ตัวประกอบของริงผลหารบนริงจำนวนเต็มกำลังสองบางชนิด

นายวัชระ ขันธวิชัย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ ภาควิชาคณิตศาสตร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2550

FACTORS OF QUOTIENT RINGS OVER SOME QUADRATIC INTEGER RINGS

Mr. Watchara Khuntavichai

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Mathematics
Department of Mathematics
Faculty of Science
Chulalongkorn University
Academic Year 2007

Thesis Title	FACTORS OF QUOTIENT RINGS OVER SOME QUADRATIC INTEGER RINGS
By	Mr. Watchara Khuntavichai
Field of Study	Mathematics
Thesis Advisor	Associate Professor Ajchara Harnchoowong, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

S. Hannongbua .... Dean of the Faculty of Science

(Professor Supot Hannongbua, Ph.D.)

THESIS COMMITTEE

Pimpen Vejjajiva .... Chairman

(Pimpen Vejjajiva, Ph.D.)

Ajchara Harnchoowong .... Thesis Advisor

(Associate Professor Ajchara Harnchoowong, Ph.D.)

Sureeporn Chaopraknoi .... Member

(Sureeporn Chaopraknoi, Ph.D.)

วัชระ ขันธวิชัย : ตัวประกอบของริงผลหารบนริงจำนวนเต็มกำลังสองบางชนิด
(FACTORS OF QUOTIENT RINGS OVER SOME QUADRATIC INTEGER RINGS)
อ. ที่ปรึกษา : รศ. ดร. อัจฉรา หาญชูวงศ์, 42 หน้า

Greg Dresden และ Wayne M. Dymacek ได้ศึกษาการหาตัวประกอบของริงผลหารของริงจำนวนเต็มเกาส์เซียน $\mathbb{Z}[i]=\{a+bi|a,b\in\mathbb{Z}\}$ เราจะขยายผลงานนี้ เพื่อหาตัวประกอบของริงผลหารของ ริงของจำนวนเต็มไอเซ็นสไตน์

$$\mathbb{Z}[\omega]=\{a+b\omega|a,b\in\mathbb{Z}\} \text{ เมื่อ } \omega=\left(-1+\sqrt{-3}\right)/2$$

และริงจำนวนเต็มกำลังสองอื่นๆ $\mathbb{Z}[\omega]$ เมื่อ $\omega=\sqrt{d}$ เมื่อ d เป็นจำนวนเต็มที่ $d\equiv 2,3(\bmod 4)$ และ $\omega=\left(1+\sqrt{d}\right)/2$ เมื่อ d เป็นจำนวนเต็มที่ $d\equiv 1(\bmod 4)$ และทั้งสองกรณี d ไม่มีตัวประกอบกำลังสอง

นอกจากนี้ James T Cross ได้ขยายฟังก์ชัน ออยเลอร์-ฟี จากริงของจำนวนเต็ม ไปยังริงของจำนวนเต็มเกาส์เซียน เราจะขยายฟังก์ชันนี้ไปยังริงของจำนวนเต็มไอเซ็นสไตน์ และ ริงจำนวนเต็มกำลังสองบางชนิด

ภาควิชา ...คณิตศาสตร์... ลายมือชื่อนิสิต..
สาขาวิชา ...คณิตศาสตร์... ลายมือชื่ออาจารย์ที่ปรึกษา..
ปีการศึกษา ......2550.......

4872455623 : MAJOR MATHEMATICS

KEY WORDS : QUADRATIC INTEGERS / QUOTIENT RINGS / EULER ϕ−FUNCTION

WATCHARA KHUNTAVICHAI : FACTORS OF QUOTIENT RINGS OVER SOME QUADRATIC INTEGER RINGS. THESIS ADVISOR : ASSOC. PROF. AJCHARA HARNCHOOWONG, Ph.D., 42 pp.

Greg Dresden and Wayne M. Dymacek obtained factors of quotient rings over ring of Gaussian integers $\mathbb{Z}[i] = \{a+bi|a, b \in \mathbb{Z}\}$.We generalize their idea to obtain factors of quotient rings of the ring of Eisenstein integers $\mathbb{Z}[\omega] = \{a+b\omega|a, b \in \mathbb{Z}\}$ where $\omega = \frac{(-1+\sqrt{-3})}{2}$ and some other quadratic integer rings $\mathbb{Z}[\omega] = \{a + b\omega|a, b \in \mathbb{Z}\}$ for $\omega = \sqrt{d}$ where d is an integer such that $d \equiv 2, 3 \pmod 4$ or $\omega = \frac{(1+\sqrt{d})}{2}$ where d is an integer such that $d \equiv 1 \pmod 4$ and in both cases d is squarefree.

Moreover, James T. Cross extended naturally the Euler ϕ−function of the ring of integers to the ring of Gaussian integers.We extend it to the ring of Eisenstein integers and some quadratic integers rings.

Department ....Mathematics.... Student's Signature Watchara Khuntavichai

Field of Study ....Mathematics.... Advisor's Signature Ajchara Harnchoowong

Academic Year ....2007............

ACKNOWLEDGEMENTS

I am indebted to Assoc. Prof. Dr. Ajchara Harnchoowong, my thesis supervisor, for her kind and helpful advice in preparing and writing my thesis. I would like to thank Dr. Pimpen Vejjajiva and Dr. Sureeporn Chaopraknoi, my thesis committee, for their suggestions to this thesis and all the lecturers during my study.

I acknowledge the 2-year support of the development and promotion of science and tecnology talents project .

Finally, I wish to express my gratitude to my beloved mother for her encouragement throughout my study.

CONTENTS

page

CHAPTER I
INTRODUCTION

1.1 Introduction.

A ring of quadratic integers is a subring of a quadratic field which plays the same roles as the ring of integers $\mathbb{Z}$ in the field $\mathbb{Q}$. Infact, a ring of quadratic integers is an integral domain. Some of them are principal ideal domains but some are not. Greg Dresden and Wayne M. Dymacek[1] studied about factors of quotient rings over the Gaussian integers $\mathbb{Z}[i]$. They generalized the idea of quotient rings of integers to Gaussian integers. So we generalize their idea to the general quadratic integers, in case that they are principal ideal domains.

The Euler $\phi-$function on the set of positive integers is defined to be the number of unit elements in the quotient ring of integers. James T. Cross[2] extended this function to the ring of Gaussian integers.We will study this function on our quadratic integer rings.

In Section 1.2, we give definitions, examples and also investigate some basic properties of the rings of quadratic integers.

In Chapter 2, we study factors of the quotient rings and Euler $\phi-$function over the ring of Eisenstein integers $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$. Moreover we determine the irreducible elements of the ring of Eisenstein integers.

Lastly, we generalize this idea to the general quadratic integers, in case they are principal ideal domains in Chapter 3.

We give some examples of these rings in the next section.

1.2 Definitions and Basic Properties.

A quadratic field is a field extension of $\mathbb{Q}$ of degree 2. Let K be a quadratic field. Then $|K:\mathbb{Q}| = 2$ and $K = \mathbb{Q}[\alpha]$ where α is a root of a monic irreducible polynomial of degree 2, say $f(x) = x^2+ax+b$ where $a, b \in \mathbb{Q}$, i.e. $\alpha = \frac{\left(-a\pm\sqrt{a^2-4b}\right)}{2}$. Since $a, b \in \mathbb{Q}, a^2 - 4b = \frac{d_1}{d_2} = \left(\frac{d_1 d_2}{d_2^2}\right)$ for some $d_1, d_2 \in \mathbb{Z}$ and then there exist $d, c \in \mathbb{Z}$ such that $d_1 d_2 = c^2 d$ where d is a square free integer. Hence $K = \mathbb{Q}[\alpha] = \mathbb{Q}\left[\sqrt{a^2-4b}\right] = \mathbb{Q}\left[\sqrt{d_1 d_2}\right] = \mathbb{Q}\left[\sqrt{d}\right]$ for some square free integer d.

Definition 1.2.1. Define $\omega = \frac{1+\sqrt{d}}{2}$ in case $d \equiv 1(\text{mod } 4)$ and $\omega = \sqrt{d}$ in case $d \equiv 2, 3(\text{mod } 4)$.

Definition 1.2.2. (i) If ω is as in Definition 1.2.1, then the conjugate of ω is $\bar{\omega} = \frac{1-\sqrt{d}}{2}$ in case $d \equiv 1(\text{mod } 4)$ and $\bar{\omega} = -\sqrt{d}$ in case $d \equiv 2, 3(\text{mod } 4)$.
(ii) If $a + b\omega \in \mathbb{Q}[\omega]$, then $(a + b\omega)(a + b\overline{\omega})$ is the *norm* of $a + b\omega$. We will use the notation $N(a + b\omega)$ for the *norm* of $a + b\omega$.

Theorem 1.2.3. *Let* $a + b\omega \in \mathbb{Z}[\omega]$.
(i) *If* $d \equiv 2, 3(\text{mod } 4)$, *then* $N(a + b\omega) = a^2 - b^2 d$.
(ii) *If* $d \equiv 1(\text{mod } 4)$, *then* $N(a + b\omega) = a^2 + ab + b^2\left(\frac{1-d}{4}\right)$.

Proof. (i) Suppose $d \equiv 2, 3(\text{mod } 4)$. Then $\bar{\omega} = -\sqrt{d}$, and so $\omega+\bar{\omega} = 0,\ \omega\bar{\omega} = -d$. Thus $N(a + b\omega) = (a + b\omega)(a + b\overline{\omega}) = a^2 + ab(\omega + \bar{\omega}) + b^2\omega\bar{\omega} = a^2 - b^2 d$.
(ii) Suppose $d \equiv 1(\text{mod } 4)$. Then $\bar{\omega} = (1 - \sqrt{d})/2$, and so $\omega + \bar{\omega} = 1,\ \omega\bar{\omega} = \frac{1-d}{4}$. Thus $N(a + b\omega) = (a + b\omega)(a + b\overline{\omega}) = a^2 + ab(\omega + \bar{\omega}) + b^2\omega\bar{\omega} = a^2 + ab + b^2\left(\frac{1-d}{4}\right)$. □

We next state some results about units, conjugates, and norm. The proofs are all straightforward.

Theorem 1.2.4. (i) *For any* $\alpha \in \mathbb{Z}[\omega]$, α *is a unit if and only if* $N(\alpha) = \pm 1$.
(ii) *If* α *and* β *are elements of* $\mathbb{Q}[\omega]$, *then* $N(\alpha\beta) = N(\alpha)N(\beta)$.

(iii) *If u and $u^{'}$ are units, then so are $uu^{'}$ and $\frac{1}{u}$.*

(iv) *If α and β are elements of $\mathbb{Z}[\omega]$, then $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$.*

(v) *If $\alpha \,|\beta$ in $\mathbb{Z}[\omega]$, then $N(\alpha)\,|N(\beta)$ in $\mathbb{Z}$.*

(vi) *For any $\alpha \in \mathbb{Z}[\omega]$, if $N(\alpha) = \pm p$, where p is a prime integer, then α is an irreducible element in $\mathbb{Z}[\omega]$.*

In Chapter 3 we will consider only quadratic integers which are PID and we know that if an integral domain is a Euclidean domain, then it is a PID. So we will give some examples of Euclidean quadratic integer rings.

Example 1.2.5. *If $d = -3, -2, -1, 2, 3, 5, 13, 17, 21$ then $\mathbb{Z}[\omega]$ is Euclidean domain.*

Proof. Define $\theta : \mathbb{Z}[\omega] \to \mathbb{Z}_0^+$ by $\theta(a + b\omega) = |N(a + b\omega)|$.
Clearly θ is function, $\theta(a + b\omega) \geq 0$ and ker $\theta = \{0\}$.
Let $a_1 + a_2\omega, b_1 + b_2\omega$ be nonzero elements in $\mathbb{Z}[\omega]$. By Theorem 1.2.4 (ii), $N((a_1 + a_2\omega)(b_1 + b_2\omega)) = N(a_1 + a_2\omega)N(b_1 + b_2\omega)$. Then $\theta((a_1 + a_2\omega)(b_1 + b_2\omega)) = \theta(a_1 + a_2\omega)\theta(b_1 + b_2\omega)$ and $\theta((a_1 + a_2\omega)(b_1 + b_2\omega)) \geq \theta(a_1 + a_2\omega)$.
Consider $a_1 + a_2\omega, b_1 + b_2\omega \in \mathbb{Z}[\omega]$ and $b_1 + b_2\omega \neq 0$. There exists $q_1 + q_2\omega \in \mathbb{Q}[\omega]$ such that $a_1 + a_2\omega = (b_1 + b_2\omega)(q_1 + q_2\omega)$. Let $s_1, s_2 \in \mathbb{Z}$ be the best approximations to q_1, q_2, respectively, that is,

$$|q_1 - s_1| \leq \tfrac{1}{2} \text{ and } |q_2 - s_2| \leq \tfrac{1}{2}.$$

Given $r_1 + r_2\omega = a_1 + a_2\omega - (b_1 + b_2\omega)(s_1 + s_2\omega) \in \mathbb{Z}[\omega]$. Thus $a_1 + a_2\omega = (b_1 + b_2\omega)(s_1 + s_2\omega) + r_1 + r_2\omega$ and $\theta(r_1 + r_2\omega) = \theta(a_1 + a_2\omega - (b_1 + b_2\omega)(s_1 + s_2\omega))$.
Case 1. $d \equiv 1 (\text{mod } 4)$. Since $a_1 + a_2\omega = (b_1 + b_2\omega)(q_1 + q_2\omega)$,

$$\begin{aligned}
\theta(r_1 + r_2\omega) &= \theta((b_1 + b_2\omega)(q_1 + q_2\omega) - (b_1 + b_2\omega)(s_1 + s_2\omega)) \\
&= \theta((b_1 + b_2\omega)((q_1 - s_1) + (q_2 - s_2)\omega)) \\
&= \theta(b_1 + b_2\omega)\theta((q_1 - s_1) + (q_2 - s_2)\omega) \\
&= \theta(b_1 + b_2\omega)\left|(q_1 - s_1)^2 + (q_1 - s_1)(q_2 - s_2) + (q_2 - s_2)^2(\tfrac{1-d}{4})\right| \\
&\leq \theta(b_1 + b_2\omega)\left|\tfrac{1}{4} + \tfrac{1}{4} + \tfrac{1}{4}(\tfrac{1-d}{4})\right| \\
&= \theta(b_1 + b_2\omega)\left|\tfrac{9-d}{16}\right|.
\end{aligned}$$

We have if $\left|\frac{9-d}{16}\right| < 1$ then $\mathbb{Z}[\omega]$ is Euclidean domain with the Euclidean valuation θ. Hence for $d \equiv 1 (\text{mod } 4)$, if $d = -3, 5, 13, 17, 21$, then $\mathbb{Z}[\omega]$ is Euclidean domain.

Case 2. $d \equiv 2, 3 (\text{mod } 4)$. Since $a_1 + a_2\omega = (b_1 + b_2\omega)(q_1 + q_2\omega)$,

$$\begin{aligned}
\theta(r_1 + r_2\omega) &= \theta((b_1 + b_2\omega)(q_1 + q_2\omega) - (b_1 + b_2\omega)(s_1 + s_2\omega)) \\
&= \theta((b_1 + b_2\omega)((q_1 - s_1) + (q_2 - s_2)\omega)) \\
&= \theta(b_1 + b_2\omega)\theta((q_1 - s_1) + (q_2 - s_2)\omega) \\
&= \theta(b_1 + b_2\omega)\left|(q_1 - s_1)^2 - (q_2 - s_2)^2 d\right| \\
&\leq \theta(b_1 + b_2\omega)\left|\tfrac{1}{4} - (\tfrac{1}{4})d\right| \\
&= \theta(b_1 + b_2\omega)\left|\tfrac{1-d}{4}\right|.
\end{aligned}$$

We have if $\left|\frac{1-d}{4}\right| < 1$ then $\mathbb{Z}[\omega]$ is Euclidean domain with the Euclidean valuation θ. Hence for $d \equiv 2, 3 (\text{mod } 4)$, if $d = -2, -1, 2, 3$, then $\mathbb{Z}[\omega]$ is Euclidean domain.

□

In [3], Ratinan Boonklurb gave all imaginary quadratic integer rings which are Euclidean domain.

Example 1.2.6. [3]*(Ratinan Boonklurb,1998) For $d < 0$, $\mathbb{Z}[\omega]$ is Euclidean domain if and only if $d = -11, -7 - 3, -2, -1$.*

Theorem 1.2.7. *Let D be a PID.*

(i) *Every nonzero nonunit element of D is prime if and only if it is irreducible.*

(ii) *For any $\pi \in D$, $\langle \pi \rangle$ is a maximal ideal if and only if $\langle \pi \rangle$ is a prime ideal.*

(iii) *For any $\pi \in D$, π is prime if and only if $D/\langle \pi \rangle$ is a field.*

Theorem 1.2.8. *Let D be a PID, $a_1, a_2, ..., a_n \in D$ such that for $i \neq j$, $\langle a_i \rangle + \langle a_j \rangle = D$. Then*

$$D/\langle a_1 a_2 ... a_n \rangle \cong D/\langle a_1 \rangle \oplus D/\langle a_2 \rangle \oplus ... \oplus D/\langle a_n \rangle .$$

CHAPTER II

FACTORS OF QUOTIENT RINGS OVER EISENSTEIN INTEGER RINGS

In this chapter, we study factors of the quotient rings over the ring of Eisenstein integers $\mathbb{Z}[\omega] = \{a + b\omega \,|a, b \in \mathbb{Z}\}$, where $\omega = (-1+\sqrt{-3})/2$. The field of fractions of Eisenstein integers is the field $\mathbb{Q}\left[\sqrt{-3}\right]$. We prove that it is a Euclidean domain in Chapter 1, so it is a principal ideal domain and a unique factorization domain. For any ideal $\langle a + b\omega\rangle$ of $\mathbb{Z}[\omega]$, we will find the structure of the quotient ring $\mathbb{Z}[\omega] / \langle a + b\omega\rangle$.

2.1 Factors of Quotient Rings over Ring of Eisenstein Integers

First, we have $\bar{\omega} = \left(-1-\sqrt{-3}\right)/2,\ \omega+\bar{\omega} = -1,\ \omega\bar{\omega} = 1$ and $\omega^2+\omega+1 = 0$.

Lemma 2.1.1. *If k is a positive integer, then $c+d\omega$ belongs to the ideal $\langle ak + bk\omega\rangle$ if and only if $k(a^2-ab+b^2)$ divides both $ac+bd-cb$ and $ad-cb$.*

Proof. Let k be a positive integer. Then for any $c + d\omega \in \mathbb{Z}[\omega]$,

$$\begin{aligned}\frac{c+d\omega}{ak+bk\omega} &= \frac{(c+d\omega)(ak+bk\overline{\omega})}{(ak+bk\omega)(ak+bk\overline{\omega})}\\ &= \frac{(ack+bdk-cbk)}{k^2(a^2-ab+b^2)} + \frac{(adk-cbk)\,\omega}{k^2(a^2-ab+b^2)}\\ &= \frac{(ac+bd-cb)}{k(a^2-ab+b^2)} + \frac{(ad-cb)\,\omega}{k(a^2-ab+b^2)}.\end{aligned}$$

Thus $c + d\omega \in \langle ak + bk\omega\rangle$ if and only if $k(a^2 - ab + b^2)$ divides both $ac + bd - cb$ and $ad - cb$. □

Lemma 2.1.2. *For a nonzero element $a + b\omega \in \mathbb{Z}[\omega]$, there exists a unit $u \in \{\pm 1, \pm\omega, \pm\omega^2\}$ such that $(a + b\omega)u = x + y\omega$ where x and y are positive integers.*

Proof. Let $a + b\omega \in \mathbb{Z}[\omega]$ and $a + b\omega \neq 0$.

Case 1. $a, b \in \mathbb{Z}_0^-$. Then $(a + b\omega)(-1) = -a - b\omega$ where $-a, -b \in \mathbb{Z}^+$.

Case 2. $a \in \mathbb{Z}^-$ and $b \in \mathbb{Z}^+$. Then $(a+b\omega)(-\omega) = -a\omega - b\omega^2 = -a\omega - b(-\omega - 1) = (-a + b)\omega + b$ where $(-a + b), b \in \mathbb{Z}^+$.

Case 3. $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}^-$. Then

$$\begin{aligned}(a + b\omega)(-\omega^2) &= (a + b\omega)(\omega + 1)\\ &= a\omega + b\omega^2 + a + b\omega\\ &= a\omega + b(-\omega - 1) + a + b\omega\\ &= a\omega - b + a \text{ for } a, a - b \in \mathbb{Z}^+.\end{aligned}$$

Case 4. $a, b \in \mathbb{Z}_0^+$. Then $(a + b\omega)(1) = a + b\omega$ for $a, b \in \mathbb{Z}^+$.

Hence for $a + b\omega \in \mathbb{Z}[\omega]$, there exists a unit $u \in \{\pm 1, \pm\omega, \pm\omega^2\}$ such that $(a + b\omega)u = x + y\omega$ where x and y are positive integers. □

Lemma 2.1.3. *If a is a positive integer larger than 1 ,then $\mathbb{Z}[\omega] / \langle a \rangle \cong \mathbb{Z}_a[\omega]$.*

Proof. Define $\phi : \mathbb{Z}[\omega] \to \mathbb{Z}_a[\omega]$ by $\phi(x + y\omega) = [x]_a + [y]_a\omega$. It is obvious from the definition of ϕ that ϕ is onto. Next, we will show that ϕ is a ring homomorphism. Let $x_1 + y_1\omega, x_2 + y_2\omega \in \mathbb{Z}[\omega]$. Then

$$\begin{aligned}\phi((x_1 + y_1\omega) + (x_2 + y_2\omega)) &= \phi((x_1 + x_2) + (y_1 + y_2)\omega)\\ &= [x_1 + x_2]_a + [y_1 + y_2]_a\omega\\ &= [x_1]_a + [x_2]_a + [y_1]_a\omega + [y_2]_a\omega\\ &= ([x_1]_a + [y_1]_a\omega) + ([x_2]_a + [y_2]_a\omega)\\ &= \phi(x_1 + y_1\omega) + \phi(x_2 + y_2\omega).\end{aligned}$$

Also, $\phi((x_1 + y_1\omega) \cdot (x_2 + y_2\omega)) = \phi(x_1x_2 + (x_2y_1 + x_1y_2)\omega + y_1y_2\omega^2)$

$$\begin{aligned}&= \phi(x_1x_2 + (x_2y_1 + x_1y_2)\omega - y_1y_2(\omega + 1))\\ &= \phi((x_1x_2 - y_1y_2) + (x_2y_1 + x_1y_2 - y_1y_2)\omega).\end{aligned}$$

$$
\begin{aligned}
&= [x_1x_2 - y_1y_2]_a + [x_2y_1 + x_1y_2 - y_1y_2]_a \, \omega \\
&= [x_1x_2]_a + [x_2y_1 + x_1y_2]_a \, \omega - [y_1y_2]_a \, (1+\omega) \\
&= [x_1x_2]_a + [x_2y_1 + x_1y_2]_a \, \omega + [y_1y_2]_a \, \omega^2 \\
&= ([x_1]_a + [y_1]_a \, \omega) \cdot ([x_2]_a + [y_2]_a \, \omega) \\
&= \phi\,(x_1 + y_1\omega) \cdot \phi\,(x_2 + y_2\omega).
\end{aligned}
$$

Hence ϕ is a surjective ring homomorphism. Since $\phi\,(a) = [a]_a = [0]_a\,, \langle a \rangle \subseteq \ker \phi$. Next, let $x + y\omega \in \ker \phi$. Then $[0]_a = \phi\,(x + y\omega) = [x]_a + [y]_a \, \omega$, i.e. both x and y are congruent to 0 modulo a, so we can write $x = ax'$ and $y = ay'$ for some $x', y' \in \mathbb{Z}$. Then $x + y\omega = ax' + ay'\omega \in \langle a \rangle$. Thus $\ker \phi \subseteq \langle a \rangle$. Therefore $\ker \phi = \langle a \rangle$ and so $\mathbb{Z}\,[\omega] \,/\, \langle a \rangle \cong \mathbb{Z}_a\,[\omega]$. □

Definition 2.1.4. For any $x+y\omega \in \mathbb{Z}\,[\omega]$, define the *norm* of $x+y\omega$ by $N\,(x + y\omega) = (x + y\omega)\,(x + y\bar{\omega}) = x^2 + xy(\omega + \bar{\omega}) + y^2\omega\bar{\omega} = x^2 - xy + y^2$.

Lemma 2.1.5. *Let $a + b\omega \in \mathbb{Z}\,[\omega]$ where a and b are relatively prime and $s = N\,(a + b\omega) = a^2 - ab + b^2$. Then $\mathbb{Z}\,[\omega] \,/\, \langle a + b\omega \rangle \cong \mathbb{Z}_s$. Consequently if s is a prime number, then $a + b\omega$ is irreducible.*

Proof. Let $a+b\omega \in \mathbb{Z}\,[\omega]$, where a and b are relatively prime and $s = N\,(a + b\omega) = a^2 - ab + b^2$. By Lemma 2.1.2, we can assume without loss of generality that a and b are both positive. Since $(a, b) = 1$, $(a^2, b) = 1$. Then $(b, s) = (b, a^2 - ab + b^2) = 1$, so b^{-1} exists in $\mathbb{Z}_s$. Since $a^2 - ab + b^2 \equiv 0 (\text{mod } s)$, $(ab^{-1})^2 \equiv ab^{-1} - 1 (\text{mod } s)$. To show that $\mathbb{Z}\,[\omega] \,/\, \langle a + b\omega \rangle \cong \mathbb{Z}_s$, define $\phi : \mathbb{Z}\,[\omega] \to \mathbb{Z}_s$ by

$$\phi\,(x + y\omega) = [x - (ab^{-1})\,y],$$

where $[t] = [t]_s$.

For any $m \in \mathbb{Z}$, $\phi\,(m) = [m - (ab^{-1})\,0] = [m]\,$, so ϕ is surjective.

Let $x_1 + y_1\omega$ and $x_2 + y_2\omega \in \mathbb{Z}\,[\omega]$. Thus

$$
\begin{aligned}
\phi((x_1 + y_1\omega) + (x_2 + y_2\omega)) &= \phi((x_1 + x_2) + (y_1 + y_2)\,\omega) \\
&= [(x_1 + x_2) - (ab^{-1})(y_1 + y_2)]
\end{aligned}
$$

$$
\begin{aligned}
&= \left[x_1 - \left(ab^{-1}\right) y_1\right] + \left[x_2 - \left(ab^{-1}\right) y_2\right] \\
&= \phi\left(x_1 + y_1\omega\right) + \phi\left(x_2 + y_2\omega\right), \text{ and} \\
\phi((x_1 + y_1\omega)(x_2 + y_2\omega)) &= \phi(x_1x_2 + (y_1x_2 + x_1y_2)\omega + y_1y_2\omega^2) \\
&= \phi(x_1x_2 + (y_1x_2 + x_1y_2)\omega + (-\omega - 1)y_1y_2) \\
&= \phi((x_1x_2 - y_1y_2) + (y_1x_2 + x_1y_2 - y_1y_2)\omega) \\
&= [(x_1x_2 - y_1y_2) - (ab^{-1})(y_1x_2 + x_1y_2 - y_1y_2)] \\
&= \left[x_1x_2 + \left(ab^{-1} - 1\right) y_1y_2 - \left(ab^{-1}\right)\left(y_1x_2 + x_1y_2\right)\right] \\
&= \left[x_1x_2 + \left(ab^{-1}\right)^2 y_1y_2 - \left(ab^{-1}\right)\left(y_1x_2 + x_1y_2\right)\right] \\
&= \left[x_1 - \left(ab^{-1}\right) y_1\right]\left[x_2 - \left(ab^{-1}\right) y_2\right] \\
&= \phi\left(x_1 + y_1\omega\right)\phi\left(x_2 + y_2\omega\right).
\end{aligned}
$$

Then ϕ is a ring homomorphism.

Moreover, since $\phi\left(a + b\omega\right) = \left[a - \left(ab^{-1}\right) b\right] = [0]$, $\langle a + b\omega\rangle \subseteq \ker\phi$. Next, let $c + d\omega \in \ker\phi$. Then

$$
\begin{aligned}
\frac{c + d\omega}{a + b\omega} &= \frac{\left(c + d\omega\right)\left(a + b\overline{\omega}\right)}{\left(a + b\omega\right)\left(a + b\overline{\omega}\right)} \\
&= \frac{ac + ad\omega + cb\bar{\omega} + bd\omega\bar{\omega}}{a^2 - ab + b^2} \\
&= \frac{ac + bd - cb + \left(ad - cb\right)\omega}{a^2 - ab + b^2} \\
&= \frac{\left(ac + bd - cb\right)}{a^2 - ab + b^2} + \frac{\left(ad - cb\right)\omega}{a^2 - ab + b^2}.
\end{aligned}
$$

Since $\phi\left(c + d\omega\right) = \left[c - ab^{-1}d\right] = [0], [ad - cb] = \left[c - ab^{-1}d\right][-b] = [0]$. By $[ad - cb] = [0]$, we have $[ab^2c - a^2bd] = [ad - cb]\,[-ab] = [0]$. Then $[ac - a^2b^{-2}bd]$ $= [ab^2c - a^2bd]\,[b^{-2}] = [0]$. Since $\left(ab^{-1}\right)^2 \equiv ab^{-1} - 1 (\mathrm{mod}\ (a^2 - ab + b^2)\ )$, $\left[ac - \left(ab^{-1} - 1\right) bd\right] = [0]$. Then $[ac - ad + bd] = [0]$, and so $[ac - bc + bd] = [0]$. Thus $a + b\omega\,|c + d\omega$ and $c + d\omega \in \langle a + b\omega\rangle$. Hence $\ker\phi \subseteq \langle a + b\omega\rangle$ and so $\ker\phi = \langle a + b\omega\rangle$. Then $\mathbb{Z}\left[\omega\right] / \langle a + b\omega\rangle \cong \mathbb{Z}_s$. Consequently if s is a prime number in $\mathbb{Z}$ then $\mathbb{Z}\left[\omega\right] / \langle a + b\omega\rangle$ is a field. Hence $\sigma = a + b\omega$ is an irreducible element in $\mathbb{Z}\left[\omega\right]$.

□

Lemma 2.1.6. *Let p be a prime number. Then $\mathbb{Z}_p[\omega] \cong \mathbb{Z}_p[x] / \langle x^2+x+1\rangle$. Consequently x^2+x+1 has no root in $\mathbb{Z}_p$ if and only if $\mathbb{Z}_p[\omega]$ is a field.*

Proof. Define $\varphi : \mathbb{Z}_p[x] \to \mathbb{Z}_p[\omega]$ by

$$\varphi(f(x)) = f(\omega).$$

Clearly that φ is a surjective ring homomorphism.
Next, we will show that $\ker\varphi = \langle x^2+x+1\rangle$. Since $\varphi(x^2+x+1) = 0$, $\langle x^2+x+1\rangle \subseteq \ker\varphi$. Let $f(x) \in \ker\varphi$, so $f(\omega) = 0$. Since p is prime, $\mathbb{Z}_p$ is a field. There exists $m_{\mathbb{Z}_p}(x)$ which is a minimal polynomial of ω over $\mathbb{Z}_p$. Since $\omega \notin \mathbb{Z}_p$ and $\omega^2+\omega+1 = 0$, $m_{\mathbb{Z}_p}(x)$ is a polynomial with degree 2. Thus $x^2+x+1 = bm_{\mathbb{Z}_p}(x)$ for some $b \in \mathbb{Z}_p$, and $f(x) = g(x)m_{\mathbb{Z}_p}(x)$ for some $g(x) \in \mathbb{Z}_p[x]$ such that $\deg(f(x)) = \deg(g(x)) + 2$. Then $f(x) = g(x)(b^{-1}b)m_{\mathbb{Z}_p}(x) = g(x)b^{-1}(bm_{\mathbb{Z}_p}(x)) = g(x)b^{-1}(x^2+x+1)$. Thus $f(x) \in \langle x^2+x+1\rangle$ and $\ker\varphi \subseteq \langle x^2+x+1\rangle$. Hence $\ker\varphi = \langle x^2+x+1\rangle$. By the standard isomorphism theorem, $\mathbb{Z}_p[x] / \langle x^2+x+1\rangle \cong \mathbb{Z}_p[\omega]$. Since x^2+x+1 has no root in $\mathbb{Z}_p$, it is irreducible in $\mathbb{Z}_p[x]$. Hence $\langle x^2+x+1\rangle$ is a maximal ideal in $\mathbb{Z}_p[x]$ if and only if $\mathbb{Z}_p[\omega]$ is a field.

□

Next, we will determine the irreducible elements of the ring of Eisenstein integers.

Theorem 2.1.7. *Up to association, the irreducible elements in $\mathbb{Z}[\omega]$ are exactly the followings:*
(i) *$\sigma = a+b\omega$ and $\bar{\sigma} = a+b\bar{\omega}$, where $N(\sigma) = N(\bar{\sigma})$ is a prime number in $\mathbb{Z}$ and $N(\sigma), N(\bar{\sigma}) \equiv 1 (\mathrm{mod}\ 6)$,*
(ii) *$2+\omega$, where $N(2+\omega) = 3$ and $\langle 3\rangle = \langle 2+\omega\rangle^2$,*
(iii) *π, where π is prime in $\mathbb{Z}$ such that $\pi \equiv 5(\mathrm{mod}\ 6)$,*
(iv) *2.*

Proof. (i) and (ii) follow by Lemma 2.1.5.
(iii) Let π be a prime in $\mathbb{Z}$ such that $\pi \equiv 5(\mathrm{mod}\ 6)$. Thus $(2x+1)^2 \equiv -3(\mathrm{mod}$

π) and hence $x^2 + x + 1$ has no root in $\mathbb{Z}_\pi$. By Lemma 2.1.6, $\mathbb{Z}_\pi[\omega]$ is a field. By Lemma 2.1.3, $\mathbb{Z}[\omega] / \langle \pi \rangle \cong \mathbb{Z}_\pi[\omega]$. Hence $\langle \pi \rangle$ is a maximal ideal and so π is irreducible.

(iv) Since $x^2 + x + 1$ has no root modulo 2, by Lemma 2.1.6, $\mathbb{Z}_2[\omega]$ is a field. By Lemma 2.1.3, $\mathbb{Z}[\omega] / \langle 2 \rangle \cong \mathbb{Z}_2[\omega]$, so $\langle 2 \rangle$ is a maximal ideal in $\mathbb{Z}[\omega]$. Hence 2 is irreducible.

Conversely, let β be an irreducible element in $\mathbb{Z}[\omega]$.

Case 1. $\beta = \pi \in \mathbb{Z}^+$. Since π is an irreducible in $\mathbb{Z}[\omega]$, π is a prime integer. For odd prime π, by Lemma 2.1.3 and Lemma 2.1.6,

$$\mathbb{Z}[\omega] / \langle \pi \rangle \cong \mathbb{Z}_\pi[\omega] \cong \mathbb{Z}_\pi[x] / \langle x^2 + x + 1 \rangle.$$

Thus $\mathbb{Z}_\pi[x] / \langle x^2 + x + 1 \rangle$ is a field. Then $x^2 + x + 1 \equiv 0 (\text{mod } \pi)$ has no solution. Thus $(2x+1)^2 \equiv -3 (\text{mod } \pi)$ has no solution. By $[4, page131]$, $\pi \equiv 5 \pmod 6$.

Case 2. $\beta = a + b\omega \in \mathbb{Z}^+[\omega]$. By Lemma 2.1.5, $\mathbb{Z}[\omega] / \langle a + b\omega \rangle \cong \mathbb{Z}_{N(a+b\omega)}$ Then $N(a + b\omega)$ is a prime integer. We have $N(a + b\omega) \equiv 1$ or 3 or $5 (\text{mod } 6)$.

Suppose that $N(a + b\omega) \equiv 5 (\text{mod } 6)$. By (iii), $N(a + b\omega)$ is irreducible. It contradicts $N(a + b\omega) = (a + b\omega)(a + b\bar{\omega})$. So $N(a + b\omega) \equiv 1$ or $3 (\text{mod } 6)$.

If $N(a + b\omega) \equiv 3 (\text{mod } 6)$, then $3 \mid N(a + b\omega)$. Since $N(a + b\omega)$ is a prime integer, $N(a + b\omega) = 3$. One of these is $a + b\omega = 2 + \omega$. For $N(a + b\omega) \equiv 1 (\text{mod } 6)$, we have $N(a + b\omega) = (a + b\omega)(a + b\bar{\omega}) = N(a + b\bar{\omega})$. We will show that β and $\bar{\beta}$ are not associated, suppose they are. Then $\langle a + b\omega \rangle = \langle a + b\bar{\omega} \rangle$, i.e.

$$\begin{aligned} a + b\omega &= u(a + b\bar{\omega}) \text{ for some unit } u \in \{\pm 1, \pm\omega, \pm\omega^2\} \\ &= ua + ub\bar{\omega} \\ &= ua + ub(-\omega - 1) \\ &= (ua - ub) - ub\omega. \end{aligned}$$

Thus $a = (ua - ub)$ and $b = -ub$, so $u = -1$ and $b = 2a$. Hence $N(a + b\omega) = a^2 - ab + b^2 = a^2 - 2a^2 + 4a^2 = 3a^2$, it contradics the fact that $N(a + b\omega)$ is a prime integer. Thus β and $\bar{\beta}$ are not associated.

□

Theorem 2.1.8. *If a, b and k are positive integers such that a and b are relatively prime, then*

$$\mathbb{Z}\left[\omega\right] / \left\langle ak + bk\omega \right\rangle = \left\{ \left[x^{'} + y^{'}\omega\right] : 0 \leq x^{'} < k, 0 \leq y^{'} < k\left(a^2 - ab + b^2\right) \right\}.$$

Proof. Let $[x + y\omega] \in \mathbb{Z}\left[\omega\right] / \left\langle ak + bk\omega \right\rangle$. Since $(a, b) = 1$, there exist integers s and t such that $as + bt = 1$. Then $aks + bkt = k$. Thus $k + (ak + bk\omega)(-s + \omega t) = (akt - bks - bkt)\,\omega$. Then $k \equiv (akt - bks - bkt)\,\omega(\bmod \left\langle ak + bk\omega \right\rangle)$. Let $m = akt - bks - bkt$. Then

$$k \equiv m\omega(\bmod \left\langle ak + bk\omega \right\rangle). \tag{1}$$

Since $k\left(a^2 - ab + b^2\right)\omega = (ak + bk\omega)(a + b\overline{\omega})\omega$,

$$k\left(a^2 - ab + b^2\right)\omega \equiv 0(\bmod \left\langle ak + bk\omega \right\rangle). \tag{2}$$

Thus $[x + y\omega] = \left[n_1k + x^{'} + y\omega\right]$ where $x = n_1k + x^{'}$ such that $0 \leq x^{'} < k$

$= \left[x^{'} + n_1m\omega + y\omega\right]$ by (1)

$= \left[x^{'} + (n_1m + y)\omega\right]$

$= \left[x^{'} + (n_2k\left(a^2 - ab + b^2\right) + y^{'})\omega\right]$ where $n_1m + y = n_2k(a^2 - ab$ $+b^2) + y^{'}$ such that $0 \leq y^{'} < k(a^2 - ab + b^2)$

$= \left[x^{'} + y^{'}\omega\right]$ by (2).

Hence $[x + y\omega] = \left[x^{'} + y^{'}\omega\right]$, with $0 \leq x^{'} < k, 0 \leq y^{'} < k\left(a^2 - ab + b^2\right)$.

Let $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ such that $0 \leq x_1, x_2 < k, 0 \leq y_1, y_2 < k\left(a^2 - ab + b^2\right)$ and $[x_1 + y_1\omega] = [x_2 + y_2\omega]$. Then $(x_2 - x_1) + (y_2 - y_1)\omega \in \left\langle ak + bk\omega \right\rangle$. Appealing to Lemma 2.1.1, we conclude that $k\left(a^2 - ab + b^2\right)|a(x_2 - x_1) + b(y_2 - y_1) - b(x_2 - x_1)$ and $k\left(a^2 - ab + b^2\right)|a(y_2 - y_1) - b(x_2 - x_1)$. Therefore $k\left(a^2 - ab + b^2\right)|a(a(x_2 - x_1) + b(y_2 - y_1) - b(x_2 - x_1)) + (-b)\left(a(y_2 - y_1) - b\left(x_2 - x_1\right)\right)$, and so $k\left|x_2 - x_1\right.$. Since $0 \leq x_1, x_2 < k$, $x_1 = x_2$. Then $k\left(a^2 - ab + b^2\right)|b(y_2 - y_1)$ and $k\left(a^2 - ab + b^2\right)|a(y_2 - y_1)$. We have

$$a(y_2 - y_1) = k\left(a^2 - ab + b^2\right)l_1 \text{ and}$$

$$b(y_2 - y_1) = k\left(a^2 - ab + b^2\right)l_2 \text{ for some } l_1, l_2 \in \mathbb{Z}.$$

Since $(a, b) = 1$, there exist integers s and t such that $as + bt = 1$. Then

$$a(y_2 - y_1)s = k\,(a^2 - ab + b^2)\,l_1 s \text{ and}$$
$$b(y_2 - y_1)t = k\,(a^2 - ab + b^2)\,l_2 t.$$

Thus $y_2 - y_1 = (y_2 - y_1)(as + bt) = k\,(a^2 - ab + b^2)\,(l_1 s + l_2 t)$. Hence $k\,(a^2 - ab + b^2)\,|y_2 - y_1$. Since $0 \le y_1, y_2 < k\,(a^2 - ab + b^2)$, $y_1 = y_2$. □

From Theorem 2.1.7 and $\mathbb{Z}[\omega]$ is a UFD, for any nonzero Eisenstein integer $a + b\omega$, we have

$$a + b\omega \sim 2^t \prod \sigma_i^{u_i} \cdot \prod \bar{\sigma}_i^{v_i} \cdot \prod \pi_i^{e_i} \cdot (2+\omega)^n,$$

where $u_i, v_i, e_i, t, n \in \mathbb{Z}_0^+$.

Theorem 2.1.9. *Let $a + b\omega \in \mathbb{Z}[\omega] \setminus \{0\}$ be such that*

$$a + b\omega \sim 2^t \prod \sigma_i^{u_i} \cdot \prod \bar{\sigma}_i^{v_i} \cdot \prod \pi_i^{e_i} \cdot (2+\omega)^n,$$

where $u_i, v_i, e_i, t, n \in \mathbb{Z}_0^+$, $s_1 = \prod N(\sigma_i^{u_i}), s_2 = \prod N(\bar{\sigma}_i^{v_i}), k = 2^t \cdot \prod \pi_i^{e_i}$ and $R_n = \mathbb{Z}[\omega] / \langle (2+\omega)^n \rangle$. Then $\mathbb{Z}[\omega] / \langle a + b\omega \rangle \cong \mathbb{Z}_{s_1} \oplus \mathbb{Z}_{s_2} \oplus \mathbb{Z}_k[\omega] \oplus R_n$, where $R_n \cong \mathbb{Z}_{3^m}[\omega]$ when $n = 2m$ and $R_n \cong \mathbb{Z}[x] / \langle 3^m x, 3^{m+1}, x^2 + 3x + 3 \rangle$ when $n = 2m + 1$.

Proof. Let a and b be integers, not both zero, such that

$$a + b\omega \sim 2^t \prod \sigma_i^{u_i} \cdot \prod \bar{\sigma}_i^{v_i} \cdot \prod \pi_i^{e_i} \cdot (2+\omega)^n,$$

$s_1 = \prod N(\sigma_i^{u_i}), s_2 = \prod N(\bar{\sigma}_i^{v_i}), k = 2^t \cdot \prod \pi_i^{e_i}$, and $R_n = \mathbb{Z}[\omega] / \langle (2+\omega)^n \rangle$. Applying Theorem 1.2.8, we arrive at

$$\begin{aligned}
\mathbb{Z}[\omega] / \langle a + b\omega \rangle &\cong \mathbb{Z}[\omega] / \langle \textstyle\prod \sigma_i^{u_i} \cdot \prod \bar{\sigma}_i^{v_i} \cdot 2^t \cdot \prod \pi_i^{e_i} \cdot (2+\omega)^n \rangle \\
&\cong \mathbb{Z}[\omega] / \langle \textstyle\prod \sigma_i^{u_i} \rangle \oplus \mathbb{Z}[\omega] / \langle \prod \bar{\sigma}_i^{v_i} \rangle \\
&\quad \oplus \mathbb{Z}[\omega] / \langle 2^t \cdot \textstyle\prod \pi_i^{e_i} \rangle \oplus \mathbb{Z}[\omega] / \langle (2+\omega)^n \rangle.
\end{aligned}$$

Consider $\prod \sigma_i^{u_i} = c + d\omega$. Thus $s_1 = \prod N(\sigma_i^{u_i}) = N(\prod \sigma_i^{u_i}) = N(c + d\omega) = c^2 - cd + d^2$. Clearly 2, 3 and any prime π in $\mathbb{Z}$ such that $\pi \equiv 5 (\text{mod } 6)$ cannot divide $c + d\omega$, and any prime q in $\mathbb{Z}$ with $q \equiv 1 (\text{mod } 6)$ we have $q = \sigma_h \bar{\sigma}_h$ for some h, whence q cannot divide $c + d\omega$. Thus $(c, d) = 1$. By Lemma 2.1.5, $\mathbb{Z}[\omega] / \langle \prod \sigma_i^{u_i} \rangle = \mathbb{Z}[\omega] / \langle c + d\omega \rangle \cong \mathbb{Z}_{c^2 - cd + d^2} \cong \mathbb{Z}_{s_1}$. Similarly, $\mathbb{Z}[\omega] / \langle \prod \bar{\sigma}_i^{v_i} \rangle \cong$

$\mathbb{Z}_{s_2}$. By Lemma 2.1.3, $\mathbb{Z}[\omega] / \langle 2^t \cdot \prod \pi_i^{e_i} \rangle \cong \mathbb{Z}_k[\omega]$.

For even n, let $n = 2m$ where $m > 0$. We have $\langle (2+\omega)^n \rangle = \left\langle (-3\omega^2)^m \right\rangle = \langle 3^m \rangle$. Thus $\mathbb{Z}[\omega] / \langle (2+\omega)^n \rangle = \mathbb{Z}[\omega] / \langle 3^m \rangle \cong \mathbb{Z}_{3^m}[\omega]$. Hence $\mathbb{Z}[\omega] / \langle a + b\omega \rangle \cong \mathbb{Z}_{s_1} \oplus \mathbb{Z}_{s_2} \oplus \mathbb{Z}_k[\omega] \oplus \mathbb{Z}_{3^m}[\omega]$.

For odd n, let $n = 2m+1$ where $m \geq 0$. We will show that

$$R_{2m+1} = \mathbb{Z}[\omega] / \left\langle (2+\omega)^{2m+1} \right\rangle \cong \mathbb{Z}[x] / \langle 3^m x, 3^{m+1}, x^2 + 3x + 3 \rangle.$$

First, we have
$$\begin{aligned}(2+\omega)^{2m+1} &= (2+\omega)(2+\omega)^{2m} \\ &= (2+\omega)((2+\omega)^2)^m \\ &= (2+\omega)(4+4\omega+\omega^2)^m \\ &= (2+\omega)(4+4\omega-\omega-1)^m \\ &= (2+\omega)(3+3\omega)^m \\ &= (2+\omega)(3(1+\omega))^m \\ &= (2+\omega)(3(-\omega^2))^m \\ &= (2+\omega)(3(-\omega^2))^m \\ &= (2+\omega)\,3^m(-1)^m\omega^{2m}.\end{aligned}$$

Then $(2+\omega)^{2m+1} \sim (2+\omega)\,3^m$, so $\left\langle (2+\omega)^{2m+1} \right\rangle = \langle 2 \cdot 3^m + 3^m\omega \rangle$. By Theorem 2.1.8,

$$R_{2m+1} = \mathbb{Z}[\omega] / \langle 2 \cdot 3^m + 3^m\omega \rangle = \left\{ \; [a + b\omega] : 0 \leq a < 3^m \text{ and } 0 \leq b < 3^{m+1} \; \right\}.$$

Define $\phi : \mathbb{Z}[x] \to \mathbb{Z}[\omega] / \langle 2 \cdot 3^m + 3^m\omega \rangle$ by $\phi(f(x)) = [f(\omega - 1)]$. Let $[a + b\omega] \in \mathbb{Z}[\omega] / \langle 2 \cdot 3^m + 3^m\omega \rangle$, then $[a + b\omega] = [a + b(\omega - 1) + b] = \phi(a + bx + b)$. Thus ϕ is a surjective function. Next, let $f_1(x), f_2(x) \in \mathbb{Z}[x]$.

$$\begin{aligned}\phi(f_1(x) + f_2(x)) &= [f_1(\omega-1) + f_2(\omega-1)] \\ &= [f_1(\omega-1)] + [f_2(\omega-1)] \\ &= \phi(f_1(x)) + \phi(f_2(x)), \text{ and} \\ \phi(f_1(x) \cdot f_2(x)) &= [f_1(\omega-1) \cdot f_2(\omega-1)] \\ &= [f_1(\omega-1)] \cdot [f_2(\omega-1)] \\ &= \phi(f_1(x)) \cdot \phi(f_2(x)).\end{aligned}$$

Hence ϕ is a surjective ring homomorphism.

We will show that $\ker\phi = \langle 3^m x, 3^{m+1}, x^2+3x+3\rangle$. Since

$$\begin{aligned}
\phi\left(3^m x\right) &= \left[3^m\left(\omega-1\right)\right] \\
&= \left[\omega\left(2\cdot 3^m + 3^m\omega\right)\right] \\
&= [0], \\
\phi\left(3^{m+1}\right) &= \left[3^{m+1}\right] \\
&= \left[3^m\left(2+\omega\right)\left(2+\overline{\omega}\right)\right] \\
&= \left[\left(2\cdot 3^m + 3^m\omega\right)\left(2+\overline{\omega}\right)\right] \\
&= [0] \text{ and} \\
\phi\left(x^2+3x+3\right) &= \left[(\omega-1)^2 + 3(\omega-1)+3\right] \\
&= \left[\omega^2+\omega+1\right] \\
&= [0],
\end{aligned}$$

$\langle 3^m x, 3^{m+1}, x^2+3x+3\rangle \subseteq \ker\phi$. Let $p\left(x\right) \in \ker\phi$. Since x^2+3x+3 is monic, $p\left(x\right) = \left(x^2+3x+3\right)q\left(x\right) + r\left(x\right)$ for some $q\left(x\right)$ and $r\left(x\right) = r_0 + r_1\left(x+1\right)$ in $\mathbb{Z}\left[x\right]$. Hence $r\left(x\right) \in \ker\phi$, i.e. $\left[r_0 + r_1\omega\right] = [0]$, so $r_0 + r_1\omega \in \langle 2\cdot 3^m + 3^m\omega\rangle$. Therefore $r_0 + r_1\omega = \left(u+v\omega\right)\left(2\cdot 3^m + 3^m\omega\right) = \left(2\cdot 3^m u - 3^m v\right) + \left(3^m v + 3^m u\right)\omega$ for some $u + v\omega \in \mathbb{Z}\left[\omega\right]$. Then $r\left(x\right) = r_0 + r_1\left(x+1\right) = \left(2\cdot 3^m u - 3^m v\right) + \left(3^m v + 3^m u\right)\left(x+1\right) = 3^{m+1}u + 3^m\left(u+v\right)x$. Thus $p\left(x\right) = \left(x^2+3x+3\right)q\left(x\right) + 3^{m+1}u + 3^m\left(u+v\right)x \in \langle 3^m x, 3^{m+1}, x^2+3x+3\rangle$. Then $\ker\phi \subseteq \left\langle 3^m x, 3^{m+1}, x^2+3x+3\right\rangle$, Hence $\ker\phi = \langle 3^m x, 3^{m+1}, x^2+3x+3\rangle$. Then $R_{2m+1} \cong \mathbb{Z}\left[x\right] / \left\langle 3^m x, 3^{m+1}, x^2+3x+3\right\rangle$.

□

Example 2.1.10.
$$\begin{aligned}
88 + 110\omega &= 22(4+5\omega) \\
&= 22(6+7\omega+2(-\omega-1)) \\
&= 22(6+7\omega+2\omega^2) \\
&= 2\cdot 11(3+2\omega)(2+\omega).
\end{aligned}$$

We have $N(3+2\omega) = 7 \equiv 1(\text{mod } 6)$ and $11 \equiv 5(\text{mod } 6)$.

Thus
$$\begin{aligned}
\mathbb{Z}\left[\omega\right] / \left\langle 88+110\omega\right\rangle &= \mathbb{Z}\left[\omega\right] / \left\langle 2\cdot 11(3+2\omega)(2+\omega)\right\rangle \\
&\cong \mathbb{Z}_7 \oplus \mathbb{Z}_{22}\left[\omega\right] \oplus \mathbb{Z}\left[\omega\right] / \left\langle 2+\omega\right\rangle \\
&\cong \mathbb{Z}_7 \oplus \mathbb{Z}_{22}\left[\omega\right] \oplus \mathbb{Z}\left[\omega\right] / \langle x, 3, x^2+3x+3\rangle.
\end{aligned}$$

□

2.2 The Euler $\phi-$function for Eisenstein Integers.

In this section we will consider the Euler $\phi-$function over the ring of Eisenstein integers. For $\beta \in \mathbb{Z}[\omega]$, we denote the set of all units of the quotient ring $\mathbb{Z}[\omega] / \langle \beta \rangle$ by $\Phi_{\mathbb{Z}[\omega]}(\beta)$ which forms a multiplicative group. We denote Euler $\phi-$function of β over $\mathbb{Z}[\omega]$ by $\phi_{\mathbb{Z}[\omega]}(\beta)$ which is the order of the group $\Phi_{\mathbb{Z}[\omega]}(\beta)$. In this section, we denote the types of irreducible elements in $\mathbb{Z}[\omega]$ as in Theorem 2.1.7 and $N(\sigma) = q$ where σ as in (i).

Lemma 2.2.1. *The equivalence classes of* $\mathbb{Z}[\omega]$ *modulo a power of an irreducible element are given as follows:*
(i) $\mathbb{Z}[\omega] / \langle \sigma^n \rangle = \{[x] : 0 \leq x < q^n\}$,
(ii) $\mathbb{Z}[\omega] / \langle \pi^n \rangle = \{[x + y\omega] : 0 \leq x, y < \pi^n\}$,
(iii) $\mathbb{Z}[\omega] / \langle (2+\omega)^{2m} \rangle = \{[x + y\omega] : 0 \leq x, y < 3^m\}$,
(iv) $\mathbb{Z}[\omega] / \langle (2+\omega)^{2m+1} \rangle = \{[x + y\omega] : 0 \leq x < 3^m, 0 \leq y < 3^{m+1}\}$,
(v) $\mathbb{Z}[\omega] / \langle 2^n \rangle = \{[x + y\omega] : 0 \leq x, y < 2^n\}$.

Proof. (i) Let $0 \leq x, y < q^n$ be such that $[x]_{\langle \sigma^n \rangle} = [y]_{\langle \sigma^n \rangle}$. Then $x - y \in \langle \sigma^n \rangle$, so $\sigma^n \,|x-y$ and $\overline{\sigma}^n \,|x-y$. Since σ^n and $\overline{\sigma}^n$ are not associated and $q^n = N(\sigma^n) = \sigma^n \overline{\sigma}^n$, $q^n \,|x-y$. Thus $x = y$. Next, let $\sigma^n = u - v\omega$ where $u, v \in \mathbb{Z}$, so that $v\omega \equiv u(\text{mod } \langle \sigma^n \rangle)$. Suppose that $(q, v) \neq 1$, then $q\,|v$. Then $\sigma\overline{\sigma}\,|v$, so $\sigma\,|v$. Since $v\omega \equiv u(\text{mod } \langle \sigma^n \rangle)$, $\sigma\,|u$. Thus $\overline{\sigma}\,|u$. Since $(\sigma, \overline{\sigma}) = 1$, $\sigma\overline{\sigma}\,|u$, i.e. $q\,|u$. Hence $q\,|v$ and $q\,|u$, then $q\,|\sigma^n$. It contradicts $q = \sigma\overline{\sigma} \nmid \sigma^n$. Therefore $(q, v) = 1$, and so $(q^n, v) = 1$. Then there is $r \in \mathbb{Z}$ such that $rv \equiv 1(\text{mod } q^n)$, then $rv \equiv 1(\text{mod } \langle \sigma^n \rangle)$. Thus $rv\omega \equiv ru(\text{mod } \langle \sigma^n \rangle)$ and so $\omega \equiv ru(\text{mod } \langle \sigma^n \rangle)$. Since $q^n \equiv 0(\text{mod } \langle \sigma^n \rangle)$, for any $a, b \in \mathbb{Z}$, $[a + b\omega]_{\langle \sigma^n \rangle} = [a + bru]_{\langle \sigma^n \rangle} = [x]_{\langle \sigma^n \rangle}$ where $0 \leq x < q^n$ is the remainder when dividing $a + bru$ by q^n. Thus $\mathbb{Z}[\omega] / \langle \sigma^n \rangle = \{[x] : 0 \leq x < q^n\}$. By Theorem 2.1.8, $\mathbb{Z}[\omega] / \langle ak + bk\omega \rangle = \{[x + y\omega] : 0 \leq x < k, 0 \leq y < k(a^2 - ab + b^2)\}$ where $(a, b) = 1$. Thus

$$\mathbb{Z}[\omega] / \langle \pi^n \rangle = \{[x + y\omega] : 0 \leq x, y < \pi^n\}.$$

From the proof of Theorem 2.1.9, we have $\langle (2+\omega)^{2m} \rangle = \langle (-3\omega^2)^m \rangle = \langle 3^m \rangle$ and

$\langle (2+\omega)^{2m+1}\rangle = \langle 3^m(2+\omega)\rangle = \langle 2\cdot 3^m + 3^m\omega\rangle$, so

$$\mathbb{Z}[\omega]\,/\,\langle (2+\omega)^{2m}\rangle = \{[x+y\omega] : 0 \le x, y < 3^m\}, \text{ and}$$

$$\mathbb{Z}[\omega]\,/\,\langle (2+\omega)^{2m+1}\rangle = \{[x+y\omega] : 0 \le x < 3^m, 0 \le y < 3^{m+1}\}.$$

Finally, $\mathbb{Z}[\omega]\,/\,\langle 2^n\rangle = \{[x+y\omega] : 0 \le x, y < 2^n\}$. □

Lemma 2.2.1 implies that $\mathbb{Z}[\omega]\,/\,\langle \sigma^n\rangle$ has q^n elements, $\mathbb{Z}[\omega]\,/\,\langle \pi^n\rangle$ has π^{2n} elements, $\mathbb{Z}[\omega]\,/\,\langle (2+\omega)^n\rangle$ has 3^n elements, and $\mathbb{Z}[\omega]\,/\,\langle 2^n\rangle$ has 2^{2n} elements. Now we are ready to identify the unit group of these quotient rings.

Theorem 2.2.2. (i) $\Phi_{\mathbb{Z}[\omega]}(\sigma^n) = \{[x] : 0 \le x < q^n \textit{ and } (q,x) = 1\}$,

(ii) $\Phi_{\mathbb{Z}[\omega]}(\pi^n) = \{[x+y\omega] : 0 \le x, y < \pi^n \textit{ and } (\pi,x) = 1 \textit{ or } (\pi,y) = 1\}$,

(iii) $\Phi_{\mathbb{Z}[\omega]}((2+\omega)^{2m}) = \{[x+y\omega] : 0 \le x, y < 3^m \textit{ and } 3 \nmid (x-y)\}$,

(iv) $\Phi_{\mathbb{Z}[\omega]}((2+\omega)^{2m+1}) = \{[x+y\omega] : 0 \le x < 3^m, 0 \le y < 3^{m+1} \textit{ and } 3 \nmid (x-y)\}$,

(v) $\Phi_{\mathbb{Z}[\omega]}(2^n) = \{[x+y\omega] : 0 \le x, y < 2^n \textit{ and } (2,x) = 1 \textit{ or } (2,y) = 1\}$.

Proof. Let $\alpha, \beta \in \mathbb{Z}[\omega]$. Then $[\alpha]$ is a unit in $\mathbb{Z}[\omega]\,/\,\langle\beta\rangle$ if and only if $[\alpha][\gamma] = [1]$ in $\mathbb{Z}[\omega]\,/\,\langle\beta\rangle$, for some $\gamma \in \mathbb{Z}[\omega]$. Then $[\alpha]$ is a unit in $\mathbb{Z}[\omega]\,/\,\langle\beta\rangle$ if and only if $\alpha\gamma \equiv 1 (\text{mod } \beta)$ if and only if $\beta\delta + \alpha\gamma = 1$ for some $\delta \in \mathbb{Z}[\omega]$ if and only if $(\alpha,\beta) = 1$.

(i) Let $x \in \mathbb{Z}$ such that $0 \le x < q^n$. Then

$x = \bar{x}$ and so $[x]_{\langle\sigma^n\rangle} \in \Phi_{\mathbb{Z}[\omega]}(\sigma^n)$ if and only if $(x, \sigma^n) = 1$

if and only if $\sigma \nmid x$

if and only if $\sigma \nmid x$ and $\bar{\sigma} \nmid x$

if and only if $\sigma\bar{\sigma} \nmid x$

if and only if $q \nmid x$

if and only if $(q,x) = 1$.

Thus $\Phi_{\mathbb{Z}[\omega]}(\sigma^n) = \{[x] : 0 \le x < q^n \text{ and } (q,x) = 1\}$.

(ii) Let $x, y \in \mathbb{Z}$ such that $0 \le x < \pi^n$. Then

$[x+y\omega]_{\langle\pi^n\rangle} \in \Phi_{\mathbb{Z}[\omega]}(\pi^n)$ if and only if $(x+y\omega, \pi^n) = 1$

if and only if $\pi \nmid x + y\omega$

if and only if $\pi \nmid x$ or $\pi \nmid y$

$$\text{if and only if } (\pi, x) = 1 \text{ or } (\pi, y) = 1.$$

Thus $\Phi_{\mathbb{Z}[\omega]}(\pi^n) = \{[x + y\omega] : 0 \leq x, y < \pi^n \text{ and } (\pi, x) = 1 \text{ or } (\pi, y) = 1\}$.

(iii),(iv) Consider $(x + y\omega, (2 + \omega)^n) = 1$ if and only if $2 + \omega \nmid x + y\omega$. By Lemma 2.1.1, $2 + \omega \nmid x + y\omega$ if and only if $3 \nmid (x - y)$. Thus

$$\Phi_{\mathbb{Z}[\omega]}((2 + \omega)^{2m}) = \{[x + y\omega] : 0 \leq x, y < 3^m \text{ and } 3 \nmid (x - y)\} \text{ and}$$

$$\Phi_{\mathbb{Z}[\omega]}((2 + \omega)^{2m+1}) = \{[x + y\omega] : 0 \leq x < 3^m, 0 \leq y < 3^{m+1} \text{ and } 3 \nmid (x - y)\}.$$

(v) Let $[x + y\omega]_{\langle 2^n \rangle} \in \mathbb{Z}[\omega] / \langle 2^n \rangle$. We have $[x + y\omega]_{\langle 2^n \rangle} \in \Phi_{\mathbb{Z}[\omega]}(2^n)$ if and only if $(x + y\omega, 2^n) = 1$ if and only if $2 \nmid x + y\omega$ if and only if $(2, x) = 1$ or $(2, y) = 1$. Thus

$$\Phi_{\mathbb{Z}[\omega]}(2^n) = \{[x + y\omega] : 0 \leq x, y < 2^n \text{ and } (2, x) = 1 \text{ or } (2, y) = 1\}. \qquad \square$$

Remark By Theorem 2.2.2, $\phi_{\mathbb{Z}[\omega]}(\sigma^n) = q^n - q^{n-1}$, $\phi_{\mathbb{Z}[\omega]}(\pi^n) = \pi^{2n-2}(\pi^2 - 1)$, $\phi_{\mathbb{Z}[\omega]}((2 + \omega)^{2m}) = 2 \cdot 3^{2m-1}$, $\phi_{\mathbb{Z}[\omega]}((2 + \omega)^{2m+1}) = 2 \cdot 3^{2m}$, $\phi_{\mathbb{Z}[\omega]}(2^n) = 3 \cdot 2^{2n-2}$.

Theorem 2.2.3. $\Phi_{\mathbb{Z}[\omega]}(\sigma^n) \cong \mathbb{Z}_{q^n - q^{n-1}}$.

Proof. By Theorem 2.2.2, $\Phi_{\mathbb{Z}[\omega]}(\sigma^n) = \{[x] : 0 \leq x < q^n, (q, x) = 1\}$. Then $[x]_{\langle \sigma^n \rangle} \in \Phi_{\mathbb{Z}[\omega]}(\sigma^n)$ if and only if $[x]_{q^n} \in \Phi_{\mathbb{Z}}(q^n)$. Define $f : \Phi_{\mathbb{Z}}(q^n) \to \Phi_{\mathbb{Z}[\omega]}(\sigma^n)$ by $f([x]_{q^n}) = [x]_{\langle \sigma^n \rangle}$. Let $[x_1]_{q^n}, [x_2]_{q^n} \in \Phi_{\mathbb{Z}}(q^n)$ be such that $[x_1]_{q^n} = [x_2]_{q^n}$. Then $x_1 \equiv x_2 (\text{mod } q^n)$, so $x_1 \equiv x_2 (\text{mod } \sigma^n)$. Therefore $[x_1]_{\langle \sigma^n \rangle} = [x_2]_{\langle \sigma^n \rangle}$. Thus f is a function. Clearly f is onto.

Let $[x_1]_{q^n}, [x_2]_{q^n} \in \Phi_{\mathbb{Z}}(q^n)$ such that $f([x_1]_{q^n}) = f([x_2]_{q^n})$, i.e. $[x_1]_{\langle \sigma^n \rangle} = [x_2]_{\langle \sigma^n \rangle}$. Thus $\sigma^n \,|x_1 - x_2$, so $\bar{\sigma}^n \,|x_1 - x_2$. Since $q^n = \sigma^n \bar{\sigma}^n$ and σ^n and $\bar{\sigma}^n$ are not associated, $q^n \,|x_1 - x_2$. Then $[x_1]_{q^n} = [x_2]_{q^n}$. Thus f is one to one function.

Let $[x_1]_{q^n}, [x_2]_{q^n} \in \Phi_{\mathbb{Z}}(q^n)$. Then $f([x_1]_{q^n}) + f([x_2]_{q^n}) = [x_1]_{\langle \sigma^n \rangle} + [x_2]_{\langle \sigma^n \rangle} = [x_1 + x_2]_{\langle \sigma^n \rangle} = f([x_1 + x_2]_{q^n}) = f([x_1]_{q^n} + [x_2]_{q^n})$. Next, $f([x_1]_{q^n}) \cdot f([x_2]_{q^n}) = [x_1]_{\langle \sigma^n \rangle} \cdot [x_2]_{\langle \sigma^n \rangle} = [x_1 \cdot x_2]_{\langle \sigma^n \rangle} = f([x_1 \cdot x_2]_{q^n}) = f([x_1]_{q^n} \cdot [x_2]_{q^n})$. Hence f is a ring isomorphism. The unit group of the ring $\mathbb{Z}_{q^n}$ is cyclic of order $q^n - q^{n-1}$, i.e. $\Phi_{\mathbb{Z}}(q^n) \cong \mathbb{Z}_{q^n - q^{n-1}} [5, pages\ 46 - 51](EthanD.Bolker, 1970)$. Thus $\Phi_{\mathbb{Z}[\omega]}(\sigma^n) \cong \mathbb{Z}_{q^n - q^{n-1}}$. $\square$

Lemma 2.2.4. (i) $(1+p\omega)^{p^k} \equiv 1+\omega p^{k+1} (\text{mod } p^{k+2})$ *where p is an odd prime number.*

(ii) $(1+2\omega)^{2^k} \equiv 1+2^{k+1} (\text{mod } 2^{k+2})$.

(iii) $(1+4\omega)^{2^k} \equiv 1+\omega 2^{k+2} (\text{mod } 2^{k+3})$.

Proof. Let $\beta \in \mathbb{Z}[\omega]$, r be a prime integer and k be a positive integer. Define $\rho = (1+\beta r)^{r^k}$. Then

$\rho = 1 + r^k\beta r + \frac{r^k(r^k-1)}{2}(\beta r)^2 + \frac{r^k(r^k-1)(r^k-2)}{6}(\beta r)^3 + \frac{r^k(r^k-1)(r^k-2)(r^k-3)}{24}(\beta r)^4 + ...$

Given $\beta = \omega$ and $r = p$, then

$2 \left| p^k - 1, \; 3 \right| p^k(p^k-1)(p^k-2), \; 4 \left| p^k(p^k-1)(p^k-2)(p^k-3) \right. ....$ Thus

$\rho = 1 + p^k\omega p + \frac{p^k(p^k-1)}{2}(\omega p)^2 + \frac{p^k(p^k-1)(p^k-2)}{6}(\omega p)^3 + \frac{p^k(p^k-1)(p^k-2)(p^k-3)}{24}(\omega p)^4 + ...$

$\rho = 1 + \omega p^{k+1} + \alpha p^{k+2}$ for some $\alpha \in \mathbb{Z}[\omega]$, so

$\rho \equiv 1 + \omega p^{k+1} (\text{mod } p^{k+2})$.

Hence $(1+p\omega)^{p^k} \equiv 1+\omega p^{k+1} (\text{mod } p^{k+2})$.

Given $\beta = \omega$ and $r = 2$ then

$2 \left| 2^k - 2, \; 3 \right| (2^k-1)(2^k-2), \; 4 \left| 2^k(2^k-1)(2^k-2)(2^k-3) \right., ...$ Thus

$\rho = 1 + 2^{k+1}\omega + \frac{2^k(2^k-1)}{2}(2\omega)^2 + \frac{2^k(2^k-1)(2^k-2)}{6}(2\omega)^3 + \frac{2^k(2^k-1)(2^k-2)(2^k-3)}{24}(2\omega)^4 + ...$

$\rho = 1 + \omega 2^{k+1} + \frac{2^k(2^k-1)}{2}(2\omega)^2 + \frac{2^k(2^k-1)(2^k-2)}{6}(2\omega)^3 + \alpha 2^{k+2}$ for some $\alpha \in \mathbb{Z}[\omega]$.

$$\begin{aligned}
\text{Then } \rho &\equiv 1 + \omega 2^{k+1} + \omega^2(2^k-1)2^{k+1} (\text{mod } 2^{k+2}) \\
&\equiv 1 + \omega 2^{k+1} + (-\omega-1)(2^k-1)2^{k+1} (\text{mod } 2^{k+2}) \\
&\equiv 1 + \omega 2^{k+1} - \omega(2^k-1)2^{k+1} - (2^k-1)2^{k+1} (\text{mod } 2^{k+2}) \\
&\equiv 1 + \omega 2^{k+1} - \omega 2^{2k+1} + \omega 2^{k+1} - 2^{2k+1} + 2^{k+1} (\text{mod } 2^{k+2}) \\
&\equiv 1 + \omega 2^{k+2} + 2^{k+1} (\text{mod } 2^{k+2}).
\end{aligned}$$

Hence $(1+2\omega)^{2^k} \equiv 1 + 2^{k+1} (\text{mod } 2^{k+2})$.

Given $\beta = 2\omega$ and $r = 2$ then

$\rho = 1 + 2^{k+2}\omega + \frac{2^k(2^k-1)}{2}(4\omega)^2 + \frac{2^k(2^k-1)(2^k-2)}{6}(4\omega)^3 + \frac{2^k(2^k-1)(2^k-2)(2^k-3)}{24}(4\omega)^4 + ...$

$\rho = 1 + 2^{k+2}\omega + 2^{k+3}(2^k-1)\omega^2 + \frac{(2^k-1)(2^k-2)}{3}2^{k+5}\omega^3 + ...$

$\rho \equiv 1 + 2^{k+2}\omega (\text{mod } 2^{k+3})$.

Hence $(1+4\omega)^{2^k} \equiv 1 + 2^{k+2}\omega (\text{mod } 2^{k+3})$. □

Lemma 2.2.5. (i) *The order of $[1+p\omega]$ in $\Phi_{\mathbb{Z}[\omega]}(p^n)$ is p^{n-1}, where p is an odd* *prime number.*

(ii) *The order of* $[1+2\omega]$ *in* $\Phi_{\mathbb{Z}[\omega]}(2^n)$ *is* 2^{n-1}.

(iii) *The order of* $[1+3\omega]$ *in* $\Phi_{\mathbb{Z}[\omega]}((2+\omega)^{2m})$ *is* 3^{m-1}.

(iv) *The order of* $[1+3\omega]$ *in* $\Phi_{\mathbb{Z}[\omega]}((2+\omega)^{2m+1})$ *is* 3^m.

(v) *The order of* $[1+4\omega]$ *in* $\Phi_{\mathbb{Z}[\omega]}(2^n)$ *is* 2^{n-2}.

Proof. (i) Given $k=n-1$ and $k=n-2$ in Lemma 2.2.4 (i). Then

$$\begin{aligned}(1+p\omega)^{p^{n-1}} &\equiv 1+\omega p^n (\text{mod } \langle p^{n+1}\rangle)\\ &\equiv 1 (\text{mod } \langle p^n\rangle),\\ (1+p\omega)^{p^{n-2}} &\equiv 1+\omega p^{n-1} \equiv 1(\text{mod } \langle p^n\rangle).\end{aligned}$$

Thus the order of $[1+p\omega]$ in $\Phi_{\mathbb{Z}[\omega]}(p^n)$ is p^{n-1}.

(ii) Given $k=n-1$ and $k=n-2$ in Lemma 2.2.4 (ii). Then

$$\begin{aligned}(1+2\omega)^{2^{n-1}} &\equiv 1+2^n (\text{mod } \langle 2^{n+1}\rangle)\\ &\equiv 1 (\text{mod } \langle 2^n\rangle),\\ (1+2\omega)^{2^{n-2}} &\equiv 1+2^{n-1} \equiv 1(\text{mod } \langle 2^n\rangle).\end{aligned}$$

Thus the order of $[1+2\omega]$ in $\Phi_{\mathbb{Z}[\omega]}(2^n)$ is 2^{n-1}.

(iii) Given $k=m-1$ and $k=m-2$ in Lemma 2.2.4 (i). Then

$$\begin{aligned}(1+3\omega)^{3^{m-1}} &\equiv 1+\omega 3^m (\text{mod } \langle 3^{m+1}\rangle)\\ &\equiv 1 (\text{mod } \langle 3^m\rangle),\\ (1+3\omega)^{3^{m-2}} &\equiv 1+\omega 3^{m-1} \equiv 1(\text{mod } \langle 3^m\rangle).\end{aligned}$$

Thus the order of $[1+3\omega]$ in $\Phi_{\mathbb{Z}[\omega]}((2+\omega)^{2m})$ is 3^{m-1}.

(iv) Let $\alpha = 2+\omega$. Then $\alpha^2 = -3\omega^2$ and $\alpha^{2m+1} = (-3\omega^2)^m(2+\omega)$, so $\langle \alpha^{2m+1}\rangle = \langle 3^m\alpha\rangle$. Since $3^{m+1} = 3^m\cdot 3 = 3^m(-\alpha^2\omega^{-2})$, $3^{m+2} = 3^{m+1}(-\alpha^2\omega^{-2})$, $\langle 3^{m+2}\rangle = \langle 3^{m+1}\alpha^2\rangle$.

Given $k=m$ and $k=m-1$ in Lemma 2.2.4 (i). Then

$$\begin{aligned}(1+3\omega)^{3^m} &\equiv 1+\omega 3^{m+1} (\text{mod } \langle 3^{m+2}\rangle)\\ &\equiv 1+\omega 3^m(-\alpha^2\omega^{-2}) (\text{mod } \langle 3^{m+2}\rangle)\\ &\equiv 1+\omega 3^m(-\alpha^2\omega^{-2}) (\text{mod } \langle 3^{m+1}\alpha^2\rangle)\\ &\equiv 1+\omega 3^m(-\alpha^2\omega^{-2}) (\text{mod } \langle 3^{m+1}\alpha\rangle)\\ &\equiv 1 (\text{mod } \langle 3^m\alpha\rangle).\end{aligned}$$

Then $(1+3\omega)^{3^m} \equiv 1(\text{mod } \langle \alpha^{2m+1} \rangle)$,

$$\begin{aligned}(1+3\omega)^{3^{m-1}} &\equiv 1+\omega 3^m(\text{mod } \langle 3^{m+1} \rangle)\\ &\equiv 1+\omega 3^m(\text{mod } \langle 3^m\alpha^2 \rangle)\\ &\equiv 1(\text{mod } \langle 3^m\alpha \rangle).\end{aligned}$$

Then $(1+3\omega)^{3^{m-1}} \equiv 1(\text{mod } \langle \alpha^{2m+1} \rangle)$.

Thus the order of $[1+3\omega]$ in $\Phi_{\mathbb{Z}[\omega]}(\alpha^{2m+1})$ is 3^m.

(v) Given $k = n-2$ and $k = n-3$ in Lemma 2.2.4 (iii). Then

$$\begin{aligned}(1+4\omega)^{2^{n-2}} &\equiv 1+2^n\omega(\text{mod } \langle 2^{n+1} \rangle)\\ &\equiv 1(\text{mod } \langle 2^n \rangle),\\ (1+4\omega)^{2^{n-3}} &\equiv 1+2^{n-1}\omega(\text{mod } \langle 2^n \rangle)\\ &\equiv 1(\text{mod } \langle 2^n \rangle).\end{aligned}$$

Thus the order of $[1+4\omega]$ in $\Phi_{\mathbb{Z}[\omega]}(2^n)$ is 2^{n-2}. □

Lemma 2.2.6. (i) *In* $\Phi_{\mathbb{Z}[\omega]}(2^n)$, $[1+4\omega]^k_{\langle 2^n \rangle} \neq [x]_{\langle 2^n \rangle}, [x\omega]_{\langle 2^n \rangle}$ *and* $[x\omega^2]_{\langle 2^n \rangle}$ *for all* $x \in \mathbb{Z}$.

(ii) *In* $\Phi_{\mathbb{Z}[\omega]}((2+\omega)^n)$, $[1+3\omega]^k_{\langle (2+\omega)^n \rangle} \neq [x]_{\langle (2+\omega)^n \rangle}, [x\omega]_{\langle (2+\omega)^n \rangle}$ *and* $[x\omega^2]_{\langle (2+\omega)^n \rangle}$ *for all* $x \in \mathbb{Z}$.

(iii) *In* $\Phi_{\mathbb{Z}[\omega]}(\pi^n)$, $[1+\pi\omega]^k_{\langle \pi^n \rangle} \neq [x]_{\langle \pi^n \rangle}, [x\omega]_{\langle \pi^n \rangle}$ *and* $[x\omega^2]_{\langle \pi^n \rangle}$ *for all* $x \in \mathbb{Z}$.

Proof. Let $c \in \mathbb{Z}[\omega]$ be called *special* if $[c]_{\langle 2^n \rangle} = [x]_{\langle 2^n \rangle}, [x\omega]_{\langle 2^n \rangle}$ or $[x\omega^2]_{\langle 2^n \rangle}$ for some $x \in \mathbb{Z}$. Let B denote the set of all b such that $(1+4\omega)^b \equiv c(\text{mod } 2^n)$ where $0 < b < 2^{n-2}$. Note that if $b \in B$, then $bt \in B$ for all $t \in \mathbb{Z}^+$. First, we show that $2^{n-3} \notin B$. Put $k = n-3$ in Lemma 2.2.4 (iii), we have $(1+4\omega)^{2^{n-3}} \equiv 1+2^{n-1}\omega(\text{mod } 2^n)$. Then $c \equiv 1+2^{n-1}\omega(\text{mod } 2^n)$, so $1+2^{n-1}\omega - c \equiv 0(\text{mod } 2^n)$. If $c = x \in \mathbb{Z}$, then $2^n \mid 2^{n-1}$, a contradiction. If $c = x\omega$, then $2^n \mid 1$, a contradiction. If $c = x\omega^2$, then

$$\begin{aligned}1+2^{n-1}\omega - x\omega^2 &\equiv 1+2^{n-1}\omega + x(\omega+1)(\text{mod } 2^n)\\ &\equiv (x+1)+(2^{n-1}+x)\omega(\text{mod } 2^n), \text{ so}\end{aligned}$$

$2^n \mid 2^{n-1}+x$ and $2^n \mid 1+x$. Thus $x = k2^n - 1$ for some $k \in \mathbb{Z}$, so $2^n \mid 2^{n-1}+k2^n-1$, $2^n \mid 2^{n-1}-1$, a contradiction. Then $2^{n-3} \notin B$. Let $L \in B$ be the least element. Dividing 2^{n-2} by L we have $2^{n-2} = Ld + r$ where $0 \leq r < L$. If $r = 0$, then

$L = 2^t$ for some t such that $0 < t < n-3$. Then $[1+4\omega]_{\langle 2^n\rangle}^{2^{n-3}} = [1+4\omega]_{\langle 2^n\rangle}^{L2^{n-3-t}}$. Since $L \in B, 2^{n-3} \in B$, it is an impossible. Then $r \neq 0$. Since the order of $[1+4\omega]_{\langle 2^n\rangle}$ in $\Phi_{\mathbb{Z}[\omega]}(2^n)$ is 2^{n-2}, $[1]_{\langle 2^n\rangle} = [1+4\omega]_{\langle 2^n\rangle}^{Ld+r} = [1+4\omega]_{\langle 2^n\rangle}^{Ld}[1+4\omega]_{\langle 2^n\rangle}^{r} = [s]_{\langle 2^n\rangle}[1+4\omega]_{\langle 2^n\rangle}^{r}$ some *special* s. Let $s = x, x\omega$ or $x\omega^2$ for some $x \in \mathbb{Z}$. Since $[s] \in \Phi_{\mathbb{Z}[\omega]}(2^n)$, x is odd. Then there is $y \in \mathbb{Z}$ such that $[yx]_{2^n} = [1]_{2^n}$ in $\Phi_{\mathbb{Z}}(2^n)$. Thus $[yx]_{\langle 2^n\rangle} = [1]_{\langle 2^n\rangle}$ in $\Phi_{\mathbb{Z}[\omega]}(2^n)$. Then $[y]_{\langle 2^n\rangle} = [ys]_{\langle 2^n\rangle}[1+4\omega]_{\langle 2^n\rangle}^{r}$ in $\Phi_{\mathbb{Z}[\omega]}(2^n)$. Since $s = x, x\omega$ or $x\omega^2$ for some $x \in \mathbb{Z}, r \in B$. But $r < L$, a contradiction. Thus $[1+4\omega]_{\langle 2^n\rangle}^{k} \neq [x]_{\langle 2^n\rangle}, [x\omega]_{\langle 2^n\rangle}$ and $[x\omega^2]_{\langle 2^n\rangle}$ for all $x \in \mathbb{Z}$. In the same way, $[1+3\omega]_{\langle (2+\omega)^n\rangle}^{k} \neq [x]_{\langle (2+\omega)^n\rangle}, [x\omega]_{\langle (2+\omega)^n\rangle}$ and $[x\omega^2]_{\langle (2+\omega)^n\rangle}$ for all $x \in \mathbb{Z}$ and $[1+\pi\omega]_{\langle \pi^n\rangle}^{k} \neq [x]_{\langle \pi^n\rangle}, [x\omega]_{\langle \pi^n\rangle}$ and $[x\omega^2]_{\langle \pi^n\rangle}$ for all $x \in \mathbb{Z}$. □

Next, we will consider the structure of $\Phi_{\mathbb{Z}[\omega]}(\pi^n), \Phi_{\mathbb{Z}[\omega]}((2+\omega)^n)$ and $\Phi_{\mathbb{Z}[\omega]}(2^m)$.

Theorem 2.2.7. $\Phi_{\mathbb{Z}[\omega]}(\pi^n) \cong \mathbb{Z}_{\pi^{n-1}} \times \mathbb{Z}_{\pi^{n-1}} \times \mathbb{Z}_{\pi^2-1}$.

Proof. Let H be generated by $[1+\pi\omega]_{\langle \pi^n\rangle}$. Then the order of H is π^{n-1}.
Define $f : \Phi_{\mathbb{Z}}(\pi^n) \to \Phi_{\mathbb{Z}[\omega]}(\pi^n)$ by $f([x]_{\pi^n}) = [x]_{\langle \pi^n\rangle}$. Since $\Phi_{\mathbb{Z}}(\pi^n)$ is cyclic and $\phi_{\mathbb{Z}}(\pi^n) = \pi^{n-1}(\pi-1)$, there is some $[a]_{\pi^n}$ in $\Phi_{\mathbb{Z}}(\pi^n)$ which has order π^{n-1}. Then $f([a]_{\pi^n}) = [a]_{\langle \pi^n\rangle} \in \Phi_{\mathbb{Z}[\omega]}(\pi^n)$ has order π^{n-1}. Let $K = \left\langle [a]_{\langle \pi^n\rangle} \right\rangle$. Then the order of K is π^{n-1}. By Lemma 2.2.6, $H \cap K = \{[1]\}$. Next, since π is prime in $\mathbb{Z}[\omega], \mathbb{Z}[\omega]/\langle \pi\rangle$ is a field and $\Phi_{\mathbb{Z}[\omega]}(\pi)$ is cyclic order π^2-1. Given $\Phi_{\mathbb{Z}[\omega]}(\pi) = \left\langle [\beta]_{\langle \pi^n\rangle} \right\rangle$. Then $\beta^{\pi^2-1} \equiv 1 (\mathrm{mod}\ \pi)$ in $\mathbb{Z}[\omega]$ and $\beta^{\pi^2-1} = 1+\gamma\pi$ for some $\gamma \in \mathbb{Z}[\omega]$. Then $(\beta^{\pi^2-1})^{\pi^{n-1}} = (1+\gamma\pi)^{\pi^{n-1}} \equiv 1(\mathrm{mod}\ \pi^n)$ and $(\beta^{\pi^{n-1}})^{\pi^2-1} \equiv 1(\mathrm{mod}\ \pi^n)$ in $\mathbb{Z}[\omega]$. Since the order of $[\beta]_{\langle \pi^n\rangle} \in \Phi_{\mathbb{Z}[\omega]}(\pi)$ is π^2-1 and $(\pi^{n-1}, \pi^2-1) = 1$, the order of $[\beta^{\pi^{n-1}}]_{\langle \pi^n\rangle} \in \Phi_{\mathbb{Z}[\omega]}(\pi^n)$ is π^2-1. Set $R = \left\langle [\beta^{\pi^{n-1}}]_{\langle \pi^n\rangle} \right\rangle$. Then the order of R is π^2-1. Now since every member of HK has order a power of π, $HK \cap R = \{[1]\}$, and the order of HKR is $\pi^{n-1}\pi^{n-1}(\pi^2-1) = \phi_{\mathbb{Z}[\omega]}(\pi^n)$. Thus

$$\Phi_{\mathbb{Z}[\omega]}(\pi^n) = HKR \cong \mathbb{Z}_{\pi^{n-1}} \times \mathbb{Z}_{\pi^{n-1}} \times \mathbb{Z}_{\pi^2-1}.$$

□

Theorem 2.2.8. (i) $\Phi_{\mathbb{Z}[\omega]}((2+\omega)^{2m}) \cong \mathbb{Z}_{3^{m-1}} \times \mathbb{Z}_{3^{m-1}} \times \mathbb{Z}_3 \times \mathbb{Z}_2$.
(ii) $\Phi_{\mathbb{Z}[\omega]}((2+\omega)^{2m+1}) \cong \mathbb{Z}_{3^m} \times \mathbb{Z}_{3^{m-1}} \times \mathbb{Z}_3 \times \mathbb{Z}_2$.

Proof. Let $\alpha = 2+\omega$.

(i) Define $\mu : \Phi_{\mathbb{Z}}\left(3^m\right) \to \Phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m}\right)$ by $\mu([a]_{3^m}) = [a]_{\langle\alpha^{2m}\rangle}$. Since $\Phi_{\mathbb{Z}}\left(3^m\right)$ is cyclic and $\phi_{\mathbb{Z}}\left(3^m\right) = 2\cdot 3^{m-1}$, there is some $[\beta]_{3^m} \in \Phi_{\mathbb{Z}}\left(3^m\right)$ has order 3^{m-1}.

Let $K = \left\langle [\beta]_{\langle\alpha^{2m}\rangle}\right\rangle$ in $\Phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m}\right), R = \left\langle [-1]_{\langle\alpha^{2m}\rangle}\right\rangle$ and $I = \left\langle [\omega]_{\langle\alpha^{2m}\rangle}\right\rangle$. Set $H = \left\langle [1+3\omega]_{\langle\alpha^{2m}\rangle}\right\rangle$. Then the order of H is 3^{m-1}. By Lemma 2.2.6, $H\cap K = \{[1]\}$ and the order of HK is 3^{2m-2}. Since every member of HK has order a power of 3, $HK\cap R = \{[1]\}$. By Lemma 2.2.6, $[\omega]_{\langle\alpha^{2m}\rangle} \notin H$. It is obvious that $[\omega]_{\langle\alpha^{2m}\rangle} \notin K\cup R$. Thus $HKR\cap I = \{[1]\}$. Since the order of $HKIR$ is $3^{m-1}\cdot\left(2\cdot 3^{m-1}\right)\cdot 3 = \phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m}\right)$, $\Phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m}\right) = HKIR$.

(ii) Define $\mu : \Phi_{\mathbb{Z}}\left(3^m\right) \to \Phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m+1}\right)$ by $\mu([a]_{3^m}) = [a]_{\langle\alpha^{2m+1}\rangle}$. Since $\Phi_{\mathbb{Z}}\left(3^m\right)$ is cyclic and $\phi_{\mathbb{Z}}\left(3^m\right) = 2\cdot 3^{m-1}$, there is some $[\beta]_{3^m} \in \Phi_{\mathbb{Z}}\left(3^m\right)$ has order 3^{m-1}. Let $K = \left\langle [\beta]_{\langle\alpha^{2m+1}\rangle}\right\rangle$ in $\Phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m+1}\right), R = \left\langle [-1]_{\langle\alpha^{2m+1}\rangle}\right\rangle$ and $I = \left\langle [\omega]_{\langle\alpha^{2m+1}\rangle}\right\rangle$. Set $H = \left\langle [1+3\omega]_{\langle\alpha^{2m+1}\rangle}\right\rangle$. Then the order of H is 3^m. By Lemma 2.2.6, $H\cap K = \{[1]\}$ and the order of HK is 3^{2m-1}. Since every member of HK has order a power of 3, $HK\cap R = \{[1]\}$. By Lemma 2.2.6, $[\omega]_{\langle\alpha^{2m+1}\rangle} \notin H$. It is obvious that $[\omega]_{\langle\alpha^{2m+1}\rangle} \notin K\cup R$. Thus $HKR\cap I = \{[1]\}$. Since the order of $HKIR$ is $3^m\cdot\left(2\cdot 3^{m-1}\right)\cdot 3 = \phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m+1}\right)$, $\Phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m+1}\right) = HKIR$. □

Theorem 2.2.9. $\Phi_{\mathbb{Z}[\omega]}\left(2^n\right) \cong \mathbb{Z}_{2^{n-1}}\times\mathbb{Z}_{2^{n-2}}\times\mathbb{Z}_3\times\mathbb{Z}_2$.

Proof. Let $H = \left\langle [1+2\omega]_{\langle 2^n\rangle}\right\rangle, K = \left\langle [1+4\omega]_{\langle 2^n\rangle}\right\rangle, I = \left\langle [\omega]_{\langle 2^n\rangle}\right\rangle$, and $R = \left\langle [-1]_{\langle 2^n\rangle}\right\rangle$. Then the order of H is 2^{n-1} and the order of K is 2^{n-2}.

(1) We will show that $H\cap K = \{[1]\}$. Suppose that $[1+4\omega]^{k_1}_{\langle 2^n\rangle} = [1+2\omega]^{k_2}_{\langle 2^n\rangle}$. By Lemma 2.2.6, since $(1+2\omega)^2 = -3$, k_2 is odd number. Then $([1+4\omega]^{k_1}_{\langle 2^n\rangle})^{2^{n-2}} = ([1+2\omega]^{k_2}_{\langle 2^n\rangle})^{2^{n-2}} = ([1+2\omega]^{2^{n-2}}_{\langle 2^n\rangle})^{k_2}$. Since $(1+2\omega)^{2^{n-2}} \equiv 1+2^{n-1}(\text{mod } 2^n)$, $(1+2\omega)^{2^{n-2}\cdot k_2} \equiv (1+2^{n-1})^{k_2}(\text{mod } 2^n)$. Thus $((1+4\omega)^{k_1})^{2^{n-2}} \equiv (1+2\omega)^{2^{n-2}\cdot k_2} \equiv (1+2^{n-1})^{k_2} \equiv 1+k_2 2^{n-1}(\text{mod } 2^n)$, it contradicts Lemma 2.2.5. Then $H\cap K = \{[1]\}$ and the order of HK is 2^{2n-3}. Since every member of HK has order a power of 2, $HK\cap I = \{[1]\}$.

(2) We will show that $[-1]_{\langle 2^n\rangle} \notin H\cup K\cup I$. By Lemma 2.2.6, we have $[-1]_{\langle 2^n\rangle} \notin K$. It is obvious that $[-1]_{\langle 2^n\rangle} \notin I$. Suppose that $[-1]_{\langle 2^n\rangle} = [1+2\omega]^{k}_{\langle 2^n\rangle}$for some $k\in\mathbb{Z}$.

Then $-1 \equiv (1+2\omega)^k(\text{mod } 2^n)$, $(-1)^2 \equiv (1+2\omega)^{2k}(\text{mod } 2^n)$, $1 \equiv (1+2\omega)^{2k}(\text{mod } 2^n)$. By Lemma 2.2.5, $2^{n-1} \,|2k$, so $2^{n-2}\,|k$. Then $k = t2^{n-2}$ for some $t \in \mathbb{Z}$. Thus $-1 \equiv (1+2\omega)^k \equiv (1+2\omega)^{t2^{n-2}} \equiv (1+2^{n-1})^t \equiv 1+t2^{n-1}+t\,(t-1)\,2^{2n-3}+...(\text{mod } 2^n)$. Then $0 \equiv 2\,(1+t2^{n-2})(\text{mod } 2^n)$, it is a contradiction. Hence $[-1]_{\langle 2^n \rangle} \notin H$, thus $HKI \cap R = \{[1]\}$. Since the order of $HKIR$ is $2^{n-1} \cdot 2^{n-2} \cdot 3 \cdot 2 = \phi_{\mathbb{Z}[\omega]}\,(2^n)$, $\Phi_{\mathbb{Z}[\omega]}\,(2^n) = HKIR \cong \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_3 \times \mathbb{Z}_2$. □

Theorem 2.2.10. *Let $\beta_1, \beta_2 \in \mathbb{Z}\,[\omega]$ with $(\beta_1, \beta_2) = 1$. Define $f : \Phi_{\mathbb{Z}[\omega]}\,(\beta_1) \times \Phi_{\mathbb{Z}[\omega]}\,(\beta_2) \to \mathbb{Z}\,[\omega]\,/\,\langle \beta_1\beta_2 \rangle$ by $f\,([\eta_1]\,,[\eta_2]) = [\eta]$, where $\eta \equiv \eta_i(mod\; \beta_i)$ for $i = 1, 2$. Then f is a ring monomorphism and $Imf = \Phi_{\mathbb{Z}[\omega]}\,(\beta_1\beta_2)$.*

Proof. Let $\beta_1, \beta_2 \in \mathbb{Z}\,[\omega]$ with $(\beta_1, \beta_2) = 1$.

Define $f : \Phi_{\mathbb{Z}[\omega]}\,(\beta_1) \times \Phi_{\mathbb{Z}[\omega]}\,(\beta_2) \to \mathbb{Z}\,[\omega]\,/\,\langle \beta_1\beta_2 \rangle$ by $f\,([\eta_1]\,,[\eta_2]) = [\eta]$, where $\eta \equiv \eta_i(\text{mod } \beta_i)$ for $i = 1, 2$. Let $([\mu_1]\,,[\mu_2])\,,([\theta_1]\,,[\theta_2]) \in \Phi_{\mathbb{Z}[\omega]}\,(\beta_1) \times \Phi_{\mathbb{Z}[\omega]}\,(\beta_2)$ and $([\mu_1]\,,[\mu_2]) = ([\theta_1]\,,[\theta_2])$. Then $\mu_i \equiv \theta_i(\text{mod } \beta_i)$ for $i = 1, 2$. The Chinese Remainder Theorem implies that there is a unique λ such that $\lambda \equiv \mu_i \equiv \theta_i(\text{mod } \beta_i)$ for $i = 1, 2$. Thus $f\,([\mu_1]\,,[\mu_2]) = f\,([\theta_1]\,,[\theta_2])$, f is a function. For $i = 1, 2$, if $\eta \equiv \eta_i(\text{mod } \beta_i)$ where $\eta_i \in \Phi_{\mathbb{Z}[\omega]}\,(\beta_i)$ and $(\eta_i, \beta_i) = 1$, then $(\eta, \beta_i) = 1$, thus $(\eta, \beta_1\beta_2) = 1$. Thus $Imf = \Phi_{\mathbb{Z}[\omega]}\,(\beta_1\beta_2)$, and we have $\ker f = \{0\}$.

Let $([\mu_1]\,,[\mu_2])\,,([\theta_1]\,,[\theta_2]) \in \Phi_{\mathbb{Z}[\omega]}\,(\beta_1) \times \Phi_{\mathbb{Z}[\omega]}\,(\beta_2)$, then $f\,([\mu_1]\,,[\mu_2]) + f\,([\theta_1]\,,[\theta_2]) = \mu + \theta$ where $\mu \equiv \mu_i(\text{mod } \beta_i)$ and $\theta \equiv \theta_i(\text{mod } \beta_i)$ for $i = 1, 2$. Thus $\mu + \theta \equiv \mu_i + \theta_i(\text{mod } \beta_i)$ for $i = 1, 2$. Then $f\,([\mu_1]\,,[\mu_2]) + f\,([\theta_1]\,,[\theta_2]) = \mu + \theta = f\,([\mu_1 + \theta_1]\,,[\mu_2 + \theta_2]) = f\,([\mu_1] + [\theta_1]\,,[\mu_2] + [\theta_2]) = f(([\mu_1]\,,[\mu_2]) + ([\theta_1]\,,[\theta_2]))$, f preserves an addition. We have $f\,([\mu_1]\,,[\mu_2])\,f\,([\theta_1]\,,[\theta_2]) = \mu\theta$ such that $\mu \equiv \mu_i(\text{mod } \beta_i)$ and $\theta \equiv \theta_i(\text{mod } \beta_i)$ for $i = 1, 2$. Thus $\mu\theta \equiv \mu_i\theta_i(\text{mod } \beta_i)$ for $i = 1, 2$. Then $f\,([\mu_1]\,,[\mu_2])\,f\,([\theta_1]\,,[\theta_2]) = \mu\theta = f\,([\mu_1\theta_1]\,,[\mu_2\theta_2]) = f\,([\mu_1]\,[\theta_1]\,,[\mu_2]\,[\theta_2]) = f\,(([\mu_1]\,,[\mu_2])\,([\theta_1]\,,[\theta_2]))$, f preserves a multiplication. Hence f is a ring monomorphism and $Imf = \Phi_{\mathbb{Z}[\omega]}\,(\beta_1\beta_2)$. □

Example 2.2.11. $$\begin{aligned} -72-27\omega &= 45\omega+72(-\omega-1) \\ &= 45\omega+72\omega^2 \\ &= 9\omega(5+8\omega) \\ &= 3^2\omega(9+12\omega+4(-\omega-1)) \\ &= 3^2\omega(9+12\omega+4\omega^2) \\ &= (2+\omega)^4(3+2\omega)^2. \end{aligned}$$

We have $N(3+2\omega)=7$.

Thus $$\begin{aligned} \Phi_{\mathbb{Z}[\omega]}\left(-72-27\omega\right) &= \Phi_{\mathbb{Z}[\omega]}\left((2+\omega)^4(3+2\omega)^2\right) \\ &\cong \Phi_{\mathbb{Z}[\omega]}\left((2+\omega)^4\right)\times\Phi_{\mathbb{Z}[\omega]}\left((3+2\omega)^2\right) \\ &\cong \mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_2\times\mathbb{Z}_{42}. \end{aligned}$$ □

Example 2.2.12. $19\omega=(5+3\omega)(2-3\omega)\omega$.

We have $N(5+3\omega)=N(2-3\omega)=19\equiv 1(\text{mod } 6)$.

Thus $$\begin{aligned} \Phi_{\mathbb{Z}[\omega]}\left(19\omega\right) &= \Phi_{\mathbb{Z}[\omega]}\left((5+3\omega)(2-3\omega)\right) \\ &\cong \Phi_{\mathbb{Z}[\omega]}\left(5+3\omega\right)\times\Phi_{\mathbb{Z}[\omega]}\left(2-3\omega\right) \\ &\cong \mathbb{Z}_{342}\times\mathbb{Z}_{342}. \end{aligned}$$ □

CHAPTER III

FACTORS OF QUOTIENT RINGS OVER QUADRATIC INTEGER RINGS

In this chapter, we will generalize the idea in chapter 2 to obtain factors of the quadratic integer rings $\mathbb{Z}[\omega] = \{a + b\omega \,|\, a, b \in \mathbb{Z}\}$ for $\omega = \sqrt{d}$ where d is a square free integer such that $d \equiv 2, 3(\text{mod } 4)$ or $\omega = (1 + \sqrt{d})/2$ where d is a square free integer such that $d \equiv 1(\text{mod } 4)$, which is a principal ideal domain.
Let d be a square free integer, and

$$\omega = \begin{cases} \sqrt{d} & \text{, if } \ d \equiv 2, 3(\text{mod } 4), \\ (1+\sqrt{d})/2 & \text{, if } \ d \equiv 1(\text{mod } 4). \end{cases}$$

Then the minimal polynomial of ω over $\mathbb{Q}$ is

$$m(x) = \begin{cases} x^2 - d & \text{, if } \ d \equiv 2, 3(\text{mod } 4), \\ x^2 - x + \frac{1-d}{4} & \text{, if } \ d \equiv 1(\text{mod } 4). \end{cases}$$

If $d \equiv 2, 3(\text{mod } 4)$, then $\overline{\omega} = -\sqrt{d}$ and so $\omega + \overline{\omega} = 0$, $\omega\overline{\omega} = -d$ and $\omega^2 - d = 0$.
If $d \equiv 1(\text{mod } 4)$, then $\overline{\omega} = (1 - \sqrt{d})/2$ and so $\omega + \overline{\omega} = 1$, $\omega\overline{\omega} = \frac{1-d}{4}$ and $\omega^2 - \omega + \left(\frac{1-d}{4}\right) = 0$.
For any $a + b\omega \in \mathbb{Z}[\omega]$, define the *norm* of $a + b\omega$ to be $N(a + b\omega) = (a + b\omega)(a + b\overline{\omega}) = a^2 + ab(\omega + \overline{\omega}) + b^2\omega\overline{\omega}$.

$$\text{Then } \ N(a+b\omega) = \begin{cases} a^2 - b^2 d & \text{, if } \ d \equiv 2, 3(\text{mod } 4), \\ a^2 + ab + b^2\frac{1-d}{4} & \text{, if } \ d \equiv 1(\text{mod } 4). \end{cases}$$

3.1 Factors of Quotient Rings over Ring of Quadratic Integers.

Lemma 3.1.1. *Let a and b be relatively prime integers, then* $m+n\omega$ *belongs to the ideal* $\langle ak+bk\omega\rangle$ *if and only if* $kN(a+b\omega)$ *divides both* $ma+mb+nb\left(\frac{1-d}{4}\right)$ *and* $an-mb$ *if* $d\equiv 1(\text{mod } 4)$ *and* $kN(a+b\omega)$ *divides both* $ma-nbd$ *and* $an-mb$ *if* $d\equiv 2,3(\text{mod } 4)$.

Proof. Let a and b be relatively prime integers.

Case 1. $d\equiv 1(\text{mod } 4)$. For any $m+n\omega\in\mathbb{Z}[\omega]$, we have

$$\begin{aligned}\frac{m+n\omega}{ak+bk\omega} &= \frac{(m+n\omega)(ak+bk\overline{\omega})}{(ak+bk\omega)(ak+bk\overline{\omega})}\\ &= \frac{mak+ank\omega+mbk\bar{\omega}+nbk\omega\bar{\omega}}{k^2N(a+b\omega)}\\ &= \frac{mak+mbk+nbk\left(\frac{1-d}{4}\right)}{k^2N(a+b\omega)}+\frac{(ank-mbk)\,\omega}{k^2N(a+b\omega)}\\ &= \frac{ma+mb+nb\left(\frac{1-d}{4}\right)}{kN(a+b\omega)}+\frac{(an-mb)\,\omega}{kN(a+b\omega)}.\end{aligned}$$

Thus $m+n\omega\in\langle ak+bk\omega\rangle$ if and only if $kN(a+b\omega)$ divides both $ma+mb+nb\left(\frac{1-d}{4}\right)$, and $an-mb$.

Case 2. $d\equiv 2,3(\text{mod } 4)$. For any $m+n\omega\in\mathbb{Z}[\omega]$, we have

$$\begin{aligned}\frac{m+n\omega}{ak+bk\omega} &= \frac{(m+n\omega)(ak+bk\overline{\omega})}{(ak+bk\omega)(ak+bk\overline{\omega})}\\ &= \frac{mak+ank\omega+mbk\bar{\omega}+nbk\omega\bar{\omega}}{k^2N(a+b\omega)}\\ &= \frac{mak-nbdk}{k^2N(a+b\omega)}+\frac{(ank-mbk)\,\omega}{k^2N(a+b\omega)}\\ &= \frac{ma-nbd}{kN(a+b\omega)}+\frac{(an-mb)\,\omega}{kN(a+b\omega)}.\end{aligned}$$

Thus $m+n\omega\in\langle ak+bk\omega\rangle$ if and only if $kN(a+b\omega)$ divides both $ma-nbd$, and $an-mb$. □

Lemma 3.1.2. *If a is a positive integer larger than 1, then $\mathbb{Z}\left[\omega\right]/\left\langle a\right\rangle \cong \mathbb{Z}_a\left[\omega\right]$.*

Proof. Define $\phi : \mathbb{Z}\left[\omega\right] \rightarrow \mathbb{Z}_a\left[\omega\right]$ by $\phi\left(x+y\omega\right) = \left[x\right]_a + \left[y\right]_a \omega$. It is obvious from the definition of ϕ that ϕ is onto. Next, we will show that ϕ is a ring homomorphism. Let $x_1 + y_1\omega, x_2 + y_2\omega \in \mathbb{Z}\left[\omega\right]$. Then

$$\begin{aligned}
\phi\left(x_1 + y_1\omega + x_2 + y_2\omega\right) &= \phi\left(\left(x_1 + x_2\right) + \left(y_1 + y_2\right)\omega\right) \\
&= \left[x_1 + x_2\right]_a + \left[y_1 + y_2\right]_a \omega \\
&= \left(\left[x_1\right]_a + \left[y_1\right]_a \omega\right) + \left(\left[x_2\right]_a + \left[y_2\right]_a \omega\right) \\
&= \phi\left(x_1 + y_1\omega\right) + \phi\left(x_2 + y_2\omega\right).
\end{aligned}$$

Case 1. $d \equiv 1(\text{mod } 4)$. Then

$$\begin{aligned}
\phi\left(\left(x_1 + y_1\omega\right)\left(x_2 + y_2\omega\right)\right) &= \phi((x_1x_2 - y_1y_2\left(1-d\right)/4) + \left(x_2y_1 + y_1y_2 + x_1y_2\right)\omega) \\
&= \left[x_1x_2 - y_1y_2\left(1-d\right)/4\right]_a + \left[x_2y_1 + y_1y_2 + x_1y_2\right]_a \omega \\
&= \left[x_1\right]_a\left[x_2\right]_a - \left[y_1\right]_a\left[y_2\right]_a\left(1-d\right)/4 \\
&\quad +(\left[x_2\right]_a\left[y_1\right]_a + \left[y_1\right]_a\left[y_2\right]_a + \left[x_1\right]_a\left[y_2\right]_a)\,\omega \\
&= \left[x_1\right]_a\left[x_2\right]_a + \left[y_1\right]_a\left[y_2\right]_a\left(\omega - \left(1-d\right)/4\right) \\
&\quad + \left(\left[x_2\right]_a\left[y_1\right]_a + \left[x_1\right]_a\left[y_2\right]_a\right)\omega \\
&= \left(\left[x_1\right]_a + \left[y_1\right]_a\omega\right)\left(\left[x_2\right]_a + \left[y_2\right]_a\omega\right) \\
&= \phi\left(x_1 + y_1\omega\right)\phi\left(x_2 + y_2\omega\right).
\end{aligned}$$

Case 2. $d \equiv 2, 3(\text{mod } 4)$. Then

$$\begin{aligned}
\phi\left(\left(x_1 + y_1\omega\right)\left(x_2 + y_2\omega\right)\right) &= \phi\left(x_1x_2 - y_1y_2d + (x_2y_1 + x_1y_2)\omega\right) \\
&= \left[x_1x_2 - y_1y_2d\right]_a + \left[x_2y_1 + x_1y_2\right]_a \omega \\
&= \left[x_1\right]_a\left[x_2\right]_a + \left[y_1\right]_a\left[y_2\right]_a d + \left(\left[x_2\right]_a\left[y_1\right]_a + \left[x_1\right]_a\left[y_2\right]_a\right)\omega \\
&= \left(\left[x_1\right]_a + \left[y_1\right]_a\omega\right)\left(\left[x_2\right]_a + \left[y_2\right]_a\omega\right) \\
&= \phi\left(x_1 + y_1\omega\right)\phi\left(x_2 + y_2\omega\right).
\end{aligned}$$

Hence ϕ is a surjective ring homomorphism. Since $\phi\left(a\right) = \left[a\right]_a = \left[0\right]_a, a \in \ker\phi$.

Then $\langle a\rangle \subseteq \ker\phi$. Let $x+y\omega \in \ker\phi$. Then $[0]_a = \phi(x+y\omega) = [x]_a + [y]_a\,\omega$, i.e. both x and y are congruent to 0 modulo a, so we can write $x = ax^{'}$ and $y = ay^{'}$ for some $x^{'}, y^{'} \in \mathbb{Z}$. Then $x + y\omega = ax' + ay'\omega \in \langle a\rangle$. Thus $\ker\phi \subseteq \langle a\rangle$. Then $\ker\phi = \langle a\rangle$. Hence $\mathbb{Z}[\omega]/\langle a\rangle \cong \mathbb{Z}_a[\omega]$. □

Lemma 3.1.3. *Let $a+b\omega \in \mathbb{Z}[\omega]$ where a and b are relatively prime integers and $s = N(a+b\omega)$. Then $\mathbb{Z}[\omega]/\langle a+b\omega\rangle \cong \mathbb{Z}_s$. Consequently if s is a prime number, then $a+b\omega$ is irreducible.*

Proof. Let $a+b\omega\in\mathbb{Z}[\omega]$ where a and b are relatively prime integers.

Case 1. $d \equiv 2, 3 (\text{mod } 4)$. Then $s = N(a+b\omega) = a^2 - b^2 d$. Since $(a,b) = 1$, $(a^2, b) = 1$. Then $(b, s) = (b, a^2 - b^2 d) = 1$, so b^{-1} exists in $\mathbb{Z}_s$. Since $a^2 - b^2 d \equiv 0(\text{mod } s)$, $a^2 b^{-2} - b^2 b^{-2} d \equiv 0(\text{mod } s)$. Thus $(ab^{-1})^2 \equiv d(\text{mod } s)$. To show that $\mathbb{Z}[\omega]/\langle a+b\omega\rangle \cong \mathbb{Z}_s$, define $\phi : \mathbb{Z}[\omega] \to \mathbb{Z}_s$ by

$$\phi(x+y\omega) = [x - (ab^{-1})\, y]$$

where $[t] = [t]_s$.

For any $m\in\mathbb{Z}$, $\phi(m) = [m - (ab^{-1})\,0] = [m]$, so ϕ is surjective.

Next, let $x_1 + y_1\omega$ and $x_2 + y_2\omega \in \mathbb{Z}[\omega]$. Thus

$$\begin{aligned}
\phi((x_1+y_1\omega)+(x_2+y_2\omega)) &= \phi((x_1+x_2)+(y_1+y_2)\,\omega)\\
&= [(x_1+x_2) - (ab^{-1})(y_1+y_2)]\\
&= [(x_1 - (ab^{-1})\,y_1) + (x_2 - (ab^{-1})\,y_2)]\\
&= [x_1 - (ab^{-1})\,y_1] + [x_2 - (ab^{-1})\,y_2]\\
&= \phi(x_1+y_1\omega) + \phi(x_2+y_2\omega), \text{ and}
\end{aligned}$$

$$\begin{aligned}
\phi((x_1+y_1\omega)(x_2+y_2\omega)) &= \phi((x_1x_2 + dy_1y_2) + (y_1x_2 + x_1y_2)\,\omega)\\
&= [x_1x_2 + dy_1y_2 - (ab^{-1})(y_1x_2 + x_1y_2)]\\
&= \left[x_1x_2 + (ab^{-1})^2\, y_1y_2 - (ab^{-1})(y_1x_2 + x_1y_2)\right]\\
&= [(x_1 - (ab^{-1})\,y_1)\cdot(x_2 - (ab^{-1})\,y_2)]\\
&= \phi(x_1+y_1\omega)\,\phi(x_2+y_2\omega).
\end{aligned}$$

Thus ϕ is a surjective ring homomorphism.

Moreover, since $\phi(a+b\omega) = [a-(ab^{-1})\,b] = [0]$, $\langle a+b\omega\rangle \subseteq \ker\phi$. Next, let $m+n\omega \in \ker\phi$, then

$$\begin{aligned}
\frac{m+n\omega}{a+b\omega} = \frac{(m+n\omega)(a+b\overline{\omega})}{(a+b\omega)(a+b\overline{\omega})} \\
&= \frac{ma-nbd+(an-mb)\,\omega}{N(a+b\omega)} \\
&= \frac{ma-nbd}{N(a+b\omega)} + \frac{(an-mb)\,\omega}{N(a+b\omega)} \\
&= \frac{ma-nbd}{s} + \frac{(an-mb)\,\omega}{s}.
\end{aligned}$$

Since $[0] = \phi(m+n\omega) = [m-ab^{-1}n]\,, [an-mb] = [0]$. By $[mb-an] = [0]$, we have $[mab^2 - na^2b] = [ab]\,[mb-an] = [0]\,.$ Then $[ma - na^2b^{-2}b] = [b^{-2}]\,[mab^2 - na^2b]$ $= [0]$. Since $(ab^{-1})^2 \equiv d(\text{ mod } s)$, $[ma-dbn] = [0]$. Thus $a+b\omega\,|m+n\omega$ and $m+n\omega \in \langle a+b\omega\rangle$. Hence $\ker\phi \subseteq \langle a+b\omega\rangle$ and so $\ker\phi = \langle a+b\omega\rangle$. Then $\mathbb{Z}[\omega]\,/\,\langle a+b\omega\rangle \cong \mathbb{Z}_s$. Consequently, if s is a prime number in $\mathbb{Z}$ then $\mathbb{Z}[\omega]\,/\,\langle a+b\omega\rangle$ is a field. Hence $\sigma = a+b\omega$ is irreducible in $\mathbb{Z}[\omega]$.

Case 2. $d \equiv 1(\text{mod } 4)$. Then $s = N(a+b\omega) = a^2+ab+b^2\left(\frac{1-d}{4}\right)$. Since $(a,b) = 1$, $(a^2,b) = 1$. Then $(b,s) = \left(b, a^2+ab+b^2\left(\frac{1-d}{4}\right)\right) = 1$, so b^{-1} exists in $\mathbb{Z}_s$. Since $a^2+ab+b^2\left(\frac{1-d}{4}\right) \equiv 0(\text{ mod } s)$, $a^2b^{-2}+abb^{-2}+b^2b^{-2}\left(\frac{1-d}{4}\right) \equiv 0(\text{mod } s)$. Thus $(ab^{-1})^2 \equiv -ab^{-1} - \left(\frac{1-d}{4}\right)(\text{mod } s)$. To show that $\mathbb{Z}[\omega]\,/\,\langle a+b\omega\rangle \cong \mathbb{Z}_s$, define $\phi : \mathbb{Z}[\omega] \to \mathbb{Z}_s$ by

$$\phi(x+y\omega) = [x-(ab^{-1})\,y]$$

where $[t] = [t]_s$.

For any $m \in \mathbb{Z}$, $\phi(m) = [m-(ab^{-1})\,0] = [m]$, so ϕ is surjective.

Next, let $x_1+y_1\omega$ and $x_2+y_2\omega \in \mathbb{Z}[\omega]$. Thus

$$\begin{aligned}
\phi((x_1+y_1\omega)+(x_2+y_2\omega)) &= \phi((x_1+x_2)+(y_1+y_2)\,\omega) \\
&= [(x_1+x_2)-(ab^{-1})\,(y_1+y_2)]
\end{aligned}$$

$$
\begin{aligned}
&= \left[\left(x_1 - \left(ab^{-1}\right) y_1\right) + \left(x_2 - \left(ab^{-1}\right) y_2\right)\right] \\
&= \phi\left(x_1 + y_1\omega\right) + \phi\left(x_2 + y_2\omega\right), \text{ and}
\end{aligned}
$$

$$
\begin{aligned}
\phi\left(\left(x_1 + y_1\omega\right)\left(x_2 + y_2\omega\right)\right) &= \phi((x_1x_2 - \left(\tfrac{1-d}{4}\right) y_1y_2) + \left(y_1x_2 + x_1y_2 + y_1y_2\right)\omega) \\
&= \left[x_1x_2 - \left(\tfrac{1-d}{4}\right) y_1y_2 - \left(ab^{-1}\right)\left(y_1x_2 + x_1y_2 + y_1y_2\right)\right] \\
&= \left[x_1x_2 + \left(-ab^{-1} - \left(\tfrac{1-d}{4}\right)\right) y_1y_2 - \left(ab^{-1}\right)\left(y_1x_2 + x_1y_2\right)\right] \\
&= \left[x_1x_2 + \left(ab^{-1}\right)^2 y_1y_2 - \left(ab^{-1}\right)\left(y_1x_2 + x_1y_2\right)\right] \\
&= \left[\left(x_1 - \left(ab^{-1}\right) y_1\right) \cdot \left(x_2 - \left(ab^{-1}\right) y_2\right)\right] \\
&= \phi\left(x_1 + y_1\omega\right) \phi\left(x_2 + y_2\omega\right).
\end{aligned}
$$

Thus ϕ is a ring homomorphism.

Moreover, since $\phi\left(a + b\omega\right) = \left[a - \left(ab^{-1}\right) b\right] = [0]$, $\langle a + b\omega \rangle \subseteq \ker\phi$.

Next, let $m + n\omega \in \ker\phi$, then

$$
\begin{aligned}
\frac{m + n\omega}{a + b\omega} &= \frac{\left(m + n\omega\right)\left(a + b\overline{\omega}\right)}{\left(a + b\omega\right)\left(a + b\overline{\omega}\right)} \\
&= \frac{ma + an\omega + mb\bar{\omega} + nb\omega\bar{\omega}}{N\left(a + b\omega\right)} \\
&= \frac{ma + mb + nb\left(\frac{1-d}{4}\right) + \left(an - mb\right)\omega}{N\left(a + b\omega\right)} \\
&= \frac{ma + mb + nb\left(\frac{1-d}{4}\right)}{s} + \frac{\left(an - mb\right)\omega}{s}.
\end{aligned}
$$

Since $[0] = \phi\left(m + n\omega\right) = \left[m - ab^{-1}n\right], \left[an - mb\right] = \left[m - ab^{-1}n\right]\left[-b\right] = [0]$. By $[mb - an] = [0]$, we have $\left[mab^2 - na^2b\right] = \left[mb - an\right]\left[ab\right] = [0]$. Then $\left[ma - na^2b^{-2}b\right] = \left[mab^2 - na^2b\right]\left[b^{-2}\right] = [0]$. Since $\left(ab^{-1}\right)^2 \equiv -ab^{-1} - \left(\frac{1-d}{4}\right)(\text{mod } s)$, $\left[ma + an + \left(\frac{1-d}{4}\right) bn\right] = \left[ma - \left(-ab^{-1} - \left(\frac{1-d}{4}\right)\right) bn\right] = [0]$, then $\left[ma + mb + \left(\frac{1-d}{4}\right) bn\right] = [0]$. Thus $a + b\omega \mid m + n\omega$ and $m + n\omega \in \langle a + b\omega \rangle$. Hence $\ker\phi \subseteq \langle a + b\omega \rangle$ and so $\ker\phi = \langle a + b\omega \rangle$. Then $\mathbb{Z}[\omega] / \langle a + b\omega \rangle \cong \mathbb{Z}_s$. Consequently, if s is a prime number in $\mathbb{Z}$ then $\mathbb{Z}[\omega] / \langle a + b\omega \rangle$ is a field. Hence $\sigma = a + b\omega$ is irreducible in $\mathbb{Z}[\omega]$. □

In the next lemma we use Legendre symbol so we will give the definition.

Definition 3.1.4. Let p be an odd prime number and $a \in \mathbb{Z}$ such that $p \nmid a$. Define the **Legendre symbol** as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & ,\text{if } x^2 \equiv a (\text{mod } p) \text{ has a solution in } \mathbb{Z}, \\ -1 & ,\text{otherwise.} \end{cases}$$

Lemma 3.1.5. *Let p be an odd prime number.*
Let $\overline{m}(x)$ be the polynomial obtained from reducing the coefficients of $m(x)$ modulo p. Then $\overline{m}(x)$ is irreducible in $\mathbb{Z}_p[x]$ if and only if $\left(\frac{d}{p}\right) = -1$.
In which case, $\mathbb{Z}_p[\omega] \cong \mathbb{Z}_p[x] / \langle \overline{m}(x) \rangle$ is a field.

Proof. Suppose $\left(\frac{d}{p}\right) = -1$. Then $x^2 \equiv d (\text{mod } p)$ has no solution in $\mathbb{Z}$. Suppose that $\overline{m}(x)$ has a root $\overline{a}$ in $\mathbb{Z}_p$.
Case 1. $d \equiv 2, 3 (\text{mod } 4)$. Then $\overline{m}(\overline{a}) = \overline{a}^2 - \overline{d} = 0$, i.e. $a^2 \equiv d (\text{mod } p)$, a contradiction.
Case 2. $d \equiv 1 (\text{mod } 4)$.

$$\overline{4}\overline{m}(x) = \overline{4}(x^2 - x + \overline{\tfrac{1-d}{4}}) = (\overline{2}x + \overline{1})^2 - \overline{d}.$$

Since $\overline{a}$ is a root of $\overline{m}(x)$, $(\overline{2a+1})^2 = \overline{d}$, i.e. $(2a+1)^2 \equiv d (\text{mod } p)$, a contradiction. Hence $\overline{m}(x)$ has no root in $\mathbb{Z}_p$, so $\overline{m}(x)$ is irreducible over $\mathbb{Z}_p$.
Conversely, assume that $\left(\frac{d}{p}\right) = 1$. Hence there exists an integer a such that $a^2 \equiv d (\text{mod } p)$.
Case 1. $d \equiv 2, 3 (\text{mod } 4)$. Then $m(x) = x^2 - d \equiv x^2 - a^2 = (x - a)(x + a) (\text{mod } p)$, i.e. $\overline{m}(x)$ is not irreducible in $\mathbb{Z}_p[x]$.
Case 2. $d \equiv 1 (\text{mod } 4)$. Then $4m(x) = 4x^2 - 4x + 1 - d = (2x - 1)^2 - d \equiv (2x - 1)^2 - a^2 = (2x - 1 - a)(2x - 1 + a) (\text{mod } p)$, so $\overline{4}\overline{m}(x)$ is not irreducible in $\mathbb{Z}_p[x]$.
Finally when $\overline{m}(x)$ is irreducible in $\mathbb{Z}_p[x]$, we have $\mathbb{Z}_p[\omega] \cong \mathbb{Z}_p[x] / \langle \overline{m}(x) \rangle$ is a field. □

Lemma 3.1.6. *For $d \equiv 1(\mathrm{mod}\ 4)$, let $\overline{m}(x)$ be the polynomial obtained by reducing all coefficient of $m(x)$ modulo 2. Then $\overline{m}(x)$ has no solution in $\mathbb{Z}_2$ if and only if $d \equiv 5(\mathrm{mod}\ 8)$. In which case, $\mathbb{Z}_2[\omega] \cong \mathbb{Z}_2[x]\,/\,\langle\overline{m}(x)\rangle$ is a field.*

Proof. $d \equiv 5(\mathrm{mod}\ 8)$ if and only if $\frac{1-d}{4}$ is an odd integer

if and only if $m(x) \equiv x^2 - x + \frac{1-d}{4} \equiv x^2 - x - 1(\mathrm{mod}\ 2)$

if and only if $\overline{m}(x)$ has no solution in $\mathbb{Z}_2$,

and when this happens $\overline{m}(x)$ is irreducible in $\mathbb{Z}_2[x]$. Hence $\mathbb{Z}_2[\omega] \cong \mathbb{Z}_2[x]\,/\,\langle\overline{m}(x)\rangle$ is a field. □

Lemma 3.1.7. (i) *For any odd prime integer q, $\langle q\rangle = \langle\alpha\rangle^2$ for some $\alpha \in \mathbb{Z}[\omega]$ if and only if $q\,|d$.*

(ii) *$\langle 2\rangle = \langle\alpha\rangle^2$ for some $\alpha \in \mathbb{Z}[\omega]$ if and only if $d \equiv 2, 3(\mathrm{mod}\ 4)$.*

Proof. (i) Let $\langle q\rangle = \langle\alpha\rangle^2$ for some $\alpha \in \mathbb{Z}[\omega]$.

Case 1. $d \equiv 2, 3(\mathrm{mod}\ 4)$. By Lemma 3.1.5, $\mathbb{Z}_q[x]\,/\left\langle x^2 - \overline{d}\right\rangle \cong \mathbb{Z}_q[\omega] \cong \mathbb{Z}[\omega]\,/\,\langle q\rangle \cong \mathbb{Z}[\omega]\,/\,\langle\alpha\rangle^2$. We have $\alpha + \langle\alpha\rangle^2$ is nonzero nilpotent, then there exists a monic polynomial $x + \overline{a}$ in $\mathbb{Z}_q[x]$ such that $(x + \overline{a}) + \left\langle x^2 - \overline{d}\right\rangle \in \mathbb{Z}_q[x]\,/\left\langle x^2 - \overline{d}\right\rangle$ is nonzero nilpotent. Thus $\left(\overline{k}\right)\left(x^2 - \overline{d}\right) = (x + \overline{a})^2$ for some $\overline{k} \in \mathbb{Z}_q[x]$ such that $\overline{k}$ is a polynomial with degree 0. Since q is a prime in $\mathbb{Z}$, $\overline{k}$ is a unit of $\mathbb{Z}_q[x]$ such that $\overline{k}\overline{k}^{'} = \overline{1}$. Thus $\left(x^2 - \overline{d}\right) = \overline{k}^{'}\,(x + \overline{a})^2 = \overline{k}^{'}x^2 + 2\overline{k}^{'}\overline{a}x + \overline{k}^{'}\,(\overline{a})^2$. Thus $\overline{k}^{'} = \overline{1}, \overline{a} = \overline{0}, \overline{0} = (\overline{a})^2 = -\overline{d}$. Hence $q\,|d$.

Case 2. $d \equiv 1(\mathrm{mod}\ 4)$. By Lemma 3.1.5, $\mathbb{Z}_q[x]\,/\left\langle x^2 - x + \overline{\left(\frac{1-d}{4}\right)}\right\rangle \cong \mathbb{Z}_q[\omega] \cong \mathbb{Z}[\omega]\,/\,\langle q\rangle \cong \mathbb{Z}[\omega]\,/\,\langle\alpha\rangle^2$. We have $\alpha + \langle\alpha\rangle^2$ is nonzero nilpotent, then there exists a monic polynomial $x + \overline{a}$ in $\mathbb{Z}_q[x]$ such that $(x + \overline{a}) + \left\langle x^2 - x + \overline{\left(\frac{1-d}{4}\right)}\right\rangle \in \mathbb{Z}_q[x]\,/\left\langle x^2 - x + \overline{\left(\frac{1-d}{4}\right)}\right\rangle$ is nonzero nilpotent. Thus $(\overline{k})(x^2 - x + (\overline{\frac{1-d}{4}})) = (x + \overline{a})^2$ for some $\overline{k} \in \mathbb{Z}_q[x]$ such that $\overline{k}$ is a polynomial with degree 0. Since q is a prime in $\mathbb{Z}$, $\overline{k}$ is a unit of $\mathbb{Z}_q[x]$ such that $\overline{k}\overline{k}^{'} = \overline{1}$. Thus $(x^2 - x + (\overline{\frac{1-d}{4}})) = \overline{k}^{'}\,(x + \overline{a})^2 = \overline{k}^{'}x^2 + 2\overline{k}^{'}\overline{a}x + \overline{k}^{'}\,(\overline{a})^2$. Thus $\overline{k}^{'} = \overline{1}, 2\overline{a} = \overline{-1}, (\overline{a})^2 = \overline{\left(\frac{1-d}{4}\right)}$, then $\overline{1} = 4\,(\overline{a})^2 = 4\overline{\left(\frac{1-d}{4}\right)} = \overline{1-d}$. Hence $q\,|d$.

Next, suppose that $q\,|d$. Then $x^2 - d \equiv x^2(\mathrm{mod}\ q)$ if $d \equiv 2, 3(\mathrm{mod}\ 4)$, and

$4\left(x^2 - x + \left(\frac{1-d}{4}\right)\right) \equiv 4x^2 - 4x + 1 - d = (2x-1)^2 (\text{mod } q)$ if $d \equiv 1 (\text{mod } 4)$. Hence there exists a nonzero $\overline{f}(x) \in \mathbb{Z}_q[x]$ such that $\overline{f}(x)^2 + \langle \overline{m}(x) \rangle = \langle \overline{m}(x) \rangle$. Since $\mathbb{Z}_q[x] / \langle \overline{m}(x) \rangle \cong \mathbb{Z}_q[\omega] \cong \mathbb{Z}[\omega] / \langle q \rangle$, there exists $\alpha \in \mathbb{Z}[\omega]$ such that $(\alpha + \langle q \rangle)^2 = \langle q \rangle$, i.e. $\langle \alpha \rangle^2 = \langle q \rangle$.
(ii) Suppose that $d \equiv 2, 3 (\text{mod } 4)$. By Lemma 3.1.5, $\mathbb{Z}_2[x] / \left\langle x^2 - \overline{d} \right\rangle \cong \mathbb{Z}_2[\omega] \cong \mathbb{Z}[\omega] / \langle 2 \rangle$. Since $\overline{d} = \overline{0}$ or $\overline{1}$ then $x^2 - \overline{d}$ is a square in $\mathbb{Z}_2[x]$. Therefore $\mathbb{Z}[\omega] / \langle 2 \rangle$ has nonzero nillpotent elements, so $\langle 2 \rangle = \langle \alpha \rangle^2$ for some $\alpha \in \mathbb{Z}[\omega]$.
Conversely, suppose there exists $\alpha \in \mathbb{Z}[\omega]$ such that $\langle \alpha \rangle^2 = \langle 2 \rangle$. Since $\mathbb{Z}[\omega] / \langle 2 \rangle \cong \mathbb{Z}_2[\omega] \cong \mathbb{Z}_2[x] / \langle \overline{m}(x) \rangle$ where $m(x) \in \mathbb{Z}[x]$ is minimal polynomial of ω, there exists a nonzero $\overline{f}(x) = x - \overline{a} \in \mathbb{Z}_2[x]$ such that $\langle x - \overline{a} \rangle^2 = \langle \overline{m}(x) \rangle$. Thus $\overline{m}(x)$ is square in $\mathbb{Z}_2[x]$. Suppose $\overline{m}(x) = x^2 - x - \overline{(\frac{d-1}{4})}$ is square in $\mathbb{Z}_2[x]$. Then $x^2 - x - \overline{(\frac{d-1}{4})} = \overline{m}(x) = (x - \overline{a})^2 = x^2 - \overline{a}^2$ which is a contradiction. Hence $\overline{m}(x) = x^2 - \overline{d}$, and so $d \equiv 2, 3 (\text{mod } 4)$. □

Next, we will determine the irreducible elements of the ring of the quadratic integers.

Theorem 3.1.8. *Up to association, the irreducible elements in $\mathbb{Z}[\omega]$ are exactly the followings:*
(i) $\sigma = a + b\omega, \overline{\sigma} = a + b\overline{\omega}$ *where* $|N(\sigma)| = |N(\overline{\sigma})|$ *is a prime number and* $\langle \sigma \rangle \neq \langle \overline{\sigma} \rangle$,
(ii) $\alpha = a + b\omega, \overline{\alpha} = a + b\overline{\omega}$ *where* $|N(\alpha)| = |N(\overline{\alpha})|$ *is a prime number and* $\langle \alpha \rangle = \langle \overline{\alpha} \rangle$,
(iii) π *where* π *is an odd prime number in* $\mathbb{Z}$ *such that* $\pi \nmid d$ *and* $(\frac{d}{\pi}) = -1$,
(iv) 2 *where* $d \equiv 5 (\text{mod } 8)$.

Proof. (i) and (ii) follow from Theorem 1.2.4 (vi).
(iii) Let π be an odd prime number in $\mathbb{Z}$ such that $\pi \nmid d$ and $(\frac{d}{\pi}) = -1$. By Lemma 3.1.2 and Lemma 3.1.5, $\mathbb{Z}[\omega] / \langle \pi \rangle \cong \mathbb{Z}_\pi[\omega]$ is a field. Hence π is an irreducible element.
(iv) Suppose $d \equiv 5 (\text{mod } 8)$. By Lemma 3.1.2 and Lemma 3.1.6, $\mathbb{Z}_2[\omega] \cong \mathbb{Z}[\omega] / \langle 2 \rangle$

is a field. Hence 2 is an irreducible element.

Conversely, let β be an irreducible element in $\mathbb{Z}[\omega]$.

Case 1. $\beta = 2$. Since $\mathbb{Z}[\omega] / \langle 2\rangle \cong \mathbb{Z}_2[\omega]$ and 2 is irreducible , $\mathbb{Z}_2[\omega]$ is a field. By Lemma 3.1.6, we have $d \equiv 5(\text{mod } 8)$.

Case 2. $\beta = \pi$ is odd prime integer. Since $\mathbb{Z}[\omega] / \langle \pi\rangle \cong \mathbb{Z}_\pi[\omega]$ and π is irreducible, $\mathbb{Z}_\pi[\omega] \cong \mathbb{Z}_\pi[x] / \langle \overline{m}(x)\rangle$ is a field. By Lemma 3.1.5, $(\frac{d}{\pi}) = -1$.

Case 3. $\beta = a + b\omega$. Let $q = N(a + b\omega)$ be a prime number. Since β is an irreducible element, a and b are relatively prime and $\mathbb{Z}[\omega] / \langle\beta\rangle$ is a field. By Lemma 3.1.3, $\mathbb{Z}[\omega] / \langle\beta\rangle \cong \mathbb{Z}_q$ so q is a prime number. If $\beta \nsim \bar{\beta}$, then $q = N(\beta) = \beta\bar{\beta} = N(\bar{\beta})$ so $\langle q\rangle = \langle\beta\rangle\langle\bar{\beta}\rangle$ where $\langle\beta\rangle \neq \langle\bar{\beta}\rangle$. If $\beta \sim \bar{\beta}$, then $q = N(\beta) = \beta\bar{\beta} = u\beta^2$ for some unit $u \in \mathbb{Z}[\omega]$ so $\langle q\rangle = \langle\beta^2\rangle = \langle\beta\rangle^2$ where $\langle\beta\rangle = \langle\bar{\beta}\rangle$. □

For a nonzero quadratic integer $a + b\omega$, we have

$$a + b\omega \sim 2^t \cdot \prod \sigma_i^{u_i} \cdot \prod \overline{\sigma}_i^{v_i} \cdot \prod \pi_i^{e_i} \cdot \prod \alpha_i^{k_i}$$

where $u_i, v_i, e_i, k_i, t \in \mathbb{Z}_0^+$.

Theorem 3.1.9. *If a, b, k are positive integers such that a and b are relatively prime, then*

$$\mathbb{Z}[\omega] / \langle ak + bk\omega\rangle = \left\{\left[x' + y'\omega\right] : 0 \leq x' < k\left|N(a + b\omega)\right|, 0 \leq y' < k\right\}.$$

Proof. Assume that a, b, k are positive integers such that a and b are relatively prime.

Case 1. $d \equiv 1(\text{mod } 4)$. Let $[x + y\omega] \in \mathbb{Z}[\omega] / \langle ak + bk\omega\rangle$. Since $(a, b) = 1$, there exist integers s and t such that $as + bt = 1$. Then $aks + bkt = k$. Therefore $k\omega - (ak + bk\omega)\omega s - (ak + bk\omega)t + (ak + bk\omega)s = bks\left(\frac{1-d}{4}\right) - akt + aks$. Then $k\omega \equiv bks\left(\frac{1-d}{4}\right) - akt + aks(\text{mod } \langle ak + bk\omega\rangle)$, so

$k\omega \equiv m(\text{mod } \langle ak + bk\omega\rangle)$ for $m = bks\left(\frac{1-d}{4}\right) - akt + aks \in \mathbb{Z}$. (1)

And $k\left|N(a + b\omega)\right| = |(ak + bk\omega)(a + b\overline{\omega})| \in \langle ak + bk\omega\rangle$, then

$k\left|N(a + b\omega)\right| \equiv 0(\text{mod } \langle ak + bk\omega\rangle)$. (2)

Thus $[x+y\omega] = \left[x+(n_1k+y^{'})\omega\right]$ where $y = n_1k+y^{'}$ such that $0 \leq y^{'} < k$

$= \left[x+n_1k\omega+y^{'}\omega\right]$

$= \left[x+n_1m+y^{'}\omega\right]$ by (1)

$= \left[n_2k\left|N\left(a+b\omega\right)\right|+x^{'}+y^{'}\omega\right]$ where $x+n_1m = n_2k\left|N\left(a+b\omega\right)\right|$ $+x^{'}$ such that $0 \leq x^{'} < k\left|N\left(a+b\omega\right)\right|$

$= \left[x^{'}+y^{'}\omega\right]$ by (2).

Hence $[x+y\omega] = \left[x^{'}+y^{'}\omega\right]$, with $0 \leq x^{'} < k\left|N\left(a+b\omega\right)\right|, 0 \leq y^{'} < k$.

Case 2. $d \equiv 2, 3(\bmod\ 4)$. Let $[x+y\omega] \in \mathbb{Z}[\omega] / \langle ak+bk\omega\rangle$. Since $(a,b)=1$, there exist integers s and t such that $as+bt=1$. Then $aks+bkt=k$. Therefore $k\omega-(ak+bk\omega)\omega s-(ak+bk\omega)t = -bksd-akt$. Then $k\omega \equiv -bksd-akt(\bmod\ \langle ak+bk\omega\rangle)$, so

$k\omega \equiv m(\bmod\ \langle ak+bk\omega\rangle)$ for $m = -bksd-akt \in \mathbb{Z}$. (3)

And $k\left|N\left(a+b\omega\right)\right| = |(ak+bk\omega)(a+b\overline{\omega})| \in \langle ak+bk\omega\rangle$, then

$k\left|N\left(a+b\omega\right)\right| \equiv 0(\bmod\ \langle ak+bk\omega\rangle)$. (4)

Thus $[x+y\omega] = \left[x+(n_1k+y^{'})\omega\right]$ where $y = n_1k+y^{'}$ such that $0 \leq y^{'} < k$

$= \left[x+n_1k\omega+y^{'}\omega\right]$

$= \left[x+n_1m+y^{'}\omega\right]$ by (3)

$= \left[n_2k\left|N\left(a+b\omega\right)\right|+x^{'}+y^{'}\omega\right]$ where $x+n_1m = n_2k\left|N\left(a+b\omega\right)\right|$ $+x^{'}$ such that $0 \leq x^{'} < k\left|N\left(a+b\omega\right)\right|$

$= \left[x^{'}+y^{'}\omega\right]$ by (4).

Hence $[x+y\omega] = \left[x^{'}+y^{'}\omega\right]$, with $0 \leq x^{'} < k\left|N\left(a+b\omega\right)\right|, 0 \leq y^{'} < k$.

Next, Let $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ such that $0 \leq x_1, x_2 < k\left|N\left(a+b\omega\right)\right|, 0 \leq y_1, y_2 < k$ and $[x_1+y_1\omega] = [x_2+y_2\omega]$. Then $(x_2-x_1)+(y_2-y_1)\omega \in \langle ak+bk\omega\rangle$.

Case 1. $d \equiv 1(\bmod\ 4)$. By Lemma 3.1.1, we have $kN\left(a+b\omega\right)|a(x_2-x_1)+b(y_2-y_1)\left(\frac{1-d}{4}\right)+b(x_2-x_1)$ and $kN\left(a+b\omega\right)|a(y_2-y_1)-b(x_2-x_1)$. Thus $kN\left(a+b\omega\right)|$ $b(a(x_2-x_1)+b(y_2-y_1)\left(\frac{1-d}{4}\right)+b(x_2-x_1))+b(a(y_2-y_1)-b(x_2-x_1))$ $+a(a(y_2-y_1)-b(x_2-x_1))$, then $k\,|y_2-y_1$. Since $0 \leq y_2, y_1 < k, y_2 = y_1$.

Thus $kN\left(a+b\omega\right)|\left(a+b\right)\left(x_2-x_1\right), kN\left(a+b\omega\right)|-b(x_2-x_1)$. Since $(a,b)=1, (a+b,-b)=1$. Then $kN\left(a+b\omega\right)|x_2-x_1$. Since $0 \leq x_2, x_1 < k\left|N\left(a+b\omega\right)\right|$, $x_2 = x_1$.

Case 2. $d \equiv 2,3(\text{mod } 4)$, we have $kN\,(a+b\omega)\,|a(x_2-x_1)-bd(y_2-y_1)$ and $kN\,(a+b\omega)\,|a(y_2-y_1)-b(x_2-x_1)$. Thus

$$kN\,(a+b\omega)\,|b(a(x_2-x_1)-bd(y_2-y_1))+a(a(y_2-y_1)-b(x_2-x_1)),$$

then $k\,|y_2-y_1$. Since $0 \le y_2, y_1 < k$, $y_2 = y_1$.

Therefore $kN\,(a+b\omega)\,|a(x_2-x_1)$ and $kN\,(a+b\omega)\,|-b(x_2-x_1)$. Since $(a,-b) = 1, kN\,(a+b\omega)\,|x_2-x_1$. Since $0 \le x_2, x_1 < k\,|N\,(a+b\omega)|$, $x_2 = x_1$. □

Theorem 3.1.10. *Let* $a+b\omega \in \mathbb{Z}\,[\omega]\setminus\{0\}$ *be such that*

$$a+b\omega \sim 2^t\cdot\prod\sigma_i^{u_i}\cdot\prod\overline{\sigma}_i^{v_i}\cdot\prod\pi_i^{e_i}\cdot\prod\alpha_i^{k_i}$$

where $u_i, v_i, e_i, k_i, t \in \mathbb{Z}_0^+$, $s_1 = \prod N(\sigma_i^{u_i}), s_2 = \prod N(\overline{\sigma}_i^{v_i}), s_3 = 2^t\cdot\prod\pi_i^{e_i}$, *and* $R = \mathbb{Z}\,[\omega]\,/\,\langle\prod(\alpha_i)^{k_i}\rangle$. *Then* $\mathbb{Z}\,[\omega]\,/\,\langle a+b\omega\rangle \cong \mathbb{Z}_{s_1}\oplus\mathbb{Z}_{s_2}\oplus\mathbb{Z}_{s_3}\,[\omega]\oplus R.$

Proof. Let a and b be integers, not both zero, such that $s_1 = \prod N(\sigma_i^{u_i})$, $s_2 = \prod N(\overline{\sigma}_i^{v_i}), s_3 = 2^t\cdot\prod\pi_i^{e_i}$, and $R = \mathbb{Z}\,[\omega]\,/\,\langle\prod(\alpha_i)^{k_i}\rangle$. Since

$$a+b\omega \sim 2^t\cdot\prod\sigma_i^{u_i}\cdot\prod\overline{\sigma}_i^{v_i}\cdot\prod\pi_i^{e_i}\cdot\prod\alpha_i^{k_i}$$
$$\langle a+b\omega\rangle = \langle\prod\sigma_i^{u_i}\cdot\prod\overline{\sigma}_i^{v_i}\cdot 2^t\cdot\prod\pi_i^{e_i}\cdot\prod\alpha_i^{k_i}\rangle. \qquad (1)$$

By Theorem 1.2.8, and $\mathbf{Z}[\omega]$ is a principal ideal domain, we arrive at

$$\begin{aligned}\mathbb{Z}\,[\omega]\,/\,\langle a+b\omega\rangle &\cong \mathbb{Z}\,[\omega]\,/\,\langle\prod\sigma_i^{u_i}\cdot\prod\overline{\sigma}_i^{v_i}\cdot 2^t\cdot\prod\pi_i^{e_i}\cdot\prod\alpha_i^{k_i}\rangle\\ &\cong \mathbb{Z}\,[\omega]\,/\,\langle\prod\sigma_i^{u_i}\rangle\oplus\mathbb{Z}\,[\omega]\,/\,\langle\prod\overline{\sigma}_i^{v_i}\rangle\\ &\oplus\mathbb{Z}\,[\omega]\,/\,\langle 2^t\cdot\prod\pi_i^{e_i}\rangle\oplus\mathbb{Z}\,[\omega]\,/\,\langle\prod\alpha_i^{k_i}\rangle. \qquad (2)\end{aligned}$$

Consider $\prod\sigma_i^{u_i} = m+n\omega$. We will show that $\mathbb{Z}\,[\omega]\,/\,\langle m+n\omega\rangle \cong \mathbb{Z}_{N(m+n\omega)}$.

Clearly, π_i does not divide $m+n\omega$ for all i. Next, in case $d \equiv 5(\text{mod } 8)$, 2 is irreducible then 2 does not divide $m+n\omega$. Finally, for any prime $q \in \mathbb{Z}$ such that $q \neq \pi_i$ for all i. Since $N\,(q) = q^2$, up to associated $q = ab$ where a, b are irreducible elements of $\mathbb{Z}\,[\omega]$.

If $q = \alpha_i\beta$ for some i and nonzero nonunit $\beta \in \mathbb{Z}\,[\omega]$. Then $q \nmid m+n\omega$.

If $q = \pi_i\beta$ for some i and nonzero nonunit $\beta \in \mathbb{Z}\,[\omega]$. Then $q \nmid m+n\omega$.

If $q = \sigma_i^{'}\beta$ for some i and nonzero nonunit $\beta \in \mathbb{Z}\,[\omega]$. Then $q \nmid m+n\omega$.

If $q = \sigma_i\beta$ for some i and nonzero nonunit $\beta \in \mathbb{Z}\,[\omega]$. Then $q^2 = N\,(q) = N\,(\sigma_i\beta) =$

$N(\sigma_i)\,N(\beta)$. Thus $q = N(\sigma_i) = \sigma_i\overline{\sigma}_i$. Hence q does not divide $m+n\omega$. Therefore $(m,n) = 1$. By Lemma 3.1.3, $\mathbb{Z}[\omega]\,/\,\langle\prod\sigma_i^{u_i}\rangle \cong \mathbb{Z}[\omega]\,/\,\langle m+n\omega\rangle \cong \mathbb{Z}_{N(m+n\omega)} \cong \mathbb{Z}_{\prod N(\sigma_i^{u_i})} \cong \mathbb{Z}_{s_1}$. Similarly, the second term in (2) is isomorphic to $\mathbb{Z}_{s_2}$. Thanks to Lemma 3.1.2, the third term is isomorphic to $\mathbb{Z}_{s_3}[\omega]$. Hence $\mathbb{Z}[\omega]\,/\,\langle a+b\omega\rangle \cong \mathbb{Z}_{s_1}\oplus\mathbb{Z}_{s_2}\oplus\mathbb{Z}_{s_3}[\omega]\oplus R$. □

Example 3.1.11. Let $d = 5$ then $d \equiv 1 \pmod{4}$.

By Theorem 3.1.7, up to association, the irreducible elements in $\mathbb{Z}[\omega]$ are exactly the followings:

(i) $\sigma = a+b\omega, \overline{\sigma} = a+b\overline{\omega}$ where $|N(\sigma)| = |N(\overline{\sigma})|$ is a prime number and $\langle\sigma\rangle \neq \langle\overline{\sigma}\rangle$,

(ii) $\alpha = 2+\omega, \overline{\alpha} = 2+\overline{\omega}$ where $|N(2+\omega)| = |N(2+\overline{\omega})| = 5$ and $\langle 2+\omega\rangle = \langle 2+\overline{\omega}\rangle$,

(iii) π where π is an odd prime number in $\mathbb{Z}$ such that $\pi \equiv 2, 3 (\text{mod } 5)$,

(iv) 2.

We have
$$\begin{aligned} -224+28\omega &= 28(-8+\omega) \\ &= 28(-9+\omega+1) \\ &= 28(-9+\omega^2) \\ &= 7\cdot 2^2(3+\omega)(-3+\omega) \\ &= 7\cdot 2^2(3+\omega)(2+\omega)(2-\omega). \end{aligned}$$

Next, we will show that $\langle 3+\omega\rangle \neq \langle 3+\bar{\omega}\rangle$, We have $3+\bar{\omega} = 4-\omega$ and $N(3+\omega) = N(4-\omega)$. Suppose that $\langle 3+\omega\rangle = \langle 4-\omega\rangle$, then $3+\omega = u(4-\omega)$ for some unit $u \in \mathbb{Z}[\omega]$. Thus $u = -1$ and $4u = 3$, it is a contradiction. Hence $\langle 3+\omega\rangle \neq \langle 3+\bar{\omega}\rangle$ and $N(3+\omega) = 11$. Since $2-\omega$ is a unit of $\mathbb{Z}[\omega]$, $\langle -224+28\omega\rangle = \langle 7\cdot 2^2(3+\omega)(2+\omega)\rangle$.

Thus
$$\begin{aligned} \mathbb{Z}[\omega]\,/\,\langle -224+28\omega\rangle &= \mathbb{Z}[\omega]\,/\,\langle 7\cdot 2^2(3+\omega)(2+\omega)\rangle \\ &\cong \mathbb{Z}_{11}\oplus\mathbb{Z}_{28}[\omega]\oplus\mathbb{Z}[\omega]\,/\,\langle 2+\omega\rangle. \end{aligned}$$
□

3.2 The Euler $\phi-$function for the Ring of Quadratic Integers.

In this section we will consider the Euler $\phi-$function over the ring of quadratic integers. For $\beta \in \mathbb{Z}[\omega]$, we denote the unit group of the ring of $\mathbb{Z}[\omega] / \langle\beta\rangle$ by $\Phi_{\mathbb{Z}[\omega]}(\beta)$. We denote Euler $\phi-$function of β over $\mathbb{Z}[\omega]$ by $\phi_{\mathbb{Z}[\omega]}(\beta)$ is defined to be the order of multiplicative group of $\Phi_{\mathbb{Z}[\omega]}(\beta)$. In this section, we denote irreducible element in $\mathbb{Z}[\omega]$ as in the last section.

Note. $N(\alpha) = q$ where α is as in Theorem 3.1.8 (ii).

Theorem 3.2.1. *The equivalence classes of* $\mathbb{Z}[\omega]$ *modulo a power of irreducible are given as follows :*

(i) $\mathbb{Z}[\omega] / \langle\sigma^n\rangle = \{[x] : 0 \leq x < N(\sigma)^n\}$,

(ii) $\mathbb{Z}[\omega] / \langle\pi^n\rangle = \{[x + y\omega] : 0 \leq x, y < \pi^n\}$,

(iii) $\mathbb{Z}[\omega] / \langle\alpha^{2m}\rangle = \{[x + y\omega] : 0 \leq x, y < q^m\}$,

(iv) $\mathbb{Z}[\omega] / \langle\alpha^{2m+1}\rangle = \{[x + y\omega] : 0 \leq x < q^{m+1}, 0 \leq y < q^m\}$,

(v) $\mathbb{Z}[\omega] / \langle 2^n\rangle = \{[x + y\omega] : 0 \leq x, y < 2^n\}$.

Proof. Let $\sigma^n = m + n\omega$. Claim $\mathbb{Z}[\omega] / \langle\sigma^n\rangle = \{[x] : 0 \leq x < N(\sigma)^n\}$ We have $-n\omega \equiv m(\text{mod } m + n\omega)$. Suppose that $(N(\sigma), n) \neq 1$, then $N(\sigma) | n$. Then $(m + n\omega)(m + n\overline{\omega}) | n$, $(m + n\omega) | n$, $(m + n\omega) | m$ and $(m + n\omega)(m + n\overline{\omega}) | m$, $N(m + n\omega) | m$. Thus $N(m + n\omega) | m + n\omega$ but $N(m + n\omega)$ $= (m + n\omega)(m + n\overline{\omega})$, it is impossible. Thus $(N(\sigma), n) = 1$. Therefore $(N(m + n\omega), n) = 1$. Then there is $r \in \mathbb{Z}$ such that $rn \equiv 1(\text{mod } N(m + n\omega))$, then $rn \equiv 1(\text{ mod } m + n\omega)$. Thus $-rn\omega \equiv rm(\text{ mod } m + n\omega)$,$-\omega \equiv rm(\text{mod } m + n\omega)$. Hence if $[a + b\omega] \in \mathbb{Z}[\omega] / \langle\sigma^n\rangle$ then $[a + b\omega] = [x]$ where $0 \leq x < N(m + n\omega)$,

$$\mathbb{Z}[\omega] / \langle m + n\omega\rangle = \{[x] : 0 \leq x < N(m + n\omega)\}.$$

Next, Let $[x] = [y]$ in $\{[x] : 0 \leq x < N(m + n\omega)\}$. Then $x - y \in \langle m + n\omega\rangle$. Therefore $m + n\omega \,| x - y$ and $m + n\overline{\omega} \,| x - y$. Since $m + n\omega$ and $m + n\overline{\omega}$ are not associated,

$N(m+n\omega)\,|x-y$. Thus $x=y$. Hence $\mathbb{Z}[\omega]/\langle\sigma^n\rangle=\{[x]:0\le x<N(\sigma)^n\}$. By Theorem 3.1.9, $\mathbb{Z}[\omega]/\langle ak+bk\omega\rangle=\{[x+y\omega]:0\le x<k\,|N(a+b\omega)|\,,0\le y<k\}$ where $(a,b)=1$. Thus

$$\begin{aligned}
&\mathbb{Z}[\omega]/\langle\pi^n\rangle=\{[x+y\omega]:0\le x,y<\pi^n\},\\
&\mathbb{Z}[\omega]/\langle\alpha^{2m}\rangle=\{[x+y\omega]:0\le x,y<q^m\},\\
&\mathbb{Z}[\omega]/\langle\alpha^{2m+1}\rangle=\{[x+y\omega]:0\le x<q^{m+1},0\le y<q^m\},\\
&\mathbb{Z}[\omega]/\langle 2^n\rangle=\{[x+y\omega]:0\le x,y<2^n\}.
\end{aligned}$$

□

This theorem implies that $\mathbb{Z}[\omega]/\langle\sigma^n\rangle$ has $N(\sigma)^n$ elements, $\mathbb{Z}[\omega]/\langle\pi^n\rangle$ has π^{2n} elements, $\mathbb{Z}[\omega]/\langle\alpha^n\rangle$ has q^n elements, and $\mathbb{Z}[\omega]/\langle 2^n\rangle$ has 2^{2n} elements.

Now we are ready to identify the units of the rings in Theorem 3.2.1.

Theorem 3.2.2. (i) $\Phi_{\mathbb{Z}[\omega]}(\sigma^n)=\{[x]:0\le x<N(\sigma)^n \textit{ and } (N(\sigma),x)=1\}$,

(ii) $\Phi_{\mathbb{Z}[\omega]}(\pi^n)=\{[x+y\omega]:0\le x,y<\pi^n \textit{ and } (\pi,x)=1 \textit{ or } (\pi,y)=1\}$,

(iii) *In case* $d\equiv 1(\text{mod }4)$, *let* $\alpha=u+v\omega$ *and* $N(\alpha)=q$,

$$\Phi_{\mathbb{Z}[\omega]}(\alpha^{2m})=\{[x+y\omega]:0\le x,y<q^m \textit{ and } q\nmid\left(xu+xv+yv\left(\tfrac{1-d}{4}\right)\right) \textit{ or } q\nmid(yu-xv)\},$$

In case $d\equiv 2,3(\text{mod }4)$, *let* $\alpha=u+v\omega$ *and* $N(\alpha)=q$,

$$\Phi_{\mathbb{Z}[\omega]}(\alpha^{2m})=\{[x+y\omega]:0\le x,y<q^m \textit{ and } q\nmid(xu-yud) \textit{ or } q\nmid(yu-xv)\}$$

(iv) *In case* $d\equiv 1(\text{mod }4)$, *let* $\alpha=u+v\omega$ *and* $N(\alpha)=q$,

$$\Phi_{\mathbb{Z}[\omega]}(\alpha^{2m+1})=\{[x+y\omega]:0\le x<q^{m+1},0\le y<q^m \textit{ and} q\nmid\left(xu+xv+yv\left(\tfrac{1-d}{4}\right)\right) \textit{ or } q\nmid(yu-xv)\},$$

In case $d\equiv 2,3(\text{mod }4)$, *let* $\alpha=u+v\omega$ *and* $N(\alpha)=q$,

$$\Phi_{\mathbb{Z}[\omega]}(\alpha^{2m+1})=\{[x+y\omega]:0\le x<q^{m+1},0\le y<q^m \textit{ and } q\nmid(xu-yud) \textit{ or } q\nmid(yu-xv)\},$$

(v) $\Phi_{\mathbb{Z}[\omega]}(2^n)=\{[x+y\omega]:0\le x,y<2^n \textit{ and } (2,x)=1 \textit{ or } (2,y)=1\}$

Proof. Let $a,b\in\mathbb{Z}[\omega]$. Then $[a]$ is a unit in $\mathbb{Z}[\omega]/\langle b\rangle$ if and only if $[a][c]=[1]$ in $\mathbb{Z}[\omega]/\langle b\rangle$, for some $c\in\mathbb{Z}[\omega]$. Then $[a]$ is a unit in $\mathbb{Z}[\omega]/\langle b\rangle$ if and only if $ac\equiv 1(\text{mod b})$ if and only if $be+ac=1$ for some $e\in\mathbb{Z}[\omega]$ if and only if $(a,b)=1$.

Consider $\Phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m}\right)$, let $\alpha = u+v\omega$ and $x+y\omega \in \mathbb{Z}[\omega] / \langle \alpha^{2m} \rangle$. If $d \equiv 2, 3(\text{mod } 4)$ by Lemma 3.1.1, $(u+v\omega, x+y\omega) = 1$ if and only if $u+v\omega \nmid x+y\omega$ if and only if $q \nmid (xu - yud)$ or $q \nmid (yu - xv)$. If $d \equiv 1(\text{mod } 4)$ by Lemma 3.1.1, $(u+v\omega, x+y\omega) = 1$ if and only if $u+v\omega \nmid x+y\omega$ if and only if $q \nmid \left(xu + xv + yv\left(\frac{1-d}{4}\right)\right)$ or $q \nmid (yu - xv)$. Hence if $d \equiv 1(\text{mod } 4)$,

$$\Phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m}\right) = \{[x+y\omega] : 0 \leq x, y < q^m \text{ and } q \nmid \left(xu + xv + yv\left(\tfrac{1-d}{4}\right)\right) \text{ or } q \nmid (yu - xv)\},$$

if $d \equiv 2, 3(\text{mod } 4)$,

$$\Phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m}\right) = \{[x+y\omega] : 0 \leq x, y < q^m \text{ and } q \nmid (xu - yud) \text{ or } q \nmid (yu - xv)\}.$$

In the same way, we have

if $d \equiv 1(\text{mod } 4)$,

$$\Phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m+1}\right) = \{[x+y\omega] : 0 \leq x < q^{m+1}, 0 \leq y < q^m \text{ and } q \nmid \left(xu + xv + yv\left(\tfrac{1-d}{4}\right)\right) \text{ or } q \nmid (yu - xv)\},$$

if $d \equiv 2, 3(\text{mod } 4)$,

$$\Phi_{\mathbb{Z}[\omega]}\left(\alpha^{2m+1}\right) = \{[x+y\omega] : 0 \leq x < q^{m+1}, 0 \leq y < q^m \text{ and } q \nmid (xu - yud) \text{ or } q \nmid (yu - xv)\},$$

$$\Phi_{\mathbb{Z}[\omega]}\left(\sigma^n\right) = \{[x] : 0 \leq x < N(\sigma)^n \text{ and } (N(\sigma), x) = 1\},$$

$$\Phi_{\mathbb{Z}[\omega]}\left(\pi^n\right) = \{[x+y\omega] : 0 \leq x, y < \pi^n \text{ and } (\pi, x) = 1 \text{ or } (\pi, y) = 1\},$$

$$\Phi_{\mathbb{Z}[\omega]}\left(2^n\right) = \{[x+y\omega] : 0 \leq x, y < 2^n \text{ and } (2, x) = 1 \text{ or } (2, y) = 1\}.$$ □

Example 3.2.3. In $\mathbb{Z}\left[(1+\sqrt{5})/2\right]$, $N(4+\omega) = 19$ is a prime integer. Since $17 + 9\omega = (4+\omega)^2$,

$$\begin{aligned}\Phi_{\mathbb{Z}[\omega]}(17+9\omega) &= \Phi_{\mathbb{Z}[\omega]}\left((4+\omega)^2\right)\\ &= \{[x] : 0 \leq x \leq 19^2 = 361 \text{ and } (x, 361) = 1\}.\end{aligned}$$

Thus $\phi_{\mathbb{Z}[\omega]}(17+9\omega) = 19^2 - 19 = 342$. □

References

[1]. Greg Dresden and Wayne M. Dymacek. Finding factors of factor rings over the Gaussian integers. J. Math. Monthly 112(2005) : 602-611.

[2]. James T. Cross. The Euler function in the Gaussian integers. J. Math. Monthly 90(1983) : 518-528.

[3]. Ratinan Boonklurb. Euclideanness of the ring of integers of quadratic fields. senior project Mathematics Science Chulalongkorn university, 1998.

[4]. Andrew Adler, John E. Coury. The theory of numbers. New York : Jones and Bartlett Publishers International, 1995.

[5]. Ethan D. Bolker. Elementary number theory. New York : W.A. Benjamin, 1970.

VITA

Name	Mister Watchara Khuntavichai
Date of Birth	5 March 1982
Place of Birth	Udontani, Thailand
Education	B.Sc.(Mathematics)(First Class Honors), Khon kean University, 2004
Scholarship	The development and promotion of science and tecnology talents project