Computing the Zeta Function of the Integral Quaternions

by

Nicole Chassin

A thesis submitted to the thesis committee in partial fulfillment of the requirements for the degree of

Master of Science

in

Mathematics

Carleton University
Ottawa, Ontario

© 2022
Nicole Chassin
Abstract

In rings with a reasonable arrangement of left ideals, the finite-index left ideal structure can be partially captured by the Solomon zeta function. The integral quaternions are such a ring, and serve as a beneficial example. To find the Solomon zeta function of the integral quaternions, we first describe the ring’s local structure at each prime, and then the local structure of its finite-index left ideals. When doing this for odd primes, we make use of the $p$-adic integers.
Acknowledgements

All of my good friends, and my thesis supervisors Adam Logan and Colin Ingalls.
## Contents

Abstract ................................. i

Acknowledgements ..................... ii

1 Introduction ......................... 1

2 Background ........................... 3

  2.1 The Zeta Function .................. 3
  2.2 The $p$-adic Integers $\mathbb{Z}_p$ ...... 4
  2.3 The Localization $\mathbb{Z}_{(p)}$ .......... 13
  2.4 The Integral Quaternions ............. 19
  2.5 The Norm .......................... 27

3 The Zeta Function of $H(2)$ ......... 37

  3.1 Ideals of $H(2)/2H(2)$ .............. 37
  3.2 Left Ideals Between $H(2)$ and $4H(2)$ ... 45
  3.3 Zeta Function Computation When $p$ is Even ...... 54

4 The Zeta Function of $H(p)$ When $p$ is Odd .... 60

  4.1 Hensel’s Lemma ..................... 60
4.2 Equivalence to Matrix Rings ........................................... 64
4.3 Morita Equivalence ....................................................... 66
4.4 Hermite Normal Form ..................................................... 71
4.5 Zeta Function Computation When $p$ is Odd ...................... 77

5 Conclusion and Interpretation ........................................... 80
  5.1 Zeta Function Computation for $H$ .................................. 80
  5.2 Analytic Continuation and Extension of the Zeta Function ...... 82

Bibliography ................................................................. 85
Chapter 1

Introduction

We compute the zeta function of the ring $H$ of integral quaternions. This requires us to first compute the zeta functions of the localizations $H_{(p)}$ for all primes $p$, by identifying the finite-index left ideal structure of these local rings.

In the case that $p$ is even, we find this structure of finite-index left ideals more or less directly, using the intermediary of quotient rings of the form $H_{(2)}/2^n H_{(2)}$. It turns out that all finite-index left ideals of $H_{(2)}$ lie between the ideals $2^n H_{(2)}$ and $2^{n+2} H_{(2)}$ for some $n \in \mathbb{N}$, and that the structure of left ideals between $2^n H_{(2)}$ and $2^{n+2} H_{(2)}$ is similar to that between $H_{(2)}$ and $4H_{(2)}$. We therefore start by finding the structure of left ideals between $H_{(2)}$ and $2H_{(2)}$, extend this to the structure of left ideals between $H_{(2)}$ and $4H_{(2)}$, and then extend this to the entire finite-index left ideal structure of $H_{(2)}$. We use this to compute the zeta function of $H_{(2)}$.

In the case that $p$ is odd, we proceed using a correspondence between the ring $H_{(p)}$ and the ring $H_p$, with $H_p$ being the quaternion ring over the $p$-adic integers. The ring $H_p$ then turns out to be isomorphic to the matrix ring $\mathbb{Z}_p^{2 \times 2}$, whose finite-index left ideal structure corresponds to the finite-index $\mathbb{Z}_p$-submodule structure of $\mathbb{Z}_p^2$. By
finding the finite-index $\mathbb{Z}_p$-submodule structure of $\mathbb{Z}_p^2$, we can then work backwards to the finite-index left ideal structure of $H_{(p)}$, and hence to the zeta function of $H_{(p)}$.

After finding the zeta functions for $H_{(2)}$ and $H_{(p)}$ over odd primes $p$, we put this together to determine the zeta function of $H$. 
Chapter 2

Background

2.1 The Zeta Function

Solomon [1] introduces the zeta function as a formal Dirichlet series. Similar zeta functions are studied in papers such as Lynch [2].

Definition 2.1.1. Let $A$ be a ring and let $M$ be a finitely generated $A$-module. If $M$ has only finitely many distinct submodules of index $n$ for all $n \in \mathbb{N}$, then the Solomon zeta function of $M$ as an $A$-module is

$$\zeta_{(A\!M; s)} = \sum_{X \leq M} |M/X|^{-s}$$

where the sum is over all finite index $A$-submodules of $M$.

For rings viewed as modules over themselves, the definition comes down to the following.

Definition 2.1.2. Let $R$ be a ring. If $R$ has only finitely many left ideals of index $n$
for all \( n \in \mathbb{N} \), then the (left) Solomon zeta function of \( R \) as a ring is

\[
\zeta(R; s) = \sum_{X \leq R} |R/X|^{-s}
\]

where the sum is over all finite index left ideals of \( R \).

This zeta function encapsulates the left ideal structure of a given ring. We will apply this to the ring \( H \) of integral quaternions defined in Section 2.4, by first computing the zeta function of the localizations \( H(p) \) for all prime numbers \( p \). Once we have done this, we will piece together the zeta function for \( H \) from the zeta functions for \( H(p) \) using the following theorem.

**Theorem 2.1.3.** Let \( R \) be a finitely generated \( \mathbb{Z} \)-module and let \( R(p) \) be the localization of \( R \) at \( p \). Then

\[
\zeta(R; s) = \prod_{p \in \mathbb{P}} \zeta(R(p); s)
\]

where \( \mathbb{P} \) is the set of primes in \( \mathbb{Z} \).

**Proof.** This is a consequence of Lemma 6 from Solomon [1] page 316.

2.2 The \( p \)-adic Integers \( \mathbb{Z}_p \)

Let \( p \) be a prime number. In the case that \( p \) is odd, we will find it useful to work with the ring \( \mathbb{Z}_p^{2\times2} \) of 2-by-2 matrices over the \( p \)-adic integers. This ring will turn out to have a similar ideal structure to that of the integral quaternions localized at \( p \). When \( p \) is even, this will not be the case; however, the contents of this section are an overall look at the ring \( \mathbb{Z}_p \) whether \( p \) is even or odd.
The main results in this section will be the important properties of \( \mathbb{Z}_p \), including a version of prime decomposition (Proposition 2.2.9), a divisibility criteria (Proposition 2.2.10), and an elaboration of its ideal structure (Proposition 2.2.12). The ring of \( p \)-adic integers itself is usually presented as a subring of the field \( \mathbb{Q}_p \), which is the field of \( p \)-adic numbers (Gouvêa [3, Definition 4.2.1]). However, we are only interested in the \( p \)-adic integers themselves, and will therefore introduce them using our own definition, similar to Sutherland [4] and other sources.

**Definition 2.2.1.** The ring of \( p \)-adic integers \( \mathbb{Z}_p \) is the ring of sequences \((a_i)_{i \in \mathbb{N}}\) where \( a_i \in \mathbb{Z}/p^{i+1}\mathbb{Z} \) and \( a_i \equiv a_{i+1} \mod p^{i+1} \) for all \( i \in \mathbb{N} \). Addition and multiplication in this ring are given by

\[
(a_i)_{i \in \mathbb{N}} + (b_i)_{i \in \mathbb{N}} = (a_i + b_i)_{i \in \mathbb{N}}
\]

and

\[
(a_i)_{i \in \mathbb{N}} \times (b_i)_{i \in \mathbb{N}} = (a_i \times b_i)_{i \in \mathbb{N}}
\]

for all \((a_i)_{i \in \mathbb{N}}, (b_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\), where the operations \( a_i + b_i \) and \( a_i \times b_i \) take place in the ring \( \mathbb{Z}/p^{i+1}\mathbb{Z} \) for all \( i \in \mathbb{N} \).

We now prove a number of important properties about the \( p \)-adic integers, including the fact that they are indeed a ring.

**Proposition 2.2.2.** The \( p \)-adic integers \( \mathbb{Z}_p \) form a unital commutative ring with identity element \((1)_{i \in \mathbb{N}}\).

*Proof.* This follows immediately from the definition, since the addition and multiplication in \( \mathbb{Z}_p \) are inherited directly from the rings \( \mathbb{Z}/p^{i+1}\mathbb{Z} \), and \( \mathbb{Z}/p^{i+1}\mathbb{Z} \) is a unital commutative ring for all \( i \in \mathbb{N} \). The only interesting thing to check is that addition and
multiplication in \( \mathbb{Z}_p \) preserve the condition that \( a_i \equiv a_{i+1} \mod p^{i+1} \) for all \( i \in \mathbb{N} \). In other words, we need to check that addition and multiplication in \( \mathbb{Z}_p \) are well-defined.

Let \((a_i)_{i \in \mathbb{N}}, (b_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\), and let \( c_i = a_i + b_i \) for all \( i \in \mathbb{N} \). Then \( c_i \in \mathbb{Z}/p^{i+1}\mathbb{Z} \) for all \( i \in \mathbb{N} \), and \((c_i)_{i \in \mathbb{N}} = (a_i + b_i)_{i \in \mathbb{N}} = (a_i)_{i \in \mathbb{N}} + (b_i)_{i \in \mathbb{N}}\) by definition. To see that \( c_i \equiv c_{i+1} \mod p^{i+1} \) for all \( i \in \mathbb{N} \), we first note that \( a_i \equiv a_{i+1} \mod p^{i+1} \) for all \( i \in \mathbb{N} \) and \( b_i \equiv b_{i+1} \mod p^{i+1} \) for all \( i \in \mathbb{N} \), since \((a_i)_{i \in \mathbb{N}}, (b_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\). This implies that \( c_i \equiv a_i + b_i \equiv a_{i+1} + b_{i+1} \equiv c_{i+1} \mod p^{i+1} \) for all \( i \in \mathbb{N} \), and hence that \( (c_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p \). This tells us that addition in \( \mathbb{Z}_p \) is well-defined, and a similar argument implies that multiplication in \( \mathbb{Z}_p \) is well-defined as well. Finally, we have that \((a_i)_{i \in \mathbb{N}} \times (1)_{i \in \mathbb{N}} = (a_i \times 1)_{i \in \mathbb{N}} = (a_i)_{i \in \mathbb{N}}\) for all \((a_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\), and hence that \( (1)_{i \in \mathbb{N}} \) is the identity element of \( \mathbb{Z}_p \).

The following simple statement will be useful later on.

**Proposition 2.2.3.** Let \((a_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\) and suppose that \( j, k \in \mathbb{N} \) are such that \( j \leq k \). Then \( a_j \equiv a_k \mod p^{j+1} \).

**Proof.** Let \( r \in \{j, j+1, j+2, \ldots, k-1\} \). Since \((a_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\), \( a_r \equiv a_{r+1} \mod p^{r+1} \), and

\[
\begin{align*}
    a_r &\equiv a_{r+1} \mod p^{r+1} \implies p^{r+1} | a_r - a_{r+1} \\
    &\implies p^{i+1} | a_r - a_{r+1} \\
    &\implies a_r \equiv a_{r+1} \mod p^{i+1}
\end{align*}
\]

since \( j + 1 \leq r + 1 \). We can conclude that \( a_r \equiv a_{r+1} \mod p^{j+1} \) for all \( r \in \{j, j+1, j+2, \ldots, k-1\} \), and hence that \( a_j \equiv a_{j+1} \equiv a_{j+2} \equiv \ldots \equiv a_k \mod p^{j+1} \).

\( \Box \)
Proposition 2.2.4. The natural map from $\mathbb{Z}$ to $\mathbb{Z}_p$ is injective.

Proof. The natural map from $\mathbb{Z}$ to $\mathbb{Z}_p$ is a ring homomorphism sending the element $x \in \mathbb{Z}$ to the element $(x)_{i \in \mathbb{N}} = (x \mod p^{i+1})_{i \in \mathbb{N}} \in \mathbb{Z}_p$. We then have that $(x)_{i \in \mathbb{N}} = (0)_{i \in \mathbb{N}}$ in $\mathbb{Z}_p$ if and only if $x \equiv 0 \mod p^{i+1}$ for all $i \in \mathbb{N}$. This happens if and only if $x = 0$, hence the map is injective. 

Since $\mathbb{Z}_p$ contains an isomorphic copy of $\mathbb{Z}$, we can identify elements of $\mathbb{Z}$ with their equivalents in $\mathbb{Z}_p$. This allows us to write expressions such as $x + (a)_{i \in \mathbb{N}} = (x + a)_{i \in \mathbb{N}}$ and $x \cdot (a)_{i \in \mathbb{N}} = (x \cdot a)_{i \in \mathbb{N}}$ for any $(a)_{i \in \mathbb{N}} \in \mathbb{Z}_p$ and $x \in \mathbb{Z}$, with the operations $x + a$ and $x \cdot a$ carried out in $\mathbb{Z}/p^{i+1}\mathbb{Z}$.

With these basic properties out of the way, we now introduce a very important function on the ring $\mathbb{Z}_p$, called the valuation function.

Definition 2.2.5. The valuation function $v_p : \mathbb{Z}_p \to \mathbb{N} \cup \{\infty\}$ is the function

$$v_p((x)_{i \in \mathbb{N}}) = \min\{i \mid x_i \neq 0\}$$

In the rest of the section we will prove some important properties of this function. In particular we will prove that $(x)_{i \in \mathbb{N}}$ is divisible by $(y)_{i \in \mathbb{N}}$ in $\mathbb{Z}_p$ if and only if $v_p((x)_{i \in \mathbb{N}}) \geq v_p((y)_{i \in \mathbb{N}})$ (Proposition 2.2.10).

Proposition 2.2.6. If $(x)_{i \in \mathbb{N}} \in \mathbb{Z}_p$ and $(x)_{i \in \mathbb{N}} \neq 0$, then $p^{v_p((x)_{i \in \mathbb{N}})}$ is the largest power of $p$ which divides $(x)_{i \in \mathbb{N}}$ in $\mathbb{Z}_p$.

Proof. Let $x = (x)_{i \in \mathbb{N}}$ be a nonzero element of $\mathbb{Z}_p$ and let $m = v_p(x)$. Then $m = v_p((x)_{i \in \mathbb{N}}) = \min\{i \mid x_i \neq 0\}$ is finite, and $x_m \neq 0$ while $x_n = 0$ for all $n < m$. 

7
If \( m = 0 \), then \( p^m = p^0 = 1 \) and \( 1 \cdot x = (1 \cdot x_i)_{i \in \mathbb{N}} = (x_i)_{i \in \mathbb{N}} = x \). Hence \( p^m \) certainly divides \( x \).

If \( m > 0 \), then we can think of each \( x_i \) as an integer in \( \{0, 1, 2, ..., p^{i+1} - 1\} \), with \( x_i \equiv x_{i+1} \mod p^{i+1} \), \( x_{m-1} = 0 \), and \( x_m \neq 0 \) (by Definitions 2.2.1 and 2.2.5). By Proposition 2.2.3, this implies that \( x_{m+i} \equiv x_{m-1} \equiv 0 \mod p^m \) for all \( i \in \mathbb{N} \), and hence that \( \frac{x_{m+i}}{p^m} \) is an integer for all \( i \in \mathbb{N} \). Since \( x_{m+i} \equiv x_{m+i+1} \mod p^{m+i+1} \) (again, by Definition 2.2.1) and since

\[
\begin{align*}
x_{m+i} &\equiv x_{m+i+1} \mod p^{m+i+1} \\
\implies p^{m+i+1} | x_{m+i} - x_{m+i+1} \\
\implies p^{i+1} | \frac{x_{m+i}}{p^m} - \frac{x_{m+i+1}}{p^m} \\
\implies \frac{x_{m+i}}{p^m} \equiv \frac{x_{m+i+1}}{p^m} \mod p^{i+1}
\end{align*}
\]

it follows that \( \frac{x_{m+i}}{p^m} \equiv \frac{x_{m+i+1}}{p^m} \mod p^{i+1} \) for all \( i \in \mathbb{N} \).

Since \( x_{m+i} \in \{0, 1, 2, ..., p^{m+i+1} - 1\} \), we can also find that the integer \( \frac{x_{m+i}}{p^m} \) belongs to \( \{0, 1, 2, ..., p^{i+1} - 1\} \), and hence can be interpreted as an element of \( \mathbb{Z}/p^{i+1}\mathbb{Z} \), for all \( i \in \mathbb{N} \). If \( y_i = \frac{x_{m+i}}{p^m} \), then it follows that the sequence \( y = (y_i)_{i \in \mathbb{N}} \) belongs to \( \mathbb{Z}_p \) by Definition 2.2.1.

By Proposition 2.2.3, we know that \( x_{m+i} \equiv x_i \mod p^{i+1} \) for all \( i \in \mathbb{N} \). Since \( y_i = \frac{x_{m+i}}{p^m} \), it follows that \( p^m \cdot y_i = p^m \cdot \frac{x_{m+i}}{p^m} = x_{m+i} \equiv x_i \mod p^{i+1} \) for all \( i \in \mathbb{N} \). Hence
\[ p^m \cdot y_i = x_i \text{ in } \mathbb{Z}/p^{i+1}\mathbb{Z}, \text{ and we can conclude that} \]

\[
\begin{align*}
p^m \cdot y &= (p^m)_{i \in \mathbb{N}} \cdot (y_i)_{i \in \mathbb{N}} \\
&= (p^m \cdot y_i)_{i \in \mathbb{N}} \\
&= (x_i)_{i \in \mathbb{N}} \\
&= x.
\end{align*}
\]

This implies that \( p^m \) divides \( x \) in \( \mathbb{Z}_p \).

Conversely, suppose that \( p^n \) divides \( x \) in \( \mathbb{Z}_p \). Then there exists some \((a_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p \) such that \( x = p^n \cdot (a_i)_{i \in \mathbb{N}} \), implying that \( x_i \equiv p^n \cdot a_i \mod p^{i+1} \) for all \( i \in \mathbb{N} \). It follows that that \( x_i = 0 \) for all \( i < n \), and hence that \( n \leq m \) by Definition 2.2.5 (because \( m \) was the smallest integer such that \( x_m \neq 0 \)).

We can conclude that \( p^m \) is the largest power of \( p \) dividing \( x \) in \( \mathbb{Z}_p \).

\[ \square \]

This gives us a way of reducing elements modulo a power of \( p \) in \( \mathbb{Z}_p \), which will be useful later on.

**Corollary 2.2.7.** If \((x_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p \) and \( n \in \mathbb{N} \), then \( p^{n+1} \) divides \((x_i)_{i \in \mathbb{N}} - (x_n)_{i \in \mathbb{N}} \) in \( \mathbb{Z}_p \).

**Proof.** The element \((x_i)_{i \in \mathbb{N}} - (x_n)_{i \in \mathbb{N}} \) has zeros in the first \( n + 1 \) coordinates, hence \( v((x_i)_{i \in \mathbb{N}} - (x_n)_{i \in \mathbb{N}}) \geq n + 1 \). This implies that \( p^{v((x_i)_{i \in \mathbb{N}} - (x_n)_{i \in \mathbb{N}})} \), and hence also \( p^{n+1} \), divides \((x_i)_{i \in \mathbb{N}} - (x_n)_{i \in \mathbb{N}} \) in \( \mathbb{Z}_p \) by Proposition 2.2.6.

\[ \square \]

Next, we note that invertible elements of \( \mathbb{Z}_p \) are those not divisible by \( p \).
Proposition 2.2.8. The element \((x_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\) is invertible in \(\mathbb{Z}_p\) if and only if \((x_i)_{i \in \mathbb{N}}\) is not divisible by \(p\) in \(\mathbb{Z}_p\), and hence if and only if \(v_p((x_i)_{i \in \mathbb{N}}) = 0\).

Proof. If \(x = (x_i)_{i \in \mathbb{N}}\) is not divisible by \(p\) in \(\mathbb{Z}_p\), then \(v_p(x) = 0\) by Proposition 2.2.6. This implies that \(x_0\) is nonzero in \(\mathbb{Z}/p\mathbb{Z}\), and hence that \(x_i \equiv x_0 \neq 0 \mod p\) for all \(i \in \mathbb{N}\) (Proposition 2.2.3).

Since \(x_i \neq 0 \mod p\) for all \(i \in \mathbb{N}\), each \(x_i\) is invertible in \(\mathbb{Z}/p^{i+1}\mathbb{Z}\). Hence we can build a sequence \(y = (y_i)_{i \in \mathbb{N}}\) in \(\mathbb{Z}_p\) such that \(x_i \cdot y_i = 1\) in \(\mathbb{Z}/p^{i+1}\mathbb{Z}\) for all \(i \in \mathbb{N}\). Since the inverse of \(x_i\) in \(\mathbb{Z}/p^{i+1}\mathbb{Z}\) is unique, and since \(x_i \equiv x_{i+1} \mod p^{i+1}\), we can conclude that \(y_i \equiv y_{i+1} \mod p^{i+1}\) for all \(i \in \mathbb{N}\). This implies that \(y \in \mathbb{Z}_p\). Since \(x_i \cdot y_i = 1\) for all \(i \in \mathbb{N}\), it immediately follows that \(y\) is the inverse of \(x\) in \(\mathbb{Z}_p\).

Conversely, if \(x = (x_i)_{i \in \mathbb{N}}\) is invertible in \(\mathbb{Z}_p\), then there exists an element \(y = (y_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\) such that

\[
(x_i)_{i \in \mathbb{N}} \cdot (y_i)_{i \in \mathbb{N}} = (1)_{i \in \mathbb{N}}.
\]

This implies that \(x_0 \cdot y_0 = 1\) in \(\mathbb{Z}/p\mathbb{Z}\), and hence that \(x_0 \neq 0\). By Definition 2.2.5, it follows that \(v_p(x) = 0\), and hence that \((x_i)_{i \in \mathbb{N}}\) is not divisible by \(p\) in \(\mathbb{Z}_p\) by Proposition 2.2.6.

The last part of the Proposition follows directly from Proposition 2.2.6.

Using this, we can prove two even stronger results, including a form of prime decomposition in \(\mathbb{Z}_p\), and the division criterion mentioned earlier.

Proposition 2.2.9. If \((x_i)_{i \in \mathbb{N}}\) is a nonzero element of \(\mathbb{Z}_p\), then there exists an invertible element \((u_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\) such that \((x_i)_{i \in \mathbb{N}} = p^n \cdot (u_i)_{i \in \mathbb{N}}\) where \(n = v_p((x_i)_{i \in \mathbb{N}})\).

Proof. Since \((x_i)_{i \in \mathbb{N}}\) is nonzero, \(n \in \mathbb{N}\) and \(p^n\) divides \((x_i)_{i \in \mathbb{N}}\) in \(\mathbb{Z}_p\) by Proposition 2.2.6. Therefore, there exists some \((u_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\) such that \((x_i)_{i \in \mathbb{N}} = p^n \cdot (u_i)_{i \in \mathbb{N}}\).
If $p$ divides $(u_i)_{i \in \mathbb{N}}$ in $\mathbb{Z}_p$, then there exists some $(v_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p$ with $(u_i)_{i \in \mathbb{N}} = p \cdot (v_i)_{i \in \mathbb{N}}$. This would imply that

\[
(x_i)_{i \in \mathbb{N}} = p^n \cdot (u_i)_{i \in \mathbb{N}} \\
= p^n \cdot p \cdot (v_i)_{i \in \mathbb{N}} \\
= p^{n+1} \cdot (v_i)_{i \in \mathbb{N}}.
\]

and hence that $p^{n+1}$ divides $(x_i)_{i \in \mathbb{N}}$ in $\mathbb{Z}_p$. As $n$ was the largest power of $p$ dividing $(x_i)_{i \in \mathbb{N}}$ by Proposition 2.2.6, this is a contradiction.

We must conclude that $(u_i)_{i \in \mathbb{N}}$ is not divisible by $p$, and hence that $(u_i)_{i \in \mathbb{N}}$ is invertible by Proposition 2.2.8. Hence $(x_i)_{i \in \mathbb{N}}$ is the product of an invertible element and a power of $p$.

\[
\square
\]

**Proposition 2.2.10.** Let $(x_i)_{i \in \mathbb{N}}, (y_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p$. Then $(x_i)_{i \in \mathbb{N}}$ is divisible by $(y_i)_{i \in \mathbb{N}}$ in $\mathbb{Z}_p$ if and only if $v_p((x_i)_{i \in \mathbb{N}}) \geq v_p((y_i)_{i \in \mathbb{N}})$.

**Proof.** Let $m = v_p((x_i)_{i \in \mathbb{N}})$ and $n = v_p((y_i)_{i \in \mathbb{N}})$. By Proposition 2.2.9, $n$ and $m$ are integers, and there exists $(u_i)_{i \in \mathbb{N}}, (v_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p$ such that $(x_i)_{i \in \mathbb{N}} = p^m \cdot (u_i)_{i \in \mathbb{N}}$, $(y_i)_{i \in \mathbb{N}} = p^n \cdot (v_i)_{i \in \mathbb{N}}$, and both $(u_i)_{i \in \mathbb{N}}$ and $(v_i)_{i \in \mathbb{N}}$ are invertible in $\mathbb{Z}_p$. If $m \geq n$, then

\[
(x_i)_{i \in \mathbb{N}} = p^m \cdot (u_i)_{i \in \mathbb{N}} \\
= p^{m-n} \cdot p^n \cdot (u_i)_{i \in \mathbb{N}} \\
= p^{m-n} \cdot (u_i)_{i \in \mathbb{N}} \cdot (v_i)_{i \in \mathbb{N}}^{-1} \cdot (v_i)_{i \in \mathbb{N}} \\
= p^{m-n} \cdot (u_i)_{i \in \mathbb{N}} \cdot (v_i)_{i \in \mathbb{N}}^{-1} \cdot p^n \cdot (v_i)_{i \in \mathbb{N}} \\
= p^{m-n} \cdot (u_i)_{i \in \mathbb{N}} \cdot (v_i)_{i \in \mathbb{N}}^{-1} \cdot (y_i)_{i \in \mathbb{N}}
\]
meaning that \((x_i)_{i \in \mathbb{N}}\) is divisible by \((y_i)_{i \in \mathbb{N}}\) in \(\mathbb{Z}_p\). Conversely, suppose that \((x_i)_{i \in \mathbb{N}}\) is divisible by \((y_i)_{i \in \mathbb{N}}\) in \(\mathbb{Z}_p\). Then there exists \((z_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\) such that \((x_i)_{i \in \mathbb{N}} = (z_i)_{i \in \mathbb{N}} \cdot (y_i)_{i \in \mathbb{N}}\), and hence \(x_i = z_i y_i\) in \(\mathbb{Z}/p^{i+1}\mathbb{Z}\) for all \(i\). If \(i < n\) then \(y_i\) is zero, and hence so is \(x_i\). This implies that \(m \geq n\) (Definition 2.2.5), and so we are done.

\[
\]

Using this, we can prove that \(\mathbb{Z}_p\) is an integral domain, a principal ideal domain, and in fact a Euclidean domain. We can also find the specific structure of ideals in \(\mathbb{Z}_p\), which will be important in the rest of the paper.

**Proposition 2.2.11.** The ring \(\mathbb{Z}_p\) is an integral domain.

**Proof.** If \((x_i)_{i \in \mathbb{N}}, (y_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\) are nonzero, then there exist non-negative integers \(n = v_p((x_i)_{i \in \mathbb{N}}), m = v_p((y_i)_{i \in \mathbb{N}}),\) and invertible elements \((u_i)_{i \in \mathbb{N}}, (v_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p\) such that \((x_i)_{i \in \mathbb{N}} = p^n \cdot (u_i)_{i \in \mathbb{N}}\) and \((y_i)_{i \in \mathbb{N}} = p^m \cdot (v_i)_{i \in \mathbb{N}}\) by Proposition 2.2.9. To see that \((x_i)_{i \in \mathbb{N}} \cdot (y_i)_{i \in \mathbb{N}}\) is nonzero, we note that

\[
(x_i)_{i \in \mathbb{N}} \cdot (y_i)_{i \in \mathbb{N}} \cdot (v_i)_{i \in \mathbb{N}}^{-1} \cdot (u_i)_{i \in \mathbb{N}}^{-1} = p^n \cdot (u_i)_{i \in \mathbb{N}} \cdot p^m \cdot (y_i)_{i \in \mathbb{N}} \cdot (v_i)_{i \in \mathbb{N}}^{-1} \cdot (u_i)_{i \in \mathbb{N}}^{-1}
\]

\[
= p^{n+m} \cdot (u_i)_{i \in \mathbb{N}} \cdot (v_i)_{i \in \mathbb{N}} \cdot (v_i)_{i \in \mathbb{N}}^{-1} \cdot (u_i)_{i \in \mathbb{N}}^{-1}
\]

\[
= p^{n+m}
\]

and that \(p^{n+m}\) is nonzero in \(\mathbb{Z}_p\) (by Proposition 2.2.4). Since a product involving \((x_i)_{i \in \mathbb{N}} \cdot (y_i)_{i \in \mathbb{N}}\) does not evaluate to zero, we can conclude that \((x_i)_{i \in \mathbb{N}} \cdot (y_i)_{i \in \mathbb{N}}\) itself is nonzero in \(\mathbb{Z}_p\). Since \((x_i)_{i \in \mathbb{N}}\) and \((y_i)_{i \in \mathbb{N}}\) were arbitrary, this implies that \(\mathbb{Z}_p\) is an integral domain.

\[
\]

We can deduce from this that \(\mathbb{Z}_p\) is a principal ideal domain.
Proposition 2.2.12. The ring $\mathbb{Z}_p$ is a principal ideal domain, and the distinct nonzero ideals of $\mathbb{Z}_p$ are given by $p^n\mathbb{Z}_p$ for distinct $n \in \mathbb{N}$.

Proof. Let $I$ be an ideal of $\mathbb{Z}_p$. If $I$ is the zero ideal, then we are done. If not, then $I$ contains some nonzero elements, and we can pick $x \in I$ to be such that $v_p(x)$ is minimal. By Proposition 2.2.10, every element of $I$ is divisible by $x$, since $v_p(x)$ is minimal among all elements of $I$, and hence $I = x\mathbb{Z}_p$.

Let $m = v_p(x)$. By Proposition 2.2.9, we can find that $x = p^m \cdot (u_i)_{i \in \mathbb{N}}$ for some invertible $(u_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p$. But then, $(u_i)_{i \in \mathbb{N}}$ being invertible means that $p^m = x \cdot (u_i)_{i \in \mathbb{N}} \in x\mathbb{Z}_p$. Since $p^m$ divides $x$ and $x$ divides $p^m$, it immediately follows that $p^m\mathbb{Z}_p = x\mathbb{Z}_p = I$.

Hence every nonzero ideal of $\mathbb{Z}_p$ can be written as $p^n\mathbb{Z}_p$ for some $n \in \mathbb{N}$.

If $n, m \in \mathbb{N}$ and $p^n\mathbb{Z}_p = p^m\mathbb{Z}_p$, then $p^n$ divides $p^m$ and $p^m$ divides $p^n$ in $\mathbb{Z}_p$. Hence $n = v_p(p^n) \leq v_p(p^m) = m$ by Proposition 2.2.10, and the same argument tells us that $m = v_p(p^m) \leq v_p(p^n) = n$. Hence $n = m$, meaning that different $n \in \mathbb{N}$ must give different ideals $p^n\mathbb{Z}_p$ of $\mathbb{Z}_p$.

\[ \square \]

2.3 The Localization $\mathbb{Z}_{(p)}$

We will now define the localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ as follows.

Definition 2.3.1. $\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, \ p \nmid b \right\}$ with the usual equivalence

\[ \frac{a}{b} \sim \frac{c}{d} \iff ad - bc = 0 \]

and the addition and multiplication inherited from $\mathbb{Z}$.

It is immediately apparent that $\mathbb{Z}_{(p)}$ is a commutative ring, and that every integer
not divisible by \( p \) is invertible in \( \mathbb{Z}_p \). It is also apparent that \( \mathbb{Z}_p \) is a subring of \( \mathbb{Q} \), and hence an integral domain. With the following proposition, we can further deduce that \( \mathbb{Z}_p \) is a PID, and that the distinct nonzero ideals of \( \mathbb{Z}_p \) are given by \( p^n\mathbb{Z}_p \) for distinct \( n \in \mathbb{N} \).

**Proposition 2.3.2.** Every nonzero element of \( \mathbb{Z}_p \) is the product of a unit and a power of \( p \).

*Proof.* Let \( \frac{a}{b} \) be a nonzero element of \( \mathbb{Z}_p \). Since \( \frac{a}{b} \) is nonzero, the integer \( a \) must be nonzero, and hence we can write \( a = mp^n \) for some integer \( n \) and some nonzero integer \( m \) not divisible by \( p \). Then \( \frac{a}{b} = \frac{mp^n}{b} = \frac{m}{b} \cdot p^n = u \cdot p^n \), where \( u = \frac{m}{b} \) is a unit. We know that \( u \) is a unit because \( p \nmid m \), hence \( \frac{b}{m} \in \mathbb{Z}_p \).

**Corollary 2.3.3.** The ring \( \mathbb{Z}_p \) is a principal ideal domain, and the distinct nonzero ideals of \( \mathbb{Z}_p \) are given by \( p^n\mathbb{Z}_p \) for distinct \( n \in \mathbb{N} \).

*Proof.* This follows from Proposition 2.3.2, in a similar fashion to how Proposition 2.2.12 follows from Proposition 2.2.9.

Information on localizations, including \( \mathbb{Z}_p \), can be found in many standard commutative algebra textbooks, such as Atiyah & McDonald [5, Chapter 3]; however, our interest will be in the relationship between \( \mathbb{Z}_p \) and \( \mathbb{Z}_p \), the ring defined and discussed in Section 2.2. We start by noting that \( \mathbb{Z}_p \) is isomorphic to a subring of \( \mathbb{Z}_p \), and that they have the same ideal structure, as is already suggested by Proposition 2.2.12 and Corollary 2.3.3.
Proposition 2.3.4. The map \( \phi : \mathbb{Z}_p \to \mathbb{Z}_p \) given by

\[
\phi \left( \frac{a}{b} \right) = (ab^{-1} \mod p^{i+1})_{i \in \mathbb{N}}
\]

is an injective ring homomorphism.

Proof. We start by observing that \( \phi \) is well-defined. By Proposition 2.2.4, the elements \((a)_{i \in \mathbb{N}}\) and \((b)_{i \in \mathbb{N}}\) belong to \(\mathbb{Z}_p\), since \(a\) and \(b\) are integers. Since \(p \nmid b\), the integer \(b\) is invertible in \(\mathbb{Z}/p^{i+1}\mathbb{Z}\) for all \(i \in \mathbb{N}\), and \(b \not\equiv 0 \mod p\). It follows that \(v((b)_{i \in \mathbb{N}}) = 0\) and, by the proof of Proposition 2.2.8, that \((b)_{i \in \mathbb{N}} \) is invertible in \(\mathbb{Z}_p\) with inverse 

\((b)^{-1}_{i \in \mathbb{N}} = (b^{-1})_{i \in \mathbb{N}} \in \mathbb{Z}_p\). Hence \(\phi \left( \frac{a}{b} \right) = (ab^{-1})_{i \in \mathbb{N}} = (a)_{i \in \mathbb{N}} \cdot (b^{-1})_{i \in \mathbb{N}} = (a)_{i \in \mathbb{N}} \cdot (b)^{-1}_{i \in \mathbb{N}}\) is an element of \(\mathbb{Z}_p\) by Proposition 2.2.2.

If \(\frac{c}{d} \in \mathbb{Z}_p\) and \(\frac{c}{d} = \frac{a}{b}\), then \(ad - bc = 0\) and hence \(ad = bc\). It follows that

\[
ab^{-1} \equiv a(dd^{-1})b^{-1} \mod p^{i+1} \\
\equiv (bc)d^{-1}b^{-1} \mod p^{i+1} \\
\equiv cd^{-1} \mod p^{i+1}
\]

for all \(i \in \mathbb{N}\), since neither \(b\) nor \(d\) can be divisible by \(p\) in \(\mathbb{Z}\), and hence both are invertible in \(\mathbb{Z}/p^{i+1}\mathbb{Z}\). Hence \(\phi \left( \frac{a}{b} \right) \equiv \phi \left( \frac{c}{d} \right)\), and so \(\phi\) is well-defined.

If \(\frac{a}{b}, \frac{c}{d} \in \mathbb{Z}_p\), then we also have that \(\phi \left( \frac{a}{b} \cdot \frac{c}{d} \right) = \phi \left( \frac{ac}{bd} \right) = (ac(bd)^{-1})_{i \in \mathbb{N}} = (acb^{-1}d^{-1})_{i \in \mathbb{N}} = (ab^{-1})_{i \in \mathbb{N}} \cdot (cd^{-1})_{i \in \mathbb{N}} = \phi \left( \frac{a}{b} \right) \cdot \phi \left( \frac{c}{d} \right)\). Furthermore, \(\phi \left( \frac{a}{b} + \frac{c}{d} \right) = \phi \left( \frac{ad + bc}{bd} \right) = ((ad + bc)(bd)^{-1})_{i \in \mathbb{N}} = (adb^{-1}d^{-1} + bcb^{-1}d^{-1})_{i \in \mathbb{N}} = (ab^{-1} + cd^{-1})_{i \in \mathbb{N}} = (ab^{-1})_{i \in \mathbb{N}} + (cd^{-1})_{i \in \mathbb{N}} = \phi \left( \frac{a}{b} \right) + \phi \left( \frac{c}{d} \right)\), proving that the map \(\phi\) is a homomorphism of
rings. To see that $\phi$ is injective, we observe that

$$\phi \left( \frac{a}{b} \right) = (0)_{i \in \mathbb{N}} \implies (ab^{-1} \mod p^{i+1})_{i \in \mathbb{N}} = (0)_{i \in \mathbb{N}}$$

$$\implies ab^{-1} \equiv 0 \mod p^i \quad \forall i$$

$$\implies a \equiv 0 \mod p^i \quad \forall i$$

$$\implies a = 0$$

$$\implies \frac{a}{b} = 0 \in \mathbb{Z}_{(p)}$$

hence $\phi$ is an injective ring homomorphism.

This enables us to think of $\mathbb{Z}_{(p)}$ as a subring of $\mathbb{Z}_p$, using the injection $\phi$. We already suspected that there is a one-to-one correspondence between the ideals of $\mathbb{Z}_{(p)}$ and $\mathbb{Z}_p$; we will now use $\phi$ to prove it.

**Proposition 2.3.5.** For all $n \in \mathbb{N}$, $\phi^{-1}(p^n\mathbb{Z}_p) = p^n\mathbb{Z}_{(p)}$, and hence $\phi^{-1}$ induces a one-to-one correspondence between the ideals of $\mathbb{Z}_p$ and the ideals of $\mathbb{Z}_{(p)}$.

**Proof.** Both $\mathbb{Z}_{(p)}$ and $\mathbb{Z}_p$ are commutative, so all ideals will be two-sided.
For \( n \) a non-negative integer

\[
\phi^{-1}(p^n\mathbb{Z}_p) = \left\{ \frac{a}{b} \in \mathbb{Z}_p : p^n \text{ divides } (ab^{-1} \mod p^{i+1})_{i \in \mathbb{N}} \text{ in } \mathbb{Z}_p \right\}
\]

\[
= \left\{ \frac{a}{b} \in \mathbb{Z}_p : v_p((ab^{-1} \mod p^{i+1})_{i \in \mathbb{N}}) \geq v_p(p^n) \right\}
\]

\[
= \left\{ \frac{a}{b} \in \mathbb{Z}_p : v_p((ab^{-1} \mod p^{i+1})_{i \in \mathbb{N}}) \geq n \right\}
\]

\[
= \left\{ \frac{a}{b} \in \mathbb{Z}_p : ab^{-1} \equiv 0 \mod p^{i+1} \forall i \in \{0, 1, ..., n - 1\} \right\}
\]

\[
= \left\{ \frac{a}{b} \in \mathbb{Z}_p : ab^{-1} \equiv 0 \mod p^n \right\}
\]

\[
= \left\{ \frac{a}{b} \in \mathbb{Z}_p : a \equiv 0 \mod p^n \right\}
\]

\[
= \left\{ \frac{a}{b} \in \mathbb{Z}_p : p^n \text{ divides } a \text{ in } \mathbb{Z} \right\}
\]

by Propositions 2.2.3 and 2.2.10. But if \( p^n \) divides \( a \) in \( \mathbb{Z} \), then \( \frac{a}{b} = \left(\frac{a}{p^n}\right) \cdot \frac{p^n}{b} \) certainly belongs to \( p^n\mathbb{Z}_p(p) \).

Conversely, if \( \frac{a}{b} \in p^n\mathbb{Z}_p(p) \), then there must exist \( \frac{a}{d} \in \mathbb{Z}_p(p) \) such that \( \frac{a}{b} = \left(\frac{a}{d}\right) \cdot \frac{p^n}{b} \). Since \( \frac{a}{d} \cdot p^n = \frac{a}{b} \cdot \frac{p^n}{b} \), this implies that \( \frac{a}{d} \cdot p^n = \frac{a}{b} \cdot p^n \), and hence that \( ad - bcp^n = 0 \) in \( \mathbb{Z} \). If follows that \( ad = bcp^n \), and hence that \( p^n \) divides \( ad \). Since \( d \) isn’t divisible by \( p \), this can only mean that \( p^n \) divides \( a \).

Hence \( \frac{a}{b} \in \phi^{-1}(p^n\mathbb{Z}_p) \) if and only if \( \frac{a}{b} \in p^n\mathbb{Z}_p(p) \), and we can conclude that \( \phi^{-1}(p^n\mathbb{Z}_p) = p^n\mathbb{Z}_p(p) \). By Proposition 2.2.12 and Corollary 2.3.3, it follows that \( \phi^{-1} \) induces a one-to-one correspondence between the ideals of \( \mathbb{Z}_p \) and the ideals of \( \mathbb{Z}_p(p) \).

\[\square\]

Importantly, we then get the following result.

**Proposition 2.3.6.** For all \( n \in \mathbb{N} \), the map \( \phi \) induces an isomorphism between \( \mathbb{Z}_p(p)/p^n\mathbb{Z}_p(p) \) and \( \mathbb{Z}_p/p^n\mathbb{Z}_p \).
Proof. Let $\theta_n$ be the quotient map from $\mathbb{Z}_p$ to $\mathbb{Z}_p/p^n\mathbb{Z}_p$, and consider the composition $\theta_n \circ \phi$. The result is trivial when $n = 0$, so we will assume $n \geq 1$.

To see that $\theta_n \circ \phi$ is surjective, consider an arbitrary element $\gamma \in \mathbb{Z}_p/p^n\mathbb{Z}_p$. Since the quotient $\theta_n : \mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ is surjective, we can find $(a_i)_{i \in \mathbb{N}} \in \mathbb{Z}_p$ such that $\theta_n((a_i)_{i \in \mathbb{N}}) = \gamma$. But then, $\theta_n \circ \phi(a_{n-1}) = \theta_n((a_{n-1})_{i \in \mathbb{N}}) = \gamma$ by Corollary 2.2.7 (which tells us that $p^n$ divides $(a_i)_{i \in \mathbb{N}} - (a_{n-1})_{i \in \mathbb{N}}$, and hence that $(a_i)_{i \in \mathbb{N}}$ and $(a_{n-1})_{i \in \mathbb{N}}$ represent the same element under the map $\theta_n$).

Now, consider that $x \in \ker(\theta_n \circ \phi)$ if and only if $\phi(x) \in \ker(\theta_n)$ – i.e. $\ker(\theta_n \circ \phi) = \phi^{-1}(\ker(\theta_n))$. But $\ker(\theta_n) = p^n\mathbb{Z}_p$, and so

$$\ker(\theta_n \circ \phi) = \phi^{-1}(\ker(\theta_n))$$
$$= \phi^{-1}(p^n\mathbb{Z}_p)$$
$$= p^n\mathbb{Z}_{(p)}$$

by Proposition 2.3.5.

Hence $\theta_n \circ \phi$ gives a surjective ring homomorphism from $\mathbb{Z}_{(p)}$ to $\mathbb{Z}_p/p^n\mathbb{Z}_p$, and the kernel of this homomorphism is $p^n\mathbb{Z}_{(p)}$. Therefore, the rings $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$ and $\mathbb{Z}_p/p^n\mathbb{Z}_p$ are isomorphic.

\[
\square
\]

Corollary 2.3.7. For all $n \in \mathbb{N}$, the rings $\mathbb{Z}/p^n\mathbb{Z}$, $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$ and $\mathbb{Z}_p/p^n\mathbb{Z}_p$ are isomorphic.

Proof. By Proposition 2.3.6, $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$ and $\mathbb{Z}_p/p^n\mathbb{Z}_p$ are isomorphic. To see that $\mathbb{Z}/p^n\mathbb{Z}$ and $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$ are isomorphic, let $\theta$ be the map sending $\frac{a}{b}$ in $\mathbb{Z}_{(p)}$ to the element $ab^{-1} \mod p^n$ in $\mathbb{Z}/p^n\mathbb{Z}$. Since $b$ is not divisible by $p$, this definition makes sense. Then $\theta$ is a surjective ring homomorphism and the kernel of $\theta$ is $p^n\mathbb{Z}_{(p)}$, hence
$\mathbb{Z}/p^n\mathbb{Z}$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. Therefore, all of the rings $\mathbb{Z}/p^n\mathbb{Z}$, $\mathbb{Z}/p^n\mathbb{Z}$, and $\mathbb{Z}/p^n\mathbb{Z}$ are isomorphic.

Hence the quotient rings $\mathbb{Z}/p^n\mathbb{Z}$ and $\mathbb{Z}/p^n\mathbb{Z}$ are simply isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$, which is a simple and well-known ring.

2.4 The Integral Quaternions

Here we present the most important object of study in this thesis. We will mostly be interested in the integral quaternions, which are the quaternions over the ring $\mathbb{Z}$, and in the quaternions over the rings $\mathbb{Z}/p$ or $\mathbb{Z}/p$ for some prime number $p$. We will almost always work with these specific rings, but our definition is more broad.

**Definition 2.4.1.** Let $R$ be a commutative ring and let $M$ be an $R$-module. The quaternions over the module $M$ are defined to be the $R$-module

$$H_M = \{a + bi + cj + dk | a, b, c, d \in M\}.$$

As an $R$-module, this is simply the same as the direct sum of four copies of $M$. However, we will be applying the multiplicative structure of Hamilton’s quaternions to $i$, $j$, and $k$ [6]. This means multiplication rules $i^2 = j^2 = k^2 = ijk = -1$, and the implied non-commutative products

$$ij = -ji = k,$$
$$jk = -kj = i, \text{ and}$$
$$ki = -ik = j.$$
Doing this makes $H_R$ into a ring whenever $R$ is a ring, and it makes $H_M$ into an $H_R$-module whenever $M$ is an $R$-module. Naturally, it also makes $H_A$ into an $H_R$-algebra whenever $A$ is an $R$-algebra.

We will assume that the rings $R$ and the algebras $A$ in question are always commutative. We then get the following important theorem.

**Theorem 2.4.2.** Let $R$ be a commutative ring with $M$ and $N$ being $R$-modules, and let $\nu : M \to N$ be an $R$-module homomorphism with kernel $K$. Then $\nu$ can be extended to an $H_R$-module homomorphism from $H_M$ to $H_N$ by setting

\[
\nu(i) = i, \\
\nu(j) = j, \text{ and} \\
\nu(k) = k.
\]

This extension has kernel $H_K$ and image $H_{\nu(M)}$, hence preserving both injectivity and surjectivity. If $\nu : M \to N$ is also a homomorphism of rings, then so is the extension $\nu : H_M \to H_N$.

**Proof.** The $R$-module homomorphism $\nu : M \to N$ can be extended to an $R$-module homomorphism from $H_M$ to $H_N$ by setting $\nu(i) = i$, $\nu(j) = j$, and $\nu(k) = k$, so that

\[
\nu(a + bi + cj + dk) = \nu(a) + \nu(b)i + \nu(c)j + \nu(d)k
\]

for all $a + bi + cj + dk \in H_M$. If $\nu : M \to N$ was a homomorphism of rings, then so is $\nu : H_M \to H_N$, since it preserves the multiplication of $i$, $j$, and $k$. Since $\nu : M \to N$ was $R$-linear, and since $\nu : H_M \to H_N$ fixes $i$, $j$, and $k$, we can also conclude that $\nu : H_M \to H_N$ is an $H_R$-module homomorphism.
Suppose \( \nu : M \to N \) has kernel \( K \), and that \( a + bi + cj + dk \in H_M \). Then \( \nu(a + bi + cj + dk) = 0 \) if and only if \( \nu(a) + \nu(b)i + \nu(c)j + \nu(d)k = 0 \), which happens if and only if \( \nu(a) = \nu(b) = \nu(c) = \nu(d) = 0 \), and hence if and only if \( a, b, c, d \in K \). If \( \nu : M \to N \) is injective, then we can conclude that \( \nu(a + bi + cj + dk) = 0 \) if and only if \( a = b = c = d = 0 \), and hence if and only if \( a, b, c, d \in K \). If not, then we still get that \( \nu(a + bi + cj + dk) = 0 \) if and only if \( a, b, c, d \in K \), and hence that the kernel of \( \nu : H_M \to H_N \) is \( H_K \).

Now let \( e + fi + gj + hk \in H_N \). Then \( e + fi + gj + hk \) belongs to the image of \( \nu : H_M \to H_N \) if and only if there exists some \( a + bi + cj + dk \in H_M \) such that \( \nu(a + bi + cj + dk) = e + fi + gj + hk \). But then, since \( \nu(a + bi + cj + dk) = \nu(a) + \nu(b)i + \nu(c)j + \nu(d)k \), this happens if and only if there exists \( a, b, c, d \in M \) such that \( \nu(a) = e, \nu(b) = f, \nu(c) = g, \) and \( \nu(d) = h \). This implies that the image of \( \nu : H_M \to H_N \) is \( H_{\nu(M)} \), as expected. When \( \nu : M \to N \) is surjective, then \( H_{\nu(M)} = H_N \), and hence the map \( \nu : H_R \to H_S \) is surjective too.

Considering more carefully the case of \( \nu \) being a ring homomorphism, we can see that the set \( H_K \) from Theorem 2.4.2 must be a two-sided ideal of \( H_M \). We can also prove this directly for ideals of any commutative ring \( R \) in the following proposition.

**Proposition 2.4.3.** Let \( R \) be a commutative ring and let \( I \) be an ideal of \( R \). Then \( H_I \) is a two-sided ideal of \( H_R \) and \( H_I = IH_R \), where
\[
IH_R = \left\{ \sum_{t=1}^{n} x_t \gamma_t \mid x_t \in I, \gamma_t \in H_R, n \in \mathbb{N} \right\}.
\]

**Proof.** That \( IH_R \) is closed under addition is immediate from the definition of \( IH_R \). That it is closed under multiplication by elements of \( H_R \) comes from the fact that
elements of $I$ (and in fact, all elements of $R$) belong to the center of $H_R$. So, for instance,

$$\alpha(\sum_{t=1}^{n} x_t \gamma_t) \beta = \sum_{t=1}^{n} \alpha(x_t \gamma_t) \beta = \sum_{t=1}^{n} x_t \gamma'_t$$

for all $\alpha, \beta \in H_R$ and $\sum_{t=1}^{n} x_t \gamma_t \in IH_R$, where $\gamma'_t = \alpha \gamma t \beta \in H_R$. Hence $IH_R$ is a two-sided ideal of $H_R$.

Given an element $a + bi + cj + dk \in H_R$, we know that $a + bi + cj + dk \in IH_R$ if and only if $a + bi + cj + dk = \sum_{t=1}^{n} x_t \gamma_t$ for some $x_t \in I, \gamma_t \in H_R$, and $n \in \mathbb{N}$. Writing

$$\gamma_t = a_t + b_t i + c_t j + d_t k$$

for all $t \in \{1, 2, \ldots, n\}$, we then get that $a = \sum_{t=1}^{n} x_t a_t, b = \sum_{t=1}^{n} x_t b_t, c = \sum_{t=1}^{n} x_t c_t,$ and $d = \sum_{t=1}^{n} x_t d_t$. Since $I$ is a two-sided ideal of $R$ and $x_t \in I$ for all $t \in \{1, 2, \ldots, n\}$, we can conclude that $a, b, c, d \in I$. On the other hand, if $a, b, c, d \in I$, then the element $a + bi + cj + dk$ is equal to $\sum_{t=1}^{n} x_t \gamma_t$ where $n = 4, x_1 = a, x_2 = b, x_3 = c, x_4 = d, \gamma_1 = 1, \gamma_2 = i, \gamma_3 = j,$ and $\gamma_4 = k$. This implies that $a + bi + cj + dk \in IH_R$ if and only if $a, b, c, d \in I$, and hence that $H_I = IH_R$.

From Theorem 2.4.2, we also get the following.

**Proposition 2.4.4.** For all commutative rings $R$ and $R$-modules $M$, and for all submodules $N \subseteq M$, the $H_R$-modules $H_M/H_N$ and $H_{M/N}$ are isomorphic. Furthermore, if $A$ is an $R$-algebra and $I$ is an ideal of $A$, then the $H_R$-algebras $H_A/H_I$ and $H_{A/I}$ are isomorphic.

**Proof.** If $\theta : M \to M/N$ is the projection map from $M$ to $M/N$, then Theorem 2.4.2
tells us that we can extend $\theta$ to a surjective $H_R$-module homomorphism from $H_M$ to $H_{M/N}$. Since the kernel of $\theta : M \to M/N$ is $N$, the kernel of its extension must be $H_N$, and hence $H_M/H_N$ and $H_{M/N}$ are isomorphic as $H_R$-modules. An identical argument holds for algebras.

Using this, we would like to extend the results of the previous section to the integral quaternions over $\mathbb{Z}$, $\mathbb{Z}_p$, and $\mathbb{Z}_{(p)}$. To make things simpler, we will use the notation $H$ for $H_\mathbb{Z}$, $H_p$ for $H_{\mathbb{Z}_p}$ and $H_{(p)}$ for $H_{\mathbb{Z}_{(p)}}$.

The most important result regarding the rings $H_{(p)}$ and $H_p$ is the following.

**Proposition 2.4.5.** The map $\phi : \mathbb{Z}_{(p)} \to \mathbb{Z}_p$ given in Proposition 2.3.4 extends to an injective ring homomorphism from $H_{(p)}$ to $H_p$.

**Proof.** Recall that $\phi : \mathbb{Z}_{(p)} \to \mathbb{Z}_p$ is given by

$$\phi \left( \frac{a}{b} \right) = (ab^{-1} \mod p^{i+1})_{i \in \mathbb{N}}$$

for all $\frac{a}{b} \in \mathbb{Z}_{(p)}$. It is an injective ring homomorphism from $\mathbb{Z}_{(p)}$ to $\mathbb{Z}_p$ by Proposition 2.3.4, and hence extends to an injective ring homomorphism from $H_{(p)}$ to $H_p$ by Theorem 2.4.2.

Hence we can view the ring $H_{(p)}$ as a subring of the ring $H_p$, in the same way that we can view the ring $\mathbb{Z}_{(p)}$ as a subring of the ring $\mathbb{Z}_p$.

We then get the following.

**Proposition 2.4.6.** The map $\phi$ from Proposition 2.4.5 has the property that $\phi^{-1}(p^n H_p) = p^n H_{(p)}$ for all $n \in \mathbb{N}$. 

23
Proof. First, note that \( a + bi + cj + dk \in p^nH_{(p)} \) if and only if \( a, b, c, d \in p^n\mathbb{Z}_{(p)} \), and that \( a + bi + cj + dk \in p^nH_p \) if and only if \( a, b, c, d \in p^n\mathbb{Z}_p \), from Proposition 2.4.3. Hence

\[
\phi^{-1}(p^nH_p) = \{ a + bi + cj + dk \in H_{(p)} \mid \phi(a + bi + cj + dk) \in p^nH_p \}
\]

\[
= \{ a + bi + cj + dk \in H_{(p)} \mid \phi(a) + \phi(b)i + \phi(c)j + \phi(d)k \in p^nH_p \}
\]

\[
= \{ a + bi + cj + dk \in H_{(p)} \mid \phi(a), \phi(b), \phi(c), \phi(d) \in p^n\mathbb{Z}_p \}
\]

\[
= \{ a + bi + cj + dk \in H_{(p)} \mid a, b, c, d \in \phi^{-1}(p^n\mathbb{Z}_p) \}
\]

\[
= \{ a + bi + cj + dk \in H_{(p)} \mid a, b, c, d \in p^n\mathbb{Z}_{(p)} \}
\]

\[
= p^nH_{(p)}
\]

by Proposition 2.3.5, using the extension of \( \phi \) defined in Proposition 2.4.5.

This gives us a relation between certain ideals of \( H_{(p)} \) and \( H_p \), which will allow us to more easily calculate the zeta function of \( H_{(p)} \) when \( p \) is odd (when \( p \) is even we will need a different approach). Unfortunately, it only implies a correspondence between ideals of the form \( p^nH_{(p)} \) and \( p^nH_p \). However, this can be extended to left ideals of \( H_{(p)} \) and \( H_p \) containing \( p^nH_{(p)} \) and \( p^nH_p \) with the following proposition.

**Proposition 2.4.7.** For all \( n \in \mathbb{N} \), the map \( \phi \) induces an \( H_{(p)} \)-algebra isomorphism from \( H_{(p)}/p^nH_{(p)} \) to \( H_p/p^nH_p \).

**Proof.** This follows from Proposition 2.4.6 using the same argument as in Proposition 2.3.6. In addition, one can note that \( H_{(p)}/p^nH_{(p)} \) is isomorphic to \( H_{\mathbb{Z}_{(p)}}/p^n\mathbb{Z}_{(p)} \), and that \( H_p/p^nH_p \) is isomorphic to \( H_{\mathbb{Z}_p}/p^n\mathbb{Z}_p \), by Proposition 2.4.4. Since \( \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \) is isomorphic to \( \mathbb{Z}_p/p^n\mathbb{Z}_p \) (Proposition 2.3.6), Theorem 2.4.2 implies that \( H_{\mathbb{Z}_{(p)}}/p^n\mathbb{Z}_{(p)} \) is
isomorphic to $H_{\mathbb{Z}/p^n\mathbb{Z}}$. These isomorphisms agree with $\phi$, hence the result.

Hence we get the following conclusion.

**Corollary 2.4.8.** For all $n \in \mathbb{N}$, the map $\phi^{-1}$ induces an order-preserving and index-preserving bijection between the left ideals of $H_p$ containing $p^nH_p$ and the left ideals of $H_{(p)}$ containing $p^nH_{(p)}$.

**Proof.** This follows from Proposition 2.4.7.

**Corollary 2.4.9.** The map $\phi^{-1}$ induces an order-preserving and index-preserving bijection between the left ideals of $H_p$ containing $p^nH_p$ for some $n \in \mathbb{N}$, and the left ideals of $H_{(p)}$ containing $p^mH_{(p)}$ for some $m \in \mathbb{N}$.

**Proof.** This follows from Corollary 2.4.8.

This gives us an ideal correspondence between $H_{(p)}$ and $H_p$, similar to the one we found in Proposition 2.3.5 between $\mathbb{Z}_{(p)}$ and $\mathbb{Z}_p$. We then get a similar collection of isomorphisms to the ones we found in Corollary 2.3.7.

**Corollary 2.4.10.** For all $n \in \mathbb{N}$, the rings $H_{\mathbb{Z}/p^n\mathbb{Z}}$, $H/p^nH$, $H_{(p)}/p^nH_{(p)}$ and $H_p/p^nH_p$ are isomorphic.

**Proof.** The fact that $H_{(p)}/p^nH_{(p)}$ and $H_p/p^nH_p$ are isomorphic follows from Proposition 2.4.7. Propositions 2.4.3 and 2.4.4 tell us that $H_{(p)}/p^nH_{(p)}$ is isomorphic to $H_{\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}}$, and that $H/p^nH$ is isomorphic to $H_{\mathbb{Z}/p^n\mathbb{Z}}$. Since $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$ by Corollary 2.3.7, it follows from Theorem 2.4.2 that $H_{\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}}$ is isomorphic to
Therefore, we can conclude that all of the rings \( \mathbb{Z}/p^n\mathbb{Z} \), \( H/p^n H \), \( H_{(p)}/p^n H_{(p)} \) and \( H_p/p^n H_p \) are isomorphic.

Note that we could just as easily have written \( p^n H_{(p)} \) as \( H_{p^n\mathbb{Z}(p)} \) and \( p^n H_p \) as \( H_{p^n\mathbb{Z}_p} \), from Proposition 2.4.3. We then get a few other results which are useful later on, stating with the fact that \( H_{(p)} \) is a subring of \( H_{\mathbb{Q}} \).

**Proposition 2.4.11.** If \( R \) is ring and \( S \) is a subring of \( R \), then \( H_S \) is a subring of \( H_R \).

*Proof.* This is Theorem 2.4.2 applied to the injective ring homomorphism from the ring \( S \) into the ring \( R \).

**Corollary 2.4.12.** For all prime numbers \( p \), the ring \( H_{(p)} \) is a subring of \( H_{\mathbb{Q}} \).

*Proof.* This follows from Proposition 2.4.11, since \( \mathbb{Z}_{(p)} \) is a subring of \( \mathbb{Q} \).

We then note that both \( H_{(p)} \) and \( H_p \) are Noetherian rings.

**Proposition 2.4.13.** If the ring \( R \) is Noetherian, then the ring \( H_R \) is Noetherian.

*Proof.* \( H_R \) is a finitely-generated \( R \)-module, and hence also Noetherian, both as an \( R \)-module and as a ring.

**Corollary 2.4.14.** The rings \( H_{(p)} \) and \( H_p \) are Noetherian.
Proof. The rings $\mathbb{Z}_p$ and $\mathbb{Z}_p$ are principal ideal domains by Proposition 2.2.12 and Corollary 2.3.3. Hence both rings are Noetherian. Therefore, by Proposition 2.4.13, both of the rings $H_p$ and $H_p$ are Noetherian.

Finally, we have an important $H_p$-module homomorphism that we will want to use in the case that $p = 2$.

**Proposition 2.4.15.** If $n, m \in \mathbb{N}$ and $n \leq m$, then $p^n H_p / p^m H_p$ and $H_p / p^{m-n} H_p$ are isomorphic as $H_p$-modules.

**Proof.** Let $\theta : \mathbb{Z}_p \to p^n \mathbb{Z}_p / p^m \mathbb{Z}_p$ be the map taking the element $x \in \mathbb{Z}_p$ to the element $p^n x + p^m \mathbb{Z}_p \in p^n \mathbb{Z}_p / p^m \mathbb{Z}_p$. Then $\theta$ is a surjective $\mathbb{Z}_p$-module homomorphism with kernel $p^{m-n} \mathbb{Z}_p$, and Theorem 2.4.2 tells us that we can extend $\theta$ to a surjective $H_p$-module homomorphism from $H_p$ to $H_p / p^n \mathbb{Z}_p / p^m \mathbb{Z}_p$ with kernel $H_p / p^{m-n} \mathbb{Z}_p$. Hence the $H_p$-modules $H_p / H_p / p^{m-n} \mathbb{Z}_p$ and $H_p / p^n \mathbb{Z}_p / p^m \mathbb{Z}_p$ are isomorphic.

Proposition 2.4.4 tells us that $H_p / p^n \mathbb{Z}_p / p^m \mathbb{Z}_p$ and $H_p / p^n \mathbb{Z}_p / p^m \mathbb{Z}_p$ are isomorphic, and hence that $H_p / H_p / p^{m-n} \mathbb{Z}_p$ and $H_p / p^n \mathbb{Z}_p / H_p / p^m \mathbb{Z}_p$ are isomorphic, as $H_p$-modules. By Proposition 2.4.3, $H_p / p^{m-n} \mathbb{Z}_p = p^{m-n} H_p$, $H_p / p^n \mathbb{Z}_p = p^n H_p$, and $H_p / p^m \mathbb{Z}_p = p^m H_p$, and so we can conclude that the $H_p$-modules $p^n H_p / p^m H_p$ and $H_p / p^{m-n} H_p$ are isomorphic.

\[\square\]

### 2.5 The Norm

For some of our zeta function computations, it will be important to understand the norm on $H_R$. Again, we assume that the ring $R$ is commutative.
**Definition 2.5.1.** The norm on $H_R$ is the map $N : H_R \to R$ given by $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$.

The norm on $H_R$ has many important properties, including being multiplicative and therefore preserving units. But even before that, we note that norms can be written as products in $H_R$.

**Proposition 2.5.2.** For all $a + bi + cj + dk \in H_R$,

$$N(a + bi + cj + dk) = (a - bi - cj - dk)(a + bi + cj + dk).$$

**Proof.** Through simple computation, we find that

$$(a - bi - cj - dk)(a + bi + cj + dk) = (a - (bi + cj + dk))(a + (bi + cj + dk)) = a^2 - (bi + cj + dk)^2$$

Expanding, we also have that

$$(bi + cj + dk)^2 = bi(bi + cj + dk) + cj(bi + cj + dk) + dk(bi + cj + dk) = (b^2i^2 + bci + bdik) + (bcji + c^2j^2 + cdk) + (bdki + cdkj + d^2k^2) = -b^2 - c^2 - d^2 + bc(ij + ji) + bd(ik + ki) + cd(jk + kj) = -b^2 - c^2 - d^2$$
since \( ji = -ij, kj = -jk, \) and \( ik = -ki. \)

Putting this together, we can conclude that

\[
(a - bi - cj - dk)(a + bi + cj + dk)
= a^2 - (bi + cj + dk)^2
= a^2 - (-b^2 - c^2 - d^2)
= a^2 + b^2 + c^2 + d^2
= N(a + bi + cj + dk)
\]

\[\square\]

**Corollary 2.5.3.** If \( I \) is a (left or right) ideal of \( H_R \) and \( a + bi + cj + dk \in I \), then \( N(a + bi + cj + dk) \in I \).

**Proof.** This follows immediately from Proposition 2.5.2. To see that it applies to both left and right ideals, consider the fact that

\[
N(a - bi - cj - dk) = a^2 + (-b)^2 + (-c)^2 + (-d)^2
= a^2 + b^2 + c^2 + d^2
= N(a + bi + cj + dk)
\]
and hence that

\[ N(a + bi + cj + dk) = N(a - bi - cj - dk) \]
\[ = (a - (-b)i - (-c)j - (-d)k)(a - bi - cj - dk) \]
\[ = (a + bi + cj + dk)(a - bi - cj - dk) \]

for all \( a + bi + cj + dk \in H_R \) by Proposition 2.5.2. Any left or right ideal containing \( a + bi + cj + dk \) therefore also contains \( N(a + bi + cj + dk) \).

This brings us to the most important result, which is that the norm on \( H_R \) is multiplicative.

**Proposition 2.5.4.** The norm \( N : H_R \to R \) is multiplicative.
Proof. Let \( a + bi + cj + dk \) and \( e + fi + gj + hk \) belong to \( H_R \). Then

\[
(a + bi + cj + dk)(e + fi + gj + hk) = ae + afi + agj + ahk
+ bei + bf(-1) + bgj + bhk
+cej + cfji + cg(-1) + chjk
+ dek + dfki + dgkj + dh(-1)
= ae + afi + agj + ahk
+ bei + bf(-1) + bgk + bh(-j)
+ cej + cf(-k) + cg(-1) + chi
+ dek + dfj + dg(-i) + dh(-1)
= ae - bf - cg - dh
+ (af + be + ch - dg)i
+ (ag - bh + ce + df)j
+ (ah + bg - cf + de)k
\]
and hence

\[ N((a + bi + cj + dk)(e + fi + gj + hk)) = (ae - bf - cg - dh)^2 \\
+ (af + be + ch - dg)^2 \\
+ (ag - bh + ce + df)^2 \\
+ (ah + bg - cf + de)^2 \\
= a^2e^2 - abef - aceg - adeh + b^2f^2 \\
+ bcfg + bdfh + c^2d^2 + cdgh + d^2h^2 \\
+ a^2f^2 + abef + acfh - adfg + b^2e^2 \\
+ bceh - bdeg + c^2h^2 - cdhg + d^2g^2 \\
+ a^2g^2 - abgh + aceg + adfg + b^2h^2 \\
- bceh - bdfh + c^2e^2 + cdef + d^2f^2 \\
+ a^2h^2 + abgh - acfh + adeh + b^2g^2 \\
- bcfg + bdeg + c^2f^2 - cdef + d^2e^2 \\
= a^2e^2 + b^2f^2 + c^2d^2 + d^2h^2 \\
+ a^2f^2 + b^2e^2 + c^2h^2 + d^2g^2 \\
+ a^2g^2 + b^2h^2 + c^2e^2 + d^2f^2 \\
+ a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 \\
= (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) \\
= N(a + bi + cj + dk)N(e + fi + gj + hk) \]

Alternatively, one can take an \( R \)-algebra homomorphism from \( H_R \) to \( R[i]^{2\times2} \) by
sending

\[
1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad k \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}
\]

and note that the norm of an element \(a + bi + cj + dk \in H_R\) is the determinant of its image in \(R[i]^{2 \times 2}\). Since determinants in \(R[i]^{2 \times 2}\) are multiplicative, it follows that norms are as well.

\[\square\]

**Corollary 2.5.5.** Let \(a + bi + cj + dk \in H_R\). Then \(N(a + bi + cj + dk)\) is a unit in \(R\) if and only if \(a + bi + cj + dk\) is a unit in \(H_R\).

**Proof.** If \(a + bi + cj + dk\) is a unit in \(H_R\), then

\[(a + bi + cj + dk)(e + fi + gj + hk) = 1\]

for some \(e + fi + gj + hk \in H_R\). This implies that

\[N(a + bi + cj + dk)N(e + fi + gj + hk) = N(1) = 1^2 = 1\]

by Proposition 2.5.4, and hence that \(N(a + bi + cj + dk)\) is a unit with inverse \(N(e + fi + gj + hk)\) in \(R\).

Conversely, if \(N(a + bi + cj + dk)\) is a unit in \(R\), then it is also a unit in \(H_R\), since \(R\) is a subring of \(H_R\). But then

\[N(a + bi + cj + dk) = (a - bi - cj - dk)(a + bi + cj + dk)\]
by Proposition 2.5.2, and hence \(a + bi + cj + dk\) divides a unit. This implies that \(a + bi + cj + dk\) must be a unit in \(H_R\) as well.

We now want to apply these results to the ring \(H_p\), which is the one that we are working with in this paper. In particular, we can immediately come to some conclusions about the ideal structure of \(H_p\).

**Proposition 2.5.6.** Let \(R\) be any subring of \(\mathbb{R}\), and let \(a + bi + cj + dk \in H_R\). Then \(N(a + bi + cj + dk) = 0\) if and only if \(a + bi + cj + dk = 0\).

**Proof.** In the ring \(\mathbb{R}\), the sum of squares of four elements evaluates to zero if and only if all of the four elements are zero. If \(R\) is a subring of \(\mathbb{R}\), the it follows that

\[
N(a + bi + cj + dk) = 0 \iff a^2 + b^2 + c^2 + d^2 = 0
\]

\[
\iff a = b = c = d = 0
\]

\[
\iff a + bi + cj + dk = 0
\]

for all \(a + bi + cj + dk \in H_R\).

Since \(\mathbb{Z}_p\) is a subring of \(\mathbb{Q}\), and \(\mathbb{Q}\) is a subring of \(\mathbb{R}\), the result specifically holds for \(R = \mathbb{Z}_p\) and \(R = \mathbb{Q}\).

**Proposition 2.5.7.** Every nonzero left ideal of \(H_p\) has finite index, and contains \(p^n H_p\) for some \(n \in \mathbb{N}\).

**Proof.** If \(I\) is a nonzero left ideal of \(H_p\), then \(I\) contains at least one nonzero element \(a + bi + cj + dk\). By Corollary 2.5.3, \(I\) must contain the norm \(a^2 + b^2 + c^2 + d^2\), and
by Proposition 2.5.6 this norm is nonzero. Hence $a^2 + b^2 + c^2 + d^2 = u \cdot p^n$ for some non-negative integer $n$ and some invertible element $u \in \mathbb{Z}_p$ (Proposition 2.3.2). Since $u$ is invertible, this implies that $I$ contains $p^n$, and hence that $p^n H_p = H(p)p^n \subseteq I$.

Since $p^n H_p \subseteq I$ and $H(p)/p^n H_p \simeq H/p^n H$ by Corollary 2.4.10, we can immediately conclude that $|H_p/I| \leq |H(p)/p^n H_p| = |H/p^n H| = p^{4n}$. Hence the index of $I$ is finite in $H(p)$ and, in fact, divides $p^{4n}$.

From this, our earlier results from Section 2.4 can be extended.

**Corollary 2.5.8.** There is an order-preserving and index-preserving bijection between the nonzero left ideals of $H_p$ and the left ideals of $H_p$ containing $p^n H_p$ for some $n \in \mathbb{N}$.

**Proof.** Corollary 2.4.9 and Proposition 2.5.7.

We make a similar conclusion for $H_p$ in Corollary 4.4.7, using a different method. This can not follow from the reasoning here, since Proposition 2.5.6 does not apply when $R = \mathbb{Z}_p$. Building off of Proposition 2.5.6, we also have the following.

**Proposition 2.5.9.** Let $R$ be a ring such that $N(a + bi + cj + dk) = 0$ if and only if $a + bi + cj + dk = 0$ for all $a + bi + cj + dk \in H_R$, and suppose that $R$ is an integral domain. Then $H_R$ is an integral domain.

**Proof.** Let $\alpha, \beta \in H_R$ and suppose that $\alpha \beta = 0$. Then $N(\alpha)N(\beta) = N(\alpha \beta) = N(0) = 0$ by Proposition 2.5.4. Since $R$ is an integral domain, this implies that one of $N(\alpha)$ or $N(\beta)$ is zero, and hence that one of $\alpha$ or $\beta$ is zero. Therefore, $H_R$ is an integral domain.

□
Corollary 2.5.10. The rings $H_p$ and $H_Q$ are integral domains.

Proof. Proposition 2.5.6 tells us that $N(a + bi + cj + dk) = 0$ if and only if $a + bi + cj + dk = 0$ for all $a + bi + cj + dk \in H_p$ or $H_Q$. Hence the result follows from Proposition 2.5.9.
Chapter 3

The Zeta Function of $H_{(2)}$

We will use quotients of the form $2^n H_{(2)}/2^m H_{(2)}$ to find the zeta function of $H_{(2)}$. Considering quotients of this form will enable us to build a lattice of left ideals of $H_{(2)}$, starting with left ideals between $H_{(2)}$ and $2H_{(2)}$, and then extending to left ideals lying over larger powers of 2.

3.1 Ideals of $H_{(2)}/2H_{(2)}$

To start small, we consider the quotient $H_{(2)}/2H_{(2)}$. This is a ring whose ideal structure will tell us something about the ideal structure of $H_{(2)}$ between $H_{(2)}$ and $2H_{(2)}$.

The first thing to note is that this ring is fairly small, familiar, and commutative.

**Proposition 3.1.1.** The rings $H_{(2)}/2H_{(2)}$, $H/2H$, and $H_{\mathbb{F}_2}$ are isomorphic to each other, commutative, and have 16 elements.

**Proof.** That they are isomorphic follows from Corollary 2.4.10, since $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. That they are commutative follows from the quaternion multiplication given in Section 2.4.
In particular, since $1 = -1$ in $H_{F_2}$, it follows that

$$ij = -ji = ji,$$

$$ki = -ik = ik,$$ and

$$jk = -kj = kj$$

in $H_{F_2}$. Hence $H_{F_2}$ is commutative, and so are $H_{(2)}/2H_{(2)}$ and $H/2H$. The elements of $H_R$ are in bijection with $R^4$, so $|H_{F_2}| = |F_2|^4 = 2^4 = 16$.

\[\square\]

From now on, we will use the rings $H_{(2)}/2H_{(2)}$, $H/2H$, and $H_{F_2}$ interchangeably. In all cases, we will think of an element $a + bi + cj + dk$ as having coefficients $a, b, c, d \in F_2$.

One final helpful fact about $H_{(2)}/2H_{(2)}$ is the following. This is essentially a restatement of Proposition 2.5.2 that only works in the case of $H_{(2)}/2H_{(2)}$, where the underlying ring (in this case, field) has $2 = 0$.

**Proposition 3.1.2.** If $\gamma \in H_{(2)}/2H_{(2)}$ then $N(\gamma) = \gamma^2$.

**Proof.** Let $\gamma = a + bi + cj + dk \in H_{(2)}/2H_{(2)}$. Then Proposition 2.5.2 implies that

$$N(\gamma) = N(a + bi + cj + dk) = (a - bi - cj - dk)(a + bi + cj + dk).$$

However, in the ring $F_2$, 1 and $-1$ are the same. Hence $a - bi - cj - dk = a + bi + cj + dk$. 

38
and

\[ N(\gamma) = (a - bi - cj - dk)(a + bi + cj + dk) \]
\[ = (a + bi + cj + dk)(a + bi + cj + dk) \]
\[ = \gamma^2 \]

With this, we can begin finding the ideals of \( H(2)/2H(2) \), and hence the left ideals of \( H(2) \) containing \( 2H(2) \). To start, we find the unique maximal ideal of \( H(2)/2H(2) \).

**Proposition 3.1.3.** The ring \( H(2)/2H(2) \) has a single maximal ideal

\[ \mathcal{J} = \{0, 1 + i, 1 + j, 1 + k, i + j, i + k, j + k, 1 + i + j + k\} \]

consisting of all non-unit elements of \( H(2)/2H(2) \).

**Proof.** Computing the norms of all elements in \( H(2)/2H(2) \), we find that 1, i, j, k, 1 + i + j, 1 + i + k, 1 + j + k, and i + j + k have norm 1, and that 0, 1 + i, 1 + j, 1 + k, i + j, i + k, j + k, and 1 + i + j + k have norm 0.

It follows that \( \mathcal{J} \) consists of all non-unit elements of \( H(2)/2H(2) \), by Corollary 2.5.5, and that \( \mathcal{J} = \{y \in H(2)/2H(2) \mid N(y) = 0\} \).

If \( x \in H(2)/2H(2) \) and \( y \in \mathcal{J} \), then we find that

\[ N(x \cdot y) = N(x) \cdot N(y) \]
\[ = N(x) \cdot 0 \]
\[ = 0 \]
by Proposition 2.5.4, meaning that \( x \cdot y \in \mathcal{J} \).

Furthermore, if \( x, y \in \mathcal{J} \), then we find that

\[
N(x + y) = (x + y)^2 \\
= x^2 + 2xy + y^2 \\
= x^2 + y^2 \\
= 0 + 0 \\
= 0
\]

by Proposition 3.1.2, and hence that \( x + y \in \mathcal{J} \).

It follows that \( \mathcal{J} \) is an ideal of \( H(2)/2H(2) \). Since \( \mathcal{J} \) contains all non-unit elements of \( H(2)/2H(2) \), it follows immediately that it is the unique maximal ideal of \( H(2)/2H(2) \).

The other ideals can be found by the following.

**Proposition 3.1.4.** In \( H(2)/2H(2) \), the distinct ideals of index 4 are

\[
(1 + i) = \{0, 1 + i, j + k, 1 + i + j + k\}, \\
(1 + j) = \{0, 1 + j, i + k, 1 + i + j + k\}, \text{ and} \\
(1 + k) = \{0, 1 + k, i + j, 1 + i + j + k\}
\]

and the unique ideal of index 8 is

\[
(1 + i + j + k) = \{0, 1 + i + j + k\}.
\]

**Proof.** By Proposition 3.1.1, the ring \( H(2)/2H(2) \) has 16 elements. Hence an ideal of
index 4 would have 4 elements and an ideal of index 8 would have 2 elements. Since such ideals are necessarily finitely generated, we can start by looking at principal ideals of $H(2)/2H(2)$.

Starting with the principal ideal generated by $1 + i$, we find that

$$(1+i) = \{(a+bi+cj+dk) \cdot (1+i) \mid a,b,c,d \in \mathbb{F}_2\}$$

$$= \{(a+bi+cj+dk) + (a+bi+cj+dk) \cdot i \mid a,b,c,d \in \mathbb{F}_2\}$$

$$= \{(a+bi+cj+dk) + (ai-b-ck+dk) \mid a,b,c,d \in \mathbb{F}_2\}$$

$$= \{(a+bi+cj+dk) + (ai+b+ck+dk) \mid a,b,c,d \in \mathbb{F}_2\}$$

$$= \{(a+b) \cdot (1+i) + (c+d) \cdot (j+k) \mid a,b,c,d \in \mathbb{F}_2\}$$

$$= \{x \cdot (1+i) + y \cdot (j+k) \mid x,y \in \mathbb{F}_2\}$$

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

A similar argument shows that $(1+j) = \{0,1+j,i+k,1+i+j+k\}$ and $(1+k) = \{0,1+k,i+j,1+i+j+k\}$, with all of them being principal ideals of index 4 in $H(2)/2H(2)$. Since $j$ is a unit and $j+k = j \cdot (1+i)$, the element $j+k$ gives the same principal ideal as $1+i$ in $H(2)/2H(2)$. Similarly, $i+k$ and $i+j$ give the same principal ideals as $1+j$ and $1+k$, respectively.

We then note that the intersection $(1+i) \cap (1+j) = \{0,1+i+j+k\}$ must be an ideal of $H(2)/2H(2)$, and it can only be the ideal generated by $1+i+j+k$. From Proposition 3.1.3, we know that the only nonzero non-unit elements of $H(2)/2H(2)$ are $1+i, 1+j, 1+k, i+j, i+k, j+k, 1+i+j+k$, and hence we can conclude that $(1+i), (1+j), (1+k), (1+i+j+k)$ are the only non-trivial principal ideals of $H(2)/2H(2)$.

More generally, every ideal of index 4 in $H(2)/2H(2)$ must be a 4-element subset
of $\mathcal{J} = \{0, 1 + i, 1 + j, 1 + k, i + j, i + k, j + k, 1 + i + j + k\}$, since $\mathcal{J}$ is the unique maximal ideal of $H(2)/2H(2)$ by Proposition 3.1.3. Since every 4-element subset of $\mathcal{J}$ contains one of the elements $1 + i, 1 + j, 1 + k, j + k, i + k$, or $i + j$, this means that we can only find one of the 3 ideals $(1 + i), (1 + j), (1 + k)$. Hence these are the only ideals of index 4 in $H(2)/2H(2)$.

On the other hand, every ideal of index 8 in $H(2)/2H(2)$ must be a 2-element subset of $\mathcal{J}$, and it must be generated by its only nonzero element. Since $1 + i, 1 + j, 1 + k, j + k, i + k$, and $i + j$ already generate ideals of more than 2 elements, this leaves $(1 + i + j + k)$ as the only ideal of index 8 in $H(2)/2H(2)$.

It turns out that these last Propositions cover all ideals of $H(2)/2H(2)$.

**Proposition 3.1.5.** The ideal lattice of $H(2)/2H(2)$ is given by

\[ \begin{array}{c}
H(2)/2H(2) \\
| \\
J \\
| \\
(1 + i) \\
| \\
(1 + j) \\
| \\
(1 + k) \\
| \\
(1 + i + j + k) \\
| \\
(0)
\end{array} \]

\[ \text{Proof.} \] Since $|H(2)/2H(2)| = 16$ (Proposition 3.1.1), the ideals of $H(2)/2H(2)$ must have index 1, 2, 4, 8, or 16. The only ideal of index 1 is $H(2)/2H(2)$, which contains all

42
other ideals; and the only ideal of index 16 is \((0)\), which is contained in all other ideals. The only ideal of index 2 is \(J\), since it is the unique maximal ideal of \(H(2)/2H(2)\) by Proposition 3.1.3, and it must contain all ideals except for \(H(3)/2H(2)\). The rest follows immediately from Proposition 3.1.4.

This immediately tells us generators for \(J\).

**Proposition 3.1.6.** In the ring \(H(2)/2H(2)\), the ideal \(J\) from Proposition 3.1.3 is generated by the two elements \(1+i\) and \(1+j\) (equivalently, \(1+i\) and \(1+k\), or \(1+j\) and \(1+k\)). In other words,

\[
J = (1+i, 1+j) = (1+i, 1+k) = (1+j, 1+k).
\]

**Proof.** This follows from Proposition 3.1.5, since the ideal generated by \(1+i\) and \(1+j\) in \(H(2)/2H(2)\) is the smallest ideal of \(H(2)/2H(2)\) containing both \((1+i)\) and \((1+j)\), which is \(J\).

Hence we can now determine the left ideal structure of \(H(2)\) containing \(2H(2)\). Note that in the previous Propositions, we used the notation \((\gamma_1, \gamma_2, ..., \gamma_n)\) to denote the ideal of \(H(2)\) generated by the elements \(\gamma_1, \gamma_2, ..., \gamma_n\). Normally, this is done for two-sided ideals. However, we will use this notation for left ideals as well.

**Corollary 3.1.7.** The lattice of left ideals of \(H(2)\) containing \(2H(2)\) is
Proof. This follows from Proposition 3.1.5 and the one-to-one correspondence between left ideals of $H(2)/2H(2)$ and left ideals of $H(2)$ containing $2H(2)$. This correspondence takes ideals generated by $\alpha_1, \alpha_2, \ldots, \alpha_n$ to left ideals generated by $2, \alpha_1, \alpha_2, \ldots, \alpha_n$, hence $(2, 1 + i + j + k)$ taking the place of $(1 + i + j + k)$.

The other ideals already contain the element 2 by Corollary 2.5.3, since

\[
N(1 + i) = 1^2 + 1^2 = 2,
\]
\[
N(1 + j) = 1^2 + 1^2 = 2, \text{ and}
\]
\[
N(1 + k) = 1^2 + 1^2 = 2
\]

in $H(2)$. Hence why it can be omitted as a generator. The ideal $\mathcal{J}$ in $H(2)/2H(2)$ has been replaced with $(1 + i, 1 + j)$ because of Proposition 3.1.6.
3.2 Left Ideals Between $H_{(2)}$ and $4H_{(2)}$

Note that we are interested in $4H_{(2)}$ as a left ideal, but that it is in fact two-sided, since 4 belongs to the center of $H_{(2)}$. We would like to extend the results of the previous section to an accounting of all ideals of $H_{(2)}$ containing $4H_{(2)}$, by considering the ring $H_{(2)}/4H_{(2)}$. In all cases, we will be working with left ideals, and as in Section 3.1 notation such as $(\gamma_1, \gamma_2, ..., \gamma_n)$ will denote the left ideal generated by $\gamma_1, \gamma_2, ..., \gamma_n$.

To begin, let us make the same observation about $H_{(2)}/4H_{(2)}$ that we made about $H_{(2)}/2H_{(2)}$ in Section 3.1.

**Proposition 3.2.1.** The rings $H_{(2)}/4H_{(2)}$, $H/4H$, and $\mathbb{Z}/4\mathbb{Z}$ are isomorphic to each other, and have 256 elements.

**Proof.** That they are isomorphic follows from Corollary 2.4.10. That they have 256 elements follows from the fact that $|H_{\mathbb{Z}/4\mathbb{Z}}| = |\mathbb{Z}/4\mathbb{Z}|^4 = 4^4 = (2^2)^4 = 2^8 = 256$.

From now on, we will use the rings $H_{(2)}/4H_{(2)}$, $H/4H$, and $\mathbb{Z}/4\mathbb{Z}$ interchangeably. In all cases, we will think of an element $a + bi + cj + dk$ as having coefficients $a, b, c, d \in \mathbb{Z}/4\mathbb{Z}$.

We now want to extend the results of the previous section from left ideals containing $2H_{(2)}$ to left ideals containing $4H_{(2)}$. First, we do this by noticing that the ideals between $H_{(2)}$ and $2H_{(2)}$ directly correspond to the ideals between $2H_{(2)}$ and $4H_{(2)}$.

**Proposition 3.2.2.** The $H_{(2)}$-modules $H_{(2)}/2H_{(2)}$ and $2H_{(2)}/4H_{(2)}$ are isomorphic.

**Proof.** This is an application of Proposition 2.4.15.

**Corollary 3.2.3.** The lattice of left ideals of $H_{(2)}$ lying between $2H_{(2)}$ and $4H_{(2)}$ is
Proof. Corollary 3.1.7 and Proposition 3.2.2, with the natural correspondence between $H_{(2)}/2H_{(2)}$ and $2H_{(2)}/4H_{(2)}$ taking ideals of the form $(\alpha_1, \alpha_2, ..., \alpha_n)$ to ideals of the form $(2\alpha_1, 2\alpha_2, ..., 2\alpha_n)$.

This tells us exactly which left ideals lie between $H_{(2)}$ and $2H_{(2)}$, and between $2H_{(2)}$ and $4H_{(2)}$. We now want to consider left ideals between $H_{(2)}$ and $4H_{(2)}$ that are not comparable to $2H_{(2)}$. We start by showing that such an ideal exists.

**Proposition 3.2.4.** The left ideal of $H_{(2)}$ generated by $1+i+j+k$ contains $(2+2i, 2+2j)$ and is contained in $(2, 1+i+j+k)$, but is not comparable to $2H_{(2)}$.

Proof. Since $1+i+j+k \in (2, 1+i+j+k)$, the left ideal $(1+i+j+k)$ is contained in $(2, 1+i+j+k)$. Since

$$(1-k) \cdot (1+i+j+k) = (1+i+j+k) - (k+j-i-1)$$

$$= 2+2i,$$
and

\[(1 - i) \cdot (1 + i + j + k) = (1 + i + j + k) - (i - 1 + k - j) = 2 + 2j,\]

the left ideal \((2 + 2i, 2 + 2j)\) is contained in \((1 + i + j + k)\). Hence \((1 + i + j + k)\) lies between \((2 + 2i, 2 + 2j)\) and \((2, 1 + i + j + k)\).

If the element \(1 + i + j + k\) belonged to \(2H(2)\), then there would be some element \(a + bi + cj + dk \in H(2)\) such that \((a + bi + cj + ck) \cdot 2 = 1 + i + j + k\). This would imply that \(2a = 2b = 2c = 2d = 1\) in \(\mathbb{Z}(2)\), which is impossible. Hence we can conclude that \(1 + i + j + k\) does not belong to \(2H(2)\).

On the other hand, we know that \(H(2)\) is a subring of \(H_{\mathbb{Q}}\), and that \(H_{\mathbb{Q}}\) is an integral domain by Corollary 2.5.10. The equation

\[(a + bi + cj + dk)(1 + i + j + k) = 2\]

has a unique solution given by \(a + bi + cj + dk = \frac{1}{2} - \frac{1}{2}i - \frac{1}{2}j - \frac{1}{2}k\) in \(H_{\mathbb{Q}}\) (unique because \(H_{\mathbb{Q}}\) is an integral domain), and this solution does not belong to \(H(2)\). This implies that the ring \(H(2)\) does not contain any element \(a + bi + cj + dk\) such that \((a + bi + cj + dk)(1 + i + j + k) = 2\), and hence that 2 does not belong to \((1 + i + j + k)\).

Since \(1 + i + j + k\) does not belong to \(2H(2)\) and 2 does not belong to \((1 + i + j + k)\), the left ideals \((1 + i + j + k)\) and \(2H(2)\) are not comparable.

We then find a second ideal which is also incomparable to \(2H(2)\).

**Proposition 3.2.5.** The left ideal of \(H(2)\) generated by \(3 + i + j + k\) contains \((2 + 2i, 2 + 2j)\)
and is contained in \((2, 1+i+j+k)\), but is not comparable to either \(2H(2)\) or \((1+i+j+k)\).

**Proof.** Since \(3 + i + j + k = 2 + (1 + i + j + k) \in (2, 1+i+j+k)\), the left ideal \((3 + i + j + k)\) is contained in \((2, 1+i+j+k)\). Since

\[
\left(\frac{2}{3} + \frac{1}{3}i - \frac{1}{3}k\right) \cdot (3 + i + j + k) = \frac{2}{3}(3 + i + j + k) + \frac{1}{3}(3i - 1 + k - j) - \frac{1}{3}(3k + j - i - 1) = 2 + 2i,
\]

and

\[
\left(\frac{2}{3} - \frac{1}{3}i + \frac{1}{3}j\right) \cdot (3 + i + j + k) = \frac{2}{3}(3 + i + j + k) - \frac{1}{3}(3i - 1 + k - j) + \frac{1}{3}(3j - k - 1 + i) = 2 + 2j,
\]

the left ideal \((2 + 2i, 2 + 2j)\) is contained in \((3 + i + j + k)\). Hence \((3 + i + j + k)\) lies between \((2 + 2i, 2 + 2j)\) and \((2, 1+i+j+k)\).

If the element \(3 + i + j + k\) belonged to \(2H(2)\), then there would be some element \(a + bi + cj + ck \in H(2)\) such that \((a + bi + cj + ck) \cdot 2 = 3 + i + j + k\). This would imply that \(2a = 3\) while \(2b = 2c = 2d = 1\) in \(\mathbb{Z}(2)\), which is impossible. Hence we can conclude that \(3 + i + j + k\) does not belong to \(2H(2)\).

On the other hand, we know that \(H(2)\) is a subring of \(H_\mathbb{Q}\), and that \(H_\mathbb{Q}\) is an integral domain by Corollary 2.5.10. The equation

\[
(a + bi + cj + dk)(3 + i + j + k) = 2
\]

48
has a unique solution given by $a + bi + cj + dk = \frac{1}{2} - \frac{1}{6}i - \frac{1}{6}j - \frac{1}{6}k$ in $H_Q$ (unique because $H_Q$ is an integral domain), and this solution does not belong to $H_{(2)}$. This implies that the ring $H_{(2)}$ does not contain any element $a + bi + cj + dk$ such that $(a + bi + cj + dk)(3 + i + j + k) = 2$, and hence that 2 does not belong to $(3 + i + j + k)$.

Since $3 + i + j + k$ does not belong to $2H_{(2)}$ and that 2 does not belong to $(3 + i + j + k)$, the left ideals $(3 + i + j + k)$ and $2H_{(2)}$ are not comparable. If $1 + i + j + k$ belonged to $(3 + i + j + k)$, then $(3 + i + j + k) - (1 + i + j + k) = 2$ would also belong to $(3 + i + j + k)$, which is a contradiction. If $3 + i + j + k$ belonged to $(1 + i + j + k)$, then $(3 + i + j + k) - (1 + i + j + k) = 2$ would also belong to $(1 + i + j + k)$, which is a contradiction by Proposition 3.2.4. Hence the left ideals $(3 + i + j + k)$ and $(1 + i + j + k)$ are not comparable.

These are actually the only other left ideals that can be found between $H_{(2)}$ and $4H_{(2)}$, resulting in the following proposition.

**Proposition 3.2.6.** The lattice of left ideals of $H_{(2)}/4H_{(2)}$ is
Proof. By Propositions 3.2.4 and 3.2.5, and Corollaries 3.1.7 and 3.2.3, and the one-to-one correspondence between left ideals of $H(2)/4H(2)$ and left ideals of $H(2)$ containing $4H(2)$, all of the entries in the diagram are distinct left ideals of $H(2)/4H(2)$, and are ordered in the manner shown. It suffices to show that no other left ideals of $H(2)/4H(2)$ exist, starting with the principal ones.
To see that all of the principal left ideals of $H(2)/4H(2)$ are present, let $a+bi+cj+dk$ be an arbitrary element of $H(2)/4H(2)$, and consider four cases.

**Case 1.** All of the coefficients $a$, $b$, $c$, and $d$ are even.

In this case, $a + bi + cj + dk \in (2)$ and hence $(0) \subseteq (a + bi + cj + dk) \subseteq (2)$. Corollary 3.2.3 implies that all of the left ideals of $H(2)/4H(2)$ between $(2)$ and $(0)$ have already been included, since these correspond to left ideals of $H(2)$ between $2H(2)$ and $4H(2)$. Hence the left ideal $(a + bi + cj + dk)$ is already in the lattice.

**Case 2.** Two of the coefficients $a$, $b$, $c$, and $d$ are even, and two are odd.

In this case, the norm $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$ is equal to 2 in $\mathbb{Z}/4\mathbb{Z}$. By Corollary 2.5.3, this implies that $2 \in (a + bi + cj + dk)$, and hence that $(2) \subseteq (a + bi + cj + dk) \subseteq H(2)/4H(2)$. Corollary 3.1.7 implies that all of the left ideals of $H(2)/4H(2)$ between $H(2)/4H(2)$ and $(2)$ have already been included, since these correspond to left ideals of $H(2)$ between $H(2)$ and $2H(2)$. Hence the left ideal $(a + bi + cj + dk)$ is already in the lattice.

**Case 3.** Either one or three of the coefficients $a$, $b$, $c$, and $d$ are even, and the rest are odd.

In this case, the norm $N(a+bi+cj+dk) = a^2 + b^2 + c^2 + d^2$ is odd, and hence invertible in $\mathbb{Z}/4\mathbb{Z}$. As in case 2, we can use Corollary 2.5.3 to conclude that $(a + bi + cj + dk)$ contains a unit. It follows immediately that $(a + bi + cj + dk) = H(2)/4H(2)$, and is
already included.

Case 4. All of the coefficients $a$, $b$, $c$, and $d$ are odd.

In this case, $a + bi + cj + dk$ is one of the elements

$$1 + i + j + k, \quad 1 + 3i + 3j + k,$$
$$3 + i + j + k, \quad 1 + 3i + j + 3k,$$
$$1 + 3i + j + k, \quad 1 + i + 3j + 3k,$$
$$1 + i + 3j + k, \quad 3 + 3i + 3j + k,$$
$$1 + i + j + 3k, \quad 3 + 3i + j + 3k,$$
$$3 + 3i + j + k, \quad 3 + i + 3j + 3k,$$
$$3 + i + 3j + k, \quad 1 + 3i + 3j + 3k,$$
$$3 + i + j + 3k, \quad 3 + 3i + 3j + 3k.$$

However, each of these elements can be written as $u \cdot (a + i + j + k)$ for some $a \in \{1, 3\}$ and $u \in \{\pm1, \pm i, \pm j, \pm k\}$. Hence they generate the same left ideal as either $1 + i + j + k$ or $3 + i + j + k$, which have already been included.

This shows that our lattice contains all principal left ideals of $H_{(2)}/4H_{(2)}$. We also have, from the size of the lattice and Proposition 3.2.1, that every step in the lattice represents an inclusion of index 2. Next, we note that the join of any two left ideals in the lattice is already in the lattice. This is simple to check because most of the left ideals in the lattice are contained one inside of the other, and the ones that aren’t
have another left ideal immediately above them. In this latter case, the left ideal immediately above them must be their join.

Since \( H_{(2)}/4H_{(2)} \) is finite, this implies that all left ideals of \( H_{(2)}/4H_{(2)} \) are in the lattice.

\[ \square \]

**Corollary 3.2.7.** *The lattice of left ideals of \( H_{(2)} \) containing \( 4H_{(2)} \) is*

![Diagram of lattice of left ideals]

\[ \begin{align*}
H_{(2)} & \\
(1 + i, 1 + j) & \\
(1 + i) & (1 + j) & (1 + k) \\
(2, 1 + i + j + k) & & \\
(1 + i + j + k) & 2H_{(2)} & (3 + i + j + k) \\
(2 + 2i, 2 + 2j) & & \\
(2 + 2i) & (2 + 2j) & (2 + 2k) \\
(4, 2 + 2i + 2j + 2k) & & \\
4H_{(2)} & 
\end{align*} \]
with every step in the diagram representing an inclusion with index 2.

Proof. This follows from Proposition 3.2.6, and from the one-to-one correspondence between left ideals of $H(2)/4H(2)$ and left ideals of $H(2)$ containing $4H(2)$.

\[ \square \]

### 3.3 Zeta Function Computation When $p$ is Even

Using the results of the previous section, we can get a good idea of the entire ideal structure of $H(2)$. This is, in particular, because of the following proposition.

**Proposition 3.3.1.** Every nonzero element of $H(2)$ generates a left ideal of $H(2)$ lying between $2^nH(2)$ and $2^{n+2}H(2)$ for some $n \in \mathbb{N}$.

**Proof.** Let $\alpha = a + bi + cj + dk$ be an element of $H(2)$, and assume $\alpha$ is nonzero. We consider $a$, $b$, $c$, and $d$ to be integers, since we can simply multiply the element $a + bi + cj + dk$ on the left by a unit (in $\mathbb{Z}(2)$, and hence in $H(2)$) to clear all denominators and get the exact same principal left ideal. Since $\alpha$ is nonzero, we can then consider the largest natural number $n \in \mathbb{N}$ such that $2^n$ divides $a$, $b$, $c$, and $d$.

If $e = \frac{a}{2^n}$, $f = \frac{b}{2^n}$, $g = \frac{c}{2^n}$, $h = \frac{d}{2^n}$, then $\alpha = 2^n \cdot (e + fi + gj + hk) \in 2^nH(2)$ and at least one of $e$, $f$, $g$, or $h$ is odd. Since $2^n$ is central in $H(2)$, we can conclude that the left ideal of $H(2)$ generated by $\alpha$ (henceforth referred to as $(\alpha)$) is contained in $2^nH(2)$.

From Proposition 2.5.2, we know that $(e - fi - gj - hk)(e + fi + gj + hk) = \ldots$
\[ N(e + fi + gj + hk) = e^2 + f^2 + g^2 + h^2, \] and hence that

\[
2^n \cdot (e^2 + f^2 + g^2 + h^2) = 2^n \cdot (e - fi - gj - hk)(e + fi + gj + hk) \\
= (e - fi - gj - hk) \cdot 2^n \cdot (e + fi + gj + hk) \\
= (e - fi - gj - hk) \cdot \alpha.
\]

This implies that \(2^n \cdot (e^2 + f^2 + g^2 + h^2)\) belongs to \((\alpha)\). Since \(2^n\) is a central element of \(H_{(2)}\), it follows that \((e^2 + f^2 + g^2 + h^2) \cdot 2^n\) belongs to \((\alpha)\). We consider four cases.

**Case 1.** Three of the coefficients \(e, f, g,\) and \(h\) are even, and one is odd.

In this case, the sum \(e^2 + f^2 + g^2 + h^2\) is odd, and hence invertible in \(H_{(2)}\). Since \((e^2 + f^2 + g^2 + h^2) \cdot 2^n\) belongs to \((\alpha)\), it immediately follows that \(2^n\) belongs to \((\alpha)\), and hence that \(2^{n+2} = 4 \cdot 2^n\) belongs to \((\alpha)\). Since \(2^{n+2}\) is central in \(H_{(2)}\), we can conclude that \(2^{n+2}H_{(2)}\) is contained in \((\alpha)\).

**Case 2.** One of the coefficients \(e, f, g,\) and \(h\) is even, and three are odd.

In this case, the sum \(e^2 + f^2 + g^2 + h^2\) is odd, and we can conclude that \(2^{n+2}H_{(2)}\) is contained in \((\alpha)\) for the same reason as in Case 1.

**Case 3.** Two of the coefficients \(e, f, g,\) and \(h\) are even, and two are odd.

In this case, the sum \(e^2 + f^2 + g^2 + h^2\) is congruent to 2 mod 4. This means that we can write \(e^2 + f^2 + g^2 + h^2 = u \cdot 2\) for some odd integer \(u \in \mathbb{Z}\). Being an odd integer, the
element $u$ is invertible in $H(2)$. Since $(e^2 + f^2 + g^2 + h^2) \cdot 2^n = u \cdot 2^n = u \cdot 2^{n+1}$ belongs to $(\alpha)$, it immediately follows that $2^{n+1}$ belongs to $(\alpha)$, and hence that $2^{n+2} = 2 \cdot 2^{n+1}$ belongs to $(\alpha)$. Since $2^{n+2}$ is central in $H(2)$, we can conclude that $2^{n+2}H(2)$ is contained in $(\alpha)$.

**Case 4.** All of the coefficients $e$, $f$, $g$, and $h$ are odd.

In this case, the sum $e^2 + f^2 + g^2 + h^2$ is congruent to 4 mod 8. This means that we can write $e^2 + f^2 + g^2 + h^2 = u \cdot 4$ for some odd integer $u \in \mathbb{Z}$. Being an odd integer, the element $u$ is invertible in $H(2)$. Since $(e^2 + f^2 + g^2 + h^2) \cdot 2^n = u \cdot 4 \cdot 2^n = u \cdot 2^{n+2}$ belongs to $(\alpha)$, it immediately follows that $2^{n+2}$ belongs to $(\alpha)$. Since $2^{n+2}$ is central in $H(2)$, we can conclude that $2^{n+2}H(2)$ is contained in $(\alpha)$.

Since we already found that $(\alpha)$ is contained in $2^nH(2)$, we can conclude that $(\alpha)$ lies between $2^nH(2)$ and $2^{n+2}H(2)$.

We then note that the structure of left ideals between $2^nH(2)$ and $2^{n+2}H(2)$ is similar to that between $H(2)$ and $4H(2)$.

**Proposition 3.3.2.** For all $n \in \mathbb{N}$, the $H(2)$-modules $H(2)/4H(2)$ and $2^nH(2)/2^{n+2}H(2)$ are isomorphic.

**Proof.** This follows from Proposition 2.4.15. One should note in particular that the natural isomorphism from $H(2)/4H(2)$ to $2^nH(2)/2^{n+2}H(2)$ is a multiplication by $2^n$. 

\[\square\]
Corollary 3.3.3. For all $n \in \mathbb{N}$, the left ideals of $H_{(2)}$ lying between $2^n H_{(2)}$ and $2^{n+2} H_{(2)}$ are the same as those between $H_{(2)}$ and $4 H_{(2)}$, but multiplied by $2^n$. In other words, the lattice of left ideals of of $H_{(2)}$ lying between $2^n H_{(2)}$ and $2^{n+2} H_{(2)}$ is

$$
\begin{array}{c}
2^n H_{(2)} \\
\downarrow \\
(2^n + 2^n i, 2^n + 2^n j) \\
\downarrow \\
(2^n + 2^n i) \\
\downarrow \\
(2^n + 2^n + 2^n i + 2^n j + 2^n k) \\
\downarrow \\
(2^n + 2^n i + 2^n j + 2^n k) \\
\downarrow \\
(2^n + 2^n i + 2^n j + 2^n k) \\
\downarrow \\
(3 \cdot 2^n + 2^n i + 2^n j + 2^n k) \\
\downarrow \\
(2^{n+1} H_{(2)}) \\
\downarrow \\
(2^{n+1} + 2^{n+1} i, 2^{n+1} + 2^{n+1} j) \\
\downarrow \\
(2^{n+1} + 2^{n+1} i) \\
\downarrow \\
(2^{n+1} + 2^{n+1} i + 2^{n+1} j + 2^{n+1} k) \\
\downarrow \\
(2^{n+2} + 2^{n+1} i + 2^{n+1} j + 2^{n+1} k) \\
\downarrow \\
2^{n+2} H_{(2)}
\end{array}
$$

with every step in the diagram representing an inclusion with index 2.

Proof. This follows from Proposition 3.3.2 and Corollary 3.2.7.

This gives us enough information to compute the zeta function of $H_{(2)}$. 

\[ \boxed{ } \]
Theorem 3.3.4. The zeta function for $H_{(2)}$ is

$$\zeta(H_{(2)}; s) = \frac{1 + 2^{-s} + 2^{-2s+1}}{1 - 2^{-2s}}$$

Proof. By Corollary 3.3.3, we can form a possibly incomplete lattice of left ideals starting with $H_{(2)}$ and then repeating the pattern

for all $n \in \mathbb{N}$, with every step representing an inclusion of index 2. By Proposition 3.3.1, this lattice contains all principal left ideals of $H_{(2)}$.

A similar argument to the one used in Proposition 3.2.6 implies that this lattice contains all left ideals of $H_{(2)}$, since $H_{(2)}$ is Noetherian (Corollary 2.4.14). This tells us that $H_{(2)}$ has one left ideal of index $2^{2n+1}$ for all $n \in \mathbb{N}$, three left ideals of index $2^{2n}$ for all $n \in \mathbb{N} \setminus \{0\}$, and one left ideal of index 1. Hence,
\[ \zeta(H(2); s) = \sum_{X \leq H(2)} |H(2)/X|^{-s} \]

\[ = 1 + \sum_{n=0}^{\infty} (2^{-s})^{2n+1} + 3 \cdot \sum_{n=1}^{\infty} (2^{-s})^{2n} \]

\[ = 1 + 2^{-s} \cdot \sum_{n=0}^{\infty} (2^{-2s})^{n} + 3 \cdot \sum_{n=1}^{\infty} (2^{-2s})^{n} \]

\[ = 1 + 2^{-s} \cdot \sum_{n=0}^{\infty} (2^{-2s})^{n} + 3 \cdot \sum_{n=0}^{\infty} (2^{-2s})^{n} - 3 \]

\[ = 2^{-s} \cdot \left( \frac{1}{1 - 2^{-2s}} \right) + 3 \cdot \left( \frac{1}{1 - 2^{-2s}} \right) - 2 \]

\[ = \frac{2^{-s} + 3}{1 - 2^{-2s}} - \frac{2 \cdot (1 - 2^{-2s})}{1 - 2^{-2s}} \]

\[ = \frac{1 + 2^{-s} + 2^{-2s+1}}{1 - 2^{-2s}} \]

\[ \square \]
Chapter 4

The Zeta Function of $H(p)$ When $p$ is Odd

Let $p$ be an odd prime. We use Hensel’s lemma to lift a solution to $x^2 + y^2 = 1$ from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}_p$, and use this to define a ring isomorphism from $H_p$ to $\mathbb{Z}_p^{2\times 2}$. We then show that there is a one-to-one correspondence between the finite-index left ideals of $\mathbb{Z}_p^{2\times 2}$ and the finite-index $\mathbb{Z}_p$ submodules of $\mathbb{Z}_p^2$. From this, we can find the zeta functions for $\mathbb{Z}_p^{2\times 2}$ and $H_p$, and then for $H(p)$ using Corollary 2.5.8. The zeta functions for both $H_p$ and $H(p)$ turn out to be the same.

4.1 Hensel’s Lemma

Again, let $p$ be an odd prime. We start by showing that the equation $x^2 + y^2 = -1$ has solutions in $\mathbb{Z}/p\mathbb{Z}$.

Proposition 4.1.1. There exist elements $x, y \in \mathbb{Z}/p\mathbb{Z}$ such that $x^2 + y^2 = -1$.

Proof. Let $N_p(E)$ be the number of solutions to the equation $E$ in $\mathbb{Z}/p\mathbb{Z}$. Following
Ireland & Rosen [7], we find that

\[ N_p(x^2 + y^2 = -1) = \sum_{a+b=1} N_p(x^2 = -a)N_p(y^2 = -b) \]

\[ = \sum_{a+b=1} (1 + (-a/p))(1 + (-b/p)) \]

where \((*/p)\) is the Legendre symbol. This evaluates to

\[ p + (-1/p) \sum_{a+b=1} (a/p) + (-1/p) \sum_{a+b=1} (b/p) + \sum_{a+b=1} (a/p)(b/p) \]

which implies that

\[ N_p(x^2 + y^2 = -1) = p + \sum_{a+b=1} (a/p)(b/p) \]

since \(\sum_{a+b=1}(a/p)\) and \(\sum_{a+b=1}(b/p)\) are both 0 by Ireland & Rosen [7, Section 6.3].

The sum \(\sum_{a+b=1}(a/p)(b/p)\) evaluates to 1 when \(p \equiv 3 \mod 4\), and \(-1\) when \(p \equiv 1 \mod 4\) (Ireland & Rosen [7, Section 8.3]), hence we can conclude that \(N_p(x^2 + y^2 = -1) = p - (-1)^{\frac{p-1}{2}} > 1\) in \(\mathbb{Z}/p\mathbb{Z}\), meaning that there exist \(x, y \in \mathbb{Z}/p\mathbb{Z}\) such that \(x^2 + y^2 = -1\).

\[ \square \]

Next, we prove a special case of Hensel’s Lemma (Atiyah & McDonald [5, Chapter 10, Exercise 9]) to show that the equation \(x^2 + y^2 = -1\) has solutions in \(\mathbb{Z}_p\).

**Proposition 4.1.2.** For every positive integer \(n\), there exist elements \(x, y \in \mathbb{Z}/p^n\mathbb{Z}\) such that \(x^2 + y^2 = -1\).

**Proof.** By the previous proposition (Proposition 4.1.1), we know such elements exist
in \(\mathbb{Z}/p\mathbb{Z}\). Call them \(x_0\) and \(y_0\). We would like to show by induction that they exist in 
\(\mathbb{Z}/p^{n+1}\mathbb{Z}\) for all \(n \in \mathbb{N}\).

If \(x_0\) and \(y_0\) are both zero, this would imply that 
\(-1 = x_0^2 + y_0^2 = 0^2 + 0^2 = 0\) in 
\(\mathbb{Z}/p\mathbb{Z}\), which is a contradiction. Therefore, we can assume that at least one of them is 
nonzero. Without loss of generality, since the two are interchangeable, we can assume 
that \(x_0\) is nonzero.

With this in mind, let \(a = -1 - y_0^2\), and note that \(x_0^2 = a\) in \(\mathbb{Z}/p\mathbb{Z}\). Now suppose 
that \(k_1, ..., k_n \in \{0, 1, ..., p - 1\}\) and that

\[
x_i = k_ip^i + k_{i-1}p^{i-1} + ... + k_1p + x_0
\]

is a solution to the equation \(x^2 = a\) in \(\mathbb{Z}/p^{i+1}\mathbb{Z}\), for all \(i\) up to \(n - 1\). Then \(x_{n-1}\) is a 
solution to \(x^2 = a\) in \(\mathbb{Z}/p^n\mathbb{Z}\), and hence \(a - x_{n-1}^2\) is divisible by \(p^n\) in \(\mathbb{Z}\).

Since \(p\) is an odd prime, and \(x_0\) is nonzero in \(\mathbb{Z}/p\mathbb{Z}\), both 2 and \(x_0\) are invertible 
in \(\mathbb{Z}/p\mathbb{Z}\). This implies that \(2x_0\) is invertible in \(\mathbb{Z}/p\mathbb{Z}\). Hence there exists an element 
\(k_n \in \{0, 1, ..., p - 1\}\) such that 
\(k_n = (\frac{a-x_0^2}{p^n})^{-1}(2x_0)^{-1}\) in \(\mathbb{Z}/p\mathbb{Z}\). Let us define \(x_n = 
\)

\[
k_n p^n + x_{n-1}.
\]

Since \(k_n = (\frac{a-x_0^2}{p^n})^{-1}(2x_0)^{-1}\) in \(\mathbb{Z}/p\mathbb{Z}\), the integer \(2x_0k_n - \frac{a-x_0^2}{p^n}\) is divisible by \(p\) 
in \(\mathbb{Z}\). It follows that the integer

\[
p^n(2x_0k_n - \frac{a-x_0^2}{p^n}) = 2x_0k_np^n - (a - x_{n-1}^2)
\]

\[
= x_{n-1}^2 + 2x_0k_np^n - a
\]
is divisible by $p^{n+1}$, and hence that $x_n^2 + 2x_0k_np^n = a$ in $\mathbb{Z}/p^{n+1}\mathbb{Z}$. Noting that

\[
x_{n-1}p^n = (k_{n-1}p^{n-1} + k_{n-2}p^{n-2} + \ldots + k_1p + x_0)p^n
\]
\[
= (k_{n-1}p^{n-2} + k_{n-2}p^{n-3} + \ldots + k_2p + k_1)p^{n+1} + x_0p^n
\]
\[
= x_0p^n
\]

in $\mathbb{Z}/p^{n+1}\mathbb{Z}$, and that

\[
(k_np^n)^2 = k_n^2p^np^n
\]
\[
= k_n^2p^{n-1}p^{n+1}
\]
\[
= 0
\]

in $\mathbb{Z}/p^{n+1}\mathbb{Z}$, we can conclude that

\[
x_n^2 = (k_np^n + x_{n-1})^2
\]
\[
= (k_np^n)^2 + 2x_{n-1}k_np^n + x_{n-1}^2
\]
\[
= 2x_{n-1}k_np^n + x_{n-1}^2
\]
\[
= 2k_n(x_{n-1}p^n) + x_{n-1}^2
\]
\[
= 2k_n(x_0p^n) + x_{n-1}^2
\]
\[
= 2x_0k_np^n + x_{n-1}^2
\]
\[
= a
\]

in $\mathbb{Z}/p^{n+1}\mathbb{Z}$. This implies that $x_i = k_ip^i + k_{i-1}p^{i-1} + \ldots + k_1p + x_0$ is a solution to the equation $x^2 = a$ in $\mathbb{Z}/p^{i+1}\mathbb{Z}$, for all $i$ up to $n$.

By induction, we can conclude that there exists a sequence of elements $k_1, k_2, k_3, \ldots \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ such that $x_n = k_np^n$ for all $n$. This completes the proof.
\{0, 1, 2, ..., p - 1\} such that \(x_i = k_ip^i + k_{i-1}p^{i-1} + ... + k_1p + x_0\) is a solution to the equation \(x^2 = a\) in \(\mathbb{Z}/p^{i+1}\mathbb{Z}\), for all \(i \in \mathbb{N}\).

\[\bbox{\text{Corollary 4.1.3. There exist elements } x, y \in \mathbb{Z}_p \text{ such that } x^2 + y^2 = -1.}\]

\textit{Proof.} Setting \(x = (x_i)_{i \in \mathbb{N}}\) and \(y = (y_0)_{i \in \mathbb{N}}\) from the previous proposition (Proposition 4.1.2), we have that \(x^2 + y^2 = -1\) in \(\mathbb{Z}_p\). That \(y\) is an element of \(\mathbb{Z}_p\) is obvious. That \(x\) is an element of \(\mathbb{Z}_p\) comes from the fact that \(x_{i+1} - x_i = k_{i+1}p^{i+1}\) is divisible by \(p^{i+1}\) in \(\mathbb{Z}\), and hence that \(x_i \equiv x_{i+1} \mod p^{i+1}\) for all \(i \in \mathbb{N}\).

\[\bbox{\text{4.2 Equivalence to Matrix Rings}}\]

Now that we know that there exist elements \(x, y \in \mathbb{Z}_p\) such that \(x^2 + y^2 = -1\), we can prove that \(H_p\) is isomorphic to \(\mathbb{Z}_p^{2 \times 2}\) as a \(\mathbb{Z}_p\)-algebra. This will allow us to understand the left ideal structure of \(H_p\) by first understanding the left ideal structure of \(\mathbb{Z}_p^{2 \times 2}\). Again, we assume that \(p\) is an odd prime.

\textit{Proposition 4.2.1.} Let \(R\) be a commutative ring with \(x, y \in R\) satisfying the equation \(x^2 + y^2 = -1\). Then the map \(\theta : H_R \to R^{2 \times 2}\) extended \(R\)-linearly from

\[\theta(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \theta(i) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\]
\[
\theta(j) = \begin{pmatrix} x & y \\ y & -x \end{pmatrix}
\]

and

\[
\theta(k) = \begin{pmatrix} y & -x \\ -x & y \end{pmatrix}
\]

is an \( R \)-algebra homomorphism.

**Proof.** To see that \( \theta \) is a ring homomorphism, it suffices to note that \( \theta(i)^2 = \theta(j)^2 = \theta(k)^2 = \theta(ijk) = -\theta(1) \). Since \( \theta \) is extended \( R \)-linearly from the basis elements 1, \( i \), \( j \), and \( k \) to all of \( H_R \), it is obviously an \( R \)-module homomorphism. Hence it follows immediately that \( \theta \) is an \( R \)-algebra homomorphism. \( \square \)

**Proposition 4.2.2.** If \( R \) is a commutative ring and 2 is a unit in \( R \), then the map \( \theta \) from Proposition 4.2.1 is an isomorphism.

**Proof.** Using the basis elements 1, \( i \), \( j \), and \( k \) for \( H_R \), and the basis elements

\[
\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}
\]

for \( R^{2\times 2} \), we can represent \( \theta \) using the matrix

\[
\begin{pmatrix} 1 & 0 & x & y \\ 0 & 1 & y & -x \\ 0 & -1 & y & -x \\ 1 & 0 & -x & -y \end{pmatrix}
\]
The determinant of this matrix is \(-4(x^2 + y^2)\), which is 4 since \(x^2 + y^2 = -1\). Hence \(\theta\) is an isomorphism if and only if 4 is a unit in \(R\). Since \(4 = 2^2\), this implies that \(\theta\) is an isomorphism if and only if 2 is a unit in \(R\).

\begin{proof}
This follows from the previous proposition (Proposition 4.2.2), since the condition \(p \neq 2\) ensures that 2 is a unit in \(\mathbb{Z}_p\). Hence \(H_p\) is isomorphic to \(\mathbb{Z}_p^{2 \times 2}\) as a \(\mathbb{Z}_p\)-algebra.
\end{proof}

**Corollary 4.2.3.** If \(R = \mathbb{Z}_p\), then the map \(\theta\) from Proposition 4.2.1 is an isomorphism from \(H_p\) to \(\mathbb{Z}_p^{2 \times 2}\).

**Proposition 4.2.4.** If \(R = \mathbb{Z}_p\), then the map \(\theta\) from Proposition 4.2.1 takes left ideals of \(H_p\) containing \(p^n H_p\) to left ideals of \(\mathbb{Z}_p^{2 \times 2}\) containing

\[
\begin{pmatrix}
p^n & 0 \\
0 & p^n
\end{pmatrix}
\]

and vice versa.

**Proof.** This is straightforward, since \(\theta(p^n) = \begin{pmatrix} p^n & 0 \\ 0 & p^n \end{pmatrix}\).

\end{proof}

### 4.3 Morita Equivalence

To understand the left ideal structure of \(\mathbb{Z}_p^{2 \times 2}\) for odd primes \(p\), we demonstrate a correspondence between left ideals of \(\mathbb{Z}_p^{2 \times 2}\) and \(\mathbb{Z}_p\)-submodules of \(\mathbb{Z}_p^2\). This correspon-
dence is related to the Morita-equivalence between $\mathbb{Z}_p^{2\times 2}$ and $\mathbb{Z}_p$ (Anderson & Fuller [8, Corollary 22.6]), though we are proving it directly.

**Proposition 4.3.1.** Let $R$ be a commutative ring. Then the map $\psi : (R\text{-submodules of } R^2) \to (\text{left ideals of } R^{2\times 2})$ given by

$$\psi(M) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid (a, b), (c, d) \in M \right\}$$

for all $M \subseteq R^2$ induces a one-to-one correspondence between $R\text{-submodules of } R^2$ and left ideals of $R^{2\times 2}$.

**Proof.** If

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \psi(M)$$

then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a + e & b + f \\ c + g & d + h \end{pmatrix}$$

also belongs to $\psi(M)$, since $(a, b), (c, d), (e, f), (g, h) \in M$ and hence $(a + e, b + f) = (a, b) + (e, f) \in M$ and $(c + g, d + h) = (c, d) + (g, h) \in M$. If

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \psi(M)$$

and

$$\begin{pmatrix} e & f \\ g & h \end{pmatrix} \in R^{2\times 2}$$
then
\[
\begin{pmatrix}
e & f \\
g & h
\end{pmatrix}
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}
= \begin{pmatrix}
ea + fc & eb + fd \\
ga + hc & gb + hd
\end{pmatrix}
\]
also belongs to \(\psi(M)\), since \((a, b), (c, d) \in M\) and hence \((ea + fc, eb + fd) = e(a, b) + f(c, d) \in M\) and \((ga + hc, gb + hd) = g(a, b) + h(c, d) \in M\). Hence \(\psi(M)\) is a left ideal of \(R^{2 \times 2}\) for all \(M\).

To see that \(\psi\) is injective, suppose that \(M\) and \(N\) are \(R\)-submodules of \(R^2\) and that \(\psi(M) = \psi(N)\). For every element \((a, b) \in M\), we know that
\[
\begin{pmatrix}
a & b \\
0 & 0
\end{pmatrix}
\in \psi(M).
\]
Since \(\psi(M) = \psi(N)\), this implies that
\[
\begin{pmatrix}
a & b \\
0 & 0
\end{pmatrix}
\in \psi(N).
\]
By definition, we can conclude that \((a, b) \in N\). A similar argument tells us that every element of \(N\) also belongs to \(M\), and hence that \(M = N\).

On the other hand, if \(I\) is a left ideal of \(R^{2 \times 2}\), then the set of elements \((a, b) \in R^2\) such that
\[
\begin{pmatrix}
a & b \\
0 & 0
\end{pmatrix}
\in I
\]
forms an \(R\)-submodule of \(R^2\). Applying \(\psi\) to this submodule gives back \(I\), and hence the map \(\psi\) is surjective.

Therefore \(\psi\) is a bijection.
In order to calculate the zeta function later on, we want to see how this correspondence affects quotients. For this, we need the following proposition.

**Proposition 4.3.2.** Let $R$ be a commutative ring and let $\psi$ be the map from Proposition 4.3.1. Then for every $R$-submodule $M \subseteq R^2$, there exists a surjective $R$-module homomorphism $\eta_M : R^{2 \times 2} \to R^2 / M \oplus R^2 / M$ with kernel $\psi(M)$, taking the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R^{2 \times 2}$$

to the pair $((a, b) + M, (c, d) + M)$.

**Proof.** That $\eta_M$ is a surjective $R$-module homomorphism follows immediately from the $R$-module structure of $R^{2 \times 2}$ and $R^2 / M \oplus R^2 / M$; in fact, $\eta_M$ is precisely the $R$-module homomorphism taking the basis elements

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

of $R^{2 \times 2}$ to the basis elements $((1, 0) + M, (0, 0) + M), ((0, 1) + M, (0, 0) + M), ((0, 0) + M, (1, 0) + M)$, and $((0, 0) + M, (0, 1) + M)$ of $R^2 / M \oplus R^2 / M$. To find the kernel of $\eta_M$, we note that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

belongs to the kernel of $\eta_M$ if and only if $((a, b) + M, (c, d) + M) = 0$ in $R^2 / M \oplus R^2 / M$. 

69
This happens if and only if \((a, b), (c, d) \in M\), which happens if and only if

\[
\begin{pmatrix}
a & b \\
c & d \\
\end{pmatrix}
\]

belongs to \(\psi(M)\). Hence we can conclude that the kernel of \(\eta_M\) is \(\psi(M)\).

\[\square\]

**Corollary 4.3.3.** Let \(R\) be a commutative ring and let \(\psi\) be the map from Proposition 4.3.1. Then \(\psi\) takes \(R\)-submodules of index \(\ell\) in \(R^2\) to left ideals of index \(\ell^2\) in \(R^{2 \times 2}\).

**Proof.** Since \(R^{2 \times 2}/\psi(M) \simeq R^2/M \oplus R^2/M\) by Proposition 4.3.2,

\[
|R^{2 \times 2}/\psi(M)| = |R^2/M| \times |R^2/M| = |R^2/M|^2
\]

for all \(M \subseteq R^2\) of finite index.

\[\square\]

**Corollary 4.3.4.** Left ideals of index \(\ell^2\) in \(\mathbb{Z}_p^{2 \times 2}\) are in one-to-one correspondence with \(\mathbb{Z}_p\) submodules of index \(\ell\) in \(\mathbb{Z}_p^2\).

**Proof.** This is an application of Corollary 4.3.3 to the case of \(R = \mathbb{Z}_p\).

\[\square\]

We also need some idea of how this correspondence affects ideals generated by \(p^n\).
Proposition 4.3.5. When $R = \mathbb{Z}_p$, the bijection induced by the map $\psi$ from Proposition 4.3.1 takes $\mathbb{Z}_p$-submodules of $\mathbb{Z}_p^2$ containing $p^n\mathbb{Z}_p^2$ to left ideals of $\mathbb{Z}_p^{2\times 2}$ containing 
\[
\begin{pmatrix}
  p^n & 0 \\
  0 & p^n
\end{pmatrix}
\]
for all $n \in \mathbb{N}$.

Proof. This follows immediately from the fact that $\psi(M)$ contains 
\[
\begin{pmatrix}
  p^n & 0 \\
  0 & p^n
\end{pmatrix}
\]
if and only if $M$ contains both $(p^n, 0)$ and $(0, p^n)$, which happens if and only if $M$ contains $p^n\mathbb{Z}_p^2$.

\[\square\]

4.4 Hermite Normal Form

Having related the left ideals of $H_p$ to the left ideals of $\mathbb{Z}_p^{2\times 2}$, and then the left ideals of $\mathbb{Z}_p^{2\times 2}$ to the $\mathbb{Z}_p$-submodules of $\mathbb{Z}_p^2$, we can turn to analysing in detail the $\mathbb{Z}_p$-submodule structure of $\mathbb{Z}_p^2$. First, we introduce a very basic definition, and we observe that all $\mathbb{Z}_p$-submodules of $\mathbb{Z}_p^2$ are finitely generated.

Definition 4.4.1. Let $\pi_1 : \mathbb{Z}_p^2 \rightarrow \mathbb{Z}_p$ and $\pi_2 : \mathbb{Z}_p^2 \rightarrow \mathbb{Z}_p$ be the usual projection maps $\pi_1(x, y) = x$ and $\pi_2(x, y) = y$.

Proposition 4.4.2. Every $\mathbb{Z}_p$-submodule of $\mathbb{Z}_p^2$ is finitely generated.
Proof. This follows from the fact that \( \mathbb{Z}_p \) is Noetherian, which follows from the fact (proved in Proposition 2.2.12) that it is a principal ideal domain.

Since \( \mathbb{Z}_p \)-submodules of \( \mathbb{Z}_p^2 \) are finitely generated, we now attempt to find generating sets for all possible finite-index \( \mathbb{Z}_p \)-submodules of \( \mathbb{Z}_p^2 \).

**Proposition 4.4.3.** Every finite-index submodule of \( \mathbb{Z}_p^2 \) can be generated by \((p^m, b)\) and \((0, p^k)\) for some \( m, k \in \mathbb{N} \) and \( b \in \{0, 1, ..., p^k - 1\} \).

Proof. Let \( M \) be a finite-index submodule of \( \mathbb{Z}_p^2 \) and let

\[
m = \min \{ v_p(x) \mid x \in \pi_1(M) \}
\]

If \( \pi_1(M) = \{0\} \), then \( x = 0 \) for all \((x, y) \in M\), and \( \mathbb{Z}_p^2/M \) has distinct coset representatives \((n, 0)\) for all \( n \in \mathbb{N} \). Similarly, if \( \pi_2(M) = \{0\} \), then \( y = 0 \) for all \((x, y) \in M\), and \( \mathbb{Z}_p^2/M \) has distinct coset representatives \((0, n)\) for all \( n \in \mathbb{N} \). Either case implies that \( M \) has infinite index in \( \mathbb{Z}_p^2 \).

Since we are interested in \( M \) being a finite-index submodule of \( \mathbb{Z}_p^2 \), we can therefore assume that \( \pi_1(M) \) and \( \pi_2(M) \) are nontrivial. One of the consequences of this is that \( m \) must be a non-negative integer, since there exists nonzero \( x \in \pi_1(M) \).

Let \((a, b) \in M\) be such that \( v_p(a) = m \). Then \( a = up^m \) for some invertible \( u \in \mathbb{Z}_p \) by Proposition 2.2.9. Without loss of generality, we can assume that \( a = p^m \), replacing \((a, b)\) with \( u^{-1} \cdot (a, b) = (u^{-1}up^m, u^{-1}b) = (p^m, u^{-1}b) \) if necessary. We can do this because the product \( u^{-1} \cdot (a, b) \) also belongs to \( M \).

Since \( M \) is finitely generated (Proposition 4.4.2), we can find a set of generators \((a_1, b_1), (a_2, b_2),..., (a_n, b_n)\) for \( M \) as a \( \mathbb{Z}_p \)-module. Since \( m = \min \{ v_p(x) \mid x \in \pi_1(M) \} \),
we can be certain that \( v(p^n) = m \leq v_p(a_1), v_p(a_2), ..., v_p(a_n) \). By Proposition 2.2.10, this implies that \( p^m \) divides \( a_i \) for all \( i \).

Since

\[
(a_i, b_i) = (0, b_i - \frac{a_i}{p^m} \cdot b) + \frac{a_i}{p^m} \cdot (p^m, b)
\]

for all \( i \), we can conclude that \( M \) is also generated by the set of elements

\[
\{(p^m, b), (0, d_1), (0, d_2), ..., (0, d_n)\}
\]

where \( d_i = b_i - \frac{a_i}{p^m} \cdot b \) for all \( i \). Let

\[
k = \min\{v_p(d_i) \mid i \in \{1, 2, ..., n\}\}.
\]

If \( k = \infty \), then \( d_i = 0 \) for all \( i \), and hence the index of \( M \) in \( \mathbb{Z}_p^2 \) is infinite. Otherwise, we get that \( k \in \mathbb{N} \) and \( k = v_p(d_j) \) for some \( j \). Then, as before, we can replace \( (0, d_j) \) with \( (0, p^k) \) in our set of generators, since \( (0, d_j) = (0, v \cdot p^k) = v \cdot (0, p^k) \) for some invertible \( v \in \mathbb{Z}_p \) (Proposition 2.2.9).

Since \( v_p(p^k) = k \leq v_p(d_1), v_p(d_2), ..., v_p(d_n) \), Proposition 2.2.10 implies that \( p^k \) divides \( d_i \) for all \( i \). This implies that

\[
(0, d_i) = \frac{p^k}{d_i} \cdot (0, p^k) \in \mathbb{Z}_p(0, p^k)
\]

for all \( i \), and hence that \( M \) is generated by the two elements \( (p^m, b) \) and \( (0, p^k) \).

Writing \( b = (b_i)_{i \in \mathbb{N}} \), we can then reduce \( b \) modulo \( p^k \), by replacing \( b \) with \( b_{k-1} \) (since \( (b_i)_{i \in \mathbb{N}} - (b_{k-1})_{i \in \mathbb{N}} \) has zeros in the first \( k \) entries, as explained in Corollary 2.2.7). Hence we can assume \( b \in \{0, 1, ..., p^k - 1\} \).
One might note from the proof above that we are essentially finding the Hermite normal form of a matrix with entries from the generators of the submodule $M$ (Adkins & Weintraub [9], Section 5.2). It should be unsurprising then that the generators found in Proposition 4.4.3 are unique.

**Proposition 4.4.4.** Distinct pairs of elements in Proposition 4.4.3 generate distinct submodules of $\mathbb{Z}_p^2$.

**Proof.** Suppose that $M$ is a submodule of $\mathbb{Z}_p^2$ generated by $(p^{m_1}, \beta_1)$ and $(0, p^{k_1})$ with $\beta_1 \in \{0, 1, ..., p^{k_1} - 1\}$, and that $N$ is a submodule of $\mathbb{Z}_p^2$ generated by $(p^{m_2}, \beta_2)$ and $(0, p^{k_2})$ with $\beta_2 \in \{0, 1, ..., p^{k_2} - 1\}$.

If $M$ and $N$ are the same, then $M$ must contain the elements $(p^{m_2}, \beta_2)$ and $(0, p^{k_2})$, and $N$ must contain the elements $(p^{m_1}, \beta_1)$ and $(0, p^{k_1})$. If $M$ contains $(p^{m_2}, \beta_2)$, then there exist $x, y \in \mathbb{Z}_p$ such that

$$(p^{m_2}, \beta_2) = x \cdot (p^{m_1}, \beta_1) + y \cdot (0, p^{k_1}) = (xp^{m_1}, x\beta_1 + yp^{k_1}).$$

and hence $p^{m_2} = xp^{m_1}$ and $\beta_2 = x\beta_1 + yp^{k_1}$. It follows that $p^{m_1}$ divides $p^{m_2}$ in $\mathbb{Z}_p$, and therefore that $m_1 = v_p(p^{m_1}) \leq v_p(p^{m_2}) = m_2$ by Proposition 2.2.10. Since $N$ contains $(p^{m_1}, \beta_1)$, a similar argument implies that $m_2 \leq m_1$, and hence that $m_2 = m_1$.

Since $m_1$ and $m_2$ are the same, we replace them by $m$. So $M$ is generated by the elements $(p^m, \beta_1)$ and $(0, p^{k_1})$ with $\beta_1 \in \{0, 1, ..., p^{k_1} - 1\}$, and $N$ is generated by the elements $(p^m, \beta_2)$ and $(0, p^{k_2})$ with $\beta_2 \in \{0, 1, ..., p^{k_2} - 1\}$. Since $M$ contains $(0, p^{k_2})$, we can find $x, y \in \mathbb{Z}_p$ such that

$$(0, p^{k_2}) = x \cdot (p^m, \beta_1) + y \cdot (0, p^{k_1}) = (xp^m, x\beta_1 + yp^{k_1}).$$
meaning that $0 = xp^m$ and $p^{k_2} = x\beta_1 + yp^{k_1}$. It follows that $x = 0$ and that $p^{k_1}$ divides $p^{k_2}$ in $\mathbb{Z}_p$, and hence that $m_1 = v_p(p^{m_1}) \leq v_p(p^{m_2}) = m_2$ by Proposition 2.2.10. Since $N$ contains $(0, p^{k_1})$, a similar argument implies that $k_2 \leq k_1$, and hence that $k_2 = k_1$. Since $k_1$ and $k_2$ are the same, we replace them by $k$, giving us generators $(p^m, \beta_1)$ and $(0, p^k)$ for $M$, and generators $(p^m, \beta_2)$ and $(0, p^k)$ for $N$, with $\beta_1, \beta_2 \in \{0, 1, ..., p^k - 1\}$.

Since $(p^m, \beta_2)$ belongs to $M$, we must again have $x, y \in \mathbb{Z}_p$ such that

$$(p^m, \beta_2) = x \cdot (p^m, \beta_1) + y \cdot (0, p^k) = (xp^m, x\beta_1 + yp^k)$$

This implies that $p^m = xp^m$ and that $\beta_2 = x\beta_1 + yp^k$. Since $\mathbb{Z}_p$ is an integral domain (Proposition 2.2.11), this implies that $x = 1$, and hence that $\beta_2 = \beta_1 + yp^k$. Since $\beta_1, \beta_2 \in \{0, 1, ..., p^k - 1\}$, we can conclude that $\beta_1 = \beta_2$.

Hence the generators from Proposition 4.4.3 are unique.

All of this finally lets us expand on a result we had from Section 2.5. At the time, we found a correspondence between the left ideals of $H(p)$ and $H_p$. This correspondence had certain caveats, however, the most important one being that it only applied to left ideals of $H_p$ containing $p^n H_p$ for some $n \in \mathbb{N}$. We now show that all finite-index left ideals of $H_p$ satisfy that condition.

**Corollary 4.4.5.** Every finite-index submodule of $\mathbb{Z}_p^2$ contains $p^n \mathbb{Z}_p^2$ for some $n \in \mathbb{N}$.

**Proof.** Suppose that $M$ is a finite-index submodule of $\mathbb{Z}_p^2$ and select generators $(p^m, \beta)$ and $(0, p^k)$ for $M$ as per the conditions of Proposition 4.4.3. Then set $n = m + k$. We then get that

$$(0, p^n) = (0, p^{m+k}) = p^m \cdot (0, p^k) \in M$$
and that
\[(p^n, 0) = (p^{m+k}, 0) = p^k \cdot (p^m, \beta) - \beta \cdot (0, p^k) \in M\]
so that \(M\) contains the elements \((p^n, 0)\) and \((0, p^n)\), and hence \(p^n\mathbb{Z}_p^2\).

\[\square\]

**Corollary 4.4.6.** Every finite-index left ideal of \(\mathbb{Z}_p^{2 \times 2}\) contains
\[
\begin{pmatrix}
  p^n & 0 \\
  0 & p^n
\end{pmatrix} \mathbb{Z}_p^{2 \times 2}
\]
for some \(n \in \mathbb{N}\).

*Proof.* This follows from Propositions 4.3.1 and 4.3.5, and Corollary 4.4.5.

\[\square\]

**Corollary 4.4.7.** Every finite-index left ideal of \(H_p\) contains \(p^n H_p\) for some \(n \in \mathbb{N}\).

*Proof.* This follows from Proposition 4.2.4, and Corollaries 4.2.3 and 4.4.6.

\[\square\]

**Corollary 4.4.8.** There is an order-preserving and index-preserving bijection between the nonzero left ideals of \(H_{(p)}\) and the finite index left ideals of \(H_p\).

*Proof.* This follows from Corollaries 2.5.8 and 4.4.7.

\[\square\]

Unfortunately, not all nonzero left ideals of \(H_p\) have finite index. For instance, given two elements \(x, y \in \mathbb{Z}_p\) with \(x^2 + y^2 = -1\) (as in Corollary 4.1.3), the nonzero left ideal of \(H_p\) generated by \(1 + xi + yj\) does not have finite index, since the norm of \(1 + xi + yj\) is zero. The norm of \(1 + xi + yj\) being zero implies that \(1 + xi + yj\) can
not divide any integer in $H_p$, due to Proposition 2.5.4. Hence every integer represents a distinct left coset of $1 + xi + yj$ in $H_p$.

Therefore, we have a correspondence which only works in the finite index case.

### 4.5 Zeta Function Computation When $p$ is Odd

With these results, we can now compute the zeta function for $H(p)$ when $p$ is an odd prime.

**Proposition 4.5.1.** The number of finite-index submodules of index $d$ in $\mathbb{Z}_p^2$ is 0 if $d$ is not a power of $p$ and

$$\frac{p^{n+1} - 1}{p - 1}$$

if $d = p^n$ for some $n \in \mathbb{N}$.

**Proof.** By Propositions 4.4.3 and 4.4.4, this amounts to finding the number of distinct elements $(p^m, \beta), (0, p^k) \in \mathbb{Z}_p^2$ with $m, k \in \mathbb{N}$ and $\beta \in \{0, 1, ..., p^k - 1\}$ such that the submodule generated by $(p^m, \beta)$ and $(0, p^k)$ has index $d$. It isn’t hard to see that the submodule generated by $(p^m, \beta)$ and $(0, p^k)$ is going to have index $p^{m+k}$, so this amounts to finding the number of distinct elements $(p^m, \beta), (0, p^k) \in \mathbb{Z}_p^2$ with $m, k \in \mathbb{N}$, $\beta \in \{0, 1, ..., p^k - 1\}$, and $p^{m+k} = d$.

If $d$ is not a power of $p$, then there can be no such elements.

If $d = p^n$ for some $n$, then we can choose $k \in \{0, 1, ..., n\}$ and $m = n - k$. In each case there are $p^k$ choices for $\beta$, so this amounts to

$$\sum_{y=0}^{n} p^y = 1 + p + p^2 + ... + p^n = \frac{p^{n+1} - 1}{p - 1}$$

different choices.
Corollary 4.5.2. The number of finite-index left ideals of index $d$ in $\mathbb{Z}_p^{2\times 2}$, $H_p$, or $H_{(p)}$ is 0 if $d$ is not an even power of $p$ and

$$\frac{p^{n+1} - 1}{p - 1}$$

if $d = p^{2n}$ for some $n \in \mathbb{N}$.

Proof. We get this result by replacing the condition $d = p^n$ in Proposition 4.5.1 with the condition $d = p^{2n}$, because of the ideal-to-submodule correspondence given in Corollary 4.3.4. Corollaries 4.2.3 and 4.4.8 justify the idea that $\mathbb{Z}_p^{2\times 2}$, $H_p$, and $H_{(p)}$ all have the same number of left ideals for any given finite index.

\[ \square \]

Hence our final result for this section.

Theorem 4.5.3. The zeta function for both $H_{(p)}$ and $H_p$ is

$$\zeta(H_{(p)}; s) = \frac{1}{(1 - p^{-2s+1})(1 - p^{-2s})}$$
Proof. By Corollary 4.5.2, we have

\[
\zeta(H(p); s) = \sum_{X \leq H(p)} |H(p)/X|^{-s} \\
= \sum_{n=0}^{\infty} \left( \frac{p^{n+1} - 1}{p - 1} \right) p^{-2ns} \\
= \sum_{n=0}^{\infty} \left( \frac{p^{n(-2s+1)+1} - 1}{p - 1} \right) \\
= \frac{1}{p-1} \left( \sum_{n=0}^{\infty} p^{n(-2s+1)+1} - \sum_{n=0}^{\infty} p^{-2ns} \right) \\
= \frac{1}{p-1} \left( p \sum_{n=0}^{\infty} p^{n(-2s+1)} - \sum_{n=0}^{\infty} p^{-2ns} \right) \\
= \frac{1}{p-1} \left( \frac{p}{1-p^{-2s+1}} - \frac{1}{1-p^{-2s}} \right) \\
= \frac{1}{p-1} \left( \frac{p(1-p^{-2s}) - (1-p^{-2s+1})}{(1-p^{-2s+1})(1-p^{-2s})} \right) \\
= \frac{1}{p-1} \left( \frac{p - p^{-2s+1} - 1 + p^{-2s+1}}{(1-p^{-2s+1})(1-p^{-2s})} \right) \\
= \frac{1}{p-1} \left( \frac{p - 1}{(1-p^{-2s+1})(1-p^{-2s})} \right) \\
= \frac{1}{(1-p^{-2s+1})(1-p^{-2s})}
\]

and, of course, the same is true for \(H_p\) by Corollary 4.4.8.

\[\square\]
Chapter 5

Conclusion and Interpretation

Now that we have the zeta function for $H_{(2)}$ from Chapter 3, and the zeta function for $H_{(p)}$ when $p$ is an odd prime from Chapter 4, we can finally put together a global zeta function for $H$.

5.1 Zeta Function Computation for $H$

Note that in this chapter we discuss interpretations of $\zeta(H;s)$ in which $s$ is a variable over the complex numbers. In that case, the notation $\text{Re}(s)$ denotes the real part of $s$. This is not the only interpretation of $\zeta(H;s)$, but it is an important option which allows us to consider $\zeta(H;s)$ as an actual function. In fact, we will spend the rest of the chapter focusing heavily on this interpretation of $s$.

**Theorem 5.1.1.** The zeta function for $H$ is

$$\zeta(H;s) = (1 + 2^{-s} + 2^{-2s+1})(1 - 2^{-2s+1}) \sum_{n=1}^{\infty} (n^{-2s+1}) \sum_{n=1}^{\infty} (n^{-2s})$$

In addition, when $s$ is interpreted as a variable over the complex numbers, the function
\( \zeta(H; s) \) is well defined precisely when \( \text{Re}(s) > 1 \).

**Proof.** By Theorem 2.1.3, the zeta function for \( H \) is given by

\[
\zeta(H; s) = \prod_{p \in \mathbb{P}} \zeta(H_{(p)}; s)
\]

where \( \mathbb{P} \) is the set of primes in \( \mathbb{Z} \). From Theorems 3.3.4 and 4.5.3, this implies that

\[
\zeta(H; s) = \prod_{p \in \mathbb{P}} \zeta(H_{(p)}; s)
\]

\[
= \left( \frac{1 + 2^{-s} + 2^{-2s+1}}{1 - 2^{-2s}} \right) \prod_{p \in \mathbb{P}\setminus\{2\}} \left( \frac{1}{(1 - p^{-2s+1})(1 - p^{-2s})} \right)
\]

\[
= \left( \frac{(1 + 2^{-s} + 2^{-2s+1})(1 - 2^{-2s+1})(1 - 2^{-2s})}{1 - 2^{-2s}} \right) \prod_{p \in \mathbb{P}} \left( \frac{1}{(1 - p^{-2s+1})(1 - p^{-2s})} \right)
\]

\[
= (1 + 2^{-s} + 2^{-2s+1})(1 - 2^{-2s+1}) \prod_{p \in \mathbb{P}} \left( \frac{1}{1 - p^{-2s+1}} \right) \prod_{p \in \mathbb{P}} \left( \frac{1}{1 - p^{-2s}} \right)
\]

\[
= (1 + 2^{-s} + 2^{-2s+1})(1 - 2^{-2s+1}) \sum_{n=1}^{\infty} (n^{-2s+1}) \sum_{n=1}^{\infty} (n^{-2s})
\]

using Euler’s product formula for the final step. This is the formula telling us that

\[
\sum_{n=1}^{\infty} (n^{-s}) = \prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1} \text{ (Edwards [10, Section 1.2])},
\]

with convergence on both sides when \( s \in \mathbb{C} \) with \( \text{Re}(s) > 1 \), and in which we can substitute \( 2s \) and \( 2s - 1 \) for \( s \). A caveat is that, when interpreting \( s \) as a variable over the complex numbers, the expressions \( \sum_{n=1}^{\infty} n^{-2s+1} \) and \( \sum_{n=1}^{\infty} n^{-2s} \) will converge precisely when \( \text{Re}(2s) > 1 \) and \( \text{Re}(2s - 1) > 1 \). These conditions are equivalent to \( \text{Re}(s) > \frac{1}{2} \) and \( \text{Re}(s) > 1 \), since \( \text{Re}(2s) = 2\text{Re}(s) \) and \( \text{Re}(2s - 1) = 2\text{Re}(s) - 1 \). Hence the complex function \( \zeta(H; s) \) will be well defined precisely when \( \text{Re}(s) > 1 \). 

\( \square \)
5.2 Analytic Continuation and Extension of the Zeta Function

The results of Theorem 5.1.1 can be extended so that \( \zeta(H; s) \) is a well-defined function on all of \( \mathbb{C} \), as long as we can find a way of assigning values to the otherwise divergent sums \( \sum_{n=1}^{\infty} n^{-2-s+1} \) and \( \sum_{n=1}^{\infty} n^{-2-s} \). Ramanujan [11], Edwards [10], and Candelpergher [12] do exactly that, outlining methods that can give meaningful values to sums like \( \sum_{n=1}^{\infty} n^{-2-s+1} \) and \( \sum_{n=1}^{\infty} n^{-2-s} \) for most or even all \( s \in \mathbb{C} \). Edwards’ method, which he attributes to Riemann, uses analytic continuation, while Ramanujan and Candelpergher describe a method called Ramanujan summation. Both of these methods happen to give us the same result when evaluating \( \zeta(H; s) \) at the point \( s = 0 \), hence giving us the following example computation.

**Corollary 5.2.1.** At \( s = 0 \), the zeta function \( \zeta(H; s) \) evaluates to \( -\frac{1}{6} \) under both analytic continuation and Ramanujan summation methods.

**Proof.** By Theorem 5.1.1, we know that

\[
\zeta(H; s) = (1 + 2^{-s} + 2^{-2s+1})(1 - 2^{-2s+1}) \sum_{n=1}^{\infty} (n^{-2s+1}) \sum_{n=1}^{\infty} (n^{-2s}).
\]

Substituting \( s = 0 \) into the expression \( (1 + 2^{-s} + 2^{-2s+1})(1 - 2^{-2s+1}) \) does not require any special method; we can simply calculate

\[
(1 + 2^{-0} + 2^{-20+1})(1 - 2^{-20+1}) = (1 + 2^0 + 2^1)(1 - 2^1)
\]

\[= (1 + 1 + 2)(1 - 2)\]

\[= -4.\]
Substituting $s = 0$ into the expressions $\sum_{n=1}^{\infty} (n^{-2s+1})$ and $\sum_{n=1}^{\infty} (n^{-2s})$ is more perilous, since it gives infinite sums $\sum_{n=1}^{\infty} n$ and $\sum_{n=1}^{\infty} 1$. These sums are divergent, but Edwards [10, Section 1.5] and Ramanujan [11, Chapter 6, Examples 1 & 2 of p. 135] show that they evaluate to $-\frac{1}{12}$ and $-\frac{1}{2}$ under both analytic continuation and Ramanujan summation. Hence the zeta function $\zeta(H; s)$ evaluates to

$$(-4) \cdot (-\frac{1}{12}) \cdot (-\frac{1}{2}) = -\frac{4}{24} = -\frac{1}{6}$$

at $s = 0$ under both methods.

Incidentally, using Edwards [10], we can deduce the analytic continuation of $\zeta(H; s)$ to be

$$(1 + 2^{-s} + 2^{-2s+1})(1 - 2^{-2s+1})\zeta(2s - 1)\zeta(2s)$$

on almost all of $\mathbb{C}$, where $\zeta(s)$ is the Riemann zeta function (which is to say, the special function $\zeta(s)$ defined in Edwards [10, Section 1.4] which is the analytic continuation of $\sum_{n=1}^{\infty} n^{-s}$). Hence the following.

**Proposition 5.2.2.** When $s$ is interpreted as a variable over the complex numbers, the zeta function $\zeta(H; s)$ has an analytic continuation given by

$$(1 + 2^{-s} + 2^{-2s+1})(1 - 2^{-2s+1})\zeta(2s - 1)\zeta(2s)$$

for all $s \in \mathbb{C} \setminus \{1, \frac{1}{2}\}$, where $\zeta(s)$ is the Riemann zeta function.

**Proof.** Edwards [10, Section 1.4] introduces the Riemann zeta function $\zeta(s)$, which is the analytic continuation of $\sum_{n=1}^{\infty} n^{-s}$ for all $s \in \mathbb{C} \setminus \{1\}$. Substituting $2s - 1$ and $2s$
for $s$, and recalling that

$$\zeta(H; s) = (1 + 2^{-s} + 2^{-2s+1})(1 - 2^{-2s+1}) \sum_{n=1}^{\infty} (n^{-2s+1}) \sum_{n=1}^{\infty} (n^{-2s})$$

from Theorem 5.1.1, we can immediately conclude that

$$(1 + 2^{-s} + 2^{-2s+1})(1 - 2^{-2s+1})\zeta(2s - 1)\zeta(2s)$$

is the analytic continuation of $\zeta(H; s)$ for all $s \in \mathbb{C} \setminus \{1, \frac{1}{2}\}$.

$\square$

Note that in the above, the points $s = 1$ and $s = \frac{1}{2}$ are excluded because $\zeta(2 \cdot 1 - 1) = \zeta(1)$ and $\zeta(2 \cdot \frac{1}{2}) = \zeta(1)$ are undefined. Other summation methods might work for these points.

The intention behind doing this is that gathering information about $\zeta(H; s)$ allows for comparisons with zeta functions computed for other rings, and hence to connecting the algebraic properties of rings to the features of their zeta functions. Finding analytic continuations for these function and comparing values for different $s \in \mathbb{C}$ provides a sensible starting point. Considering other interpretations of $s$ or working with the Dirichlet series directly is another option. This means that computing the zeta functions for more and more rings is of paramount importance, since it would allow the discovery of relevant patterns.
Bibliography


