbb{Z}Q) \) such that

\[
\frac{\phi_{p_{n+1}}(x)}{p_{n+1}} = \frac{f_1(x)}{m_1} \frac{\phi_{p_1}(x)}{p_1} + \frac{f_2(x)}{m_2} \frac{\phi_{p_2}(x)}{p_2} + \cdots + \frac{f_n(x)}{m_n} \frac{\phi_{p_n}(x)}{p_n},
\]

and for each \( 1 \leq \ell \leq n, f_\ell(x) \in \mathbb{Z}Q[x] \) and \( m_\ell \) is a positive integer. For each \( \ell \), let \( \alpha_\ell \) be the constant coefficient of \( f_\ell(x) \).

Now, the coefficient of \( x^2 \) in \( \frac{\phi_{p_{n+1}}(x)}{p_{n+1}} \) is \( \frac{1}{p_{n+1}} \). We know that \( \phi_{p_\ell}(x) = (x^{p^{\ell^2}} - x)(x^{p^\ell} - x) \) for each \( 1 \leq \ell \leq n \), so the coefficient of \( x^2 \) in \( \frac{f_\ell(x)}{m_\ell} \frac{\phi_{p_\ell}(x)}{p_\ell} \) equals \( \frac{\alpha_\ell}{m_\ell p_\ell} \). By equating the coefficients of \( x^2 \) in (*) we get

\[
\frac{1}{p_{n+1}} = \frac{\alpha_1}{m_1 p_1} + \frac{\alpha_2}{m_2 p_2} + \cdots + \frac{\alpha_n}{m_n p_n}. \tag{**}
\]

For each \( 1 \leq \ell \leq n \), we have \( \alpha_\ell = f_\ell(0) \) and \( \frac{f_\ell(x)}{m_\ell} \in \text{Int}(\mathbb{Z}Q) \), so \( \alpha_\ell \in (m_\ell) \) in \( \mathbb{Z}Q \). Thus, for each \( \ell \), there exists \( \beta_\ell \in \mathbb{Z}Q \) such that \( \alpha_\ell = m_\ell \beta_\ell \). So, (***) becomes

\[
\frac{1}{p_{n+1}} = \frac{\beta_1}{p_1} + \frac{\beta_2}{p_2} + \cdots + \frac{\beta_n}{p_n}.
\]

However, this is impossible; among other things, it would imply that \( p_{n+1} \) is invertible in \( \mathbb{Z}_{(p_{n+1})}Q \) (here, \( \mathbb{Z}_{(p_{n+1})} \) is the localization of \( \mathbb{Z} \) at the prime ideal \( (p_{n+1}) \)). We reached this contradiction by supposing that \( \frac{\phi_{p_{n+1}}(x)}{p_{n+1}} \in I_n \), so we conclude that \( \frac{\phi_{p_{n+1}}(x)}{p_{n+1}} \notin I_n \).

It now follows that \( I_{n+1} \neq I_n \) for all \( n > 0 \). Hence, \( I_1 \subset I_2 \subset I_3 \subset \cdots \) is a strictly increasing chain of ideals in \( \text{Int}(\mathbb{Z}Q) \), and therefore \( \text{Int}(\mathbb{Z}Q) \) is non-Noetherian. \( \square \)
As we shall see in Chapter 5, the polynomials $\phi_p(x)$ are also elements of $\text{Int}(\mathbb{Z}H)$, so the previous theorem shows that $\text{Int}(\mathbb{Z}H)$ is non-Noetherian. In fact, the theorem applies to $\text{Int}(R)$ for any overring $R$ of $\mathbb{Z}Q$ in which infinitely many primes of $\mathbb{Z}$ remain prime.
5.1 Quotient Rings of $\mathbb{Z}H$

The material covered in Chapter 4 focused on $\mathbb{Z}Q$ and $\text{Int}(\mathbb{Z}Q)$. However, the majority of what we accomplished falls through to $\mathbb{Z}H$ and $\text{Int}(\mathbb{Z}H)$ without much change. The reason for this is that whenever $n$ is an odd number, $\mathbb{Z}H/(n) \cong \mathbb{Z}Q/(n)$, a fact that we now prove.

**Theorem 5.1.1.**

(i) If $n$ is an odd integer, then $\mathbb{Z}H/(n) \cong \mathbb{Z}Q/(n)$.

(ii) Let $I$ be a non-zero ideal of $\mathbb{Z}H$, let $R = \mathbb{Z}H/I$, and assume that $n = \text{char}(R)$ is odd. Then, $R$ is isomorphic to a quotient ring of $\mathbb{Z}Q/(n)$.

**Proof.** (i) Assume $n$ is odd. Let $\iota : \mathbb{Z}Q \to \mathbb{Z}H$ be the injection map, let $\pi : \mathbb{Z}H \to \mathbb{Z}H/(n)$ be the canonical quotient map, and let $\phi = \pi \circ \iota$. We will use $\phi$ to get the desired isomorphism. Note that $(n)$ in $\mathbb{Z}Q$ is contained in $\text{Kern}(\phi)$, and if $\alpha \in \text{Kern}(\phi)$, then $\iota(\alpha) = n\beta$ for some $\beta \in \mathbb{Z}H$. By Theorem 2.2.3, $\beta = \beta' + e\mu$ for some $\beta' \in \mathbb{Z}Q$ and $e \in \{0, 1\}$. So, $n\beta = n\beta' + ne\mu$. If $e = 1$, then $ne\mu \notin \mathbb{Z}Q$, since $n$ is
odd. Hence, $e = 0$ and $\alpha = n\beta = n\beta' \in (n)$ in $\mathbb{Z}Q$. This shows that $\text{Kern}(\phi) = (n)$, and so $\mathbb{Z}H/(n)$ contains $\mathbb{Z}Q/(n)$ as a subring.

It remains to show that $\phi$ is onto. Let $\gamma \equiv a + bi + cj + dk + E\mu$ be a residue in $\mathbb{Z}H/(n)$, where $a, b, c, d \in \mathbb{Z}$ and $E \in \{0, 1\}$. If $E = 0$, then $\gamma \in \text{Im}(\phi)$, so assume that $E = 1$. Since $n$ is odd, 2 is invertible in $\mathbb{Z}H/(n)$; hence, $\mu \equiv y(1 + i + j + k)$ for some $y \in \mathbb{Z}$, and

$$
\gamma \equiv a + bi + cj + dk + E\mu \\
\equiv (a + y) + (b + y)i + (c + y)j + (d + y)k,
$$

which is also in $\text{Im}(\phi)$. Thus, $\phi$ is onto and $\mathbb{Z}Q/(n) \cong \mathbb{Z}H/(n)$.

(ii) Since $n \equiv 0 \mod I$, we have $(n) \subseteq I$ in $\mathbb{Z}H$. So, $R$ is a quotient ring of $\mathbb{Z}H/(n)$, which by (i) is isomorphic to $\mathbb{Z}Q/(n)$.

Because of this theorem, everything that was proven in Chapter 4 for quotient rings of $\mathbb{Z}Q$ of odd characteristic also holds for quotient rings of $\mathbb{Z}H$ of odd characteristic. The other theorems from Chapter 4 either hold for $\mathbb{Z}H$ without change or need only minor modifications. Explicitly,

- Correspondence 4.1.1, Theorem 4.3.2, and Lemma 4.3.5 hold without change when $\mathbb{Z}Q$ is replaced $\mathbb{Z}H$ in the statement and proof.

- Proposition 4.1.3 can be proved using the fact that the maximal ideals of $\mathbb{Z}H$ are $(1 + i)$ and $(p)$, where $p$ is an odd prime.

- Proposition 4.1.4 requires modification, but can be proved in the same way as Theorem 3.1.1.
• Proposition 4.1.5 is true if we work with all the monic quadratic polynomials in \( \mathbb{Z}/n\mathbb{Z} \), not just those of the form \( x^2 + 2bx + c \).

All the other results in Chapter 4 are stated for quotient rings of \( \mathbb{Z}Q \) of odd characteristic, and hence are valid for \( \mathbb{Z}H \) because of Theorem 5.1.1. Finally, the conjecture (4.3.11) about \( \text{Muff}(R) \) when \( R \) is a quotient ring of \( \mathbb{Z}Q \) and \( \text{char}(R) \) is even also has its analogue. We conjecture that when \( R \) is a quotient ring of \( \mathbb{Z}H \) of even characteristic \( n \), then

\[
\text{Muff}(R) = (\phi_R, (1 + i)\widetilde{\text{Muff}}(R/\text{Ann}(1 + i)), \\
p_1\widetilde{\text{Muff}}(R/\text{Ann}(p_1)), \ldots, p_t\widetilde{\text{Muff}}(R/\text{Ann}(p_t)))
\]  

(5.1.2)

where \( \phi_R \) is a monic polynomial in \( \text{Muff}(R) \cap (\mathbb{Z}/n\mathbb{Z})[x] \) of minimal degree, and \( p_1, \ldots, p_t \) are all the odd primes dividing \( n \). The reason we do not have \((1 + j)\widetilde{\text{Muff}}(R/\text{Ann}(1 + j))\) in (5.1.2) is because in \( \mathbb{Z}H \), \( \mu(1 + i)\mu^{-1} = 1 + j \), so the ideal generated by \( 1 + i \) and \( 1 + j \) is principal with generator \( 1 + i \).

Just as in the \( \mathbb{Z}Q \) case, for (5.1.2) to hold, it suffices

1) to have Theorem 4.3.6 hold for quotient rings of \( \mathbb{Z}H \) of even characteristic, and

2) to prove that if \( R \) is a quotient ring of \( \mathbb{Z}H \), \( f \in \text{Muff}(R) \), and \( \text{con}(f) \subseteq (1 + i) \), then \( f \) is contained in the ideal generated by \((1 + i)\widetilde{\text{Muff}}(R/\text{Ann}(1 + i))\).

What is nice about the \( \mathbb{Z}H \) situation is that we have proofs for 1) and 2) (given in Theorems 5.3.2 and 5.3.4, respectively). Ultimately, the reason we will be able to establish 1) and 2) is because \( \mathbb{Z}H \) is a principal ideal ring. Since the maximal ideal of \( \mathbb{Z}H \) above (2) is generated by \( 1 + i \), we will be able to keep quotient rings...
of \(ZH\) of characteristic \(2^m\) “under control,” and we will be able to give convenient characterizations of these rings. Another useful consequence of our work with quotient rings of \(ZH\) will be a proof that \(\text{Int}(ZH)\) is closed under bar conjugation.

We begin with a number theoretic lemma. This lemma is elementary and is unlikely to be a new result, but the author could not find a proof in the available literature.

**Lemma 5.1.3.** Let \(a, b, c, d \in \mathbb{Z}\), and let \(m > 0\).

(i) If \(a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{2^{2m}}\), then all of \(a, b, c,\) and \(d\) are divisible by \(2^{m-1}\).

(ii) If \(b^2 + c^2 + d^2 \equiv 0 \pmod{2^{2m}}\), then all of \(b, c,\) and \(d\) are divisible by \(2^m\).

**Proof.** (i) We use induction on \(m\). There is nothing to prove if \(m = 1\), so assume that \(m > 1\) and that the result is true for \(m - 1\).

Let \(a = 2^{n_1}q_1, b = 2^{n_2}q_2, c = 2^{n_3}q_3,\) and \(d = 2^{n_4}q_4,\) where \(n_1, n_2, n_3,\) and \(n_4\) are all greater than or equal to 0, and \(q_1, q_2, q_3,\) and \(q_4\) are all odd. Assume that \(a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{2^{2m}}\). Then,

\[
2^{2n_1}q_1^2 + 2^{2n_2}q_2^2 + 2^{2n_3}q_3^2 + 2^{2n_4}q_4^2 \equiv 0 \pmod{2^{2m}}.
\]

Suppose that some \(n_\ell = 0;\) WLOG, assume that \(n_1 = 0\). Since \(m > 1, 2^{2m} \geq 16,\) so the above equivalence is valid mod 8, i.e.

\[
a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{8}.
\]

But, \(n_1 = 0\) and \(q_1\) is odd, so \(a^2 \equiv 2^{2n_1}q_1^2 \equiv 1 \pmod{8}.\) Hence,

\[
1 + b^2 + c^2 + d^2 \equiv 0 \pmod{8},
\]

for integers \(b, c,\) and \(d,\) which is impossible. So, each \(n_\ell > 0.\)
Now, since each $n_\ell > 0$ and $2^{2n_1}q_1^3 + 2^{2n_2}q_2^2 + 2^{2n_3}q_3^2 + 2^{2n_4}q_4^2 \equiv 0 \mod 2^{2m}$, we have

$$2^{2(n_1-1)}q_1^3 + 2^{2(n_2-1)}q_2^2 + 2^{2(n_3-1)}q_3^2 + 2^{2(n_4-1)}q_4^2 \equiv 0 \mod 2^{2(m-1)}.$$ 

By induction, all of $n_1 - 1$, $n_2 - 1$, $n_3 - 1$, and $n_4 - 1$ are greater than or equal to $m - 2$. Hence, $n_1$, $n_2$, $n_3$, and $n_4$ are all greater than or equal to $m - 1$, and therefore $a$, $b$, $c$, and $d$ are all divisible by $2^{m-1}$.

(ii) Assume that $b^2 + c^2 + d^2 \equiv 0 \mod 2^{2m}$. By applying part (i) with $a = 0$, we see that each of $b$, $c$, and $d$ is divisible by $2^{m-1}$. Write $b = 2^{m-1}b_1$, $c = 2^{m-1}c_1$, and $d = 2^{m-1}d_1$ for some $b_1, c_1, d_1 \in \mathbb{Z}$. Since $b^2 + c^2 + d^2 \equiv 0 \mod 2^{2m}$, we have $2^{2m-2}(b_1^2 + c_1^2 + d_1^2) \equiv 0 \mod 2^{2m}$. This means that $b_1^2 + c_1^2 + d_1^2 \equiv 0 \mod 4$. Thus, $b_1$, $c_1$, and $d_1$ must all be even, and therefore $b$, $c$, and $d$ are all divisible by $2^m$. \qed

Next, we have the following proposition, which establishes a standard form for the residues in $\mathbb{Z}H/(2^m)$.

**Proposition 5.1.4.** Let $m > 1$, let $R = \mathbb{Z}Q/(2^m)$, and let $I = (2^{m-1} + 2^{m-1}i + 2^{m-1}j + 2^{m-1}k)$ in $R$. Then, $\mathbb{Z}H/(2^m)$ contains a subring $S$ that is isomorphic to $R/I$, and $\mathbb{Z}H/(2^m) = S[\mu]$.

**Proof.** Let $\iota : \mathbb{Z}Q \rightarrow \mathbb{Z}H$ be the injection map, let $\pi : \mathbb{Z}H \rightarrow \mathbb{Z}H/(2^m)$ be the canonical quotient map, and let $\phi = \pi \circ \iota$. Let $S = \text{Im}(\phi)$. Then, $(2^m)$ in $\mathbb{Z}Q$ is contained in $\text{Kern}(\phi)$, so $S$ is isomorphic to a quotient ring of $R = \mathbb{Z}Q/(2^m)$.

Note that if $\alpha \in \text{Kern}(\phi)$, then $\iota(\alpha) = 2^m\beta$ for some $\beta \in \mathbb{Z}H$, so $N(\alpha) = N(2^m\beta)$ is divisible by $2^{2m}$. By Lemma 5.1.3 part (i), $\alpha$ lies in $(2^{m-1})$ in $\mathbb{Z}Q$. Now, a residue in $R$ is both equivalent to an element of $(2^{m-1})$ in $\mathbb{Z}Q$ and has norm divisible by $2^{2m}$.
if and only if it lies in $I$. So, we conclude that $\text{Kern}(\phi) = I$ and $S \cong R/I$. Finally, since $S$ is the image of $\mathbb{Z}Q$ under $\phi$, $S$ consists of all the residues in $\mathbb{Z}H/(2^m)$ that can written as $a + bi + cj + dk + e\mu$ with $e = 0$. It follows that we can obtain the entire quotient ring $\mathbb{Z}H/(2^m)$ by adjoining $\mu$ to $S$. Thus, $\mathbb{Z}H/(2^m) = S[\mu]$.  

The effect of Proposition 5.1.4 is best illustrated with an example. Consider $\mathbb{Z}H/(2)$. Each residue in $\mathbb{Z}Q/(2)$ represents a residue in $\mathbb{Z}H/(2)$, but $1+i+j+k = 2\mu$ in $\mathbb{Z}H$, so $1+i+j+k \equiv 0$ in $\mathbb{Z}H/(2)$. Thus, $1+i \equiv j+k$, $1+j \equiv i+k$, $1+j+k \equiv i$, etc., so the image of $\mathbb{Z}Q$ in $\mathbb{Z}H/(2)$ consists of the eight residues in the following set:

$$\{0, 1, i, j, k, 1+1, 1+j, 1+k\}.$$ 

Hence, $\mathbb{Z}H/(2)$ is a ring of order 16 that may be expressed as the following set of residues:

$$\{0, 1, i, j, k, 1+1, 1+j, 1+k, 
\mu, 1+\mu, i+\mu, j+\mu, k+\mu, 1+i+\mu, 1+j+\mu, 1+k+\mu\}.$$ 

Analogous expressions hold for $\mathbb{Z}H/(2^m)$ whenever $m > 1$. In general, whenever we choose elements from $\mathbb{Z}H/(2^m)$, we shall assume the elements come from a set of residues like the one above.

We can now prove some interesting results about elements and quotient rings of $\mathbb{Z}H$. Our first theorem gives a nice characterization of those elements of $\mathbb{Z}H$ that lie in $(2^m)$.

**Theorem 5.1.5.** Let $\alpha \in \mathbb{Z}H$ and let $m > 0$. Then, $\alpha \in (2^m)$ if and only if $N(\alpha) \equiv 0 \mod 2^{2m}$.
Proof. (⇒) Assume that $\alpha \equiv 0 \mod 2^m$. Then, either each coefficient of $\alpha$ is divisible by $2^m$, or $\alpha \equiv 2^{m-1} + 2^{m-1}i + 2^{m-1}j + 2^{m-1}k \mod 2^m$. In the former case, it is easy to see that $N(\alpha) \equiv 0 \mod 2^m$, and in the latter case we have $\alpha = 2^{m-1}(1+i+j+k) + 2^m \beta$ for some $\beta \in \mathbb{Z}H$. Let $\beta = x + yi + zj + wk + e\mu$, where $x, y, z, w \in \mathbb{Z}$ and $e \in \{0, 1\}$. Then,

$$\alpha = 2^{m-1}(1+i+j+k+2(x+yj+wkw+e\mu))$$

$$= 2^{m-1}(2x+e+1+(2y+e+1)i+(2z+e+1)j+(2w+e+1)k),$$

so we have

$$N(\alpha) = 2^{2m-2}((2x+e+1)^2 + (2y+e+1)^2 + (2z+e+1)^2 + (2w+e+1)^2)$$

$$= 2^{2m-2}(4(x^2+y^2+z^2+w^2) + 4(x+y+z+w)(e+1) + 4(e+1)^2)$$

$$\equiv 0 \mod 2^{2m}.$$  

(⇐) Assume that $N(\alpha) \equiv 0 \mod 2^{2m}$, and write $\alpha = a + bi + cj + dk + e\mu$, where $a, b, c, d \in \mathbb{Z}$ and $e \in \{0, 1\}$. If $e = 1$, then

$$N(\alpha) = (a + \frac{1}{2})^2 + (b + \frac{1}{2})^2 + (c + \frac{1}{2})^2 + (d + \frac{1}{2})^2$$

$$= a^2 + b^2 + c^2 + d^2 + a + b + c + d + 4(\frac{1}{4})$$

$$\equiv 1 \mod 2, \text{ because } a, b, c, d \in \mathbb{Z}.$$

which contradicts the assumption that $N(\alpha) \equiv 0 \mod 2^{2m}$. So, we may assume that $e = 0$. Then, $\alpha \in \mathbb{Z}Q$ and $a^2 + b^2 + c^2 + d^2 \equiv 0 \mod 2^{2m}$. By Lemma 5.1.3 part (i), all of $a, b, c, d$ are divisible by $2^{m-1}$.

Assume that some coefficient of $\alpha$ is divisible by $2^m$. WLOG, assume that $a \equiv 0 \mod 2^m$. Then, $a^2 \equiv 0 \mod 2^{2m}$, so $b^2 + c^2 + d^2 \equiv 0 \mod 2^{2m}$. By Lemma 5.1.3
part (ii), b, c, and d are all congruent to 0 mod $2^m$. So, $\alpha \in (2^m)$ in this case. If no coefficient of $\alpha$ is divisible by $2^m$, then each coefficient of $\alpha$ is congruent to $2^{m-1}$ mod $2^m$, and so in $\mathbb{Z}H/(2^m)$,

$$\alpha \equiv 2^{m-1} + 2^{m-1}i + 2^{m-1}j + 2^{m-1}k \equiv 2^m \mu \equiv 0.$$ 

Thus, $\alpha$ is once again in $(2^m)$. \hfill \Box

Note that Theorem 5.1.5 does not hold in $\mathbb{Z}Q$, since for any $m > 0$, the norms of $2^m$ and $2^{m-1}(1 + i + j + k)$ are both equal to $2^{2m}$, but $2^{m-1}(1 + i + j + k) \notin (2^m)$.

The first calculation in the proof of the reverse implication of Theorem 5.1.5 is useful enough that we record it separately:

**Lemma 5.1.6.** Let $\alpha \in \mathbb{Z}H$ and write $\alpha = a + bi + cj + dk + e\mu$ where $a, b, c, d \in \mathbb{Z}$ and $e = 1$. Then, the norm of $\alpha$ is odd.

Using Lemma 5.1.6, we can prove the following proposition.

**Proposition 5.1.7.** Let $R = \mathbb{Z}H/(2)$, and let $I = (1+i)$ in $R$. Then, $I$ is a maximal ideal of $R$, and $R/I \cong \mathbb{F}_4$, the field with 4 elements. Furthermore, $\mathbb{Z}H/(1+i) \cong \mathbb{F}_4$.

**Proof.** Recall that after Proposition 5.1.4 we determined that $R$ is a ring of order 16 consisting of the following residues:

$$\{0, 1, i, j, k, 1 + 1, 1 + j, 1 + k, \\
\mu, 1 + \mu, i + \mu, j + \mu, k + \mu, 1 + i + \mu, 1 + j + \mu, 1 + k + \mu\}.\$$

By Lemma 5.1.6, those residues not in $I = \{0, 1 + i, 1 + j, 1 + k\}$ all have odd norm, and hence are units in $R$. So, $I$ must be a maximal ideal of $R$, and $R/I$ is a division ring of order 4; hence, $R/I \cong \mathbb{F}_4$. Finally, $\mathbb{Z}H/(1+i) \cong \mathbb{F}_4$ because $\mathbb{Z}H/(1+i) \cong R/I$. \hfill \Box

65
We can get a result similar to Theorem 5.1.5 for the ideal of $\mathbb{Z}H$ generated by $2^m + 2^m i$, but we need the help of a lemma.

**Lemma 5.1.8.**

(i) Let $\alpha \in \mathbb{Z}H$. Then, there exist $\beta, \gamma \in \mathbb{Z}H$ such that $\alpha(1 + i) = (1 + i)\beta$ and $(1 + i)\alpha = \gamma(1 + i)$.

(ii) Let $m \geq 0$ and let $\alpha \in (2^m + 2^m i)$ in $\mathbb{Z}H$. Then, there exist $\beta, \gamma \in \mathbb{Z}H$ such that $\alpha = (2^m + 2^m i)\beta$ and $\alpha = \gamma(2^m + 2^m i)$. Thus, the two-sided ideal $(2^m + 2^m i)$ equals both the right ideal $(2^m + 2^m i)\mathbb{Z}H$ and the left ideal $\mathbb{Z}H(2^m + 2^m i)$.

(iii) For each $\alpha \in \mathbb{Z}H$, $\alpha \in (1 + i)$ if and only if $N(\alpha)$ is even.

**Proof.** (i) It suffices to prove this for each $u \in \{i, j, k, \mu\}$. Then, the stated result follows by writing $\alpha$ in the standard form $\alpha = a + bi + cj + dk + e\mu$ with $a, b, c, d \in \mathbb{Z}$ and $e \in \{0, 1\}$.

If $u \in \{i, j, k\}$, then since $\mathbb{Z}Q/(2)$ is commutative, we have $u(1 + i) \equiv (1 + i)u \pmod{2}$. Hence, there exists $\delta \in \mathbb{Z}Q$ such that

$$u(1 + i) = (1 + i)u + 2\delta = (1 + i)(u + (1 - i)\delta)$$

and we can take $\beta = (u + (1 - i)\delta)$. The existence of $\gamma$ in the case where $u \in \{i, j, k\}$ can be proved in a similar manner.

If $u = \mu$, then one need merely notice that $\mu(1 + i) = (1 + i)(\mu - k)$ and $(1 + i)\mu = (\mu - j)(1 + i)$, so we may take $\beta = \mu - k$ and $\gamma = \mu - j$.

(ii) Since $\alpha \in (2^m + 2^m i)$, we may write $\alpha = \sum_{r=1}^{n} \alpha_r(2^m + 2^m i)\beta_r$ for some $\alpha_r, \beta_r$ $(1 \leq r \leq n)$ in $\mathbb{Z}H$. By part (i), for each $r$ there exist $\alpha'_r, \beta'_r \in \mathbb{Z}H$ such that

$$\sum_{r=1}^{n} \alpha'_r(2^m + 2^m i)\beta'_r$$

is in $(2^m + 2^m i)$.
\( \alpha_r(1 + i) = (1 + i)\alpha'_r \) and \( (1 + i)\beta_r = \beta'_r(1 + i) \). Hence,

\[
\alpha = \sum_{r=1}^{n} \alpha_r(2^m + 2^m i)\beta_r = \sum_{r=1}^{n} (2^m)(1 + i)\alpha'_r\beta_r = (2^m + 2^m i) \sum_{r=1}^{n} \alpha'_r\beta_r, \text{ and }
\]

\[
\alpha = \sum_{r=1}^{n} \alpha_r(2^m + 2^m i)\beta_r = \sum_{r=1}^{n} \alpha_r\beta'_r(2^m)(1 + i) = \left( \sum_{r=1}^{n} \alpha_r\beta'_r \right) (2^m + 2^m i),
\]

so we can take \( \beta = \sum_{r=1}^{n} \alpha'_r\beta_r \) and \( \gamma = \sum_{r=1}^{n} \alpha_r\beta'_r \).

(iii) \((\Rightarrow)\) Assume first that \( \alpha \in (1 + i) \). By part (i), \( \alpha = (1 + i)\beta \) for some \( \beta \in \mathbb{Z}H \), so \( N(\alpha) = N(1 + i)N(\beta) = 2N(\beta) \).

\((\Leftarrow)\) Assume that \( \alpha \in \mathbb{Z}H \) has even norm. Then, the residue of \( \alpha \) modulo 2 is not invertible in \( \mathbb{Z}H/(2) \), so \( \alpha \) mod 2 lies in the maximal ideal of \( \mathbb{Z}H/(2) \) that is generated by \( (1 + i) \). Note that part (ii) also holds in \( \mathbb{Z}H/(2) \), so we may write \( \alpha \equiv (1 + i)\beta \) mod 2 for some \( \beta \in \mathbb{Z}H \). Thus, there exists \( \alpha' \in \mathbb{Z}H \) such that

\[
\alpha = (1 + i)\beta + 2\alpha' = (1 + i)(\beta + (1 - i)\alpha'),
\]

and hence \( \alpha \in (1 + i) \).

\[\square\]

**Theorem 5.1.9.** Let \( \alpha \in \mathbb{Z}H \) and let \( m \geq 0 \). Then, \( \alpha \in (2^m + 2^m i) \) if and only if \( N(\alpha) \equiv 0 \text{ mod } 2^{2m+1} \).

*Proof.* \((\Rightarrow)\) Assume that \( \alpha \in (2^m + 2^m i) \). Then, by Lemma 5.1.8 part (ii), \( \alpha = (2^m + 2^m i)\beta \) for some \( \beta \in \mathbb{Z}H \), and hence \( N(\alpha) = N(2^m + 2^m i)N(\beta) = 2^{2m+1}N(\beta) \).

\((\Leftarrow)\) Assume that \( N(\alpha) \equiv 0 \text{ mod } 2^{2m+1} \). Then, \( N(\alpha) \equiv 0 \text{ mod } 2^m \), so by Theorem 5.1.5, \( \alpha \in (2^m) \) in \( \mathbb{Z}H \) and \( \alpha = 2^m\beta \) for some \( \beta \in \mathbb{Z}H \). Since \( N(\alpha) \) is divisible by \( 2^{2m+1} \) and \( N(2^m) = 2^m \), the norm of \( \beta \) must be even. By Lemma 5.1.8, \( \beta \in (1 + i) \).
and we may write $\beta = (1 + i)\gamma$ for some $\gamma \in \mathbb{Z}H$. Then, $\alpha = 2^m \beta = (2^m + 2^m i)\gamma \in (2^m + 2^m i)$.

The remainder of this section will be dedicated to classifying the quotient rings of $\mathbb{Z}H$ of characteristic $2^m$. Most of the work for the classification is done in the following theorem.

**Theorem 5.1.10.** Let $m \geq 0$. If $I$ is an ideal of $\mathbb{Z}H$ such that $(2^m + 1) \subset I \subset (2^m)$, then $I = (2^m + 2^m i)$.

**Proof.** Since $(2^m + 1) \subset (2^m + 2^m i) \subset (2^m)$, there exist ideals of $\mathbb{Z}H$ properly between $(2^m + 1)$ and $(2^m)$. So, let $I$ be such an ideal of $\mathbb{Z}H$.

Let $R = \mathbb{Z}H/(2^m + 1)$ and let $\pi : \mathbb{Z}H \rightarrow R$ be the quotient map. We will prove that the only ideal of $R$ properly between $2^{m+1}R$ and $2^m R$ is $(2^m + 2^m i)R$. Then, since there is an inclusion preserving bijection between ideals of $R$ and ideals $\mathbb{Z}H$ containing $(2^m + 1)$, we may conclude that $I = \pi^{-1}((2^m + 2^m i)R) = (2^m + 2^m i)$.

Let $\alpha \in 2^m R$. Since $\mathbb{Z}H$ is a principal ideal ring, the same is true for $R$, so it suffices to show that $(\alpha)$ in $R$ equals one of $2^m R$, $2^{m+1} R$, or $(2^m + 2^m i) R$. Let

$$S = \{0, 1, i, j, k, 1 + 1, 1 + j, 1 + k, \\
\mu, 1 + \mu, i + \mu, j + \mu, k + \mu, 1 + i + \mu, 1 + j + \mu, 1 + k + \mu\}$$

(theses are the residues for $\mathbb{Z}H/(2)$ that were given following Proposition 5.1.4). Then, $\alpha \equiv 2^m \beta$ for some $\beta \in S$. If $\beta \notin \{0, 1 + 1, 1 + j, 1 + k\}$, then by Lemma 5.1.6, $\beta$ has odd norm, and hence is a unit in $R$. In this case, $(\alpha) = 2^m R$. If $\beta = 0$, then $(\alpha) = (0)$; that is, $(\alpha) = 2^{m+1} R$. Thus, the only way that $(\alpha) \neq 2^m R$ and $(\alpha) \neq 2^{m+1} R$ is if $\beta \in \{1 + 1, 1 + j, 1 + k\}$, in which case $(\alpha) = (2^m + 2^m i) R$. \qed
Corollary 5.1.11. Let $m > 0$ and let $R = \mathbb{Z}H/(2^m)$. Then, the ideals of $R$ are linearly ordered under inclusion.

Proof. First, let $\alpha \in R - \{0\}$ and let $N(\alpha) = 2^nq$, where $0 \leq n \leq 2m - 1$ and $q$ is odd. If $n$ is even, then $n = 2\ell$ for some $\ell \in \mathbb{Z}$, $\ell \leq m - 1$, and by Theorems 5.1.5 and 5.1.9, $\alpha \in 2^{\ell}R$ but $\alpha \notin (2^{\ell} + 2^\ell i)R$, so $(\alpha) = 2^{\ell}R$ by Theorem 5.1.10. Similarly, if $n$ is odd and $n = 2\ell + 1$, then $(\alpha) = (2^{\ell} + 2^\ell i)R$.

Next, let $I = (\beta)$ and $J = (\gamma)$ be two ideals in $R$ (here, we are using the fact that $R$, like $\mathbb{Z}H$, is a principal ideal ring). Let $N(\beta) = 2^{n_1}q_1$ and $N(\gamma) = 2^{n_2}q_2$, where $n_1, n_2 \geq 0$ and $q_1$ and $q_2$ are odd. By the arguments of the preceding paragraph, we see that if $n_1 \geq n_2$, then $I \subseteq J$, and if $n_2 \geq n_1$, then $J \subseteq I$. We have containment in either case, so the ideals of $R$ are linearly ordered under inclusion. \qed

Corollary 5.1.12. Let $m > 0$ and let $R$ be quotient ring of $\mathbb{Z}H$ with $\text{char}(R) = 2^m$. Then, either $R \cong \mathbb{Z}H/(2^m)$ or $R \cong \mathbb{Z}H/(2^{m-1} + 2^{m-1}i)$.

Proof. Since $\text{char}(R) = 2^m$, $R$ is isomorphic to a quotient ring of $S = \mathbb{Z}H/(2^m)$. Let $I$ be the ideal of $S$ such that $R \cong S/I$.

If $2^{m-1}S \subseteq I$, then $\text{char}(R) \leq 2^{m-1}$, which is a contradiction. By Corollary 5.1.11, $I$ is an ideal of $S$ properly contained in $2^{m-1}S$. By Theorem 5.1.10, either $I = (2^{m-1} + 2^{m-1}i)S$ or $I = 2^mS$. In the former case, $R \cong \mathbb{Z}H/(2^{m-1} + 2^{m-1}i)$, and in the latter case $R \cong \mathbb{Z}H/(2^m)$.

\qed

5.2 Int($\mathbb{Z}H$) is Closed Under Bar Conjugation

Using the results of the previous section, we can prove that Int($\mathbb{Z}H$) is closed under bar conjugation. The gist of the proof is embodied in the following theorem.
Theorem 5.2.1. The ring $\text{Int}(\mathbb{Z}H)$ is closed under bar conjugation if and only if for each prime $p$ and each $m > 0$, the ideal $\text{Muff}(\mathbb{Z}H/(p^m))$ of $((\mathbb{Z}H/(p^m))[x]$ is closed under bar conjugation.

Proof. $(\Rightarrow)$ Assume that $\text{Int}(\mathbb{Z}H)$ is closed under bar conjugation. Let $p$ be a prime, let $m > 0$, and let $f(x) \in \text{Muff}(\mathbb{Z}H/(p^m))$. Then, $f(x)/p^m \in \text{Int}(\mathbb{Z}H)$. Since $\text{Int}(\mathbb{Z}H)$ is closed under bar conjugation, $\overline{f(x)/p^m} \in \text{Int}(\mathbb{Z}H)$, which implies that $\overline{f(x)} \in \text{Muff}(\mathbb{Z}H/(p^m))$.

$(\Leftarrow)$ Assume that for each prime $p$ and each $m > 0$, $\text{Muff}(\mathbb{Z}H/(p^m))$ is closed under bar conjugation. Let $f(x) \in \text{Int}(\mathbb{Z}H)$. Then, we may write $f(x) = \frac{g(x)}{n}$ for some $g(x) \in \mathbb{Z}H[x]$ and some $n > 0$. If $n = 1$, then $f(x) \in \mathbb{Z}H[x]$, so $\overline{f(x)} \in \mathbb{Z}H[x] \subseteq \text{Int}(\mathbb{Z}H)$ and we are done. So, assume that $n > 1$.

Next, consider the case where $n$ is a power of a prime. Assume that $n = p^e$ for some prime $p$ and some $e > 0$. Then, $f(x) = \frac{g(x)}{n} \in \text{Int}(\mathbb{Z}H)$, so $g(x) \mod p^e$ is in $\text{Muff}(\mathbb{Z}H/(p^e))$. Since $\text{Muff}(\mathbb{Z}H/(p^e))$ is closed under bar conjugation, we have $\overline{g(x)} \mod p^e \in \text{Muff}(\mathbb{Z}H/(p^e))$, and so $\overline{f(x)} = \frac{\overline{g(x)}}{p^e} \in \text{Int}(\mathbb{Z}H)$.

Finally, assume that $n$ has prime factorization $n = p_1^{e_1} \cdots p_t^{e_t}$, where $t > 1$. Notice that if $n$ factors as $n = q_1 q_2$ for relatively prime integers $q_1$ and $q_2$, then there exist $a, b \in \mathbb{Z}$ such that $aq_1 + bq_2 = 1$. In this case, $\frac{g(x)}{n} = \frac{b g(x)}{q_1} + \frac{a g(x)}{q_2}$, and both $\frac{g(x)}{q_1}$ and $\frac{g(x)}{q_2}$ are elements of $\text{Int}(\mathbb{Z}H)$. Now, since $n = p_1^{e_1} \cdots p_t^{e_t}$, there exist $a_1, a_2, \ldots, a_t \in \mathbb{Z}$ such that $\frac{g(x)}{n} = \sum_{r=1}^{t} \frac{a_r g(x)}{p_r^{e_r}}$ and each $\frac{g(x)}{p_r^{e_r}} \in \text{Int}(\mathbb{Z}H)$. By the previous paragraph, $\overline{\frac{g(x)}{p_r^{e_r}}} \in \text{Int}(\mathbb{Z}H)$ for each $r$. Hence, $\overline{f(x)} = \frac{\overline{g(x)}}{n} = \sum_{r=1}^{t} \frac{a_r \overline{g(x)}}{p_r^{e_r}} \in \text{Int}(\mathbb{Z}H)$, and we conclude that $\text{Int}(\mathbb{Z}H)$ is closed under bar conjugation. \qed
Our strategy is now clear: to prove that $\text{Int}(\mathbb{Z}H)$ is closed under bar conjugation, it suffices to work in $\mathbb{Z}H/(p^m)$, where $p$ is a prime. When $p$ is odd, proving that $\text{Muff}(\mathbb{Z}H/(p^m))$ is closed under bar conjugation is easy given some of our previous results, but things are more difficult when $p = 2$, and we will rely heavily on the theorems in Section 5.1. The closure of the needed muffin ideals follows from Theorem 5.2.3, where we will actually achieve a stronger result that will be used when we establish a generating set for $\text{Int}(\mathbb{Z}H)$ in Section 5.3. Before dealing with Theorem 5.2.3, we prove one more result that will be useful.

**Theorem 5.2.2.** Let $R$ be a quotient ring of $\mathbb{Z}H$ with $\text{char}(R) = 2^m$. Let $\alpha \in R$. Then, the following are equivalent:

(i) $(1 + i)\alpha \equiv 0$ in $R$

(ii) $\alpha(1 + i) \equiv 0$ in $R$

(iii) $\alpha \in \text{Ann}_R(1 + i)$

**Proof.** The implications (iii) $\Rightarrow$ (i) and (iii) $\Rightarrow$ (ii) are clear. We will first prove that (i) $\Leftrightarrow$ (ii). By Theorem 5.1.12, either $R \cong \mathbb{Z}H/(2^m)$ or $R \cong \mathbb{Z}H/(2^{m-1} + 2^{m-1}i)$. In the former case, we have

\[(1 + i)\alpha \equiv 0 \text{ in } R \iff (1 + i)\alpha \equiv (2^m) \text{ in } \mathbb{Z}H \]

\[\iff N((1 + i)\alpha) \equiv 0 \text{ mod } 2^{2m} \]

\[\iff N(\alpha(1 + i)) \equiv 0 \text{ mod } 2^{2m} \]

\[\iff \alpha(1 + i) \equiv 0 \text{ in } R , \]

and so (i) holds if and only if (ii) holds. Similarly, (i) $\Leftrightarrow$ (ii) is true when $R \cong \mathbb{Z}H/(2^{m-1} + 2^{m-1}i)$. This establishes that (i) $\Leftrightarrow$ (ii).

71
To complete the proof, it suffices to show that (i) $\Rightarrow$ (iii). Assume that $(1+i)\alpha \equiv 0$ in $R$. Then, $\alpha(1+i)$ is also equivalent to 0. Let $\beta \in (1+i)$. By Lemma 5.1.8 part (ii), there exist $\gamma, \delta \in \mathbb{H}$ such that $\beta \equiv \gamma(1+i)$ and $\beta \equiv (1+i)\delta$. Then,

$$\beta\alpha \equiv \gamma(1+i)\alpha \equiv 0, \quad \text{and} \quad \alpha\beta \equiv \alpha(1+i)\delta \equiv 0.$$ 

Thus, (iii) holds, and we are done. \qed

We can now prove that the muffins ideals in $\mathbb{H}/(p^m)$ are closed under bar conjugation. The proof of the following theorem is quite lengthy, and we break it up into several cases.

**Theorem 5.2.3.** Let $p$ be a prime and let $m > 0$. Let $R$ be a quotient ring of $\mathbb{H}$ with char$(R) = p^m$, and let $f \in \text{Muff}(R)$. Then, $\overline{f} \in \text{Muff}(R)$.

**Proof.** Assume first that $p$ is odd. Recall Lemma 3.1.3, where it was shown that for any $g(x) \in \mathbb{H}[x]$ and any $\beta \in \mathbb{H}$, we have

$$\overline{g}(\beta) = \frac{1}{2} \left( g(\overline{\beta}) + \overline{g(\beta)} \right) + \frac{1}{2} \left( g(-i\overline{\beta})i + g(-i\overline{\beta})i \right) i$$

$$+ \frac{1}{2} \left( g(-j\overline{\beta})j + g(-j\overline{\beta})j \right) j + \frac{1}{2} \left( g(-k\overline{\beta}k)k + g(-k\overline{\beta}k)k \right) k.$$

Since 2 is invertible in $R$, this expression is also true over $R$. So, for each $\beta \in R$, we have

$$\overline{f}(\beta) \equiv \frac{1}{2} \left( f(\overline{\beta}) + \overline{f(\beta)} \right) + \frac{1}{2} \left( f(-i\overline{\beta})i + f(-i\overline{\beta})i \right) i$$

$$+ \frac{1}{2} \left( f(-j\overline{\beta})j + f(-j\overline{\beta})j \right) j + \frac{1}{2} \left( f(-k\overline{\beta}k)k + f(-k\overline{\beta}k)k \right) k.$$

Since $f \in \text{Muff}(R)$, each term on the right-hand side of the equivalence is congruent to 0 in $R$. Thus, $\overline{f}(\beta) \equiv 0$ for each $\beta \in R$, and therefore $\overline{f} \in \text{Muff}(R)$. This completes the proof in the case where $p$ is odd.
Assume from now on that \( p = 2 \). Let \( \alpha \in R \). Since \( \min_\alpha(x) \) is monic, we have

\[
f(x) = q(x) \min_\alpha(x) + \gamma x + \delta
\]

for some \( q(x) \), \( \gamma x + \delta \in R[x] \). Now, \( \min_\alpha(x) \) has integer coefficients, so \( \min_\alpha(x) \) is central in \( R[x] \) and \( \overline{\min_\alpha(x)} = \min_\alpha(x) \). This means that

\[
\overline{q(x) \min_\alpha(x)} = \overline{\min_\alpha(x)} \overline{q(x)} = \min_\alpha(x) \overline{q(x)} = \overline{q(x) \min_\alpha(x)} .
\]

So, we have

\[
\overline{f(x)} = \overline{q(x) \min_\alpha(x) + \gamma x + \delta} .
\]

We wish to show that \( \overline{f(\alpha)} \equiv 0 \). By the above, we have \( \overline{f(\alpha)} \equiv \overline{q(\alpha)} \min_\alpha(\alpha) + \overline{\gamma} \alpha + \overline{\delta} \equiv \overline{\gamma} \alpha + \overline{\delta} \), so it suffices to show that \( \overline{\gamma} \alpha + \overline{\delta} \equiv 0 \). Notice that

\[
\overline{\gamma} \alpha + \overline{\delta} \equiv 0 \iff \overline{\gamma} \alpha + \overline{\delta} \equiv 0
\]

\[
\iff \overline{\alpha} \gamma + \overline{\delta} \equiv 0
\]

\[
\iff \overline{\alpha} \gamma + \overline{\delta} \equiv f(\alpha) \equiv \gamma \alpha + \delta
\]

\[
\iff \gamma \alpha - \overline{\alpha} \gamma \equiv 0 . \quad (\ast)
\]

We will show that \( (\ast) \) holds.

If \( \min_\alpha(x) \) is linear, then \( \gamma \equiv 0 \), so \( (\ast) \) holds. So, we may assume that \( \min_\alpha(x) \) is quadratic, i.e. that \( \alpha \notin \mathbb{Z}/2m\mathbb{Z} \) in \( R \).

Now, whenever \( \beta \in R \) and \( \min_\beta(x) = \min_\alpha(x) \), we have \( 0 \equiv f(\beta) \equiv \gamma \beta + \delta \).

Assume that \( \alpha \equiv a + bi + cj + dk + e\mu \), where \( a, b, c, d \in \mathbb{Z} \) and \( e \in \{0, 1\} \). If \( e = 1 \), then

\[
\alpha - (-i\alpha i) \equiv (a + bi + cj + dk + \mu) - (a - bi + cj + dk + (\mu - i))
\]

\[
\equiv (a + bi + cj + dk + \mu) - (a - (b + 1)i + cj + dk + \mu)
\]

\[
\equiv (2b + 1)i,
\]

73
which is unit in $R$ since $2b + 1$ is odd. Hence,
\[
0 \equiv f(\alpha) - f(-i\alpha i)
\equiv (\gamma \alpha + \delta) - (\gamma(-i\alpha i) + \delta)
\equiv \gamma(\alpha - (-i\alpha i))
\equiv (2b + 1)\gamma i,
\]
implying that $\gamma \equiv 0$. Thus, (*) holds when $e = 1$, and we may assume that $e = 0$.

Since $e = 0$, we have $\alpha \equiv a + bi + cj + dk$, and we compute that

\[
\gamma\alpha - \alpha\gamma \equiv b(\gamma i + i\gamma) + c(\gamma j + j\gamma) + d(\gamma k + k\gamma).
\]

So, it suffices to show that

\[
b(\gamma i + i\gamma) + c(\gamma j + j\gamma) + d(\gamma k + k\gamma) \equiv 0.
\]  

(***)

If $R = \mathbb{Z}H/(1 + i)$, then $R \cong \mathbb{F}_4$, the field with 4 elements, in which case $R$ is commutative and

\[
b(\gamma i + i\gamma) + c(\gamma j + j\gamma) + d(\gamma k + k\gamma) \equiv 2b\gamma i + 2c\gamma j + 2d\gamma k \equiv 0,
\]

so (**) is true. So, assume that $|R| > 4$, and let $I = \text{Ann}_R(2)$ and $J = \text{Ann}_R(1 + i)$. Since $0 \equiv f(\alpha) - f(-i\alpha i) \equiv 2b\gamma$, we have $b\gamma \in I$. Similarly, $c\gamma, d\gamma \in I$. Furthermore, let $\alpha' \equiv a - ci - bj + dk$. Then, $\min_{\alpha'}(x) = \min_{\alpha}(x)$, so

\[
0 \equiv f(\alpha) - f(\alpha')
\equiv \gamma((b + c)i + (b + c)j)
\equiv (b + c)\gamma(i + j).
\]
Since $i + j$ is a generator for $(1+i)R$, Lemma 5.2.2 tells us that $(b+c)\gamma \in J$. Similarly, $(b+d)\gamma, (c+d)\gamma \in J$.

From here, we have two broad cases to consider, depending on the isomorphism type of $R$. By Corollary 5.1.12, either $R \cong \mathbb{Z}H/(2^m)$ or $R \cong \mathbb{Z}H/(2^{m-1} + 2^{m-1}i)$.

**Case 1: $R \cong \mathbb{Z}H/(2^m)$**

In this case, $I = 2^{m-1}R$ and $J = (2^{m-1} + 2^{m-1}i)R$. Then, $J = \{0, 2^{m-1} + 2^{m-1}i, 2^{m-1} - 2^{m-1}i, 2^{m-1} - 2^{m-1}j, 2^{m-1} - 2^{m-1}k\}$; in particular, note that $J \subseteq I$. Let

$$J' = J \cup \{2^{m-1}, 2^{m-1}i, 2^{m-1}j, 2^{m-1}k\}.$$

Then, $J \subset J' \subset I$, and $J'$ is not an ideal of $R$, but $J'$ is closed under addition. Furthermore, notice that each element of $J'$ commutes (modulo $2^m$) with $i$, $j$, and $k$.

Now, we showed above that $b\gamma, c\gamma, d\gamma \in I$ and $(b+c)\gamma, (b+d)\gamma, (c+d)\gamma \in J$. If $b\gamma \in J'$, then

$$c\gamma \equiv (b+c)\gamma - b\gamma \in J', \text{ and}$$

$$d\gamma \equiv (b+d)\gamma - b\gamma \in J'.$$

Similarly, having $c\gamma$ or $d\gamma$ in $J'$ forces all three of $b\gamma, c\gamma, d\gamma$ to be in $J'$. So, either all three of $b\gamma, c\gamma, d\gamma$ are in $J'$, or all three are in $I - J'$. Thus, we have two subcases to consider.

**Subcase 1a: $b\gamma, c\gamma, d\gamma \in J'$**

In this case, since each element of $J'$ commutes with $i$, $j$, and $k$, we have

$$b(\gamma i + i\gamma) + c(\gamma j + j\gamma) + d(\gamma k + k\gamma) \equiv 2b\gamma i + 2c\gamma j + 2d\gamma k \equiv 0.$$
so (**) holds and we are done.

**Subcase 1b:** $b\gamma, c\gamma, d\gamma \in I - J'$

Let $\varepsilon \in I - J'$. Then, $\varepsilon \equiv 2^{m-1}\varepsilon'$, where $\varepsilon'$ is an element of

$$\{\mu, 1 + \mu, i + \mu, j + \mu, k + \mu, 1 + i + \mu, 1 + j + \mu, 1 + k + \mu\},$$

so we may write

$$\varepsilon \equiv u_12^{m-2} + u_22^{m-2}i + u_32^{m-2}j + u_42^{m-2}k,$$

where $u_1, u_2, u_3, u_4 \in \{\pm 1\}$. Then, since $2^{m-1} \equiv -2^{m-1}$,

$$\varepsilon i + i\varepsilon \equiv 2^{m-2}(-u_2 + u_1i + u_4j - u_3k) + 2^{m-2}(-u_2 + u_1i - u_4j + u_3k)$$

$$\equiv -2^{m-1} + 2^{m-1}i$$

$$\equiv 2^{m-1} + 2^{m-1}i.$$  

Similarly, $\varepsilon j + j\varepsilon \equiv 2^{m-1} + 2^{m-1}j$ and $\varepsilon k + k\varepsilon \equiv 2^{m-1} + 2^{m-1}k$. Since $b\gamma$, $c\gamma$, and $d\gamma$ are all in $I - J'$, we get

$$b(\gamma i + i\gamma) + c(\gamma j + j\gamma) + d(\gamma k + k\gamma)$$

$$\equiv (2^{m-1} + 2^{m-1}i) + (2^{m-1} + 2^{m-1}j) + (2^{m-1} + 2^{m-1}k)$$

$$\equiv 2^{m-1} + 2^{m-1}i + 2^{m-1}j + 2^{m-1}k$$

$$\equiv 0.$$  

Thus, (**) holds.

There are no more subcases, so Case 1 is complete.
Case 2: \( R \cong \mathbb{Z}H/(2^{m-1} + 2^{m-1}i) \)

We use a strategy similar to that employed in Case 1. However, in this case it is more difficult to establish when two elements of \( R \) are equivalent. When in doubt, the best way to check whether \( \beta_1, \beta_2 \in R \) are equivalent is to compute \( N(\beta_1 - \beta_2) \). If this norm is divisible by \( 2^{2m-1} = N(2^{m-1} + 2^{m-1}i) \), then \( \beta_1 \equiv \beta_2 \) in \( R \). In light of this, it is not hard to see that

\[
2^{m-1}, 2^{m-1}i, 2^{m-1}j, \text{ and } 2^{m-1}k \text{ are all equivalent in } R.
\]

Keeping this relationship in mind will help expedite the calculations that follow.

Proceeding as in Case 1, we have

\[
I = (2^{m-2} + 2^{m-2}i)R, \ J = 2^{m-1}R, \text{ and } J \subseteq I.
\]

As in Case 1, \( |I| = 16 \) and \( |J| = 4 \). Considering \( I \) and \( J \) as additive groups, this means that \( J \) is an index 4 subgroup of \( I \). We will compute the cosets of \( J \) in \( I \), which will allow us to partition \( I \) into subsets that are amenable to the same sort of calculations done in Case 1. Using the fact that \( 2^{m-1}, 2^{m-1}i, 2^{m-1}j, \text{ and } 2^{m-1}k \) all represent the same residue in \( R \), we can compute that

\[
J = \{0, 2^{m-1}, 2^{m-1}u, 2^{m-1}(1+\mu)\}.
\]

Then, the other cosets of \( J \) in \( I \) are given by

\[
J_1 = 2^{m-2} + 2^{m-2}i + J = \{2^{m-2} \pm 2^{m-2}i, 2^{m-2}j \pm 2^{m-2}k\},
\]

\[
J_2 = 2^{m-2} + 2^{m-2}j + J = \{2^{m-2} \pm 2^{m-2}j, 2^{m-2}i \pm 2^{m-2}k\}, \text{ and}
\]

\[
J_3 = 2^{m-2} + 2^{m-2}k + J = \{2^{m-2} \pm 2^{m-2}k, 2^{m-2}i \pm 2^{m-2}j\},
\]

so that \( I \) is the disjoint union of \( J, J_1, J_2, \) and \( J_3 \).

Now, \( b\gamma \) lies in exactly one of the cosets \( J, J_1, J_2, \) or \( J_3 \); assume that \( b\gamma \in \beta + J \), where \( \beta \) is an element of \( \{0, 2^{m-2} + 2^{m-2}i, 2^{m-2} + 2^{m-2}j, 2^{m-2} + 2^{m-2}k\} \). Since \( (b+c)\gamma \) is in \( J \), we must have \( c\gamma \in \beta + J \). Similarly, \( d\gamma \in \beta + J \).
Note that each element of $J$ commutes (in $R$) with $i$, $j$, and $k$. Since $b\gamma \in \beta + J$, we have $b\gamma \equiv \beta + \varepsilon$ for some $\varepsilon \in J$. Then,

$$b(\gamma i + i\gamma) \equiv \beta i + i\beta + \varepsilon i + i\varepsilon$$

$$\equiv \beta i + i\beta + 2\varepsilon i$$

$$\equiv \beta i + i\beta,$$

where the last equivalence follows because $\varepsilon \in I$, so $2\varepsilon \equiv 0$. Similarly, we can compute that

$$c(\gamma j + j\gamma) \equiv \beta j + j\beta \quad \text{and} \quad d(\gamma k + k\gamma) \equiv \beta k + k\beta.$$

Thus, to establish that $(**)$, it suffices to verify that

$$(\beta i + i\beta) + (\beta j + j\beta) + (\beta k + k\beta) \equiv 0$$

as $\beta$ runs along the coset representatives $\{0, 2^{m-2} + 2^{m-2} i, 2^{m-2} + 2^{m-2} j, 2^{m-2} + 2^{m-2} k\}$. This is certainly true when $\beta \equiv 0$. If $\beta \equiv 2^{m-2} + 2^{m-2} i$, then

$$\beta i + i\beta \equiv 2(-2^{m-2} + 2^{m-2} i) \equiv 0,$$

$$\beta j + j\beta \equiv 2^{m-1} j,$$

and $\beta k + k\beta \equiv 2^{m-1} k$, so

$$(\beta i + i\beta) + (\beta j + j\beta) + (\beta k + k\beta) \equiv 0 + 2^{m-1} j + 2^{m-1} k \equiv 0.$$  

Similarly, $(\beta i + i\beta) + (\beta j + j\beta) + (\beta k + k\beta) \equiv 0$ when $\beta \equiv 2^{m-2} + 2^{m-2} j$ or $\beta \equiv 2^{m-2} + 2^{m-2} k$. Therefore, we conclude that $(**)$ holds in all instances. This proves Case 2.

There are no more cases to consider, so the proof is complete.

**Corollary 5.2.4.** $\text{Int}(\mathbb{Z}H)$ is closed under conjugation; that is, if $f \in \text{Int}(\mathbb{Z}H)$, then $f \in \text{Int}(\mathbb{Z}H)$.

**Proof.** This follows from Theorems 5.2.1 and 5.2.3. □
5.3 A Generating Set for $\text{Int}(\mathbb{Z}H)$

Having established that $\text{Int}(\mathbb{Z}H)$ is closed under bar conjugation, we now have enough tools to construct a generating set for $\text{Int}(\mathbb{Z}H)$. The first step in this process is to extend Theorem 4.3.6 to quotient rings of $\mathbb{Z}H$. We shall do this in stages, with Theorems 5.3.1 through 5.3.3. Before stating Theorem 5.3.1, we recall two definitions from Chapter 4. By the content of a polynomial $f$, we mean the ideal generated by the coefficients of $f$ (see the paragraph prior to Lemma 4.3.5). Also, when $R$ is a quotient ring of $\mathbb{Z}H$ of characteristic $n$, the polynomial $\phi_R$ is a monic polynomial of minimal degree in $\text{Muff}(R) \cap (\mathbb{Z}/n\mathbb{Z})[x]$ (see Section 4.2).

**Theorem 5.3.1.** Let $R$ be a quotient ring of $\mathbb{Z}H$ with $\text{char}(R) = 2^m$, where $m > 0$. Assume that $f$ is a content 1 polynomial of minimal degree in $\text{Muff}(R)$. Then, the leading coefficient of $f$ is a unit, so we may assume that $f$ is monic.

**Proof.** We use induction on $|R|$. The base case occurs when $R \cong \mathbb{Z}H/(1+i) \cong \mathbb{F}_4$. In this case, $R[x]$ is a PID, so $\text{Muff}(R) = (\phi_R)$ and we may take $f = \phi_R$. Since $\phi_R$ is monic, we are done.

So, assume that $|R| > 4$ and that the result holds for any finite, non-zero quotient ring $S$ of $\mathbb{Z}H$ such that $\text{char}(S)$ is a power of 2 and $|S| < |R|$. Let $\gamma$ be the leading coefficient of $f$; then, $\gamma \neq 0$ in $R$. We want to show that $\gamma$ is a unit in $R$. Let $M = (1+i)R$. By Corollary 5.1.11, $M$ is the unique maximal ideal of $R$ and $M = R - R^\times$. Suppose that $\gamma \in M$. Let $I = \text{Ann}_R(\gamma)$ and let $S = R/I$. Since $\gamma \in M$, $I \neq (0)$, so $S \neq R$.

Let $g$ be a content 1 polynomial of minimal degree in $\text{Muff}(S)$. By the inductive hypothesis, we may assume that $g$ is monic. Now, since $\text{con}(f) = (1)$, we have...
\[ \text{con}(f \mod I) = (1), \text{ so} \]
\[ \deg(f) \geq \deg(f \mod I) \geq \deg(g). \]

Now, let \( G \) be a polynomial in \( R[x] \) such that \( G \) is monic, \( \deg(G) = \deg(g) \), and \( G \equiv g \mod I \) (such a \( G \) must exist because we can always take \( G = g \), where we abuse notation and consider the coefficients of \( g \) to be elements of \( R \)). Since \( g \in \text{Muff}(S) \), for all \( \alpha \in R \) we have \( G(\alpha) \in I = \text{Ann}(\gamma) \). Hence, \( \gamma G(\alpha) = 0 \) in \( R \) for all \( \alpha \in R \) and so \( \gamma G \in \text{Muff}(R) \). By the above, \( \deg(\gamma G) = \deg(g) \leq \deg(f) \). Let \( d = \deg(f) - \deg(\gamma G) \). Then, \( h = f - \gamma x^d G \in \text{Muff}(R) \), and since \( G \) is monic, either \( h = 0 \) or \( \deg(h) < \deg(f) \). If \( h = 0 \), then \( f = \gamma x^d G \) and \( \text{con}(f) \subseteq \gamma R \subseteq M \), which is a contradiction. So, \( \deg(h) < \deg(f) \).

Since \( \text{con}(f) = (1) \), there exists \( t \in \{0, 1, \ldots, \deg(f)\} \) such that the coefficient \( \alpha_t \) of \( x^t \) in \( f \) is a unit (if all the coefficients of \( f \) are non-units, then \( \text{con}(f) \subseteq M \)).

Let \( \beta_t \) be the coefficient of \( x^t \) in \( x^d G \). Then, \( \alpha_t - \gamma \beta_t \) is the coefficient of \( x^t \) in \( h \).

Since \( \alpha_t \notin M \) but \( \gamma \beta_t \in M \), we cannot have \( \alpha_t - \gamma \beta_t \in M \). Thus, \( \text{con}(h) = (1) \).

This contradicts the minimality of \( \deg(f) \). Hence, \( \gamma \) must be a unit, and \( \gamma^{-1} f \) is a monic, content 1 polynomial in \( \text{Muff}(R) \) with the same degree as \( f \). This completes the proof. \( \square \)

**Theorem 5.3.2.** Let \( R \) be a quotient ring of \( \mathbb{Z}H \) with \( \text{char}(R) = 2^m \), where \( m > 0 \). If \( f \) is a content 1 polynomial in \( \text{Muff}(R) \), then \( \deg(f) \geq \deg(\phi_R) \).

**Proof.** Since \( \text{con}(\phi_R) = (1) \), \( \text{Muff}(R) \) contains polynomials of content 1. Let \( f \) be such a polynomial of minimal degree. We need to show that \( \deg(f) \geq \deg(\phi_R) \).

Assume first that \( f \) has a coefficient \( \alpha \) of the form \( \alpha \equiv a + bi + cj + dk + e\mu \), where \( a, b, c, d \in \mathbb{Z} \) and \( e = 1 \). By Theorem 5.2.3, \( \overline{f} \in \text{Muff}(R) \), so \( f + \overline{f} \in \text{Muff}(R) \).
has a coefficient equivalent to $\alpha + \overline{\alpha} \equiv 2a + e$. Since $e = 1$, $\alpha + \overline{\alpha}$ is a unit in $R$. So, $\text{con}(f + \overline{f}) = (1)$. Since $f + \overline{f} \in \text{Muff}(R) \cap (\mathbb{Z}/2^m\mathbb{Z})[x]$, we may apply Lemma 4.3.5 to $f + \overline{f}$ to conclude that $\deg(f + \overline{f}) \geq \deg(\phi_R)$. Thus,

$$\deg(f) \geq \deg(f + \overline{f}) \geq \deg(\phi_R)$$

in this case. So, we may assume that $f$ has coefficients in $\mathbb{Z}Q/(2^m)$.

By Theorem 5.3.1, we may assume that $f$ is monic. Letting $f_1, f_i, f_j, \text{ and } f_k$ be the component polynomials of $f$ (see Definition 4.3.4), we have $\deg(f) = \deg(f_1)$, and this degree is strictly larger than $\deg(f_i), \deg(f_j), \text{ or } \deg(f_k)$.

Now, since $\overline{f} \in \text{Muff}(R), 2f_1 = f + \overline{f} \in \text{Muff}(R) \cap (\mathbb{Z}/2^m\mathbb{Z})[x]$. Similarly, since $-if, -jf, \text{ and } -kf$ are all in $\text{Muff}(R)$, we get $2f_i, 2f_j, 2f_k \in \text{Muff}(R) \cap (\mathbb{Z}/2^m\mathbb{Z})[x]$. Also,

$$f + \mu f \mu^{-1} + \mu^2 f \mu^{-2} = 3f_1 + (i+j+k)(f_i + f_j + f_k) \in \text{Muff}(R) .$$

Let $g = f_i + f_j + f_k$. Then,

$$f_1 + (i+j+k)g \equiv f + \mu f \mu^{-1} + \mu^2 f \mu^{-2} - 2f_1 \in \text{Muff}(R) .$$

By Corollary 5.1.12, either $R \cong \mathbb{Z}H/(2^m)$ or $R \cong \mathbb{Z}H/(2^{m-1} + 2^{m-1}i)$, so we have two cases to consider.

**Case 1: $R \cong \mathbb{Z}H/(2^m)$**

Let $\beta \in R$. Then, since $2f_1 \in \text{Muff}(R)$, we have $2f_1(\beta) \equiv 0$ in $R$. This means that $f_1(\beta) \in \text{Ann}_R(2) = 2^{m-1}R$. Similarly, $f_i(\beta), f_j(\beta), f_k(\beta) \in 2^{m-1}R$. So, $g(\beta) \in 2^{m-1}R$ and hence $g(\beta) \equiv 2^{m-1}\gamma$ for some $\gamma \in R$. Since $2^{m-1} + 2^{m-1}i + 2^{m-1}j + 2^{m-1}k \equiv 0$
in $R$,

$$(i + j + k)g(\beta) \equiv (i + j + k)2^{m-1}\gamma$$

$$\equiv (2^{m-1}i + 2^{m-1}j + 2^{m-1}k)\gamma$$

$$\equiv 2^{m-1}\gamma$$

$$\equiv g(\beta).$$

Now, $f_1 + (i + j + k)g \in \text{Muff}(R)$, so

$$0 \equiv (f_1 + (i + j + k)g)(\beta)$$

$$\equiv f_1(\beta) + (i + j + k)g(\beta)$$

$$\equiv f_1(\beta) + g(\beta)$$

$$\equiv (f_1 + g)(\beta).$$

Since $\beta$ was an arbitrary element of $R$, we conclude that $f_1 + g \in \text{Muff}(R)$. Furthermore, since $f_1 + g$ has coefficients in $\mathbb{Z}/2^m\mathbb{Z}$, we have $f_1 + g \in \text{Muff}(R) \cap (\mathbb{Z}/2^m\mathbb{Z})[x]$. So, by Lemma 4.3.5, $\text{deg}(f_1 + g) \geq \text{deg}(\phi_R)$. As mentioned above, the degrees of $f_i$, $f_j$, and $f_k$ are all strictly less than $\text{deg}(f_1)$, so $\text{deg}(f_1 + g) = \text{deg}(f_1)$. Therefore,

$$\text{deg}(f) = \text{deg}(f_1) = \text{deg}(f_1 + g) \geq \text{deg}(\phi_R).$$

This proves Case 1.

**Case 2: $R \cong \mathbb{Z}[H/(2^{m-1} + 2^{m-1}i)]$**

As in Case 1, let $\beta \in R$. In this case, the condition $2f_1(\beta) \equiv 0$ in $R$ forces $f_1(\beta) \in (2^{m-2} + 2^{m-2}i)R$. Similarly, $f_i(\beta), f_j(\beta), f_k(\beta) \in (2^{m-2} + 2^{m-2}i)R$, so $g(\beta) \in \mathbb{Z}/2^m\mathbb{Z}$. Therefore, $g(\beta) \equiv 0$ in $R$. This proves Case 2.
\[(2^{m-1} + 2^{m-1}i)R \text{ and there exists } \gamma \in R \text{ such that } g(\beta) \equiv (2^{m-2} + 2^{m-2}i)\gamma. \text{ Then,} \]
\[(i + j + k)g(\beta) \equiv (i + j + k)(2^{m-2} + 2^{m-2}i)\gamma \]
\[\equiv (2^{m-2}i + 2^{m-2}j + 2^{m-2}k - 2^{m-2} + 2^{m-2}j - 2^{m-2}k)\gamma \]
\[\equiv (-2^{m-2} + 2^{m-2}i + 2^{m-1}j)\gamma \]
\[\equiv (2^{m-2} + 2^{m-2}i + (2^{m-1} + 2^{m-1}j))\gamma \]
\[\equiv g(\beta). \]

At this point, proceeding as in Case 1 shows that \(\deg(f) \geq \deg(\phi_R)\), which proves Case 2.

There are no more cases, so we are done. \qed

**Theorem 5.3.3.** Let \(R\) be a finite, non-zero quotient ring of \(\mathbb{Z}H\). Let \(f \in \text{Muff}(R)\), and assume that \(\text{con}(f) = (1)\). Then, \(\deg(f) \geq \deg(\phi_R)\).

**Proof.** Let \(n = \text{char}(R)\), and assume that \(n\) has prime factorization \(n = p_1^{e_1} \cdots p_t^{e_t}\). By using Theorem 4.3.6 and Theorem 5.3.2, we see that, for all \(1 \leq \ell \leq t\),

\[\deg(f) \geq \deg(f \text{ mod } p_\ell^{e_\ell}R) \geq \deg(\phi_R/p_\ell^{e_\ell}R).\]

Thus, by Theorem 4.3.2,

\[\deg(f) \geq \max_{1 \leq \ell \leq t}\{\deg(\phi_R/p_\ell^{e_\ell}R)\} = \deg(\phi_R). \]

\qed

Theorem 5.3.3 establishes point 1' in Section 5.1. Proving the second point, 2'), is not nearly as arduous.
Theorem 5.3.4. Let \( R \) be a finite, non-zero quotient ring of \( \mathbb{Z}H \), and let \( n = \text{char}(R) \). Assume that \( n \) is even. If \( f \in \text{Muff}(R) \) and \( \text{con}(f) \subseteq (1 + i)R \), then \( f \) is contained in the ideal of \( R[x] \) generated by \( (1 + i)\widetilde{\text{Muff}}(R/\text{Ann}_R(1 + i)) \).

Proof. Assume that \( f \in \text{Muff}(R) \) and \( \text{con}(f) \subseteq (1 + i)R \). Write \( f(x) = \sum_r \alpha_r x^r \).

Then, each \( \alpha_r \in (1 + i)R \), so for each \( r \) there exists \( \beta_r \in R \) such that \( \alpha_r \equiv (1 + i)\beta_r \).

Let \( g(x) = \sum_r \beta_r x^r \). Then, \( f(x) = \sum_r \alpha_r x^r = (1 + i)g(x) \).

We would like to show that \( g(\alpha) \in \text{Ann}_R(1 + i) \) for each \( \alpha \in R \). If that is the case, then we can show that \( f \in (1 + i)\widetilde{\text{Muff}}(R/\text{Ann}_R(1 + i)) \). So, fix \( \alpha \in R \). Then, \( f(\alpha) \equiv 0 \), so \( (1 + i)g(\alpha) \equiv 0 \). Let \( \beta \in (1 + i)R \). It suffices to show that \( \beta g(\alpha) \equiv 0 \) and \( g(\alpha)\beta \equiv 0 \). By Lemma 5.1.8, there exist \( \gamma, \delta \in R \) such that \( \beta \equiv \gamma(1 + i) \) and \( \beta \equiv (1 + i)\delta \). Using \( \beta \equiv \gamma(1 + i) \) gives \( \beta g(\alpha) \equiv \gamma(1 + i)g(\alpha) \equiv 0 \). So, we just need to prove that \( g(\alpha)\beta \equiv 0 \).

Factor \( n \) as \( n = 2^m q \), where \( m > 0 \) and \( q \) is odd. Let \( I_1 = 2^m R \), \( I_2 = qR \), \( R_1 = R/I_1 \) and \( R_2 = R/I_2 \). In \( R_1 \), \( (1 + i)g(\alpha) \equiv 0 \) and \( \text{char}(R_1) = 2^m \), so by Theorem 5.2.2 we have \( g(\alpha)(1 + i) \equiv 0 \) mod \( I_1 \). So, \( g(\alpha)(1 + i) \in I_1 \) in \( R \). Note that we are done if \( q = 1 \), so assume that \( q > 1 \). Then, \( R_2 \) is a non-zero ring.

In \( R_2 \), we have \( (1 + i)g(\alpha) \equiv 0 \). Since \( \text{char}(R_2) = q \) is odd, \( 1 + i \) is a unit in \( R_2 \). So, \( g(\alpha) \equiv 0 \) in \( R_2 \), which means that \( g(\alpha) \in I_2 \) in \( R \). Thus, \( g(\alpha)(1 + i) \in I_2 \) in \( R \), and therefore \( g(\alpha)(1 + i) \in I_1 \cap I_2 = (0) \). Now, using \( \beta \equiv (1 + i)\delta \), we have \( g(\alpha)\beta \equiv g(\alpha)(1 + i)\delta \equiv 0 \). Hence, \( g(\alpha) \in \text{Ann}_R(1 + i) \).

We have shown that \( g(\alpha) \in \text{Ann}_R(1 + i) \) for each \( \alpha \in R \), so \( g(x) \mod \text{Ann}_R(1 + i) \) lies in \( \text{Muff}(R/\text{Ann}_R(1 + i)) \) and \( f(x) = (1 + i)g(x) \in (1 + i)\widetilde{\text{Muff}}(R/\text{Ann}_R(1 + i)) \), as required. \( \square \)
We can now describe the generators of $\text{Muff}(R)$ for any finite, non-zero quotient ring of $\mathbb{Z}H$.

**Theorem 5.3.5.** Let $R$ be a finite, non-zero quotient ring of $\mathbb{Z}H$, and let $n = \text{char}(R)$. Let $p_1, \ldots, p_t$ be all the odd primes dividing $n$.

(i) If $n$ is odd, then $\text{Muff}(R) = (\phi_R, p_1 \widehat{\text{Muff}}(R/\text{Ann}(p_1)), \ldots, p_t \widehat{\text{Muff}}(R/\text{Ann}(p_t)))$.

(ii) If $n$ is even, then

$$\text{Muff}(R) = (\phi_R, (1 + i) \widehat{\text{Muff}}(R/\text{Ann}(1 + i)),\linebreak p_1 \widehat{\text{Muff}}(R/\text{Ann}(p_1)), \ldots, p_t \widehat{\text{Muff}}(R/\text{Ann}(p_t))).$$

Proof. (i) If $n$ is odd, then $\mathbb{Z}H/(n) \cong \mathbb{Z}Q/(n)$, so this is just a restatement of Theorem 4.3.7.

(ii) If $n$ is even, then we can proceed just as in the proof of Theorem 4.3.7, noting that the maximal ideals of $R$ are exactly $p_1 R, \ldots, p_t R,$ and $(1 + i) R$. \hfill \Box

**Corollary 5.3.6.**

(i) For each $n > 1$, $\text{Muff}(\mathbb{Z}H/(n))$ can be generated by polynomials of the form $\gamma f$, where $\gamma \in \mathbb{Z}H/(n)$ and $f \in (\mathbb{Z}/n\mathbb{Z})[x]$. In fact, we may assume that $\gamma \in \{1, 1 + i\}$.

(ii) $\text{Int}(\mathbb{Z}H)$ can be generated over $\mathbb{Z}H$ by polynomials of the form $\frac{\gamma f}{n}$, where $\gamma \in \mathbb{Z}H$, $f \in \mathbb{Z}[x]$, and $n \geq 1$. In fact, we may assume that $\gamma \in \{1, 1 + i\}$.

Proof. (i) If $R$ is a simple quotient ring of $\mathbb{Z}H$, then either $R \cong \mathbb{Z}H/(1 + i) \cong \mathbb{F}_4$, or $R \cong \mathbb{Z}H/(p) \cong \mathbb{Z}Q/(p)$ for some odd prime $p$. In the former case, $\text{Muff}(R) = (\phi_R)$
because $R[x]$ is a PID, and in the latter case $\text{Muff}(R) = (\phi_R)$ by Theorem 4.3.3. So, the result holds for simple quotient rings of $\mathbb{Z}H$.

Now, let $R = \mathbb{Z}H/\langle n \rangle$ and let $n$ have prime factorization $n = p_1^{e_1} \cdots p_t^{e_t}$. If $t = 1$, then for convenience let $p = p_1$ and $e = e_1$. We use induction on $e$. If $p$ is odd and $e = 1$, then we are done by the previous paragraph. If $p = 2$ and $e = 1$, then Theorem 5.3.5 shows that $\text{Muff}(R) = (\phi_R, (1 + i)\phi_{\mathbb{Z}H/\langle 1+i \rangle})$, so we are done in this case as well. The result for the case $t = 1$ now follows by Theorem 5.3.5 and induction on $e$.

If $t > 1$, then this can be proven using Theorem 5.3.5 and induction on $t$.

To prove that we may assume each $\gamma \in \{1, 1 + i\}$, let $\delta f$ be a generator for $\text{Muff}(R)$, where $f \in (\mathbb{Z}/n\mathbb{Z})[x]$. By Theorem 5.3.5, we may assume that $\delta$ is a product of integers and powers of $1 + i$. Since $(1 + i)^2 = 2i$, $(1 + i)^3 = -2(1 - i)$, and $(1 + i)^4 = -4$, we have $\delta = a(1 + i)^m$, where $a \in \mathbb{Z}/n\mathbb{Z}$ and $0 \leq m \leq 3$. There is nothing to prove if $m = 0$ or $m = 1$. If $m = 2$, then there is no loss in using $i\delta f$ to generate $\text{Muff}(R)$. If $m = 3$, then we may use $-j\delta f j = (1 - \delta j)f$ in place of $f$. So, in each case we may write $\delta f$ as $\gamma g$, where $\gamma \in \{1, 1 + i\}$ and $g \in (\mathbb{Z}/n\mathbb{Z})[x]$, as required.

(ii) We know that $\mathbb{Z}H[x] \subseteq \text{Int}(\mathbb{Z}H)$, so to prove (ii) it suffices to focus on polynomials in $\text{Int}(\mathbb{Z}H)$ that may be written as $f(x)/n$ with $n > 1$. For each $n > 1$, let $\gamma_{n_1}, \gamma_{n_2}, \ldots, \gamma_{n_m} \in \mathbb{Z}H/\langle n \rangle$ and $f_{n_1}, f_{n_2}, \ldots, f_{n_m} \in (\mathbb{Z}/n\mathbb{Z})[x]$ be such that $\text{Muff}(\mathbb{Z}H/\langle n \rangle) = (\gamma_{n_1}f_{n_1}, \ldots, \gamma_{n_m}f_{n_m})$. Furthermore, for each $n > 1$, let $\mathcal{P}_n = \{\frac{\gamma_{n_1}f_{n_1}}{n}, \ldots, \frac{\gamma_{n_m}f_{n_m}}{n}\} \subseteq \text{Int}(\mathbb{Z}H)$. Take $\mathcal{P}_1 = \{x\}$ and let $\mathcal{P} = \bigcup_{n=1}^{\infty} \mathcal{P}_n$. We wish to show that $\text{Int}(\mathbb{Z}H) = \mathbb{Z}H[\mathcal{P}]$. The inclusion $\text{Int}(\mathbb{Z}H) \supseteq \mathbb{Z}H[\mathcal{P}]$ is easily verified, so we just need to show that $\text{Int}(\mathbb{Z}H) \subseteq \mathbb{Z}H[\mathcal{P}]$. 86
Let \( f \in \text{Int}(\mathbb{Z}H) \), and write \( f = \frac{g}{n} \) for some \( g \in \mathbb{Z}H[x] \) and some \( n \geq 1 \). If \( n = 1 \), then \( f \in \mathbb{Z}H[x] \), and we are done. If \( n > 1 \), then \( g \mod n \in \text{Muff}(\mathbb{Z}H/(n)) \), so we can express \( g \mod n \) as the finite sum

\[
g \mod n = \sum_{r=1}^{t} F_r h_r G_r,
\]

where for each \( 1 \leq r \leq t \), \( h_r \in \{ \gamma_{n_1} f_{n_1}, \ldots, \gamma_{n_m} f_{n_m} \} \) and \( F_r, G_r \in (\mathbb{Z}H/(n))[x] \). This means that over \( \mathbb{Z}H \),

\[
g = nG_0 + \sum_{r=1}^{t} F_r h_r G_r
\]

for some \( G_0 \in \mathbb{Z}H[x] \). So,

\[
f = \frac{g}{n} = \frac{1}{n} \left( nG_0 + \sum_{r=1}^{t} F_r h_r G_r \right) = G_0 + \sum_{r=1}^{t} \frac{F_r h_r G_r}{n},
\]

which is an element of \( \mathbb{Z}H[P] \). Thus, \( \text{Int}(\mathbb{Z}H) \) can be generated over \( \mathbb{Z}H \) by the set \( P \), and each polynomial in \( P \) has the desired form. The last assertion, that we can take each \( \gamma \in \{ 1, 1+i \} \), can be proven just as in part (i). \( \square \)
6.1 Prime Ideals in Noncommutative Rings

In this chapter, we will begin to describe the prime ideals of 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 will use the following standard definition for a prime ideal in a noncommutative ring.

**Definition 6.1.1.** 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 the following proposition. The proof is given in §10 of [6].

**Proposition 6.1.2.** For a proper ideal $P$ in a ring $R$, the following are equivalent:

(i) $P$ is prime

(ii) whenever $I$ and $J$ are ideals of $R$ such that $IJ \subseteq P$, then either $I \subseteq P$ or $J \subseteq P
(iii) whenever \(a, b \in R\) with \((a)(b) \subseteq P\), then either \(a \in P\) or \(b \in P\)

(iv) whenever \(I\) and \(J\) are left ideals of \(R\) such that \(IJ \subseteq P\), then either \(I \subseteq P\) or \(J \subseteq P\)

(v) whenever \(I\) and \(J\) are right ideals of \(R\) such that \(IJ \subseteq P\), then either \(I \subseteq P\) or \(J \subseteq P\)

Note that when \(R\) is commutative, the new definition for a prime ideal reduces to the customary one.

6.2 Prime Ideals in Rings of Integer-Valued Polynomials

We first consider some of the prime ideals in \(\text{Int}(D)\), where \(D\) is a (commutative) integral domain. Given a (commutative) integral domain \(D\), a prime ideal \(P\) of \(D\), and \(a \in D\), we define

\[ \mathfrak{P}_{P,a} := \{ f \in \text{Int}(D) \mid f(a) \in P \} . \]

Then, it is not difficult to show that \(\mathfrak{P}_{P,a}\) is a prime ideal of \(\text{Int}(D)\) (although not every prime ideal of \(\text{Int}(D)\) needs to have this form; see [2], Chapter V). We will use this type of ideal as a model to construct prime ideals in \(\text{Int}(\mathbb{Z}Q)\). To do this, we first need to extend the definition of \(\mathfrak{P}_{P,a}\) to noncommutative rings.

Recall that in Corollary 2.2.4, we determined the unit groups of \(\mathbb{Z}Q\) and \(\mathbb{Z}H\) to be

\[ (\mathbb{Z}Q)^\times = \{ \pm 1, \pm i, \pm j, \pm k \} \]
and

$$(\mathbb{Z}H)^\times = \{ \pm 1, \pm i, \pm j, \pm k, \pm \mu, \pm i\mu, \pm j\mu, \pm k\mu, \pm \mu^2, \pm i\mu^2, \pm j\mu^2, \pm k\mu^2 \}.$$ 

We use these facts in the following definition.

**Definition 6.2.1.** Given an overring $R$ of $\mathbb{Z}Q$ in $\mathbb{Q}Q$ and an element $\alpha \in R$, we denote the (full) multiplicative conjugacy class of $\alpha$ in $R$ by $\text{Conj}_R(\alpha)$ (or simply $\text{Conj}(\alpha)$ if the ring $R$ is clear from context). That is, $\text{Conj}_R(\alpha) = \{ u\alpha u^{-1} \mid u \in R \text{ is a unit} \}$.

Let $S = R \cap \mathbb{Q}$. If $R = SQ$, then we define the **restricted multiplicative conjugacy class** $\text{Konj}_R(\alpha)$ to be $\text{Konj}_R(\alpha) = \{ u\alpha u^{-1} \mid u \in (\mathbb{Z}Q)^\times \}$. If $R \neq SQ$, then $R = SH$ and we define $\text{Konj}_R(\alpha) = \{ u\alpha u^{-1} \mid u \in (\mathbb{Z}H)^\times \}$. As with the full multiplicative conjugacy class, we write $\text{Konj}(\alpha)$ if $R$ is clear from context.

While $\text{Conj}_R(\alpha)$ and $\text{Konj}_R(\alpha)$ are the same when $R = \mathbb{Z}Q$ or $\mathbb{Z}H$ and $\alpha \in R$, the importance of the restricted multiplicative conjugacy class arises when dealing with arbitrary overrings of $\mathbb{Z}Q$. For an arbitrary overring of $R$ of $\mathbb{Z}Q$ and $\alpha \in R$, the full multiplicative conjugacy class $\text{Conj}_R(\alpha)$ might be infinite, whereas $\text{Konj}_R(\alpha)$ is always finite. This difference will be important if we are to extend some of our results, such as Theorem 6.2.3 below, to overrings of $\mathbb{Z}Q$.

The following fact regarding multiplicative conjugacy in quaternion rings will be used several times and is worth pointing out: if $\beta \in \text{Conj}_R(\alpha)$, 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 6.2.2. Given an overring $R$ of $\mathbb{Z}Q$ in $\mathbb{Q}Q$, an ideal $I$ of $R$, and an element $\alpha \in R$, we define $\mathfrak{P}_{I,\alpha} := \{ f \in \text{Int}(R) \mid f(\beta) \in I \text{ for all } \beta \in \text{Konj}_R(\alpha) \}$.

If the ring $R$ is a (commutative) 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 $R$ is an overring of $\mathbb{Z}Q$ in $\mathbb{Q}Q$, $\alpha \in R$, and $P$ is a prime ideal of $R$, then when is the set $\mathfrak{P}_{P,\alpha}$ a prime ideal of $\text{Int}(R)$? Currently, we have answers to this question only for the case when $R = \mathbb{Z}Q$, although the techniques we use should also work for $\mathbb{Z}H$ and other overrings of $\mathbb{Z}Q$.

In Chapter 3 of [4], we are told that the prime ideals of $\mathbb{Z}Q$ are $(0), (1+i, 1+j)$, and $(p)$, where $p$ is an odd prime of $\mathbb{Z}$. Our first 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 6.2.3. Let $n \in \mathbb{Z}$ and let $I = (n)$ in $\mathbb{Z}Q$. Let $\alpha \in \mathbb{Z}Q$. Then, $\mathfrak{P}_{I,\alpha}$ is an ideal of $\text{Int}(\mathbb{Z}Q)$, and when $n \neq 0$, $\text{Int}(\mathbb{Z}Q)/\mathfrak{P}_{I,\alpha}$ is a finite ring.

Proof. This is similar to the proofs of Theorem 3.1.1 and Proposition 4.1.4. 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 $\mathfrak{P}_{I,\alpha}$ is closed under addition.
Now, fix \( f(x) = \sum_r \alpha_r x^r \in \Psi_{I,\alpha} \), and let \( g(x) \in \text{Int}(\mathbb{Z}Q) \). Let \( \beta \in \text{Konj}(\alpha) \). Then, there exist \( s, t, u, v \in \mathbb{Z} \) such that \( g(\beta) = s + ti + uj + vk \). We have

\[
(fg)(\beta) = \sum_r \alpha_r g(\beta) \beta^r \\
= \sum_r \alpha_r (s + ti + uj + vk) \beta^r \\
= sf(\beta) + t(fi)(\beta) + u(fj)(\beta) + v(fk)(\beta) \\
= sf(\beta) + tf(-i\beta i) + uf(-j\beta j) + vf(-k\beta k)k.
\]

Since \( \beta \in \text{Konj}(\alpha) \), so are \(-i\beta i, -j\beta j, \) and \(-k\beta k\). Since \( f \in \Psi_{I,\alpha} \), each of \( f(\beta), f(-i\beta i), f(-j\beta j), \) and \( f(-k\beta k) \) is in \( I \). So, \( (fg)(\beta) \in I \) and hence \( fg \in \Psi_{I,\alpha} \).

To prove the first assertion in our theorem, it remains to show that \( gf \in \Psi_{I,\alpha} \). Writing \( f(\beta) = a + bi + cj + dk \) for some integers \( a, b, c, \) and \( d \) and using the same steps as above, we get

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

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

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

\[
F^* : \text{Konj}(\alpha) \to \mathbb{Z}Q/(n) \\
\beta \mapsto F(\beta) \mod n.
\]
Then, for all $F, G \in \text{Int}(\mathbb{Z}Q)$,

$$F^* = G^* \iff F^*(\beta) = G^*(\beta) \text{ for all } \beta \in \text{Konj}(\alpha)$$

$$\iff F(\beta) \equiv G(\beta) \mod n \text{ for all } \beta \in \text{Konj}(\alpha)$$

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

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

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

These equivalences show that for any $F \in \text{Int}(\mathbb{Z}Q)$, the residue of $F$ modulo $\mathfrak{P}_{I,\alpha}$ 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 $\text{Konj}(\alpha)$ to $\mathbb{Z}Q/(n)$. Since both $\text{Konj}(\alpha)$ and $\mathbb{Z}Q/(n)$ are finite sets, there are only finitely many maps between them. Therefore, we conclude that $\mathcal{R} = \text{Int}(\mathbb{Z}Q)/\mathfrak{P}_{I,\alpha}$ is a finite ring. □

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. In Section 6.4, we will prove the theorem for $(1+i, 1+j)$ by using some different techniques. It is also likely that the proof of Theorem 6.2.3 will extend to arbitrary overrings of $\mathbb{Z}Q$, but for now we will remain focused on $\mathbb{Z}Q$.

Theorem 6.2.3 indicates that $\mathfrak{P}_{I,\alpha}$ is an ideal of $\text{Int} (\mathbb{Z}Q)$ whenever $I$ is generated by an integer. A necessary condition for $\mathfrak{P}_{I,\alpha}$ to be prime is that $I$ is prime ideal of $\mathbb{Z}Q$.

**Proposition 6.2.4.** Let $n > 1$ and let $I = (n)$ in $\mathbb{Z}Q$. Assume that $I$ is not a prime ideal of $\mathbb{Z}Q$. Then, for any $\alpha \in \mathbb{Z}Q$, $\mathfrak{P}_{I,\alpha}$ is not a prime ideal of $\text{Int}(\mathbb{Z}Q)$. 

93
Proof. Since $I$ is not a prime ideal of $\mathbb{Z}[Q]$, $n$ is either composite or $n = 2$. Assume first that $n$ is composite with factorization $n = \ell m$. Then, for any $\alpha$, the set $\ell \text{Int}(\mathbb{Z}[Q]) m \subseteq \mathfrak{P}_{I,\alpha}$, but neither $\ell$ nor $m$ is in $\mathfrak{P}_{I,\alpha}$. So, $\mathfrak{P}_{I,\alpha}$ is not prime.

Next, assume that $I = (2)$. We will show that $(1 + i)\text{Int}(\mathbb{Z}[Q])(1 - i)$ is contained in $\mathfrak{P}_{I,\alpha}$, and since neither $1 + i$ nor $1 - i$ is in $(2)$, this will be enough to conclude that $\mathfrak{P}_{I,\alpha}$ is not prime. Let $\varepsilon = 1 + i$. Then, the inverse of $\varepsilon$ in $\mathbb{Q}[Q]$ is $\varepsilon^{-1} = \frac{1 - i}{2}$. Now, if $\beta = a + bi + cj + dk \in \mathbb{Z}[Q]$, then direct computation shows that

$$\varepsilon \beta \varepsilon^{-1} = a + bi - dj + ck,$$

and

$$\varepsilon^{-1} \beta \varepsilon = a + bi + dj - ck,$$

so both $\varepsilon \beta \varepsilon^{-1}$ and $\varepsilon^{-1} \beta \varepsilon$ are elements of $\mathbb{Z}[Q]$ (in fact, since multiplicative conjugation by $\varepsilon$ also respects the ring operations in $\mathbb{Z}[Q]$, we have exhibited an automorphism of $\mathbb{Z}[Q]$).

We claim that whenever $f \in \text{Int}(\mathbb{Z}[Q])$, the polynomial $\varepsilon f \varepsilon^{-1}$ is also in $\text{Int}(\mathbb{Z}[Q])$. To see this, notice that whenever $\beta \in \mathbb{Z}[Q]$, we have

$$(\varepsilon f \varepsilon^{-1})(\beta) = \varepsilon (f(\varepsilon^{-1} \beta \varepsilon)) \varepsilon^{-1}.$$  

Since $f \in \text{Int}(\mathbb{Z}[Q])$ and $\varepsilon^{-1} \beta \varepsilon \in \mathbb{Z}[Q]$, we have $f(\varepsilon^{-1} \beta \varepsilon) \in \mathbb{Z}[Q]$. Thus, $\varepsilon (f(\varepsilon^{-1} \beta \varepsilon)) \varepsilon^{-1} \in \mathbb{Z}[Q]$ and $\varepsilon f \varepsilon^{-1} \in \text{Int}(\mathbb{Z}[Q])$. Let $g(x) = (1 + i)f(x)(1 - i) \in (1 + i)\text{Int}(\mathbb{Z}[Q])(1 - i)$. Then, for any $\beta \in \mathbb{Z}[Q]$,

$$g(\beta) = 2(\varepsilon f \varepsilon^{-1})(\beta) \in (2).$$

Thus, $(1 + i)\text{Int}(\mathbb{Z}[Q])(1 - i) \subseteq \mathfrak{P}_{I,\alpha}$ regardless of the choice of $\alpha$. However, neither $1 + i$ nor $1 - i$ can be in $\mathfrak{P}_{I,\alpha}$, so $\mathfrak{P}_{I,\alpha}$ is never a prime ideal. This completes the proof. □

The question remains whether $\mathfrak{P}_{I,\alpha}$ is prime if $I$ 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 $P = (p)$ and
$p$ is an odd prime. The case $P = (0)$ is true without restrictions on $\alpha$, as we show in the next proposition.

**Proposition 6.2.5.** Let $P = (0)$ in $\mathbb{Z}[\mathbb{Q}]$. Then, for any $\alpha \in \mathbb{Z}[\mathbb{Q}]$, $\mathfrak{P}_{P,\alpha}$ is a prime ideal of $\text{Int}(\mathbb{Z}[\mathbb{Q}])$.

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

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

$$0 = (fug(\beta)g)(\beta)$$

$$= \sum_r \alpha_r (ug(\beta)g)(\beta)\beta^r$$

$$= \sum_r \alpha_r ug(\beta)g(\beta)\beta^r$$

$$= \sum_r \alpha_r uN(g(\beta))\beta^r$$

$$= N(g(\beta)) \sum_r \alpha_r u\beta^r$$

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

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

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

95
When $P \neq (0)$, not every $\mathfrak{P}_{P,\alpha}$ ideal is prime; it depends on $P$ and $\alpha$. Furthermore, showing that $\mathfrak{P}_{P,\alpha}$ is prime is more difficult. However, there is one instance that is easy to deal with.

**Proposition 6.2.6.** Let $P$ be any prime ideal of $\mathbb{Z}Q$, and let $\alpha \in \mathbb{Z}$. Then, $\mathfrak{P}_{P,\alpha}$ is a prime ideal of $\text{Int}(\mathbb{Z}Q)$.

**Proof.** The key to the proof is the fact that since $\alpha$ is central in $\mathbb{Q}Q$, we have $(fg)(\alpha) = f(\alpha)g(\alpha)$ for any $f, g \in \mathbb{Q}Q[x]$. We will use this fact freely.

Since $P$ is an arbitrary prime ideal of $\mathbb{Z}Q$, we first need to check that $\mathfrak{P}_{P,\alpha}$ is an ideal. If $f, g \in \mathfrak{P}_{P,\alpha}$ and $h \in \text{Int}(\mathbb{Z}Q)$, then $(f + g)(\alpha) = f(\alpha) + g(\alpha) \in P$, $(fh)(\alpha) = f(\alpha)h(\alpha) \in P$, and $(hf)(\alpha) = h(\alpha)f(\alpha) \in P$, so $\mathfrak{P}_{P,\alpha}$ is an ideal.

Next, assume that $f\text{Int}(\mathbb{Z}Q)g \subseteq \mathfrak{P}_{P,\alpha}$. Since $\alpha \in \mathbb{Z}$, we have $\text{Konj}(\alpha) = \{\alpha\}$, so to verify the primality of $\mathfrak{P}_{P,\alpha}$ it suffices to have either $f(\alpha) \in P$ or $g(\alpha) \in P$. Now, $\gamma \in \text{Int}(\mathbb{Z}Q)$ for any $\gamma \in \mathbb{Z}Q$, so

$$(f\gamma g)(\alpha) = f(\alpha)\gamma g(\alpha) \in P$$

and thus $f(\alpha)\mathbb{Z}Qg(\alpha) \subseteq P$. Since $P$ is prime, either $f(\alpha) \in P$ or $g(\alpha) \in P$, and we are done. 

\[\square\]

### 6.3 Maximal Ideals in $\text{Int}(\mathbb{Z}Q)$

As mentioned in the previous section, when $P = (p)$ for an odd prime $p$, the ideal $\mathfrak{P}_{P,\alpha}$ is not always prime. The goal of this section is to determine necessary and sufficient conditions under which $\mathfrak{P}_{P,\alpha}$ is a prime ideal of $\text{Int}(\mathbb{Z}Q)$.

Before proceeding, we require 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 [3]. The first theorem gives the well-known condition under which an integer can be written as a sum of three integral squares.

**Theorem 6.3.1.** Let $M \in \mathbb{Z}$ be positive, and write $M = 4^m u$, where $m \geq 0$ and $4 \nmid u$. Then, there exist $y, z, w \in \mathbb{Z}$ such that $M = y^2 + z^2 + w^2$ if and only if $u \not\equiv 7 \mod 8$.

The second result is a weakened form of Theorem 8.7 in Chapter 5 of [3].

**Theorem 6.3.2.** Let $u$ be a positive integer. If $u \equiv 1, 2, 3, 5, \text{ or } 6 \mod 8$, then there exist $y, z, w \in \mathbb{Z}$ such that $u = y^2 + z^2 + w^2$ and $\gcd(y, z, w) = 1$.

**Remark.** Calling Theorem 6.3.2 a weakening of Theorem 8.7 in Chapter 5 of [3] is a bit of an understatement. The theorem in [3] gives a precise count of the number of triples $(y, z, w) \in \mathbb{Z}^3$ such that $u = y^2 + z^2 + w^2$ and $\gcd(y, z, w) = 1$. However, these counts rely on the orders of class groups of quadratic forms, and a worthwhile discussion of that topic would take us too far afield.

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

**Theorem 6.3.3.** Let $p$ be an odd prime, let $P = (p)$ in $\mathbb{Z}Q$, and let $\alpha \in \mathbb{Z}Q$. Let $T = \{a + bi + cj + dk \in \mathbb{Z}Q \mid a, b, c, d \in \{0, 1, \ldots, p - 1\}\} \text{ and let } L = \{\alpha_1 x + \alpha_0 \in \mathbb{Z}Q[x] \mid \alpha_1, \alpha_0 \in T\}$. 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 $\pi(L) = \mathcal{R}$.

Let $m(x)$ be a monic polynomial in $\mathbb{Z}[x]$ of minimal positive degree such that $m(\alpha) \in P$. Then, $\deg(m(x)) \leq 2$, because if $\alpha \equiv a \mod p$ for some $a \in \mathbb{Z}$, then we
can take \( m(x) = x - a \), and if not, then we can take \( m(x) = \min_{\alpha}(x) \). Note that \( m(x) \in P_{P,\alpha} \), so \((m(x), p) \subseteq P_{P,\alpha} \). This means that whenever \( f \in \mathbb{Z}Q[x] \), there exist \( g \in (\mathbb{Z}Q/(p))[x] \) and \( h \in L \) such that \( f(x) \equiv m(x)g(x) + h(x) \mod p \). 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 \( n \in \mathbb{Z} \) such that \( f(x) = \frac{F(x)}{n} \). Write \( n = p^e q \), where \( e \geq 0 \) and \( \gcd(p, q) = 1 \). Then, \( q \) is invertible mod \( p \), so \( \pi\left(\frac{F(x)}{n}\right) = \pi(q)^{-1} \pi\left(\frac{F(x)}{p^e}\right) \). Thus, it suffices to show that \( \pi\left(\frac{F(x)}{p^e}\right) \) lies in \( \pi(L) \).

If \( e = 0 \), then \( f(x) \in \mathbb{Z}Q[x] \) and we are done. So, assume \( e > 0 \). By Corollary 4.3.10 part (i), there exist polynomials \( g_0, g_1, \ldots, g_e \in \mathbb{Z}Q[x] \) such that

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

and for each \( 1 \leq m \leq e \), we have \( \frac{\phi_{p^m}(x)}{p^m} \in \text{Int}(\mathbb{Z}Q) \). Thus, it suffices to show that for every \( m > 0 \), \( \frac{\phi_{p^m}(x)}{p^m} \) can be represented mod \( \mathfrak{P}_{P,\alpha} \) by a residue in \( L \). Assuming this to be the case, we can then represent the residue of \( f(x) = \frac{F(x)}{n} \) in \( \mathcal{R} \) by a polynomial \( G(x) \in \mathbb{Z}Q[x] \), i.e. there will exist \( G(x) \in \mathbb{Z}Q[x] \) such that \( \pi(f) = \pi(G) \), and we know that \( \pi(G) \in \pi(L) \) for such a \( G \).

So, let \( m > 0 \), and let \( \phi(x) = \frac{\phi_{p^m}(x)}{p^m} \in \text{Int}(\mathbb{Z}Q) \). Consider first the case where \( \alpha \in \mathbb{Z} \). Since \( \phi \) has rational coefficients, \( \phi(\alpha) \) must lie in \( \mathbb{Z} \). So, \( \alpha \) and \( \phi(\alpha) \) are both integers, and hence there exists \( A \in \{0, 1, \ldots, p - 1\} \) such that \( \phi(\alpha) - (\alpha - A) \in P \). Because \( \alpha \in \mathbb{Z} \), this is enough to conclude that \( \phi(x) - (x - A) \in \mathfrak{P}_{P,\alpha} \). So, \( \pi(\phi) = \pi(x - A) \in \pi(L) \).
From now on, assume that $\alpha \notin \mathbb{Z}$. Since $\phi_{p^m} \in \mathbb{Z}[x]$, Theorem 2.3.1 tells us that there exist $C, D \in \mathbb{Z}$ such that $\phi_{p^m}(\alpha) = C\alpha + D$. Write $\alpha = a + bi + cj + dk$. Then,

$$\phi(\alpha) = \frac{\phi_{p^m}(\alpha)}{p^m} = \frac{C\alpha + D}{p^m} = \frac{(Ca + D)}{p^m} + \frac{Cbi + Ccj + Cdk}{p^m} = \frac{Ca + D}{p^m} + \frac{Cb}{p^m}i + \frac{Cc}{p^m}j + \frac{Cd}{p^m}k. $$

**Claim:** $p^m \mid C$ and $p^m \mid D$

**Proof of Claim:** Assume first that $\alpha \equiv a \mod p$. Then, either $p \nmid b, p \nmid c$, or $p \nmid d$. WLOG, assume that $p \nmid b$. Since $\phi \in \text{Int}(\mathbb{Z}Q)$, we must have $\phi(\alpha) \in \mathbb{Z}Q$, so $\frac{Cb}{p^m} \in \mathbb{Z}$ and $p^m \mid Cb$. The condition $p \nmid b$ now forces $p^m \mid C$, as desired. Since $\frac{Ca+D}{p^m}$ is also an integer, we get $p^m \mid D$.

Next, assume that $\alpha \equiv a \mod p$. Let $M = b^2 + c^2 + d^2$. Since $\alpha \notin \mathbb{Z}, M > 0$. So, we may write $M = 4^\ell u$, where $\ell \geq 0, u > 0$, and $4 \nmid u$. Since $M$ is a sum of three squares, Theorem 6.3.1 shows that $u \not\equiv 7 \mod 8$. Since $4 \nmid u$, we see that $u \equiv 1, 2, 3, 5$, or $6 \mod 8$. Thus, by Theorem 6.3.2 there exist $y, z, w \in \mathbb{Z}$ such that $u = y^2 + z^2 + w^2$ and $\gcd(y, z, w) = 1$. So,

$$M = 4^\ell u = 2^{2\ell}(y^2 + z^2 + w^2) = (2^{\ell}y)^2 + (2^{\ell}z)^2 + (2^{\ell}w)^2. $$

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 $N(\alpha) = a^2 + M = N(\beta)$. By Theorem 2.3.1, this means that $\phi_{p^m}(\beta) = C\beta + D$. Hence,

$$\phi(\beta) = \frac{Ca + D}{p^m} + \frac{2^{\ell}Cy}{p^m}i + \frac{2^{\ell}Cz}{p^m}j + \frac{2^{\ell}Cw}{p^m}k$$

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 $2^{\ell}$ because $p$ is odd. Proceeding as in the case where $\alpha \not\equiv a \mod p$
now gives $p^m \mid C$ and $p^m \mid D$. This completes the proof of the Claim.

By the Claim, there exist $C', D' \in \mathbb{Z}$ such that $\phi(\alpha) = (C'a + D') + C'bi + C'cj + C'dk = C'\alpha + D'$. Let $\psi(x) = C'x + D' \in \mathbb{Z}[x]$. Then, because both $\phi$ and $\psi$ have rational coefficients, we have, for any unit $v \in \mathbb{Z}$,

$$\phi(v\alpha v^{-1}) = v\phi(\alpha)v^{-1} = v\psi(\alpha)v^{-1} = \psi(v\alpha v^{-1}).$$

Thus,

$$\phi(\gamma) = \psi(\gamma) \text{ for all } \gamma \in \text{Konj}(\alpha). \quad (*)$$

Recall that in the proof of Theorem 6.2.3, we introduced the following notation:

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

**Corollary 6.3.4.** Let $p$ be an odd prime, let $P = (p)$ in $\mathbb{Z}$, and let $\alpha \in \mathbb{Z}$. Then,

$$\left| \text{Int}(\mathbb{Z})/\mathfrak{P}_{P,\alpha} \right| \leq p^8.$$

**Proof.** Let $L$ be as in the statement of Theorem 6.3.3. Then, $\left| \text{Int}(\mathbb{Z})/\mathfrak{P}_{P,\alpha} \right| \leq |L| = p^8. \hfill \Box$

Now that we know that any residue in $\text{Int}(\mathbb{Z})/\mathfrak{P}_{P,\alpha}$ can be represented by a linear polynomial, we can begin to analyze the structure of these quotient rings.
Theorem 6.3.5. Let $p$ be an odd prime, let $P = (p)$ in $\mathbb{Z}Q$, and let $\alpha \in \mathbb{Z}Q$. Let $\mathcal{R} = \text{Int}(\mathbb{Z}Q)/\mathfrak{P}_{P,\alpha}$ and 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$(m)$ 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 6.3.3, 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 1.4.2 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 $\text{min}_\alpha(x)$ is a monic quadratic polynomial in $\mathfrak{P}_{P,\alpha}$. Thus, we can assume that $m(x)$ has degree 2. Let $I$ be the ideal of $\mathbb{Z}[x]$ generated by $p$ and $m(x)$. In $\text{Int}(\mathbb{Z}Q)$, both $m(x)$ and $p$ are contained in $\mathfrak{P}_{P,\alpha}$, so the ring $\mathcal{R}$ contains a subring $\mathcal{F}$ isomorphic to $\mathbb{Z}[x]/I \cong \mathbb{F}_{p^2}$. Furthermore, $\mathcal{F}$ can be represented by polynomials with integer coefficients, and hence $\mathcal{F}$ is a central subring of $\mathcal{R}$. 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 Corollary 6.3.4, $|\mathcal{R}| \leq p^8$. 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 1.4.2 shows that $\mathcal{R} \cong M_2(\mathbb{F}_{p^2})$, a simple ring.

The known results about maximal ideals of $\text{Int}(\mathbb{Z}Q)$ are summarized in the following corollary.

**Corollary 6.3.6.** Let $p$ be an odd prime, let $P = (p)$ in $\mathbb{Z}Q$, and let $\alpha \in \mathbb{Z}Q$. Let $\mathcal{R} = \text{Int}(\mathbb{Z}Q)/\mathfrak{P}_{P,\alpha}$ and 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 $\text{Int}(\mathbb{Z}Q)$ 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 $\text{Int}(\mathbb{Z}Q)$ and $\mathcal{R} \cong \mathbb{Z}Q/(p) \cong M_2(\mathbb{F}_p)$.

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

(iv) if $m(x)$ is quadratic and reducible mod $p$, then $\mathfrak{P}_{P,\alpha}$ is not a prime ideal of $\text{Int}(\mathbb{Z}Q)$. 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 $\text{Int}(\mathbb{Z}Q)$, and $\text{Int}(\mathbb{Z}Q)/\mathfrak{M} \cong \mathbb{Z}Q/(p) \cong M_2(\mathbb{F}_p)$.

**Proof.** Parts (i), (ii), and (iii) were all shown in Theorem 6.3.5.

(iv) Since $m(x)$ is reducible mod $p$, there exist integers $a$ and $b$ such that $\min_\alpha(x) \equiv (x - a)(x - b) \mod p$, and $(\beta - a)(\beta - b) \in P$ in $\mathbb{Z}Q$ for all $\beta \in \text{Konj}(\alpha)$. Consider $(x - a)\text{Int}(\mathbb{Z}Q)(x - b)$. We wish to show that this set of polynomials lies in $\mathfrak{P}_{P,\alpha}$. 


Toward that end, let $h(x) \in \text{Int}(\mathbb{Z}Q)$ and let $H(x) = (x - a)h(x)(x - b)$. We have, for any $\beta \in \text{Konj}(\alpha)$,

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

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 $\text{Int}(\mathbb{Z}Q)$, we have $(x - a)\text{Int}(\mathbb{Z}Q)(x - b) \subseteq \mathfrak{P}_{P,\alpha}$. 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 6.3.5 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 6.3.3, we see that $\text{Int}(\mathbb{Z}Q)/\mathfrak{m} \cong \mathcal{R}/\mathcal{I}$ 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 $\text{Int}(\mathbb{Z}Q)/\mathfrak{m} \cong \mathbb{Z}Q/(p) \cong M_2(\mathbb{F}_p)$.

6.4 Some Primes of $\text{Int}(\mathbb{Z}Q)$ above $(1 + i, 1 + j)$

In Section 6.3, we described when $\mathfrak{P}_{P,\alpha}$ is a prime ideal of $\text{Int}(\mathbb{Z}Q)$ for the cases $P = (0)$ and $P = (p)$, where $p$ is an odd prime. In this section, we will determine what happens when $P = (1 + i, 1 + j)$. We begin with a lemma concerning elements of $P$ and the quotient ring $\mathbb{Z}Q/P$.

**Lemma 6.4.1.** Let $P = (1 + i, 1 + j)$ in $\mathbb{Z}Q$. Then,
(i) If $\alpha \in P$, then there exist $\gamma, \delta, \gamma', \delta' \in \mathbb{Z}Q$ such that $\alpha = \gamma(1 + i) + \delta(1 + j)$ and $\alpha = (1 + i)\gamma' + (1 + j)\delta'$. Thus, the two-sided ideal $(1 + i, 1 + j)$ equals both the right ideal $(1 + i, 1 + j)\mathbb{Z}Q$ and the left ideal $\mathbb{Z}Q(1 + i, 1 + j)$.

(ii) $\mathbb{Z}Q/P \cong \mathbb{F}_2$, the field with 2 elements.

Proof. (i) Let $\alpha \in P$. Then, we may write $\alpha = \sum_r \gamma_r\beta_r\delta_r$, where each $\gamma_r, \delta_r \in \mathbb{Z}Q$ and each $\beta_r \in \{1 + i, 1 + j\}$. Let $S = \{r \mid \beta_r = 1 + i\}$ and $T = \{r \mid \beta_r = 1 + j\}$. Since $\mathbb{Z}Q/(2)$ is commutative, we have, working mod 2,

$$\alpha \equiv \sum_r \gamma_r\beta_r\delta_r \equiv \sum_{r \in S} \gamma_r\delta_r(1 + i) + \sum_{r \in T} \gamma_r\delta_r(1 + j).$$

So, in $\mathbb{Z}Q$, $\alpha = \sum_{r \in S} \gamma_r\delta_r(1 + i) + \sum_{r \in T} \gamma_r\delta_r(1 + j) + 2\varepsilon$, for some $\varepsilon \in \mathbb{Z}Q$. Since $2 = (1 - i)(1 + i)$, we get

$$\alpha = \sum_{r \in S} \gamma_r\delta_r(1 + i) + \sum_{r \in T} \gamma_r\delta_r(1 + j) + 2\varepsilon$$

$$= \sum_{r \in S} \gamma_r\delta_r(1 + i) + \sum_{r \in T} \gamma_r\delta_r(1 + j) + \varepsilon(1 - i)(1 + i)$$

$$= (\sum_{r \in S} \gamma_r\delta_r + \varepsilon(1 - i))(1 + i) + \sum_{r \in T} \gamma_r\delta_r(1 + j)$$

$$= \gamma(1 + i) + \delta(1 + j),$$

where $\gamma = \sum_{r \in S} \gamma_r\delta_r + \varepsilon(1 - i)$ and $\delta = \sum_{r \in T} \gamma_r\delta_r$. The existence of $\gamma'$ and $\delta'$ can be proved similarly, so part (i) holds.

(ii) Let $R = \mathbb{Z}Q/(2)$. Then, it is not hard to see that $M = (1 + i, 1 + j)$ in $R$ is the unique maximal ideal of $R$ and $R/M \cong \mathbb{F}_2$. But then, $\mathbb{Z}Q/P = \mathbb{Z}Q/(2, 1 + i, 1 + j) \cong R/M \cong \mathbb{F}_2$. 

In the proof of Proposition 6.2.4, we showed that when $\varepsilon = (1 + i)$ and $\alpha \in \mathbb{Z}Q$, we always have $\varepsilon\alpha\varepsilon^{-1} \in \mathbb{Z}Q$. We now record this formally as a lemma.
Lemma 6.4.2. Let $\varepsilon \in \{1 + i, 1 + j\}$. Then, for all $\alpha \in \mathbb{Z}Q$, $\varepsilon \alpha \varepsilon^{-1} \in \mathbb{Z}Q$.

Proof. Let $\alpha = a + bi + cj + dk \in \mathbb{Z}Q$. Assume first that $\varepsilon = 1 + i$. Then, $\varepsilon^{-1} = \frac{1-i}{2}$ and direct computation shows that

$$\varepsilon \alpha \varepsilon^{-1} = a + bi - dj + ck \in \mathbb{Z}Q.$$ 

Similarly, when $\varepsilon = 1 + j$, we have

$$\varepsilon \alpha \varepsilon^{-1} = a + di + cj - bk \in \mathbb{Z}Q.$$ 

\[ \square \]

We can now prove that when $P = (1 + i, 1 + j)$ and $\alpha \in \mathbb{Z}Q$, the set $\mathfrak{P}_{P,\alpha}$ is not just an ideal of $\text{Int}(\mathbb{Z}Q)$, but is in fact a maximal ideal of $\text{Int}(\mathbb{Z}Q)$.

Theorem 6.4.3. Let $P = (1 + i, 1 + j)$ in $\mathbb{Z}Q$, and let $\alpha \in \mathbb{Z}Q$. Then,

(i) $\mathfrak{P}_{P,\alpha}$ is an ideal of $\text{Int}(\mathbb{Z}Q)$.

(ii) $\mathfrak{P}_{P,\alpha}$ is a maximal ideal of $\text{Int}(\mathbb{Z}Q)$, and $\text{Int}(\mathbb{Z}Q)/\mathfrak{P}_{P,\alpha} \cong \mathbb{F}_2$.

Proof. (i) Let $f \in \mathfrak{P}_{P,\alpha}$ and $g \in \text{Int}(\mathbb{Z}Q)$. We need to show that $(fg)(\beta), (gf)(\beta) \in P$ for all $\beta \in \text{Konj}(\alpha)$. Let $\beta \in \text{Konj}(\alpha)$. Showing that $(fg)(\beta) \in P$ may be done just as in the proof of Theorem 6.2.3. To show that $(gf)(\beta) \in P$, we use Lemma 6.4.1. Let $g(x) = \sum_{r} \beta_r x^r$. Since $f(\beta) \in P$, there exist $\gamma, \delta \in \mathbb{Z}Q$ such that $f(\beta) = \gamma + \delta \in P$. 

105
\( \gamma(1 + i) + \delta(1 + j) \). For convenience, let \( \varepsilon_1 = 1 + i \) and \( \varepsilon_2 = 1 + j \). Then,

\[
(gf)(\beta) = \sum_r \beta_r f(\beta)\beta^r \\
= \sum_r \beta_r (\gamma \varepsilon_1 + \delta \varepsilon_2)\beta^r \\
= \sum_r \beta_r \gamma \varepsilon_1 \beta^r + \sum_r \beta_r \delta \varepsilon_2 \beta^r \\
= \sum_r \beta_r \gamma \varepsilon_1 \beta^r \varepsilon_1^{-1} \varepsilon_1 + \sum_r \beta_r \delta \varepsilon_2 \beta^r \varepsilon_2^{-1} \varepsilon_2 \\
= (g_\gamma)(\varepsilon_1 \beta \varepsilon_1^{-1}) \varepsilon_1 + (g_\delta)(\varepsilon_2 \beta \varepsilon_2^{-1}) \varepsilon_2.
\]

By Lemma 6.4.2, both \( \varepsilon_1 \varepsilon_1^{-1} \) and \( \varepsilon_2 \varepsilon_2^{-1} \) are in \( \mathbb{Z}Q \). Since \( g_\gamma, g_\delta \in \text{Int}(\mathbb{Z}Q) \), we have \( (g_\gamma)(\varepsilon_1 \beta \varepsilon_1^{-1}) \in \mathbb{Z}Q \) and \( (g_\delta)(\varepsilon_2 \beta \varepsilon_2^{-1}) \in \mathbb{Z}Q \). Since \( \varepsilon_1, \varepsilon_2 \in P \), the above equation tells us that \( (gf)(\beta) \in P \). It follows that \( \mathfrak{P}_{P,\alpha} \) is an ideal of \( \text{Int}(\mathbb{Z}Q) \).

(ii) Let \( \mathcal{R} = \text{Int}(\mathbb{Z}Q)/\mathfrak{P}_{P,\alpha} \). It suffices to show that \( \mathcal{R} \cong \mathbb{F}_2 \), since this will force \( \mathfrak{P}_{P,\alpha} \) to be a maximal ideal of \( \text{Int}(\mathbb{Z}Q) \).

Let \( f \in \text{Int}(\mathbb{Z}Q) \) and let \( \varepsilon = 1 + i \). Then, \( \varepsilon \in \mathfrak{P}_{P,\alpha} \), so \( f \varepsilon = f + fi \in \mathfrak{P}_{P,\alpha} \). In particular, this means that \( f(\alpha) + f(-i\alpha)i = f(\alpha) + (fi)(\alpha) \in P \). Thus,

\[
f(\alpha) \in P \iff f(-i\alpha)i \in P \iff f(-i\alpha) \in P.
\]

Similar results hold when \( \varepsilon = 1 + j \) or \( \varepsilon = 1 + k \), so we see that

\[
f(\alpha) \in P \iff f(\beta) \in P \text{ for all } \beta \in \text{Konj}(\alpha)
\]

\[
\iff f \in \mathfrak{P}_{P,\alpha}.
\]

Now, since \( \mathbb{Z}Q/P \cong \mathbb{F}_2 \), either \( f(\alpha) \in P \) or \( f(\alpha) + 1 \in P \). Thus, either \( f \in \mathfrak{P}_{P,\alpha} \) or \( f + 1 \in \mathfrak{P}_{P,\alpha} \). Stated differently, this means that the residue of \( f \) in \( \mathcal{R} \) is equivalent either to 0 or to 1. Since \( f \) was an arbitrary element of \( \text{Int}(\mathbb{Z}Q) \), we conclude that \( \mathcal{R} \cong \mathbb{F}_2 \), which completes the proof. \( \square \)
CHAPTER 7

INTEGER-VALUED POLYNOMIALS ON SUBSETS

7.1 Subsets and Muffins

When $D$ is a (commutative) integral domain with field of fractions $K$ and $E$ is any subset of $D$, one may define

$$\text{Int}(E, D) := \{ f(x) \in K[x] \mid f(a) \in D \text{ for all } a \in E \},$$

and it is not difficult to show that $\text{Int}(E, D)$ is a ring, which we call the ring of integer-valued polynomials on $E$. In this chapter, we investigate how the notion of integer-valued polynomials on subsets may be extended to quaternion rings. For now, we will work exclusively with $\mathbb{Z}Q$.

As mentioned above, $\text{Int}(E, D)$ is always a ring when $D$ is a (commutative) integral domain and $E \subseteq D$. However, this might not be true when working over $\mathbb{Z}Q$. To illustrate the disparity with the commutative case, we begin with a simple negative example.

Example 7.1.1. Define $\text{Int}\{i\}, \mathbb{Z}Q = \{ f(x) \in \mathbb{Q}Q[x] \mid f(i) \in \mathbb{Z}Q \}$. Notice that $\frac{x-i}{3}, x-j \in \text{Int}\{i\}, \mathbb{Z}Q$. However, letting $f(x) = \frac{x-i}{3}(x-j) = \frac{x^2-(i+j)x+k}{3}$, we have
\[ f(i) = \frac{2i}{3} \notin \mathbb{Z}Q. \] Thus, \( \text{Int}\{i\}, \mathbb{Z}Q \) is not closed under multiplication, and therefore cannot be a ring.

As the example above shows, it is non-trivial to determine which subsets of \( \mathbb{Z}Q \) give rise to rings of integer-valued polynomials. A satisfactory resolution to this problem is the goal of the present chapter. Toward that end, we begin with some definitions.

**Definition 7.1.2.** For any subset \( S \subseteq \mathbb{Z}Q \), define the set \( \text{Int}(S, \mathbb{Z}Q) \) to be

\[ \text{Int}(S, \mathbb{Z}Q) = \{ f(x) \in \mathbb{Q}Q[x] \mid f(S) \subseteq \mathbb{Z}Q \}. \]

For any quotient ring \( R \) of \( \mathbb{Z}Q \), define the set \( \text{Muff}_R(S) \) to be

\[ \text{Muff}_R(S) = \{ f(x) \in R[x] \mid f(\alpha) = 0 \text{ in } R, \text{ for all } \alpha \in S \}. \]

We call \( \text{Muff}_R(S) \) the *muff* of \( S \) in \( R \). Lastly, a *ringset* is defined to be a subset \( S \) of \( \mathbb{Z}Q \) such that \( \text{Int}(S, \mathbb{Z}Q) \) is a ring.

Recall Correspondence 4.1.1, which gave convenient ways to write and work with elements of \( \text{Int}(\mathbb{Z}Q) \). A similar result exists for elements of \( \text{Int}(S, \mathbb{Z}Q) \): any \( f(x) \in \text{Int}(S, \mathbb{Z}Q) \) may be written as

\[ f(x) = \frac{g(x)}{n} \in \text{Int}(S, \mathbb{Z}Q) \text{ with } g(x) \in \mathbb{Z}Q[x] \text{ and } n \in \mathbb{Z}, \text{ and when } f(x) \text{ is expressed in this way, } g(x) \text{ mod } n \text{ is in } \text{Muff}_R(S), \text{ where } R = \mathbb{Z}Q/(n). \]

The theorems in this section more carefully analyze the relationship between the sets \( \text{Int}(S, \mathbb{Z}Q) \) and \( \text{Muff}_R(S) \), where \( R \) is a quotient ring of \( \mathbb{Z}Q \).

Generally, we will be trying to show either that \( \text{Int}(S, \mathbb{Z}Q) \) is a ring, or that \( \text{Muff}_R(S) \) is an ideal of \( R[x] \). It is easy to verify that for any \( S \subseteq \mathbb{Z}Q \) and any quotient ring \( R \) of \( \mathbb{Z}Q \), the sets \( \text{Int}(S, \mathbb{Z}Q) \) and \( \text{Muff}_R(S) \) are groups under addition. Thus, to prove (or disprove) that \( \text{Int}(S, \mathbb{Z}Q) \) is a ring or that \( \text{Muff}_R(S) \) is an ideal of \( R[x] \), it is enough to consider the multiplicative aspects of the relevant structure. This technique makes the proof of our first result especially brief.
Proposition 7.1.3. Let $S \subseteq \mathbb{Z}$. Then, $S$ is a ringset.

Proof. Let $f, g, \in \text{Int}(S, \mathbb{Z}Q)$ and let $a \in S$. Then, $f(a), g(a) \in \mathbb{Z}$ and $(fg)(a) = f(a)g(a) \in \mathbb{Z}$, so $fg \in \text{Int}(S, \mathbb{Z}Q)$. Thus, $\text{Int}(S, \mathbb{Z}Q)$ is closed under multiplication and therefore is a ring, i.e. $S$ is a ringset. \qed

Theorem 7.1.4. Let $S \subseteq \mathbb{Z}Q$, and for all $n > 1$, let $R_n = \mathbb{Z}Q/(n)$. Then, the following are equivalent:

(i) $\text{Int}(S, \mathbb{Z}Q)$ is ring

(ii) for each $n > 1$, $\text{Muff}_{R_n}(S)$ is an ideal of $R_n[x]

(iii) for each prime $p$ and for every $e > 0$, $\text{Muff}_{R_{pe}}(S)$ is an ideal of $R_{pe}[x]

Proof. (i) $\Rightarrow$ (ii) Assume $\text{Int}(S, \mathbb{Z}Q)$ is a ring. Fix $n > 1$, let $f(x) \in \text{Muff}_{R_n}(S)$, and let $g(x) \in R_n[x]$. It suffices to show that $(fg)(x)$ and $(gf)(x)$ are in $\text{Muff}_{R_n}(S)$. By abusing notation, we may consider $f(x)$ and $g(x)$ to have coefficients in $\mathbb{Z}Q$, in which case $\frac{f(x)}{n} \in \text{Int}(S, \mathbb{Z}Q)$ and $g(x) \in \mathbb{Z}Q[x] \subseteq \text{Int}(S, \mathbb{Z}Q)$. Since $\text{Int}(S, \mathbb{Z}Q)$ is a ring, both $\frac{(fg)(x)}{n}$ and $\frac{(gf)(x)}{n}$ are in $\text{Int}(S, \mathbb{Z}Q)$. It follows that mod $n$, both $(fg)(x)$ and $(gf)(x)$ are in $\text{Muff}_{R_n}(S)$, and therefore $\text{Muff}_{R_n}(S)$ is an ideal of $R_n[x]$.

(ii) $\Rightarrow$ (i) Assume that for each $n > 1$, $\text{Muff}_{R_n}(S)$ is an ideal of $R_n[x]$. It suffices to show that $\text{Int}(S, \mathbb{Z}Q)$ is closed under multiplication. Let $\frac{f(x)}{n_1}, \frac{g(x)}{n_2} \in \text{Int}(S, \mathbb{Z}Q)$, where $f(x), g(x) \in \mathbb{Z}Q[x]$ and $n_1, n_2 > 0$. We want to show that $\frac{(fg)(x)}{n_1n_2} \in \text{Int}(S, \mathbb{Z}Q)$.

Let $\alpha \in S$ and let $g(\alpha) = a + bi + cj + dk \in \mathbb{Z}Q$. Then, $(fg)(\alpha) = af(\alpha) + b(fi)(\alpha) + c(fj)(\alpha) + d(fk)(\alpha)$. Since $\frac{g(x)}{n_2} \in \text{Int}(S, \mathbb{Z}Q)$, we have $g(\alpha) \in (n_2)$ in $\mathbb{Z}Q$, so each of $a, b, c, d$ is divisible by $n_2$.

Now, $f(x) \mod n_1$ is in $\text{Muff}_{R_{n_1}}(S)$, and $\text{Muff}_{R_{n_1}}(S)$ is an ideal of $R_{n_1}[x]$, so $(fi)(x), (fj)(x), (fk)(x)$ are also in $\text{Muff}_{R_{n_1}}(S)$. In $\mathbb{Z}Q$, this means that each
of \( f(\alpha), (fi)(\alpha), (fj)(\alpha), \) and \((fk)(\alpha)\) are in \(n_1\). Combining this with the above paragraph, we see that each of \(af(\alpha), b(fi)(\alpha), c(fj)(\alpha), \) and \(d(fk)(\alpha)\) is in \((n_1 n_2)\) in \(\mathbb{Z}Q\). Thus, \(\frac{(fg)(\alpha)}{n_1 n_2} \in \mathbb{Z}Q\). Since \(\alpha \in S\) was arbitrary, we have \(\frac{(fg)(\alpha)}{n_1 n_2} \in \text{Int}(S, \mathbb{Z}Q)\), as required.

(ii) \(\Rightarrow\) (iii) This is immediate.

(iii) \(\Rightarrow\) (ii) Let \(n > 1\), let \(f \in \text{Muff}_{R_n}(S)\), and let \(g \in R_n[x]\). Assume that \(n\) has prime factorization \(n = p_1^{e_1} \cdots p_t^{e_t}\). Fix \(m\) between 1 and \(t\), and let \(p = p_m\) and \(e = e_m\).

Let \(F = f \mod p^e\) and let \(G = g \mod p^e\). Then, \(F \in \text{Muff}_{R_{p^e}}(S)\) and \(G \in R_{p^e}[x]\), and since \(\text{Muff}_{R_{p^e}}(S)\) is an ideal, we see that \(FG \in \text{Muff}_{R_{p^e}}(S)\). Fix \(\alpha \in S\). Then, 

\[(FG)(\alpha) \equiv 0 \mod p^e\] 

for all \(\alpha \in S\), so in \(R_n\), we have \((fg)(\alpha) \in p^e R_n\). Since \(p\) was an arbitrary prime dividing \(n\), we conclude that

\[(fg)(\alpha) \in \bigcap_{m=1}^{t} p_m^{e_m} R_n = \{0\};\]

thus, \((fg)(\alpha) \equiv 0 \mod n\). Similarly, \((gf)(\alpha) \equiv 0 \mod n\). Since \(\alpha\) was an arbitrary element of \(S\), we get \(fg, gf \in \text{Muff}_{R_n}(S)\), and therefore \(\text{Muff}_{R_n}(S)\) is an ideal of \(R_n[x]\).

Recall Definition 6.2.1: for any \(\alpha \in \mathbb{Z}Q\), we define the restricted multiplicative conjugacy class \(\text{Konj}(\alpha)\) of \(\alpha\) to be \(\text{Konj}(\alpha) = \{u\alpha u^{-1} | u \in (\mathbb{Z}Q)^x\}\); here, \((\mathbb{Z}Q)^x = \{\pm 1, \pm i, \pm j, \pm k\}\).

**Theorem 7.1.5.** Let \(n > 1\), let \(R = \mathbb{Z}Q/(n)\), and let \(S \subseteq \mathbb{Z}Q\). Then, \(\text{Muff}_R(S)\) is an ideal of \(R[x] \iff \text{for all } f \in \text{Muff}_R(S), \text{for all } \alpha \in S, \text{and for all } \beta \in \text{Konj}(\alpha), \text{we have } f(\beta) \equiv 0 \mod n.\)

**Proof.** \((\Rightarrow)\) Assume that \(\text{Muff}_R(S)\) is an ideal of \(R[x]\). Let \(f \in \text{Muff}_R(S), \alpha \in S, \) and \(\beta \in \text{Konj}(\alpha)\). Then, there exists \(u \in \{\pm 1, \pm i, \pm j, \pm k\}\) such that \(\beta = u\alpha u^{-1}\). Since
Muff\(_R(S)\) is an ideal of \(R[x]\), \((fu)(x) \mod n \in \text{Muff}_R(S)\) and \((fu)(\alpha) \equiv 0 \mod n\). Thus,
\[
f(\beta) \equiv f(u\alpha u^{-1}) \equiv (fu)(\alpha)u^{-1} \equiv 0 \mod n,
\]
proving the forward implication.

\((\Leftarrow)\) This proof is almost identical to that of Proposition 4.1.4. Assume that for all \(f \in \text{Muff}_R(S)\), for all \(\alpha \in S\), and all \(\beta \in \text{Konj}(\alpha)\), we have \(f(\beta) \equiv 0 \mod n\). Let \(f(x) \in \text{Muff}_R(S)\), \(g(x) \in R[x]\), and \(\alpha \in S\). Let \(f(x) = \sum_r \alpha_r x^r\), let \(g(x) = \sum_r \beta_r x^r\), and let \(a, b, c, d \in \mathbb{Z}\) be such that \(g(\alpha) \equiv a + bi + cj + dk\). Then,
\[
(gf)(\alpha) \equiv \sum_r \beta_r f(\alpha)\alpha^r \equiv 0,
\]
and
\[
(fg)(\alpha) \equiv \sum_r \alpha_r g(\alpha)\alpha^r \\
\quad \equiv \sum_r \alpha_r(a + bi + cj + dk)\alpha^r \\
\quad \equiv af(\alpha) + b(fi)(\alpha) + c(fj)(\alpha) + d(fk)(\alpha) \\
\quad \equiv af(\alpha) + bf(-i\alpha)i + cf(-j\alpha)j + df(-k\alpha)k.
\]
Because \(\alpha, -i\alpha, -j\alpha, \) and \(-k\alpha\) are all in \(\text{Konj}(\alpha)\) we see that \((fg)(\alpha) \equiv 0 \mod n\). Thus, both \((fg)(x)\) and \((gf)(x)\) are in \(\text{Muff}_R(S)\), and therefore \(\text{Muff}_R(S)\) is an ideal of \(R[x]\).

\[\Box\]

**Corollary 7.1.6.** Let \(S \subseteq \mathbb{Z}Q\), and for all \(n > 1\), let \(R_n = \mathbb{Z}Q/(n)\). Then, the following are equivalent:

(i) \(\text{Int}(S, \mathbb{Z}Q)\) is ring

(ii) for all \(n > 1\), for all \(f \in \text{Muff}_{R_n}(S)\), for all \(\alpha \in S\), and for all \(\beta \in \text{Konj}(\alpha)\), we have \(f(\beta) \equiv 0 \mod n\)
(iii) for all primes $p$, for all $e > 0$, for all $f \in \text{Muff}_{R_p}(S)$, for all $\alpha \in S$, and for all $\beta \in \text{Konj}(\alpha)$, we have $f(\beta) \equiv 0 \mod p^e$

Proof. This is just a combination of Theorems 7.1.4 and 7.1.5.

### 7.2 Some Sufficient Conditions

The following two theorems provide sufficient conditions for $S$ to be a ringset.

**Theorem 7.2.1.** Let $S \subseteq \mathbb{Z}Q$. Assume that for all $u \in \{i, j, k\}$ we have $uSu^{-1} \subseteq S$. Then, $S$ is a ringset.

Proof. This is a direct application of Corollary 7.1.6. Let $n > 1$, let $R = \mathbb{Z}Q/(n)$, let $f \in \text{Muff}_R(S)$, let $\alpha \in S$, and let $\beta \in \text{Konj}(\alpha)$. Since $\alpha \in S$, we have $\text{Konj}(\alpha) \subseteq S$. Thus, $f(\beta) \equiv 0 \mod n$. By Corollary 7.1.6, we conclude that $\text{Int}(S, \mathbb{Z}Q)$ is a ring.

By the preceding theorem, for $S$ to be a ringset it is enough that $S$ be closed under multiplicative conjugation. However, this condition is not necessary.

**Example 7.2.2.** Consider $S = \{i, j\}$, and let our notation be as in Corollary 7.1.6. Given $f \in \text{Muff}_{R_n}(S)$, we know that $f(i) \equiv f(j) \equiv 0 \mod n$, and it suffices to have $f(-i) \equiv 0$ and $f(-j) \equiv 0$. Since $\pm i$ and $\pm j$ all share the same norm and constant coefficient, Theorem 2.3.1 implies that there exist $\gamma, \delta \in R_n[x]$ such that $f(\alpha) \equiv \gamma \alpha + \delta$ for all $\alpha \in \{\pm i, \pm j\}$. So, $0 \equiv f(i) - f(j) \equiv \gamma(i - j)$. Multiplying this equivalence on the right by $-i + j$ yields $0 \equiv 2\gamma$. But then, $f(i) - f(-i) \equiv 2\gamma i \equiv 0$, from which we conclude that $f(-i) \equiv 0$. Similarly, $f(-j) \equiv 0$, and thus $S$ is a ringset in this case.

In the next theorem, we generalize the technique used in the above example. Recall some notation from previous chapters: for any $\alpha = a + bi + cj + dk \in \mathbb{Z}Q - \mathbb{Z}$, we define the minimal polynomial $\min_\alpha(x)$ of $\alpha$ to be $\min_\alpha(x) = x^2 - 2ax + N(\alpha)$. 112
Theorem 7.2.3. Let \( S \subseteq \mathbb{Z}Q \). Assume that for all \( \alpha \in S - \mathbb{Z} \) and all \( u \in \{ i, j, k \} \), there exists \( \beta \in S \) and \( \varepsilon \in \mathbb{Z}Q \) such that

1. \( \min_\alpha(x) = \min_\beta(x) \), and

2. \( (\alpha - \beta)\varepsilon = \alpha - u\alpha u^{-1} \).

Then, \( S \) is a ringset.

Proof. We first deal with any integers that might lie in \( S \). For any \( a \in S \cap \mathbb{Z} \) and any \( f(x), g(x) \in \text{Int}(S, \mathbb{Z}Q) \), we have \((fg)(a) = f(a)g(a) \in \mathbb{Z}Q \) and \((gf)(a) = g(a)f(a) \in \mathbb{Z}Q \), so no obstacles will arise from \( S \cap \mathbb{Z} \). So, assume that \( S - \mathbb{Z} \neq \emptyset \).

Let \( n > 1 \), let \( R = \mathbb{Z}Q/(n) \), let \( f \in \text{Muff}_R(S) \), let \( \alpha \in S - \mathbb{Z} \), and let \( u \in \{ i, j, k \} \). By Theorem 2.3.1 part (iii) and condition (1) above, it follows that there exist \( \gamma, \delta \in R \) such that \( \gamma \alpha + \delta \equiv 0 \mod n \) and \( \gamma \beta + \delta \equiv 0 \mod n \). Subtracting these two equivalences and applying condition (2) above, we have

\[
0 \equiv \gamma(\alpha - \beta)
\equiv \gamma(\alpha - \beta)\varepsilon
\equiv \gamma(\alpha - u\alpha u^{-1})
\equiv \gamma \alpha + \delta - (\gamma u\alpha u^{-1} + \delta)
\equiv -(\gamma u\alpha u^{-1} + \delta)
\equiv -f(u\alpha u^{-1}),
\]

where the last equivalence follows because \( \alpha \) and \( u\alpha u^{-1} \) share the same minimal polynomial. By Corollary 7.1.6, we conclude that \( S \) is a ringset.

As with Theorem 7.2.1, the conditions specified by Theorem 7.2.3 are not necessary for \( S \) to be a ringset. \( \square \)
Example 7.2.4. Pick $\alpha \in \mathbb{Z}Q - \mathbb{Z}$, and for each $n > 1$, let $\alpha_n = \alpha + n$ and $S_n = \text{Konj}(\alpha_n)$. Let

$$S = \left( \bigcup_{n=1}^{\infty} S_n \right) \cup \{\alpha\}.$$

Then, no element of $S$ has the same constant coefficient as $\alpha$, so $\min_{\beta}(x) \neq \min_{\alpha}(x)$ whenever $\beta \in S - \{\alpha\}$. So, the only way that condition (1) of Theorem 7.2.3 can be met for $\alpha$ is to take $\beta = \alpha$. However, in that case condition (2) becomes

$$0 = \alpha - u\alpha u^{-1} \text{ for all } u \in \{i, j, k\}.$$

Since $\alpha \notin \mathbb{Z}$, there exists $u \in \{i, j, k\}$ such that $\alpha$ and $u$ do not commute, and for this $u$, we have $\alpha - u\alpha u^{-1} \neq 0$. Thus, the conditions of Theorem 7.2.3 do not apply. Nevertheless, $S$ is a ringset, which we prove as follows. Given $\beta \in \text{Konj}(\alpha)$ and $n > 1$, there exists $\beta_n \in \text{Konj}(\alpha_n) \subseteq S$ such that $\beta \equiv \beta_n \text{ mod } n$. Hence, if $f \in \text{Muff}_{\mathbb{Z}Q/(n)}(S)$, then $f(\beta) \equiv f(\beta_n) \equiv 0 \text{ mod } n$. Therefore, we can meet the conditions of Corollary 7.1.6 and conclude that $\text{Int}(S, \mathbb{Z}Q)$ is a ring.

In Section 7.4, we shall give necessary and sufficient conditions for some subsets of $\mathbb{Z}Q$ to be ringsets; in Section 7.5, we will give necessary and sufficient conditions for any finite subset of $\mathbb{Z}Q$ to be a ringset. The hope is that the insight gained from these cases will allow us to determine necessary and sufficient conditions that work for more general $S \subseteq \mathbb{Z}Q$. Before proceeding to those results, however, we prove two more useful theorems that hold for general subsets of $\mathbb{Z}Q$.

Theorem 7.2.5.

(i) Let $S, T \subseteq \mathbb{Z}Q$, let $n > 1$, and let $R = \mathbb{Z}Q/(n)$. Assume that $S \subseteq T$. Then,

$$\text{Int}(T, \mathbb{Z}Q) \subseteq \text{Int}(S, \mathbb{Z}Q) \text{ and } \text{Muff}_R(T) \subseteq \text{Muff}_R(S).$$
(ii) Let \( \{S_\ell\}_{\ell \in I} \) be a collection of subsets of \( \mathbb{Z}Q \) such that \( S_\ell \) is a ringset for each \( \ell \in I \). Let \( S = \bigcup_{\ell \in I} S_\ell \). Then, \( S \) is a ringset.

Proof. (i) Let \( \alpha \in S, f \in \text{Int}(T, \mathbb{Z}Q) \), and \( g \in \text{Muff}_R(T) \). Then, \( \alpha \in T \), so \( f(\alpha) \in \mathbb{Z}Q \) and \( g(\alpha) \equiv 0 \mod n \). Hence, \( f \in \text{Int}(S, \mathbb{Z}Q) \) and \( g \in \text{Muff}_R(S) \).

(ii) Let \( n > 1 \), let \( R = \mathbb{Z}Q/(n) \), let \( f \in \text{Muff}_R(S) \), and let \( \alpha \in S \). Then, there exists \( m \in I \) such that \( \alpha \in S_m \subseteq S \). Since \( f \in \text{Muff}_R(S) \subseteq \text{Muff}_R(S_m) \) and \( \text{Int}(S_m, \mathbb{Z}Q) \) is a ring, Corollary 7.1.6 tells us that \( f(\beta) \equiv 0 \mod n \) for all \( \beta \in \text{Konj}(\alpha) \). Thus, \( \text{Muff}_R(S) \) is an ideal of \( R[x] \) and \( S \) is a ringset.

As the previous theorem shows, the collection of all ringsets of \( \mathbb{Z}Q \) is closed under unions. However, this collection is not closed under intersections, since, for instance, \( \text{Int}(\{i, j\}, \mathbb{Z}Q) \) and \( \text{Int}(\{i, k\}, \mathbb{Z}Q) \) are both rings, but \( \text{Int}(\{i\}, \mathbb{Z}Q) \) is not. Thus, there is not any obvious way to give \( \mathbb{Z}Q \) a topology that can help identify ringsets.

**Definition 7.2.6.** For any \( S \subseteq \mathbb{Z}Q \), any \( n \in \mathbb{Z} \), and any \( m \in \mathbb{Z} - \{0\} \), we define the sets \( S + n \) and \( mS \) to be \( S + n = \{\alpha + n \mid \alpha \in S\} \) and \( mS = \{m\alpha \mid \alpha \in S\} \).

**Theorem 7.2.7.** Let \( S \subseteq \mathbb{Z}Q \), let \( n \in \mathbb{Z} \), and let \( m \in \mathbb{Z} - \{0\} \). Then, the following are equivalent:

(i) \( S \) is a ringset

(ii) \( S + n \) is a ringset

(iii) \( mS \) is a ringset

Proof. (i) \( \iff \) (ii) Assume first that \( S \) is a ringset. It suffices to show that \( \text{Int}(S + n, \mathbb{Z}Q) \) is closed under multiplication. Let \( f(x), g(x) \in \text{Int}(S + n, \mathbb{Z}Q) \), and
define $F(x) = f(x + n)$ and $G(x) = g(x + n)$. Then, $F(x)$ and $G(x)$ are polynomials in $\mathbb{Q}Q[x]$, and since $n \in \mathbb{Z}$, for all $\alpha \in S$ we have $F(\alpha) = f(\alpha + n) \in \mathbb{Z}Q$ and $G(\alpha) = g(\alpha + n) \in \mathbb{Z}Q$, so $F(x), G(x) \in \text{Int}(S, \mathbb{Z}Q)$. Furthermore, letting $f(x) = \sum \alpha_r x^r$, we have, for all $\alpha + n \in S + n$,

$$(fg)(\alpha + n) = \sum \alpha_r g(\alpha + n)(\alpha + n)^r$$

$$= \sum \alpha_r G(\alpha)(\alpha + n)^r$$

$$= (FG)(\alpha) \in \mathbb{Z}Q.$$ 

Thus, $(fg)(x) \in \text{Int}(S + n, \mathbb{Z}Q)$. Thus, $\text{Int}(S + n, \mathbb{Z}Q)$ is a ring.

If we assume that $S + n$ is a ringset, then the same proof works when we take $f(x), g(x) \in \text{Int}(S, \mathbb{Z}Q), F(x) = f(x - n)$, and $G(x) = g(x - n)$. This proves the equivalence of (i) and (ii).

(i) $\iff$ (iii) This proof is similar to the one above. Assume first that $S$ is a ringset, let $f(x), g(x) \in \text{Int}(mS, \mathbb{Z}Q)$, and define $F(x), G(x) \in \text{Int}(S, \mathbb{Z}Q)$ by $F(x) = f(mx)$ and $G(x) = g(mx)$. Then, as in the proof that (i) and (ii) are equivalent, we can show that $(fg)(mx) = (FG)(x)$, from which we conclude that $\text{Int}(mS, \mathbb{Z}Q)$ is closed under multiplication, and hence is a ring.

To prove that (iii) $\Rightarrow$ (i), one would take $f(x), g(x) \in \text{Int}(S, \mathbb{Z}Q)$, define $F(x), G(x) \in \text{Int}(mS, \mathbb{Z}Q)$ by $F(x) = f(x/m)$ and $G(x) = g(x/m)$, and then proceed as before. 

\begin{proof}

\end{proof}
7.3 Results for Reduced Subsets of \( \mathbb{Z}Q \)

As the examples in the previous sections show, deciding whether a subset of \( \mathbb{Z}Q \) is a ringset can be challenging. In this section, we begin to derive necessary and sufficient conditions for a certain type of finite subset of \( \mathbb{Z}Q \) to be a ringset. Our first theorem examines what happens with one-element subsets of \( \mathbb{Z}Q \).

**Theorem 7.3.1.** Let \( \alpha \in \mathbb{Z}Q \). Then, \( \text{Int}(\{\alpha\}, \mathbb{Z}Q) \) is a ring \( \iff \alpha \in \mathbb{Z} \).

**Proof.** (\( \Leftarrow \)) This follows from Proposition 7.1.3.

(\( \Rightarrow \)) We prove the contrapositive. Assume that \( \alpha \notin \mathbb{Z} \). Then, there exists \( u \in \{i, j, k\} \) such that \( \alpha \) and \( u \) do not commute, i.e. \( \alpha u - u \alpha \neq 0 \).

Now, let \( f(x) = x - \alpha \). Then, \( \frac{f(x)}{n} \in \text{Int}(\{\alpha\}, \mathbb{Z}Q) \) for all \( n > 0 \). However, \( \alpha u - u \alpha \neq 0 \), so there exists \( m > 0 \) such that \( \frac{\alpha u - u \alpha}{m} \notin \mathbb{Z}Q \). Let \( g(x) = (x - \alpha)(x - u) = x^2 - (\alpha + u)x + \alpha u \). Then, \( g(\alpha) = \alpha u - u \alpha \), so \( \frac{x - \alpha}{m} (x - u) = \frac{g(x)}{m} \notin \text{Int}(\{\alpha\}, \mathbb{Z}Q) \), even though both \( \frac{x - \alpha}{m} \) and \( x - u \) are in \( \text{Int}(\{\alpha\}, \mathbb{Z}Q) \). Thus, \( \text{Int}(\{\alpha\}, \mathbb{Z}Q) \) is not closed under multiplication and therefore is not a ring.

The technique used in Theorem 7.3.1 of multiplying a polynomial by one of \( x - i \), \( x - j \), or \( x - k \) will be employed frequently enough that we shall record some of the relevant computations. Assume that \( \alpha = a + b i + c j + d k \) and let \( g_1(x) = (x - \alpha)(x - i) \), \( g_2(x) = (x - \alpha)(x - j) \), and \( g_3(x) = (x - \alpha)(x - k) \). Then,

\[
g_1(\alpha) = \alpha i - i \alpha = 2dj - 2ck
\]

\[
g_2(\alpha) = \alpha j - j \alpha = -2di + 2bk, \quad \text{and} \quad \tag{7.3.2}
g_3(\alpha) = \alpha k - k \alpha = 2ci - 2bj.
\]
When $S$ is not a singleton subset of $\mathbb{Z}Q$, the situation is more complicated. In Theorem 7.2.3, we found a sufficient condition for a subset $S$ of $\mathbb{Z}Q$ to be a ringset, and in that theorem it was important to consider the minimal polynomials of elements of $S$. So, it seems reasonable to focus on subsets of $\mathbb{Z}Q$ in which every element has the same minimal polynomial. Assume that $S$ is such a set. Then, every element of $S$ has the same constant coefficient $a$, and by Theorem 7.2.6 part (ii), $S$ is a ringset if and only if $S - a$ is a ringset. Each element of $S - a$ has constant coefficient equal to 0, so there is no loss in assuming that each element of $S$ has constant coefficient equal to 0. Furthermore, by applying Theorem 7.2.6 part (iii), there is no loss in assuming that the elements of $S$ have no common positive integer factor other than 1. This leads us to the following definition.

**Definition 7.3.3.** A subset $S \subseteq \mathbb{Z}Q - \mathbb{Z}$ is called *reduced* if

1) all elements of $S$ have the same minimal polynomial,

2) all elements of $S$ have constant coefficient equal to 0, and

3) for all $n > 1$, $S \not\subseteq (n)$ in $\mathbb{Z}Q$.

A subset $S \subseteq \mathbb{Z}Q - \mathbb{Z}$ is called *reducible* if there exists a reduced set $T \subseteq \mathbb{Z}Q - \mathbb{Z}$, $a \in \mathbb{Z}$, and $m \in \mathbb{Z}$, $m > 0$ such that $S = mT + a$. If such a $T$ exists, we call it the *reduction* of $S$.

To illustrate this definition, we give some examples. The set $\{4 + 5i, 4 - 5k\}$ is reducible with reduction $\{i, -k\}$ and the set $\{7 + 3j, 7 - i + 2j + 2k, 7 - 3k\}$ is reducible with reduction $\{3j, -i + 2j + 2k, -3k\}$. On the other hand, the set $\{6 - 4k, 4j\}$ is not reducible and $\{2i + 2k, 2j - 2k\}$ is reducible but not reduced. As the next proposition shows, a reducible set is precisely a set where every element has the same minimal polynomial.
Proposition 7.3.4.

(i) A reduced subset of \( \mathbb{Z}Q \) must be non-empty and finite.

(ii) Let \( S \) be a subset of \( \mathbb{Z}Q - \mathbb{Z} \). Then, \( S \) is reducible if and only if every element of \( S \) has the same minimal polynomial.

(iii) Assume \( S \) is a reducible subset of \( \mathbb{Z}Q \), and let \( T \) be the reduction of \( S \). Then, \( S \) is a ringset if and only if \( T \) is a ringset.

Proof. (i) By condition 3) in the definition above, a reduced subset of \( \mathbb{Z}Q \) must be non-empty. Also, for any positive integer \( n \), there are only finitely many elements of \( \mathbb{Z}Q \) with norm \( n \); thus, given any monic quadratic polynomial \( f(x) \in \mathbb{Z}[x] \), there are only finitely many elements of \( \mathbb{Z}Q \) that have \( f(x) \) as a minimal polynomial. Thus, by condition 1), a reduced subset of \( \mathbb{Z}Q \) must be finite.

(ii) \((\Rightarrow)\) Assume that \( S \) is reducible with reduction \( T \). Then, there exist \( a, m \in \mathbb{Z} \), \( m \neq 0 \), such that \( S = mT + a \). Since \( T \) is reduced, every element of \( T \) has the same minimal polynomial; equivalently, every element of \( T \) has the same norm \( n \) and constant coefficient \( A \), and we know that \( A = 0 \). So, every element of \( S \) has norm \( a^2 + m^2 n \) and constant coefficient \( a \). Thus, every element of \( S \) solves the polynomial \( x^2 - 2ax + a^2 + m^2 n \).

\((\Leftarrow)\) Since every element of \( S \) has the same minimal polynomial, there exists \( a \in \mathbb{Z} \) such that each element of \( S \) has constant coefficient equal to \( a \). Let \( m \) be the largest positive integer such that \( S - a \subseteq (m) \) in \( \mathbb{Z}Q \), and let \( T = \{ \frac{\alpha - a}{m} | \alpha \in S \} \). Then, \( T \) is reduced and \( S = mT + a \), so we are done.
(iii) This follows from Theorem 7.2.6.

If we define a relation $\sim$ on $\mathbb{Z}Q$ by $\alpha \sim \beta \iff \min_{\alpha}(x) = \min_{\beta}(x)$, then it is not hard to see that $\sim$ is an equivalence relation on $\mathbb{Z}Q$. Thus, any subset of $\mathbb{Z}Q - \mathbb{Z}$ may be expressed as the disjoint union of reducible subsets. It seems plausible that if we can characterize which reducible subsets are ringsets, then we can obtain information about arbitrary subsets of $\mathbb{Z}Q$. Necessary and sufficient conditions for reducible sets to be ringsets are given by Theorem 7.4.6, and these conditions will be extended to any finite subset of $\mathbb{Z}Q$ in Section 7.5. However, finding a theorem that works for general subsets of $\mathbb{Z}Q$ is an open problem.

The classification given in Theorem 7.4.6 depends on the following numerical quantity.

**Definition 7.3.5.** For any subset $S \subseteq \mathbb{Z}Q$, we define the integer $\Gamma(S)$ to be $\Gamma(S) = \gcd \left( \{ N(\alpha - \beta) \}_{\alpha, \beta \in S} \right)$. To avoid confusion with the definition of $\gcd(\{0\})$, when $S$ is a singleton set we take $\Gamma(S) = 0$.

**Remark.** When $S$ is reduced and $|S| > 1$, taking distinct elements $\alpha = bi + cj + dk$ and $\beta = yi + zj + wk$ in $S$ and computing $N(\alpha - \beta)$ gives $N(\alpha - \beta) = 2N(\alpha) - 2(by + cz + dw)$. Thus, when $S$ is reduced, $\Gamma(S)$ is always an even number.

As we shall see, when $S$ is reduced we can often use $\Gamma(S)$ to determine whether or not $S$ is a ringset (although $\Gamma(S)$ falls just short of giving us a complete classification). The most interesting result is the following.

**Theorem 7.3.6.** Let $S$ be a reduced subset of $\mathbb{Z}Q$. If $S$ is a ringset, then $\Gamma(S)$ equals $2, 4, \text{ or } 8$. 

120
The proof of Theorem 7.3.6 is involved and requires several intermediate theorems and lemmas. It is given after Lemma 7.3.12. To illustrate the flavor of the proof and to motivate our subsequent results, we work through an example with a reduced three-element subset of \( \mathbb{Z}Q \).

**Example 7.3.7.** Let \( S = \{3i + 4j + 12k, -12i + 5k, -12i + 5j\} \); for convenience, let \( \alpha = 3i + 4j + 12k, \beta = -12i + 5k, \) and \( \gamma = -12i + 5j \). Then, \( S \) is reduced, and we compute that

\[
\alpha - \beta = 15i + 4j + 7k, \text{ of norm } 290, \\
\alpha - \gamma = 15i - j + 12k, \text{ of norm } 370, \text{ and} \\
\beta - \gamma = -5j + 5k, \text{ of norm } 50,
\]

so \( \Gamma(S) = 10 \). Furthermore, notice that

\[
\beta - \alpha \equiv \gamma - \alpha \equiv -4j - 2k \mod 5.
\]

So, letting \( f(x) = (4j + 2k)(x - \alpha) \), we have

\[
f(\alpha) \equiv 0 \mod 5, \\
f(\beta) \equiv N(\beta - \alpha) \equiv 0 \mod 5, \text{ and} \\
f(\gamma) \equiv N(\gamma - \alpha) \equiv 0 \mod 5.
\]

Thus, \( \frac{f(x)}{5} \) is a non-trivial element of \( \text{Int}(S, \mathbb{Z}Q) \). Now, if \( \text{Int}(S, \mathbb{Z}Q) \) were a ring, then \( g(x) = \frac{f(x)}{5}(x - j) \) would be in \( \text{Int}(S, \mathbb{Z}Q) \). However, we can compute that

\[
g(\alpha) = \frac{-12 + 24i - 48j + 96k}{5}, \text{ which is not in } \mathbb{Z}Q.
\]

Therefore, we conclude that \( \text{Int}(S, \mathbb{Z}Q) \) is not a ring.

Two things power this example. The first is the fact that \( 4j + 2k \) will kill all three of \( \alpha - \beta, \alpha - \gamma, \) and \( \beta - \gamma \) modulo 5; this allows us to determine that the
polynomial $\frac{f(x)}{5}$ is in Int$(S, \mathbb{Z}Q)$. Secondly, to demonstrate that Int$(S, \mathbb{Z}Q)$ is not a ring, it sufficed to multiply $\frac{f(x)}{5}$ by the “nice” polynomial $x - j$. As we shall see, neither of these developments was an accident. Given a reduced subset $S$ and an odd prime $p$ that divides $\Gamma(S)$, we will prove (essentially) that there always exists a linear polynomial $f(x) \in \mathbb{Z}Q[x]$ such that $\frac{f(x)}{p} \in$ Int$(S, \mathbb{Z}Q)$, and furthermore that at least one of $\frac{f(x)}{p}(x - i), \frac{f(x)}{p}(x - j)$, or $\frac{f(x)}{p}(x - k)$ is not in Int$(S, \mathbb{Z}Q)$. A similar technique will work when $\Gamma(S)$ is a power of 2 greater than 8.

The process of proving Theorem 7.3.6 begins with the following proposition.

**Proposition 7.3.8.** Let $S \subseteq \mathbb{Z}Q$ be a reduced set. Assume that $S$ is a ringset. Then, for any odd prime $p$, Muff$_{\mathbb{Z}Q/(p)}(S)$ contains no linear polynomials.

**Proof.** Let $p$ be an odd prime, and let $R = \mathbb{Z}Q/(p)$. Let $\gamma, \delta \in R$ be such that $f(x) = \gamma x + \delta \in$ Muff$_{R}(S)$. It suffices to show that $\gamma \equiv 0 \pmod{p}$, since this will force $\delta \equiv 0$ and consequently $f(x) = 0$.

Now, for all $\alpha, \beta \in S$, we have $0 \equiv f(\alpha) - f(\beta) \equiv \gamma(\alpha - \beta) \pmod{p}$. This means that for all $\alpha \in S$, the polynomial $\gamma(x - \alpha) \in$ Muff$_{R}(S)$. Since $S$ is reduced, there exists $\beta = yi + zj + wk \in S$ such that $\beta \notin (p)$ in $\mathbb{Z}Q$. Then, $\gamma(x - \beta) \in$ Muff$_{R}(S)$, and since $S$ is a ringset, we know that Muff$_{R}(S)$ is an ideal of $R[x]$. Hence, the following polynomials are in Muff$_{R}(S)$:

$$g_1(x) = \gamma(x - \beta)(x - i),$$
$$g_2(x) = \gamma(x - \beta)(x - j),$$
and
$$g_3(x) = \gamma(x - \beta)(x - k).$$
Evaluating these polynomials at $\beta$ yields

\[ g_1(\beta) \equiv \gamma(\beta i - i\beta) \equiv 2\gamma(wj - zk), \]
\[ g_2(\beta) \equiv \gamma(\beta j - j\beta) \equiv 2\gamma(-wi + yk), \text{ and} \]
\[ g_3(\beta) \equiv \gamma(\beta k - k\beta) \equiv 2\gamma(zi - yj). \]

Since $p$ is odd and $g_1(x), g_2(x), \text{ and } g_3(x)$ are all in $\text{Muff}_R(S)$, the above equivalences imply that

\[ \gamma(wj - zk) \equiv 0, \quad \gamma(-wi + yk) \equiv 0, \quad \text{and} \quad \gamma(zi - yj) \equiv 0. \]

Thus,

\[ 0 \equiv \gamma(wj - zk)(wj - zk) \equiv \gamma(z^2 + w^2), \]
\[ 0 \equiv \gamma(-wi + yk)(-wi + yk) \equiv \gamma(y^2 + w^2), \text{ and} \]
\[ 0 \equiv \gamma(zi - yj)(zi - yj) \equiv \gamma(y^2 + z^2). \]

Now, suppose that $y^2 + z^2$, $y^2 + w^2$, and $z^2 + w^2$ are all congruent to 0 mod $p$. Then,

\[ 0 \equiv (y^2 + z^2) - (y^2 + w^2) \equiv z^2 - w^2, \]

so we get

\[ 0 \equiv z^2 + w^2 + z^2 - w^2 \equiv 2z^2, \]

from which we conclude that $z \equiv 0$. Similarly, $y \equiv w \equiv 0$. But then, $\beta = yi + zj + wk \in (p)$ in $\mathbb{Z}Q$, a contradiction. Thus, at least one of $y^2 + z^2$, $y^2 + w^2$, or $z^2 + w^2$ is non-zero, and hence a unit, mod $p$. By the equivalences in ($\ast$), we must have $\gamma \equiv 0$ mod $p$, and we are done. \qed

Proposition 7.3.8 generalizes the second major step—that of causing a problem by multiplying a suitable polynomial by $x - i$, $x - j$, or $x - k$—in Example 7.3.7. What
remains is to determine what the “suitable” polynomial is, and doing that requires a couple of lemmas.

**Lemma 7.3.9.** Let $p$ be an odd prime, and let $R = \mathbb{Z}Q/(p)$. Let $\mathfrak{N} = \{\alpha \in R \mid \alpha \text{ is nilpotent}\}$. Then,

(i) $|\mathfrak{N}| = p^2$

(ii) $\mathfrak{N}$ is not closed under addition

*Proof.* (i) We exploit the isomorphism $R \cong M_2(\mathbb{F}_p)$ (see Corollary 1.4.2). A matrix in $M_2(\mathbb{F}_p)$ is nilpotent if and only if both its trace and determinant are 0. Assume that $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{F}_p)$ is nilpotent. Then, we must have $d = -a$ and $0 = \det(A) = a^2 - bc$.

From here, we have two cases. If $b \neq 0$, then to ensure that $a^2 - bc = 0$ we must have $c = b^{-1}a^2$. In this situation, we have $p - 1$ choices for $b$ and $p$ choices for $a$, giving $(p - 1)p$ different nilpotent matrices. If $b = 0$, then $a = 0$. In this case, we have $p$ choices for $c$, yielding an additional $p$ nilpotent matrices. These two cases exhaust all the possibilities for $A$, so we have a total of $(p - 1)p + p = p^2$ nilpotent matrices in $M_2(\mathbb{F}_p)$. It follows that $|\mathfrak{N}| = p^2$.

(ii) Let $\alpha \in \mathfrak{N} - \{0\}$. Then, by Proposition 4.2.1, $\alpha \equiv bi + cj + dk$ for some $b, c, d \in \mathbb{Z}/p\mathbb{Z}$. Since $\alpha \neq 0$, at least one of $b, c$, or $d$ is not congruent to 0 mod $p$. WLOG, assume that $b \neq 0$. Now, $-i\alpha i$ is also in $\mathfrak{N}$, but $\alpha + (-i\alpha i) \equiv 2bi$ is a unit mod $p$. Hence, $\alpha + (-i\alpha i) \not\in \mathfrak{N}$, and $\mathfrak{N}$ is not closed under addition. $\square$
In the next lemma and associated theorem, we will use the following notation: for any \( \alpha \in \mathbb{Z}_p \), we let \( \langle \alpha \rangle = \{ n\alpha \mid n \in \mathbb{Z}/p\mathbb{Z} \} \). That is, \( \langle \alpha \rangle \) is the cyclic subgroup generated by \( \alpha \) within the additive group \( \mathbb{Z}_p \).

**Lemma 7.3.10.** Let \( p \) be an odd prime, and let \( \alpha \) and \( \beta \) be nilpotent elements of \( \mathbb{Z}_p \). Assume that \( \alpha - \beta \) is also nilpotent. Then, either \( \alpha \in \langle \beta \rangle \) or \( \beta \in \langle \alpha \rangle \).

**Proof.** Write \( \alpha \equiv bi + cj + dk \) and \( \beta \equiv yi + zj + wk \). Then, since \( \alpha, \beta \) and \( \alpha - \beta \) are all nilpotent, we have \( N(\alpha) \equiv b^2 + c^2 + d^2 \equiv 0 \), \( N(\beta) \equiv y^2 + z^2 + w^2 \equiv 0 \), and

\[
0 \equiv N(\alpha - \beta) \\
\equiv (b - y)^2 + (c - z)^2 + (d - w)^2 \\
\equiv b^2 + c^2 + d^2 + y^2 + z^2 + w^2 - 2(by + cz + dw) \\
\equiv -2(by + cz + dw) .
\]

Now, for all \( n, m \in \mathbb{Z}/p\mathbb{Z} \), \( n\alpha + m\beta \) has constant coefficient equivalent to 0, and

\[
N(n\alpha + m\beta) \equiv (nb + my)^2 + (nc + mz)^2 + (nd + mw)^2 \\
\equiv n^2(b^2 + c^2 + d^2) + m^2(y^2 + z^2 + w^2) + 2nm(by + cz + dw) \\
\equiv 0,
\]

so \( n\alpha + m\beta \) is also nilpotent.

Let \( G = \{ n\alpha + m\beta \mid n, m \in \mathbb{Z}/p\mathbb{Z} \} \) be the additive subgroup of \( \mathbb{Z}_p \) generated by \( \alpha \) and \( \beta \). Then, by the above, each element of \( G \) is nilpotent. By Lemma 7.3.9 part (i), \(|G| \leq p^2\); furthermore, \(|G| \) divides \(|\mathbb{Z}_p| = p^4\). However, \( G \) is closed under addition, so by Lemma 7.3.9 part (ii), \(|G| \neq p^2\). Thus, either \( G = \{0\} \) or \(|G| = p\).
If $G = \{0\}$, then $\alpha \equiv \beta \equiv 0$; if $|G| = p$, then $G$ is cyclic and either $G = \langle \alpha \rangle$ or $G = \langle \beta \rangle$. In any of these cases, we have reached the desired conclusion, so we are done.

We can now prove that $\Gamma(S)$ must be a power of 2 in order for $\text{Int}(S, \mathbb{Z}Q)$ to be a ring.

**Theorem 7.3.11.** Let $S$ be a reduced subset of $\mathbb{Z}Q$. If $S$ is a ringset, then $\Gamma(S)$ must be a power of 2.

**Proof.** We prove the contrapositive. The only way that $\Gamma(S)$ can be 0 is if $S$ is a singleton set, in which case $\text{Int}(S, \mathbb{Z}Q)$ is not a ring by Theorem 7.3.1. So, assume that $|S| > 1$. Then, by the remark following Definition 7.3.5, $\Gamma(S)$ is a positive even number. We are assuming that $\Gamma(S)$ is not a power of 2, so let $p$ be an odd prime that divides $\Gamma(S)$. We want to show that $S$ is not a ringset. Let $R = \mathbb{Z}Q/(p)$. By Proposition 7.3.8, it suffices to show that $\text{Muff}_R(S)$ contains a linear polynomial.

Let $D = \{\alpha - \beta \mid \alpha, \beta \in S\}$, the set of differences of elements of $S$. Since $S$ is reduced and $p \mid \Gamma(S)$, each element of $D$ is nilpotent in $R$. Next, fix $\beta_0 \in S$ and let $D_0 = \{\alpha - \beta_0 \mid \alpha \in S\} \subseteq D$. Note that since $|S| > 1$, $D_0 \neq \{0\}$.

Next, let $\pi : \mathbb{Z}Q \to R$ be the canonical quotient map. We will use the following:

**Claim:** for each non-empty subset $T \subseteq \pi(D_0)$, there exists $\gamma \in T$ such that $T \subseteq \langle \gamma \rangle$

**Proof of Claim:** We proceed by induction on $|T|$. If $|T| = 1$, then $T = \{\gamma\} \subseteq \langle \gamma \rangle$ for some $\gamma \in \pi(D_0)$ and we are done. So, assume that $|T| > 1$ and that the Claim is true for any subset of $\pi(D_0)$ of cardinality less than $|T|$. Let $\delta \in T$. By induction, there exists $\varepsilon \in T - \{\delta\}$ such that $T - \{\delta\} \subseteq \langle \varepsilon \rangle$. Now, $\delta$ and $\varepsilon$ are elements of
\[\pi(D),\] so both \(\delta\) and \(\varepsilon\) are nilpotent in \(R\). Furthermore, there exist \(\delta_0, \varepsilon_0 \in S\) such that \(\delta \equiv \delta_0 - \beta_0\) and \(\varepsilon \equiv \varepsilon_0 - \beta_0\). So, \(\delta - \varepsilon \equiv \delta_0 - \varepsilon_0\) and \(\delta_0 - \varepsilon_0 \in D\), so \(\delta - \varepsilon\) is also nilpotent. By Lemma 7.3.10, either \(\delta \in \langle \varepsilon \rangle\) or \(\varepsilon \in \langle \delta \rangle\). Thus, either \(T \subseteq \langle \delta \rangle\) or \(T \subseteq \langle \varepsilon \rangle\). This proves the Claim.

Now, if \(\pi(D_0) = \{0\}\) (i.e. every element of \(D_0\) is congruent to 0 mod \(p\)), then the polynomial \(x - \beta_0\) is in \(\text{Muff}_R(S)\), and we are done. So, assume that \(\pi(D_0) \neq \{0\}\), i.e. some element of \(D_0\) is non-zero in \(R\), and consequently \(|\pi(D_0)| > 1\). Applying the Claim with \(T = \pi(D_0)\), we have \(\pi(D_0) \subseteq \langle \gamma \rangle\) for some \(\gamma \in \pi(D_0)\). Let \(f(x) = \gamma(x - \beta_0) \in R[x]\). Note that \(\gamma\) is non-zero (since \(\pi(D_0) \neq \{0\}\)) and nilpotent (since \(\gamma \in \pi(D_0) \subseteq \pi(D)\)), so \(f(x) \neq 0\) in \(R[x]\) and \(N(\gamma) \equiv N(\gamma) \equiv 0\).

We know that, for each \(\alpha \in S\), the residue of \(\alpha - \beta_0\) modulo \(p\) is in \(\pi(D_0)\). But, \(\pi(D_0) \subseteq \langle \gamma \rangle\), so for each \(\alpha \in S\) there exists \(n_\alpha \in \mathbb{Z}/p\mathbb{Z}\) such that \(\alpha - \beta_0 \equiv n_\alpha \gamma\). Thus, for each \(\alpha \in S\),

\[f(\alpha) \equiv \gamma(\alpha - \beta_0) \equiv \gamma n_\alpha \gamma \equiv n_\alpha N(\gamma) \equiv 0,\]

so \(f(x)\) is a linear polynomial in \(\text{Muff}_R(S)\). Therefore, by Proposition 7.3.8, \(S\) is not a ringset. \(\square\)

Proving Theorem 7.3.11 is the most difficult part in showing that Theorem 7.3.6 is true. From here, things are fairly straightforward.

**Lemma 7.3.12.** Let \(S\) be a reduced subset of \(\mathbb{Z}Q\). Then, for all \(\alpha \in S\), some coefficient of \(\alpha\) is odd.

**Proof.** Suppose there exists \(\alpha \in S\) such that all coefficients of \(\alpha\) are even. Then, \(N(\alpha) \equiv 0\) mod 4. Let \(\beta \in S\). Since \(S\) is reduced, \(N(\beta) \equiv N(\alpha) \equiv 0\) mod 4. But
then, $N(\beta) \equiv 0 \mod 4$ is a sum of three squares, implying that all coefficients of $\beta$ are even. Since $\beta$ was an arbitrary element of $S$, we conclude that $S \subseteq (2)$ in $\mathbb{Z}Q$, a contradiction. Therefore, every element of $S$ has some coefficient that is odd.

We are now ready for the proof of Theorem 7.3.6.

**Proof of Thm. 7.3.6:**

Assume that $S$ is a ringset. By Theorem 7.3.11, $\Gamma(S)$ must be a power of 2. Suppose by way of contradiction that $\Gamma(S)$ is greater than 8. Then, for all $\alpha, \beta \in S$, the norm of $\alpha - \beta$ is divisible by 16. Since $N(\alpha - \beta)$ is a sum of three squares, Lemma 5.1.3 tells us that each coefficient of $\alpha - \beta$ is divisible by 4. Thus, for any $\beta \in S$, the polynomial $x - \beta/4 \in \text{Int}(S, \mathbb{Z}Q)$.

Now, fix $\beta = yi + zj + wk \in S$ and let $f(x) = \frac{x - \beta}{4}$. By Lemma 7.3.12, some coefficient of $\beta$ must be odd. WLOG, assume that $y$ is odd, and let $g(x) = f(x)(x - j)$ (if either $z$ or $w$ were odd, we would take $g(x) = f(x)(x - i)$). Then, employing (7.3.2) shows that $g(\beta) = \frac{-2wi + 2wk}{4}$, which is not an element of $\mathbb{Z}Q$ because $y$ is odd. Thus, $g(x) \notin \text{Int}(S, \mathbb{Z}Q)$, which contradicts the fact that $\text{Int}(S, \mathbb{Z}Q)$ is a ring. Therefore, $\Gamma(S)$ must be 2, 4, or 8. □

So far, we have only given negative results about whether $S$ is a ringset. The next theorem shows that if $S$ is reduced and $\Gamma(S) = 2$ or 4, then $S$ is a ringset. Unfortunately, the case where $\Gamma(S) = 8$ turns out to be ambiguous. We will study that situation in more detail in Section 7.4.

**Theorem 7.3.13.**
(i) Let $S \subseteq \mathbb{Z}_Q$ be such that all elements of $S$ have the same minimal polynomial. If $\Gamma(S) = 2$, then $S$ is a ringset.

(ii) Let $S$ be a reduced subset of $\mathbb{Z}_Q$. If $\Gamma(S) = 4$, then $S$ is a ringset.

Proof. (i) Let $n > 1$, let $R_n = \mathbb{Z}_Q/(n)$, and let $f \in \text{Muff}_{R_n}(S)$. Since all elements of $S$ share the same minimal polynomial, there exist $\gamma, \delta \in \mathbb{Z}_Q$ such that for all $\alpha \in S$, $f(\alpha) \equiv \gamma \alpha + \delta \mod n$. So,

$$\text{for all } \alpha, \beta \in S, \quad 0 \equiv f(\alpha) - f(\beta) \equiv \gamma(\alpha - \beta) \mod n. \quad (*)$$

Next, since $\Gamma(S) = 2$, there exist $\alpha_1, \alpha_2, \ldots, \alpha_t, \beta_1, \beta_2, \ldots, \beta_t \in S$ such that

$$\gcd(N(\alpha_1 - \beta_1), N(\alpha_2 - \beta_2), \ldots, N(\alpha_t - \beta_t)) = 2.$$

So, there exist $A_1, A_2, \ldots, A_t \in \mathbb{Z}$ such that

$$2 = A_1 N(\alpha_1 - \beta_1) + A_2 N(\alpha_2 - \beta_2) + \cdots + A_t N(\alpha_t - \beta_t).$$

Hence,

$$2\gamma \equiv A_1 \gamma N(\alpha_1 - \beta_1) + A_2 \gamma N(\alpha_2 - \beta_2) + \cdots + A_t \gamma N(\alpha_t - \beta_t)$$

$$\equiv A_1 \gamma (\alpha_1 - \beta_1)(\overline{\alpha_1 - \beta_1}) + A_2 \gamma (\alpha_2 - \beta_2)(\overline{\alpha_2 - \beta_2}) + \cdots + A_t \gamma (\alpha_t - \beta_t)(\overline{\alpha_t - \beta_t})$$

$$\equiv 0, \quad \text{by } (*).$$

Now, for any $\alpha \in S$ and any $\beta \in \text{Konj}(\alpha)$, there exists $\varepsilon \in \mathbb{Z}_Q$ such that $\alpha - \beta = 2\varepsilon$. Thus, modulo $n$ we have

$$-f(\beta) \equiv f(\alpha) - f(\beta) \equiv \gamma(\alpha - \beta) \equiv 2\gamma \varepsilon \equiv 0.$$

Therefore, $S$ is a ringset by Corollary 7.1.6.
(ii) Assume that $\Gamma(S) = 4$. By Corollary 7.1.6, to show that $S$ is a ringset, it suffices to show that $\text{Muff}_{\mathbb{Z}Q/(p^e)}(S)$ is an ideal of $(\mathbb{Z}Q/(p^e))[x]$ for all prime powers $p^e$. So, let $p$ be any prime, and let $e > 0$. Let $R = \mathbb{Z}Q/(p^e)$, and let $f \in \text{Muff}_R(S)$. Since $S$ is reduced, there exist $\gamma, \delta \in \mathbb{Z}Q$ such that $f(\alpha) \equiv \gamma \alpha + \delta \mod p^e$ for all $\alpha \in S$. We have two cases to consider.

**Case 1: $p$ is odd**

Since $\Gamma(S) = 4$, there exist $\alpha, \beta \in S$ such that $N(\alpha - \beta)$ is not divisible by $p$. So, $\alpha - \beta$ is a unit mod $p^e$. Hence, having $0 \equiv f(\alpha) - f(\beta) \equiv \gamma(\alpha - \beta) \mod p^e$ implies that $\gamma \equiv 0 \mod p^e$. Thus, for all $\alpha' \in S$ and all $\beta' \in \text{Konj}(\alpha')$,

$$-f(\beta') \equiv f(\alpha') - f(\beta') \equiv \gamma(\alpha' - \beta') \equiv 0 \mod p^e.$$  By Theorem 7.1.5, it follows that $\text{Muff}_R(S)$ is an ideal of $R[x]$.

**Case 2: $p = 2$**

Since $\Gamma(S) = 4$, there exist $\alpha, \beta \in S$ such that $N(\alpha - \beta) = 4n$, where $n$ is odd. Since $S$ is reduced, $N(\alpha - \beta)$ is a sum of three squares. But, $N(\alpha - \beta) \equiv 0 \mod 4$, so each coefficient of $\alpha - \beta$ must be even. Thus, there exists $\varepsilon \in \mathbb{Z}Q$ such that $\alpha - \beta = 2\varepsilon$, and we must have $N(\varepsilon) = n$. Hence, $\varepsilon$ is invertible mod $2^e$.

Now, $f(\alpha) - f(\beta) \equiv \gamma(\alpha - \beta) \equiv 2\gamma\varepsilon \mod 2^e$, implying that $2\gamma \equiv 0$. Taking $\alpha' \in S$ and $\beta' \in \text{Konj}(\alpha')$, there exists $\varepsilon' \in \mathbb{Z}Q$ such that $\alpha' - \beta' = 2\varepsilon'$, and working mod $2^e$ we get

$$-f(\beta') \equiv f(\alpha') - f(\beta') \equiv \gamma(\alpha' - \beta') \equiv 2\gamma\varepsilon' \equiv 0.$$
Hence, we once again conclude that $\text{Muff}_R(S)$ is an ideal of $R[x]$.

There are no more cases to consider, so the proof of part (ii) of the theorem is complete. 

7.4 The Case $\Gamma(S) = 8$ and the Classification of Reducible Subsets

As the next example demonstrates, when the reduced set $S$ satisfies $\Gamma(S) = 8$, $S$ may or may not be a ringset.

Example 7.4.1. Let $S = \{i + j + k, i - j - k, -i + j - k, -i - j + k\}$. Then, it is easy to see that $S$ is reduced and $\Gamma(S) = 8$. Furthermore, $S = \text{Konj}_{\mathbb{Q}}(i + j + k)$, so $S$ is a ringset by Theorem 7.2.1.

Next, let $T = \{2i + 3j + 4k, -5j - 2k, -2i + 3j + 4k\}$. Then, $T$ is reduced, and one may verify that $\Gamma(T) = 8$. Letting $\alpha = 2i + 3j + 4k$, $\beta = -5j - 2k$, and $\gamma = -2i + 3j + 4k$, we have

$$
\alpha - \beta \equiv 2i + 2k \equiv \gamma - \beta \mod 4,
$$

so $f(x) = \frac{(i + k)(x - \beta)}{4} \in \text{Int}(S, \mathbb{ZQ})$. Let $g(x) = f(x)(x - i)$. Then, evaluation at $\beta$ yields $g(\beta) = \frac{-10 + 4i - 10j - 4k}{4} \notin \mathbb{ZQ}$, so $\text{Int}(S, \mathbb{ZQ})$ is not a ring.

We shall give necessary and sufficient conditions under which a reduced set $S$ with $\Gamma(S) = 8$ is a ringset, but the conditions are somewhat obtuse and unenlightening. Nevertheless, the first step is to investigate properties of $S$ when $\Gamma(S) = 8$.

Lemma 7.4.2. Let $S$ be a reduced subset of $\mathbb{ZQ}$ such that $\Gamma(S) = 8$. Let $D = \{\alpha - \beta \mid \alpha, \beta \in S\}$. Then,
(i) for all $\delta \in D$, every coefficient of $\delta$ must be even.

(ii) there exists $\delta \in D$ such that some coefficient of $\delta$ is congruent to $2 \mod 4$.

(iii) for all $\delta \in D$, at least two coefficients of $\delta$ are congruent to $0 \mod 4$.

(iv) for all $\delta \in D$, either exactly two coefficients of $\delta$ are congruent to $0 \mod 4$, or every coefficient of $\delta$ is congruent to $0 \mod 4$; that is, for all $\delta \in D$, the residue of $\delta \mod 4$ lies in $\{0, 2i + 2j, 2i + 2k, 2j + 2k\}$.

(v) there exists $\delta \in D$ such that exactly two coefficients of $\delta$ are congruent to $0 \mod 4$; that is, the residue of $\delta \mod 4$ lies in $\{2i + 2j, 2i + 2k, 2j + 2k\}$.

Proof. First, note that by the way we defined $D$, we have $\Gamma(S) = \gcd(\{N(\delta) \mid \delta \in D\})$. Second, since $S$ is reduced, the constant coefficient of every element of $D$ is equal to 0, so for all of the following proofs, it suffices to focus on the coefficients of $i, j$, and $k$.

(i) Since $S$ is reduced and $\Gamma(S) = 8$, the norm of any element of $D$ is a sum of three squares that is divisible by 4. Hence, each coefficient of every element of $D$ must be even.

(ii) Suppose not. Then, each $\delta \in D$ would lie in $(4)$ in $\mathbb{Z}Q$, and thus 16 would divide $N(\delta)$ for all $\delta \in D$. But then, $16 | \Gamma(S)$, a contradiction.

(iii) Suppose not. Then, there exists $\delta \in D$ such that $N(\delta) \equiv 4 \mod 8$, implying that $\Gamma(S) \neq 8$. 
(iv) By (iii), for each \( \delta \in D \) at least two coefficients of \( \delta \) are congruent to 0 mod 4. If there exists \( \delta \in D \) such that exactly three coefficients of \( \delta \) are congruent to 0 mod 4, then \( N(\delta) \equiv 4 \mod 8 \), which forces \( \Gamma(S) \neq 8 \).

(v) Apply (ii) and (iv).

The next lemma gives one final property of a reduced set \( S \) with \( \Gamma(S) = 8 \). It was not included in the previous lemma because the statement and proof are longer.

**Lemma 7.4.3.** Let \( S \) be a reduced subset of \( \mathbb{Z}Q \) such that \( \Gamma(S) = 8 \). Let \( p \) be a prime, let \( e > 1 \), let \( R = \mathbb{Z}Q/(p^e) \), let \( f \in \text{Muff}_R(S) \), and let \( \gamma_1, \gamma_0 \in \mathbb{Z}Q \) be such that for all \( \alpha \in S \), \( f(\alpha) \equiv \gamma_1 \alpha + \gamma_0 \mod p^e \). Then, \( 4\gamma_1 \equiv 0 \mod p^e \).

**Proof.** First, note that \( \gamma_1 \) and \( \gamma_0 \) as given in the statement of the lemma exist because \( S \) is reduced. Let \( D = \{ \alpha - \beta \mid \alpha, \beta \in S \} \). Note that for any \( \delta = \alpha - \beta \in D \), we have

\[
0 \equiv f(\alpha) - f(\beta) \equiv \gamma_1 \delta \mod p^e.
\]

Now, if \( p \) is odd, then \( p \nmid \Gamma(S) \), so there exists \( \delta \in D \) such that \( p \nmid N(\delta) \). Hence,

\[
0 \equiv \gamma_1 \delta \equiv \gamma_1 \delta \equiv \gamma_1 N(\delta),
\]

and \( N(\delta) \) is invertible mod \( p^e \), so we must have \( \gamma_1 \equiv 0 \).

So, assume that \( p = 2 \). Since \( \Gamma(S) = 8 \), there exists \( \varepsilon \in D \) such that \( N(\varepsilon) = 8n \), where \( n \) is an odd number (if no such \( \varepsilon \) exists, then \( 16 \mid \Gamma(S) \), which we know to be false). By part (i) of Lemma 7.4.2, there exists \( \varepsilon' \in \mathbb{Z}Q \) such that \( \varepsilon = 2\varepsilon' \), and we must have \( N(\varepsilon') = 2n \). Thus, modulo \( p^e \), we have

\[
0 \equiv 4\gamma_1 \varepsilon \equiv 2\gamma_1 \varepsilon' \equiv 2\gamma_1 \varepsilon' \equiv 4n\gamma_1,
\]

and \( 4\gamma_1 \) must be equivalent to 0 because \( n \) is invertible mod \( p^e \). \( \square \)
We will prove one more lemma before proceeding to the classification theorem of those reduced sets $S$ with $\Gamma(S) = 8$ that are ringsets. This lemma should really be part of the proof of that theorem, but the proof of the lemma is long enough that we deal with it separately.

**Lemma 7.4.4.** Let $S$ be a reduced subset of $\mathbb{Z}Q$ such that $\Gamma(S) = 8$. Let $D = \{\alpha - \beta \mid \alpha, \beta \in S\}$. Assume there exist $\delta, \varepsilon \in D$ such that the residues of $\delta$ and $\varepsilon \mod 4$ lie in $\{2i + 2j, 2i + 2k, 2j + 2k\}$, but $\delta \not\equiv \varepsilon \mod 4$. Then, for each $\alpha = bi + cj + dk \in S$, the coefficients $b, c, \text{ and } d$ are all odd.

**Proof.** Let $\pi : \mathbb{Z}Q \rightarrow \mathbb{Z}Q/(4)$ be the standard quotient map. By Lemma 7.4.2 part (iv), $\pi(D) \subseteq \{0, 2i + 2j, 2i + 2k, 2j + 2k\}$. Since $0 \in D$, the residue of $0 \mod 4$ lies in $\pi(D)$; hence, the conditions on $\delta$ and $\varepsilon$ imply that $|\pi(D)| > 2$.

Now, let $\alpha = bi + cj + dk \in S$. By Lemma 7.3.12, at least one of $b, c, \text{ or } d$ is odd. We have two cases to consider, and we will derive a contradiction in each one.

**Case 1:** exactly one of $b, c$ or $d$ is even

WLOG, assume that $d$ is even and $b$ and $c$ are both odd. Then, $d = 2E$ for some $E \in \mathbb{Z}$. Let $\beta = yi + zj + wk \in S$. Then, we have $\alpha - \beta \in D$, so Lemma 7.4.2 part (i) tells us that $b - y, c - z$ and $d - k$ are all even. Hence, $y$ and $z$ must be odd and $w$ must be even; let $W \in \mathbb{Z}$ be such that $w = 2W$.

Next, suppose that $E \not\equiv W \mod 2$. Since $N(\alpha) = N(\beta)$, we have $b^2 + c^2 + d^2 = y^2 + z^2 + w^2$, and so $b^2 + c^2 + 4E^2 = y^2 + z^2 + 4W^2$. The terms $b^2, c^2, y^2, \text{ and } z^2$ are all congruent to $1 \mod 8$ (because $b, y, z, \text{ and } w$ are all odd), so $4E^2 \equiv 4W^2 \mod 8$. However, one of $E$ or $W$ is odd and the other is even. Thus, one of $4E^2$ or $4W^2$ is
congruent to 4 mod 8, and the other is congruent to 0 mod 8. This is a contradiction, so we must have \( E \equiv W \) mod 2.

Since \( E \equiv W \) mod 2, we have \( 2E \equiv 2W \) mod 4. So, the coefficient of \( k \) in \( \alpha - \beta \) is congruent to 0 mod 4. Hence, by Lemma 7.4.2 part (iv), the residue of \( \alpha - \beta \) mod 4 lies in \{0, 2i + 2j\}. Since \( \beta \in S \) was arbitrary, for any \( \beta_1, \beta_2 \in S \) we have, modulo 4,

\[
\beta_1 - \beta_2 \equiv (\beta_1 - \alpha) - (\beta_2 - \alpha) \in \{0, 2i + 2j\}.
\]

But then, \( \pi(D) \subseteq \{0, 2i + 2j\} \), which is a contradiction.

**Case 2:** exactly two of \( b, c \) or \( d \) are even

WLOG, assume that \( c \) and \( d \) are even and \( b \) is odd. Then, there exist \( C, E \in \mathbb{Z} \) such that \( c = 2C \) and \( d = 2E \). Let \( \beta = yi + zj + wk \in S \). Applying Lemma 7.4.2 part (i) as in Case 1, we see that \( y \) is odd but \( z \) and \( w \) must be even; so we may write \( z = 2Z \) and \( w = 2W \) for some \( Z, W \in \mathbb{Z} \).

Now, by Lemma 7.4.2 part (iv), \( \alpha - \beta \) mod 4 lies in \{0, 2i + 2j, 2i + 2k, 2j + 2k\}. We will show that \( \alpha - \beta \) mod 4 lies in \{0, 2j + 2k\}.

Suppose first that \( \alpha - \beta \equiv 2i + 2j \) mod 4. Then, \( d \equiv w \) mod 4, so \( E \equiv W \) mod 2. Similarly, \( c \not\equiv z \) mod 4, so \( C \neq Z \) mod 2. So, one of \( C \) or \( Z \) is odd and the other is even; WLOG, assume that \( C \) is odd and \( Z \) is even. Then,

\[
b^2 \equiv y^2 \mod 8 \quad \text{(since both} \, b \, \text{and} \, y \, \text{are odd)},
\]

\[
c^2 \equiv 4C^2 \equiv 4 \mod 8,
\]

\[
z^2 \equiv 4Z^2 \equiv 0 \mod 8, \quad \text{and}
\]

\[
d^2 \equiv 4E^2 \equiv 4W^2 \equiv w^2 \mod 8.
\]
However, this implies that $N(\alpha) \not\equiv N(\beta) \mod 8$, which is a contradiction because $N(\alpha) = N(\beta)$. So, we conclude that $\alpha - \beta \not\equiv 2i + 2j \mod 4$.

If $\alpha - \beta \equiv 2i + 2k \mod 4$, then we may derive a contradiction just as in the preceding paragraph. So, we are forced to conclude that $\alpha - \beta \mod 4$ lies in $\{0, 2j + 2k\}$. As in Case 1, it now follows that $\pi(D) \subseteq \{0, 2j + 2k\}$, which again contradicts the fact that $|\pi(D)| > 2$.

We get a contradiction in both Case 1 and Case 2, so all three of $b, c$, and $d$ must be odd. This proves the lemma. \qed

We can now prove the promised classification theorem.

**Theorem 7.4.5.** Let $S$ be a reduced subset of $\mathbb{Z}Q$ such that $\Gamma(S) = 8$. Let $D = \{\alpha - \beta \mid \alpha, \beta \in S\}$. Then, $S$ is a ringset $\iff$ there exist $\delta, \varepsilon \in D$ such that the residues of $\delta$ and $\varepsilon \mod 4$ lie in $\{2i + 2j, 2i + 2k, 2j + 2k\}$, but $\delta \not\equiv \varepsilon \mod 4$.

**Proof.** ($\Rightarrow$) We prove the contrapositive. Assume for all $\delta, \varepsilon \in D$ that either $\delta \equiv 0 \mod 4$, $\varepsilon \equiv 0 \mod 4$, or $\delta \equiv \varepsilon \mod 4$. Now, by Lemma 7.4.2 part (iv), the residue modulo 4 of any element of $D$ lies in $\{0, 2i + 2j, 2i + 2k, 2j + 2k\}$, and by Lemma 7.4.2 part (v), there exists $\delta \in D$ such that the residue of $\delta$ lies in $\{2i + 2j, 2i + 2k, 2j + 2k\}$. Hence, for all $\varepsilon \in D$, either $\varepsilon \equiv 0 \mod 4$ or $\varepsilon \equiv \delta \mod 4$.

Now, WLOG, assume that $\delta \equiv 2i + 2j \mod 4$. Let $\beta = yi + zj + wk \in S$ and let $f(x) = \frac{(i+j)(x-\beta)}{4}$. By the preceding paragraph, for each $\alpha \in S$ either $\alpha - \beta \equiv 2i + 2j \mod 4$ or $\alpha - \beta \equiv 0 \mod 4$. In either case, $(i + j)(\alpha - \beta) \equiv 0 \mod 4$, so $f(x) \in$
\( \text{Int}(S, \mathbb{Z}Q) \). Next, we compute that

\[
(i + j)(\beta i - i\beta) = (i + j)(2wj - 2zk) = -2w - 2zi + 2zj + 2wk, \quad \text{and}
\]

\[
(i + j)(\beta j - j\beta) = (i + j)(-2wi + 2yk) = 2w + 2yi - 2yj + 2wk.
\]

By Lemma 7.3.12, at least one of \( y, z \), or \( w \) is odd. If \( y \) is odd, then letting \( g(x) = f(x)(x-j) \) and evaluating \( g(x) \) at \( \beta \) yields

\[
g(\beta) = \frac{(i+j)(\beta i - i\beta)}{4} = \frac{-2w - 2zi + 2zj + 2wk}{4} \notin \mathbb{Z}Q.
\]

In either case, \( g(x) \notin \text{Int}(S, \mathbb{Z}Q) \), so \( \text{Int}(S, \mathbb{Z}Q) \) is not a ring.

\((\Leftarrow)\) Assume that there exist \( \delta, \varepsilon \in D \) as in the statement of the theorem. Then, \( \delta \) and \( \varepsilon \) are congruent mod 4 to different elements of \( \{2i + 2j, 2i + 2k, 2j + 2k\} \).

Now, WLOG, assume that \( \delta \equiv 2i + 2j \) and \( \varepsilon \equiv 2i + 2k \). Let \( p \) be a prime, let \( e > 1 \), let \( R = \mathbb{Z}Q/(p^e) \), and let \( f \in \text{Muff}_R(S) \). Since \( S \) is reduced, there exist \( \gamma, \gamma_0 \in \mathbb{Z}Q \) such that \( f(\alpha) \equiv \gamma\alpha + \gamma_0 \mod p^e \) for all \( \alpha \in S \). Then, \( \gamma\zeta \equiv 0 \mod p^e \) for all \( \zeta \in D \), and \( 4\gamma \equiv 0 \mod p^e \) by Lemma 7.4.3.

Let \( \alpha = bi + cj + dk \in S \). To show that \( S \) is a ringset, it suffices to show that \( f(\beta) \equiv 0 \) for all \( \beta \in \text{Konj}(\alpha) \), and to establish this latter condition it suffices to show that \( \gamma(\alpha - \beta) \equiv 0 \) for all \( \beta \in \text{Konj}(\alpha) \). By Lemma 7.4.4, all of \( b, c, \) and \( d \) are odd, so

\[
\alpha - (-j\alpha j) = 2bi + 2dk \equiv \varepsilon \mod 4, \quad \text{and}
\]

\[
\alpha - (-k\alpha k) = 2bi + 2cj \equiv \delta \mod 4.
\]

Thus, there exist \( \delta', \varepsilon' \in \mathbb{Z}Q \) such that

\[
\alpha - (-j\alpha j) = \varepsilon + 4\varepsilon', \quad \text{and}
\]

\[
\alpha - (-k\alpha k) = \delta + 4\delta'.
\]
Hence, in \( R \),

\[
\gamma(\alpha - (-j\alpha j)) \equiv \gamma\varepsilon + 4\gamma\varepsilon' \equiv 0, \quad \text{and}
\]
\[
\gamma(\alpha - (-k\alpha k)) \equiv \gamma\delta + 4\gamma\delta' \equiv 0,
\]

and so \( f(-j\alpha j) \equiv f(-k\alpha k) \equiv f(\alpha) \equiv 0 \).

It remains to show that \( \gamma(\alpha - (-i\alpha i)) \equiv 0 \) in \( R \). We know that \( \alpha - (-i\alpha i) = 2cj + 2dk \), and it is easy to see that \( -j\alpha j - (-k\alpha k) = 2cj - 2dk \). Since \( f(-j\alpha j), f(-k\alpha k), \) and \( 4\gamma \) are all equivalent to 0 in \( R \), we have

\[
0 \equiv f(-j\alpha j) - f(-k\alpha k) \\
\equiv \gamma(-j\alpha j - (-k\alpha k)) \\
\equiv \gamma(2cj - 2dk) \\
\equiv \gamma(2cj - 2dk) + 4\gamma dk \\
\equiv \gamma(2cj + 2dk) \\
\equiv \gamma(\alpha - (-i\alpha i)).
\]

Thus, \( f(-i\alpha i) \equiv 0 \). It now follows by Corollary 7.1.6 that \( S \) is a ringset. \( \square \)

**Remark.** An examination of the proof of Theorem 7.4.5 shows that if \( S \) is reduced, \( \Gamma(S) = 8 \), and \( S \) is a ringset, then it must be true that every \( \alpha = bi + cj + dk \in S \) has \( b, c, \) and \( d \) all odd. However, this condition is not sufficient; a simple counterexample is \( S = \{i + j + k, i - j - k\} \). Thus, we must use the more cumbersome condition given in the theorem.

Combining Theorem 7.3.6, Theorem 7.3.13, and Theorem 7.4.5 gives a complete classification of those reducible subsets \( S \) of \( ZQ \) that are ringsets.
Theorem 7.4.6. Let $S$ be a reducible subset of $\mathbb{Z}Q$ with reduction $T$ and let $D = \{\alpha - \beta \mid \alpha, \beta \in T\}$. Then, $S$ is a ringset if and only if exactly one of the following holds:

(i) $\Gamma(T) = 2$,

(ii) $\Gamma(T) = 4$, or

(iii) $\Gamma(T) = 8$ and there exist $\delta, \varepsilon \in D$ such that the residues of $\delta$ and $\varepsilon$ mod 4 lie in

$$\{2i + 2j, 2i + 2k, 2j + 2k\}, \text{ but } \delta \not\equiv \varepsilon \mod 4.$$ 

Theorem 7.4.6 is particularly nice when applied to two-element reducible subsets.

Corollary 7.4.7. Let $S$ be a two-element reducible subset of $\mathbb{Z}Q$, and let $T = \{\alpha, \beta\}$ be the reduction of $S$. Then, $S$ is a ringset if and only if $N(\alpha - \beta) = 2$ or 4.

Proof. Let $D$ be as in the statement of Theorem 7.4.6. Then, $D = \{\pm(\alpha - \beta)\}$, so condition (iii) cannot hold for $T$. Also, $\Gamma(T) = N(\alpha - \beta)$, so $S$ is a ringset if and only if $N(\alpha - \beta) = 2$ or 4. \qed

7.5 Necessary and Sufficient Conditions for Finite Subsets

In the previous section, we derived necessary and sufficient conditions for a reduced subset of $\mathbb{Z}Q$ to be a ringset. It turns out that we can extend these conditions to work for any finite subset of $\mathbb{Z}Q$. The idea is to first take a finite subset $S$ of $\mathbb{Z}Q$ and partition $S$ into reducible subsets. There is more than one way to achieve such a partition, but when it is done in a certain way, we will show that $S$ is a ringset if and only if each of the reducible subsets in the partition of $S$ is a ringset. The relevant partition is described in the following definition.
**Definition 7.5.1.** Let \( S \) be a finite subset of \( \mathbb{Z}Q \). Let \( S_0 = S \cap \mathbb{Z} \) and let \( m_1(x), m_2(x), \ldots, m_t(x) \) be all the distinct minimal polynomials of elements of \( S - S_0 \). That is, if \( \alpha \in S - S_0 \), then \( \min_{\alpha}(x) = m_\ell(x) \) for some \( 1 \leq \ell \leq t \); \( m_{\ell_1}(x) \neq m_{\ell_2}(x) \) unless \( \ell_1 = \ell_2 \); and for each \( 1 \leq \ell \leq t \), there exists \( \alpha_\ell \in S - S_0 \) such that \( m_\ell(x) = \min_{\alpha_\ell}(x) \). For each \( 1 \leq \ell \leq t \), let \( S_\ell = \{ \alpha \in S \mid \min_{\alpha}(x) = m_\ell(x) \} \). Then, \( S \) can be expressed as the disjoint union \( S = \bigcup_{\ell=0}^{t} S_\ell \). When \( S \) is written in this way, we call it the *minimal polynomial partition* of \( S \).

When \( S \) is a finite subset of \( \mathbb{Z}Q \) with minimal polynomial partition \( S = \bigcup_{\ell=0}^{t} S_\ell \), each \( S_\ell \) with \( 1 \leq \ell \leq t \) is a reducible subset of \( \mathbb{Z}Q \), so we can use Theorem 7.4.6 to decide whether \( S_\ell \) is a ringset. As we will show below in Corollary 7.5.5, \( S \) is a ringset if and only if \( S_\ell \) is a ringset for each \( 1 \leq \ell \leq t \) (\( S_0 \) is always a ringset because it lies in \( \mathbb{Z} \)). With this goal in mind, we first more closely examine how a reduced subset can fail to be a ringset. In the proofs of Theorems 7.3.1, 7.3.11, 7.3.6, and 7.4.5, our strategy for showing that a reduced subset \( S \) was not a ringset was always the same: we exhibited two linear polynomials in \( \text{Int}(S, \mathbb{Z}Q) \) whose product was not in \( \text{Int}(S, \mathbb{Z}Q) \). It will be useful to recall what these linear polynomials were. In the following lemma, we summarize the different cases that occurred.

**Lemma 7.5.2.** Let \( T \) be a reduced subset of \( \mathbb{Z}Q \) that is not a ringset. Then, there exist \( \beta \in T, \gamma \in \mathbb{Z}Q, n > 0, \) and \( u \in \{i, j, k\} \) such that \( \frac{\gamma(x-\beta)}{n}, x - u \in \text{Int}(T, \mathbb{Z}Q) \), but \( \frac{\gamma(x-\beta)(x-u)}{n} \notin \text{Int}(T, \mathbb{Z}Q) \).

*Proof.* We have already verified this result, but the proof is spread out over several theorems, so for convenience we collect everything here.
Since $T$ is not a ringset, $\Gamma(T)$ must be a non-negative integer different than 2 or 4. This gives us several cases to consider.

**Case 1: $\Gamma(T) = 0$**

The only way this case can occur is if $T$ is a singleton set. As in Theorem 7.3.1, we take $\beta$ to be the lone element of $T$, $\gamma = 1$, $u \in \{i, j, k\}$ such that $\beta u - u \beta \neq 0$, and $n$ such that $\beta u - u \beta$ is not divisible by $n$.

**Case 2: $p | \Gamma(T)$ for some odd prime $p$**

In this case, we refer to Theorem 7.3.11, where we showed that we can take $n = p$, any $\beta \in T - (p)$, and (depending on the situation) either $\gamma = 1$ or a particular $\gamma \in \mathbb{Z}Q$ such that $N(\gamma) \equiv 0 \mod p$. Also, the $u$ that we choose will depend on $\beta$, but will be an element of $\{i, j, k\}$, as shown in Proposition 7.3.8.

**Case 3: $16 | \Gamma(T)$**

For this case, Theorem 7.3.6 shows that we can use $n = 4$, any $\beta \in T$, and $\gamma = 1$. As in Case 2, $u$ will depend on $\beta$.

**Case 4: $\Gamma(T) = 8$**

Finally, since we are assuming that $T$ is not a ringset, Theorem 7.4.5 demonstrates that we can take $n = 4$ and any $\beta \in T$. Then, there exist $\gamma \in \{i + j, i + k, j + k\}$ and $u \in \{i, j, k\}$ (both depending on $\beta$) such that the Lemma holds.

There are no more cases to consider, so we are done. \qed
We need one more lemma that will be useful in the theorem that follows. The lemma is a straightforward result about polynomials over noncommutative rings. The result is well-known, but a proof could not be found in the available literature, so one is provided below.

**Lemma 7.5.3.** Let \( R \) be a noncommutative ring and let \( f(x), g(x) \in R[x] \). Assume that \( f(x) \) is central in \( R[x] \). Then, for any \( \alpha \in R \), we have \((fg)(\alpha) = (gf)(\alpha) = g(\alpha)f(\alpha)\).

**Proof.** Let \( f(x) = \sum_r a_r x^r \) and \( g(x) = \sum_s \beta_s x^s \). Since \( f(x) \) is central in \( R[x] \), each \( a_r \) is central in \( R \). Let \( \alpha \in R \). We have

\[
(fg)(\alpha) = \sum_r a_r g(\alpha) \alpha^r \\
= \sum_r g(\alpha) a_r \alpha^r \quad \text{because each } a_r \text{ is central in } R \\
= g(\alpha) \sum_r a_r \alpha^r \\
= g(\alpha)f(\alpha).
\]

Similarly,

\[
(gf)(\alpha) = \sum_s \beta_s f(\alpha) \alpha^s \\
= \sum_s \beta_s \alpha^s f(\alpha) \quad \text{because } f(\alpha) \text{ and } \alpha^s \text{ commute for each } s \\
= g(\alpha)f(\alpha).
\]

Thus, the lemma holds. \( \square \)

We now show what goes wrong when one of the reducible subsets in the minimal polynomial partition of a finite set fails to be a ringset.
Theorem 7.5.4. Let $S$ be a finite subset of $\mathbb{Z}Q$ with minimal polynomial partition $S = \bigcup_{\ell=0}^{t} S_{\ell}$. Let $T$ be a reducible subset of $\mathbb{Z}Q$ such that $(\bigcup_{\ell=0}^{t} S_{\ell}) \cup T$ is the minimal polynomial partition of $S \cup T$. That is, if $m(x)$ is the minimal polynomial corresponding to $T$ and $\varepsilon$ is any element of $S$, then $\min_{\varepsilon}(x)$ does not equal $m(x)$. Assume that $T$ is not a ringset. Then, $S \cup T$ is not a ringset.

Proof. First, since $T$ is reducible, there exists a reduced subset $T' \subseteq \mathbb{Z}Q$, $a \in \mathbb{Z}$, and $b \in \mathbb{Z} - \{0\}$ such that $T = a + bT'$. Notice that $(S - a) \cup (T - a) \subseteq \mathbb{Z}Q$, so by Theorem 7.2.7, $S \cup T$ is a ringset if and only if $(S - a) \cup (T - a)$ is a ringset. Thus, from here on we may assume WLOG that $a = 0$, i.e. that $T = bT'$. Now, while $\frac{1}{b}T \subseteq \mathbb{Z}Q$, there is no guarantee that $\frac{1}{b}S \subseteq \mathbb{Z}Q$. So, the best we can assume is that $T = bT'$. Under this assumption, for each $\alpha \in T$ there exists $\alpha' \in T'$ such that $\alpha = b\alpha'$.

Next, for each $1 \leq \ell \leq t$, let $f_{\ell}(x)$ be the minimal polynomial corresponding to $S_{\ell}$. Additionally, let $f_{0}(x) = \prod_{A \in S_{0}} (x - A)$, and let $f(x) = \prod_{\ell=0}^{t} f_{\ell}(x)$. Then, $f(\varepsilon) = 0$ for all $\varepsilon \in S$. Let $m(x)$ be the minimal polynomial corresponding to $T$. By assumption, $m(x) \neq f_{\ell}(x)$ for all $1 \leq \ell \leq t$, so $f_{\ell}(\alpha) \neq 0$ for all $\alpha \in T$ and all $1 \leq \ell \leq t$. Furthermore, $f_{0}(\alpha) \neq 0$ for all $\alpha \in T$ (if $f_{0}(\alpha) = 0$ for some $\alpha \in T$, then $\prod_{A \in S_{0}} (A - \alpha) = 0$, which is impossible because $\mathbb{Z}Q$ has no zero divisors and $\alpha \notin \mathbb{Z}$), so $f(\alpha) \neq 0$ for all $\alpha \in T$.

Note that $f(x)$ has coefficients in $\mathbb{Z}$, hence is central in $\mathbb{Z}Q[x]$. Thus, Lemma 7.5.3 applies to $f(x)$. We will freely use this fact in the calculations that follow.

As in Lemma 7.5.2, we have several cases to consider, depending on the value of $\Gamma(T')$. 
Case 1: $\Gamma(T') = 0$

We proceed as in Theorem 7.3.1. Since $\Gamma(T') = 0$, both $T'$ and $T$ are singleton sets, so there exists $\beta \in \mathbb{Z}Q - \mathbb{Z}$ such that $T = \{\beta\}$. Let $g(x) = (x - \beta)f(x)$. Then, $g(\varepsilon) = 0$ for all $\varepsilon \in S \cup T$, so $\frac{g(x)}{n} \in \text{Int}(S \cup T, \mathbb{Z}Q)$ for all $n > 0$. However, $\beta \notin \mathbb{Z}$, so there exists $u \in \{i, j, k\}$ such that $\beta u - u\beta \neq 0$. Let $h(x) = g(x)(x - u)$, we have $h(\varepsilon) = 0$ for all $\varepsilon \in S$, but $h(\beta) = (\beta u - u\beta)f(\beta) \neq 0$, so there exists $n > 1$ such that $\frac{h(\beta)}{n} \notin \mathbb{Z}Q$. Thus, $\frac{g(x)}{n}$ and $x - u$ are in $\text{Int}(S \cup T, \mathbb{Z}Q)$ while $\frac{h(x)}{n} = \frac{g(x)(x-u)}{n}$ is not. Hence, $S \cup T$ is not a ringset.

Case 2: $p \mid \Gamma(T')$ for some odd prime $p$

Let $\beta' \in T'$, $\gamma \in \mathbb{Z}Q$, and $u \in \{i, j, k\}$ be as in the second case in Lemma 7.5.2, when applied to the reduced set $T'$. Let $\beta \in T$ be such that $\beta = b\beta'$. Then, for all $\alpha' \in T'$, we have $\gamma(\alpha' - \beta') \equiv 0 \mod p$. Factor $b$ as $b = p^{e_1}q_1$, where $e_1 \geq 0$ and $p \nmid q_1$. Then, we have

$$
\gamma(\alpha - \beta) = b\gamma(\alpha' - \beta') \equiv 0 \mod p^{e_1+1} \text{ for all } \alpha \in T.
$$

Next, consider $f(x)$. Since $T$ is reducible, by Theorem 2.3.1 there exist $C, D \in \mathbb{Z}$ such that $f(\alpha) = C\alpha + D$ for all $\alpha \in T$. Let $F(x) = f(x)(-Cx + D)$. Then, since $F(x)$ has integer coefficients and each $\alpha \in T$ has constant coefficient equal to 0, we have

$$
F(\alpha) = f(\alpha)(-C\alpha + D) = (C\alpha + D)(C\alpha + D) = N(C\alpha + D) \in \mathbb{Z}.
$$

Furthermore, since each element of $T$ has the same norm, it is not difficult to see that for any $\alpha, \delta \in T$ we have $N(C\alpha + D) = D^2 + C^2N(\alpha) = D^2 + C^2N(\delta) = N(C\delta + D)$. Lastly, we know that $f(\alpha) \neq 0$ for all $\alpha \in T$, so $N(C\alpha + D) \neq 0$. Thus, there exists
a positive integer $y$ such that $F(\alpha) = y$ for all $\alpha \in T$. Factor $y$ as $y = p^{e_2}q_2$, where $e_2 \geq 0$ and $p \nmid q_2$. Then,

$$F(\alpha) \equiv 0 \mod p^{e_2} \text{ for all } \alpha \in T. \quad (**)$$

Now, let $R = \mathbb{Z}Q/(p^{e_1+e_2+1})$ and let $g(x) = \gamma(x - \beta)F(x)$. Then, $F(\varepsilon) = 0$ for all $\varepsilon \in S$, so $g(\varepsilon) = 0$ for all $\varepsilon \in S$. By (*) and (**), we see that $g(\alpha) \equiv 0 \mod p^{e_1+e_2+1}$ for all $\alpha \in T$. Hence, $g(x) \in \text{Muff}_R(S \cup T)$.

Finally, let $h(x) = \gamma(x - \beta)(x - u)$ and $H(x) = g(x)(x - u)$. Then,

$$H(x) = g(x)(x - u) = \gamma(x - \beta)F(x)(x - u) = \gamma(x - \beta)(x - u)F(x) = h(x)F(x).$$

By construction, we know that $\gamma(\beta' u - u\beta') \not\equiv 0 \mod p$, so

$$
\begin{align*}
    h(\beta) &= \gamma(\beta u - u\beta) \\
    &= b\gamma(\beta' u - u\beta') \\
    &= p^{e_1}q_1\gamma(\beta' u - u\beta') \\
    &\not\equiv 0 \mod p^{e_1+1}.
\end{align*}
$$

Thus,

$$
\begin{align*}
    H(\beta) &= h(\beta)F(\beta) \\
    &= p^{e_1}q_1\gamma(\beta' u - u\beta')y \\
    &= p^{e_1+e_2}q_1q_2\gamma(\beta' u - u\beta') \\
    &\not\equiv 0 \mod p^{e_1+e_2+1},
\end{align*}
$$

and therefore $H(x) \notin \text{Muff}_R(S \cup T)$. However, $H(x) = g(x)(x - u)$ with $g(x) \in \text{Muff}_R(S \cup T)$ and $x - u \in R[x]$; thus, $\text{Muff}_R(S \cup T)$ is not an ideal of $R[x]$. It
follows that $S \cup T$ is not a ringset.

**Case 3:** $4 \mid \Gamma(T')$

We handle both Case 3 and Case 4 from Lemma 7.5.2 at once. The proof for this case is similar to the one where $p \mid \Gamma(T')$.

As above, let $\beta' \in T'$, $\gamma \in \mathbb{Z}Q$, and $u \in \{i, j, k\}$ be as in Lemma 7.5.2, when applied to the reduced set $T'$. First, factor $b$ as $b = 2^{e_1}q_1$, where $e_1 \geq 0$ and $2 \nmid q_1$. Then, by construction, $\gamma(\alpha' - \beta') \equiv 0 \mod 4$ for all $\alpha' \in T'$, so $\gamma(\alpha - \beta) \equiv 0 \mod 2^{e_1+2}$ for all $\alpha \in T$. Next, let $F(x)$ and $y$ be as in the previous case of this proof, and factor $y$ as $y = 2^{e_2}q_2$, where $e_2 \geq 0$ and $2 \nmid q_2$. Let $R = \mathbb{Z}Q/(2^{e_1+e_2+2})$ and let $g(x) = \gamma(x - \beta)F(x)$. Then, $g(x) \in \text{Muff}_R(S \cup T)$, but following the same steps used in the previous case will show that $g(x)(x - u) \notin \text{Muff}_R(S \cup T)$. Hence, $S \cup T$ is not a ringset in this case.

There are no more cases to consider, so the proof is complete. \qed

We end this section with the necessary and sufficient conditions for a finite subset of $\mathbb{Z}Q$ to be a ringset.

**Corollary 7.5.5.** Let $S$ be a finite subset of $\mathbb{Z}Q$ with minimal polynomial partition $S = \bigcup_{\ell=0}^{t} S_{\ell}$. Then, $S$ is a ringset if and only if $S_{\ell}$ is a ringset for all $1 \leq \ell \leq t$.

**Proof.** $(\Leftarrow)$ This is true because of Proposition 7.1.3 and Theorem 7.2.5.

$(\Rightarrow)$ There is nothing to prove if $t = 0$, so assume that $t > 1$. We prove the contrapositive. Assume that $S_{\ell}$ is not a ringset for some $\ell \in \{1, 2, \ldots, t\}$. WLOG,
assume that $S_t$ is not a ringset. Applying Theorem 7.5.4 to $(\bigcup_{\ell=0}^{t-1} S_\ell) \cup S_t$ shows that $S$ is not a ringset, as required.


