EÜFBED - Fen Bilimleri Enstitüsü Dergisi Cilt-Sayı: 6-2 Yıl: 2013 165-174

ON THE FACTOR RINGS OF EISENSTEIN INTEGERS

EISENSTEIN TAMSAYILARI HALKASININ BÖLÜM HALKALARI ÜZERİNE

Rukiye ÖZTÜRK[1], Ali AYDOĞDU[1] and Engin ÖZKAN[2*]

[1] *Atatürk Üniversitesi, Fen Fakültesi, Matematik Bölümü, Erzurum*

[2] *Erzincan Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Erzincan*

Geliş Tarihi: 16 Nisan 2013 **Kabul Tarihi:** 12 Kasım 2013

ABSTRACT

In this study, we will answer the question "What can we say about the factor rings of Eisenstein integers which arise naturally when we consider the factor rings of the ring of integers which is the fundamental concept of abstract algebra. In other words, we will characterize the structure of factor rings for the ring of Eisenstein integers.

Keywords : Factor rings; The ring of Eisenstein Integers; Euclidean rings and their generalizations; Principal ideal rings.

ÖZET

Bu çalışmada, soyut cebirin temel kavramlarından biri olan tamsayılar halkasının bölüm halkaları düşünüldüğünde doğal olarak ortaya çıkan "Eisenstein tamsayıları halkasının bölüm halkaları hakkında ne söyleyebiliriz?" sorusu cevaplanacaktır. Başka bir deyişle, Eisenstein tamsayıları halkası için bölüm halkalarının yapısı karakterize edilecektir.

Anahtar Kelimeler: Bölüm Halkaları, Eisenstein tamsayılar halkası, Euclidean halkaları ve genelleştirmeleri, Esas ideal halkaları

1. INTRODUCTION

In [1], it is generalized the idea of factor rings from the integers to the Gaussian integers and at the conclusion part of this work, the writer states that generalization can be done in $\mathbb{Z}[w]$ where $w=\dfrac{-1+i\sqrt{3}}{2}$. So, in this study, we characterize the factor rings of $\mathbb{Z}[w]$ by assuming [1] as a basis.

***Sorumlu Yazar:** eozkan@erzincan.edu.tr**

Whichever ring including $\mathbb{Z}$ is applied, each work has a certain value because it gives the general theory of the factor rings of the related ring [1].(for example, in [2], [1] is applied to $\mathbb{Z}\left[\sqrt{-2}\right]$).

In summary, in this study we obtain the rings isomorphic to factor rings of Eisenstein integers, prove some properties about the factor rings of Eisenstein integers and find the factors of them.

2. THE CHARACTERIZATION OF FACTOR RINGS OF EISENSTEIN INTEGERS

Throughout this section, Ω_n shall denote the set $\mathbb{Z}_n[w]=\{a+bw : a,b\in\mathbb{Z}_n\}$. We start by stating a remark on the ring of Eisenstein integers.

2.1. Remark

$$\mathbb{Z}[w]/\langle a+bw\rangle \cong \mathbb{Z}[w]/\langle -a-bw\rangle \cong \mathbb{Z}[w]/\langle b-a-bw\rangle \cong \mathbb{Z}[w]/\langle a-b+aw\rangle$$
$$\cong \mathbb{Z}[w]/\langle -b+w(a-b)\rangle \cong \mathbb{Z}[w]/\langle b-w(a-b)\rangle$$
$$\text{for } a,b\in\mathbb{Z}.$$

Now, we give our first main theorem characterizing the factor rings of $\mathbb{Z}[w]$.

2.2. Theorem

$$\mathbb{Z}[w]/\langle a\rangle \cong \Omega_a$$

where $a>1$ is an integer.

Proof. Let $\varphi:\mathbb{Z}[w]\to\Omega_a$ be given by $\varphi(p+rw)=\overline{p}+\overline{r}w$ where $\overline{x}$ is a residue class modulo a for any $x\in\mathbb{Z}$. Then, this is an epimorphism with the kernel $\langle a\rangle$. Indeed, since $\varphi(a)=\overline{a}=\overline{0}$, a is in Ker φ and conversely, if $p+rw\in$ Ker φ, then, $a|p$ and $a|r$ implying that $p+rw\in\langle a\rangle$. The result follows by First Isomorphism Theorem,

It is recalled from elementary abstract algebra when a factor ring of a commutative ring with unity is an integral domain or a field.

The following theorem and corallary state the situation that Ω_a is an integral domain or a field.

2.3. Theorem

Let $a>1$ be an integer. Then, Ω_a is a field iff a is a rational prime congruent to 2 modulo 3.

Proof. Suppose Ω_a is a field. It follows that a must be a prime. Since $\mathbb{Z}_2[w]$ is a field, a can be 2 and if $a>2$, then, a is a rational prime and $a \equiv 2$ (mod 3) by [4]. Conversely, let a be a rational prime congruent to 2 modulo 3. If $a=2$, the claim is true. Let $a>2$ and consider the ring homomorphism $\phi : \mathbb{Z}_a[x] \to \Omega_a$ given by $\phi(x)=w$. Since a is odd, *Ker* $\phi = \langle x^2+x+1 \rangle$. By First Isomorphism Theorem, $\Omega_a \cong \mathbb{Z}_a[x] / \langle x^2+x+1 \rangle$. Suppose that $x^2+x+1 \equiv 0(a)$ has a solution, say u. Thus, $u^2+u+1 \equiv 0(a)$ i.e $a \mid (u^2+u+1) = (u-w)(u-w^2)$ and a does not divide both $u-w$ and $u-w^2$ but a is a prime in $\mathbb{Z}[w]$. Contradiction. Then, x^2+x+1 is irreducible in $\mathbb{Z}_a[x]$ implyig that Ω_a is a field.

2.4. Corallary

Let $a>1$ be an integer. Then, Ω_a is an integral domain iff a is a rational prime congruent to 2 modulo 3.

We know give a lemma which we use later. It is a direct consequence of the equation

$$\frac{c+dw}{a+bw} = \frac{ac+bd-bc}{a^2-ab+b^2} + w\left(\frac{ad-bc}{a^2-ab+b^2}\right)$$

where $a,b,c,d \in \mathbb{Z}$.

2.5. Lemma

Let $a,b,c,d \in \mathbb{Z}$. Then, $c+dw \in \langle ak+bkw \rangle$ iff $k\left(a^2-ab+b^2\right) \mid (ac+bd-bc)$ and $k\left(a^2-ab+b^2\right) \mid (ad-bc)$.

We now state our second main theorem characterizing the factor rings of $\mathbb{Z}[w]$.

2.6. Theorem Let $a,b\in\mathbb{Z}$ and $(a,b)=1$. Then, $\mathbb{Z}[w]/\langle a+bw\rangle \cong \mathbb{Z}_{a^2-ab+b^2}$

Proof. Before all else, Remark 2.1. allows us to assume without lost of generality that a and b are both positive. Now, we can prove the theorem: Since $(a,b)=1$, $(b,a^2-ab+b^2)=1$ so a has an inverse, say a^{-1} , in $\mathbb{Z}_{a^2-ab+b^2}$ and also note that since $a^2-ab+b^2\equiv 0\left(a^2-ab+b^2\right)$, $\left(ab^{-1}\right)^2\equiv ab^{-1}-1\left(a^2-ab+b^2\right)$. Let us define $\psi:\mathbb{Z}[w]\to\mathbb{Z}_{a^2-ab+b^2}$ by $\psi(x+yw)=x-ab^{-1}y$ modulo a^2-ab+b^2. It is easy to see that ψ is onto and preserves addition. We use the congruence $\left(ab^{-1}\right)^2\equiv ab^{-1}-1\left(a^2-ab+b^2\right)$ to see that ψ preserves multiplication:

Let $\gamma=x_1+y_1w$ and $\delta=x_2+y_2w$. Then, we have

$$\begin{aligned}
\psi(\gamma)\psi(\delta) &= \psi(x_1+y_1w)\psi(x_2+y_2w)\\
&=\left(x_1-ab^{-1}y_1\right)\left(x_2-ab^{-1}y_2\right)\\
&=x_1x_2-ab^{-1}x_1y_2-ab^{-1}y_1x_2+\left(ab^{-1}\right)^2y_1y_2\\
&=x_1x_2-y_1y_2-ab^{-1}\left(x_1y_2+y_1x_2-y_1y_2\right)\\
&=\psi\left(x_1x_2-y_1y_2+\left(x_1y_2+y_1x_2-y_1y_2\right)w\right)\\
&=\psi\left((x_1+y_1w)(x_2+y_2w)\right)\\
&=\psi(\gamma\delta)
\end{aligned}$$

Furthermore, the kernel of ψ is $\langle a+bw\rangle$. Indeed, because $\psi(a+bw)=a-ab^{-1}b\equiv 0\ \left(a^2-ab+b^2\right)$, $\langle a+bw\rangle\subseteq Ker\ \psi$. Conversely, let $c+dw\in Ker\ \psi$ and $c+dw=(a+bw)(x+yw)$ where $x,y\in\mathbb{Q}$. Since $\psi(c+dw)=c-ab^{-1}d\equiv 0$ modulo a^2-ab+b^2, $bc-ad\equiv 0\left(a^2-ab+b^2\right)$ implying that y is an integer and also

$$bc-ad\equiv 0\left(a^2-ab+b^2\right)\Rightarrow ab^2c-a^2bd\equiv 0\left(a^2-ab+b^2\right)$$
$$\Rightarrow ac-\left(ab^{-1}\right)^2bd\equiv 0\left(a^2-ab+b^2\right)$$
$$\Rightarrow ac-ad+bd\equiv 0\left(a^2-ab+b^2\right)$$

Thus, $a^2-ab+b^2\,\middle|\,ad-bc$ and $a^2-ab+b^2\,\middle|\,ac-ad+bd$ imply that $a^2-ab+b^2\,\middle|\,ac+bd-bc$ which makes x an integer. Since x, y in $\mathbb{Z}$, we have $Ker\ \psi\subseteq\langle a+bw\rangle$.

The required result follows by First Isomorphism Theorem.

The following corallaries are about when $\mathbb{Z}[w]/\langle a+bw\rangle$ is a field or an integral domain:

2.7. Corallary

Let $a,b\in\mathbb{Z}$ and $(a,b)=1$. Then, $\mathbb{Z}[w]/\langle a+bw\rangle$ is a field iff a^2-ab+b^2 is a rational prime.

2.8. Corallary

Let $a,b\in\mathbb{Z}$ and $(a,b)=1$. Then, $\mathbb{Z}[w]/\langle a+bw\rangle$ is an integral domain iff a^2-ab+b^2 is a rational prime.

Thanks to Corallary 2.8 we get the following corallary:

2.9. Corallary

Let $a,b\in\mathbb{Z}$ and $(a,b)=1$. Then, $a+bw$ is a prime in $\mathbb{Z}[w]$ iff a^2-ab+b^2 is a rational prime congruent to 1 modulo 3.

We know prove our third main theorem about the elements of any factor ring of $\mathbb{Z}[w]$:

2.10. Theorem

Let $a,b,t\in\mathbb{Z}^+$ and $(a,b)=1$. Then,

$$\mathbb{Z}[w]/\langle at+btw\rangle=\left\{[x+yw]:0\le x<t\left(a^2-ab+b^2\right),0\le y<t\right\}$$

where $[x+yw]=x+yw+\langle at+btw\rangle$.

Proof. We first show that the equivalence classes given in the theorem are distinct: Let $[x_1+y_1w]=[x_2+y_2w]$ with $0\le x_1,x_2<t(a^2-ab+b^2)$ and $0\le y_1,y_2<k$. It means that $x_2-x_1+(y_2-y_1)w\in\langle at+btw\rangle$. Appealing Lemma 2.5., we get

$$t(a^2-ab+b^2)\,\big|\,a(x_2-x_1)+b(y_2-y_1)-b(x_2-x_1)$$

(1)

and

$$t(a^2-ab+b^2)\,\big|\,a(y_2-y_1)-b(x_2-x_1)$$

(2)

Using (1) and (2) , we have the followings:

$$t(a^2-ab+b^2)\,\big|\,a^2y_2-a^2y_1-a^2x_2+a^2x_1-aby_2+aby_1$$

(3)

$$t(a^2-ab+b^2)\,\big|\,-a^2x_1+a^2x_2+b^2y_2-b^2y_1+aby_2-aby_1-b^2x_2+b^2x_1$$

(4)

$$t(a^2-ab+b^2)\,\big|\,-aby_2+aby_1+b^2x_2-b^2x_1$$

(5)

By (4) and (5), we get

$$t(a^2-ab+b^2)\,\big|\,a^2x_2-a^2x_1+b^2y_2-b^2y_1$$

(6)

and by (3) and (6) , we get

$$t(a^2-ab+b^2)\,\big|\,a^2y_2-aby_2+b^2y_2-a^2y_1+aby_1-b^2y_1=(y_2-y_1)(a^2-ab+b^2)$$

which simplifies to the statement that $t\,|\,y_2-y_1$ and so this requires $y_1=y_2$. Thus, $t(a^2-ab+b^2)\,\big|\,a(x_2-x_1)-b(x_2-x_1)$ and $t(a^2-ab+b^2)\,\big|\,b(x_2-x_1)$ imply that $x_1=x_2$.

We now show that any $x+yw$ is in one of the equivalence classes given in the theorem: There exists integers s_1 and s_2 such that $ats_1+bts_2=t$ because $(a,b)=1$. Using this, we see that $tw-(at+btw)ws_1-(at+btw)s_2-(at+btw)s_1$ is a real number. This means that tw is congruent to a real number modulo $at+btw$ so that $[x+yw]=[x'+y'w]$ for some $0\leq y'<t$ and also it is clear that $t(a^2-ab+b^2)\in\langle at+btw\rangle$ imply that $[x+yw]=[x''+y''w]$ for some $0\leq x''<t(a^2-ab+b^2)$. Thus, we have the required result.

2.10 Theorem gives us the following nice result:

2.11. Corallary

For any $a,b\in\mathbb{Z}$ with $(a,b)=1$, the characteristic of the factor ring $\mathbb{Z}[w]/\langle at+btw\rangle$ is $|t|(a^2-ab+b^2)$.

This corallary produces the following corallary:

2.12. Corallary

For any $a,b,t\in\mathbb{Z}$ with $(a,b)=1$ and $t>1$, $\mathbb{Z}[w]/\langle at+btw\rangle$ is a commutative ring with identiy but not an integral domain and so certainly not a field.

Given a nonzero Eisenstein integer $a+bw$, we know that we can factor it in the manner

$$a+bw=\mp w^d.\prod\sigma_m{}^{u_m}.\prod\sigma_m'{}^{v_m}.\prod p_m{}^{e_m}.(1-w)$$

where $N(\sigma_m)$ and $N(\sigma_m')$ are rational primes congruent to 1 modulo 3, p_m is a rational prime congruent to 2 modulo 3 and $d,u_m,v_m,e_m,n\in\mathbb{Z}^+$. Also we can assume that $u_m\leq v_m$ without lost of generality. (Here note that $N(a+bw)=(a+bw)(a+bw^2)$ for any $a+bw\in\mathbb{Z}[w]$).

Let $s_1 = \prod \left[N\left(\sigma_m\right)\right]^{u_m}$, $s_2 = \prod \left[N\left(\sigma'_m\right)\right]^{v_m}$ and $t = \prod p_m{}^{e_m}$.(Note that $s_1 | s_2$)

We now give our forth main theorem about the factors of any factor ring of $\mathbb{Z}[w]$:

2.13. Theorem Let $a, b \in \mathbb{Z}$ not both zero. Then, with the notation above and with $\theta_n = \mathbb{Z}[w] / \left\langle (1-w)^n \right\rangle$, the following hold:

$$\mathbb{Z}[w]/\langle a+bw\rangle \cong \mathbb{Z}_{s_1} \oplus \mathbb{Z}_{s_2} \oplus \Omega_t \oplus \Omega_{3^{n/2}}$$

for even n and

$$\mathbb{Z}[w]/\langle a+bw\rangle \cong \mathbb{Z}_{s_1} \oplus \mathbb{Z}_{s_2} \oplus \Omega_t \oplus \theta_n$$

for odd n.

Proof. We can write

$$a+bw = \mp w^d . \prod \sigma_m{}^{u_m} . \prod \sigma'_m{}^{v_m} . \prod p_m{}^{e_m} . (1-w) \tag{7}$$

Since $\mathbb{Z}[w]$ is an Euclidean domain, we can apply the Euclidean algorithm to any two relatively prime elements $x, y \in \mathbb{Z}[w]$ to find s and t such that $sx+ty=1$. It follows that $\langle x\rangle + \langle y\rangle = \mathbb{Z}[w]$. We can also say that $\langle x\rangle \cap \langle y\rangle = \langle xy\rangle$ and thus, we can use the Chinese Remainder Theorem for rings (see [4, p.331] to have

$$\mathbb{Z}[w]/\langle xy\rangle \cong \mathbb{Z}[w]/\langle x\rangle \oplus \mathbb{Z}[w]/\langle y\rangle$$

Applying this to (7), we get

$$\begin{aligned} \mathbb{Z}[w]/\langle a+bw\rangle &\cong \mathbb{Z}[w]/\left\langle \prod \sigma_m{}^{u_m} \right\rangle \oplus \mathbb{Z}[w]/\left\langle \prod \sigma'_m{}^{u_m} \right\rangle \\ &\quad \oplus \mathbb{Z}[w]/\left\langle \prod p_m{}^{e_m} \right\rangle \oplus \mathbb{Z}[w]/\left\langle (1-w)^n \right\rangle \end{aligned} \tag{8}$$

We now show that (8) implies the result given in the theorem: Write $\prod \sigma_m{}^{u_m} = c+dw$. Any rational prime q with $q \equiv 2 (mod\ 3)$ is a prime in $\mathbb{Z}[w]$ and so does not divide $c+dw$. For any rational prime

prime with $q \equiv 1(mod\ 3)$ we have $q = \sigma_m \sigma'_m$ for some m whence q can not divide $c + dw$. Thus, $(c,d) = 1$. By Theorem 2.6 we get

$$\begin{aligned}\mathbb{Z}[w] / \langle \prod \sigma_m{}^{u_m} \rangle &= \mathbb{Z}[w] / \langle c + dw \rangle \\ &\cong \mathbb{Z}_{c^2 - cd + d^2} \\ &\cong \mathbb{Z}_{s_1}\end{aligned}$$

Likewise we get

$$\mathbb{Z}[w] / \langle \prod \sigma'_m{}^{u_m} \rangle \cong \mathbb{Z}_{s_2}$$

Thanks to Therem 2.2. the third term is isomorphic to Ω_t and clearly the fourth term is θ_n.

Now, let n be even. Since $(1-w)^2 = -3w$,

$$\langle (1-w)^n \rangle = \langle \left[(1-w)^2\right]^{n/2} \rangle = \langle (-3w)^{n/2} \rangle = \langle 3^{n/2} \rangle$$

Thus, $\mathbb{Z}[w] / \langle (1-w)^n \rangle \cong \mathbb{Z}[w] / \langle 3^{n/2} \rangle \cong \Omega_{3^{n/2}}$

For odd values of n, we have the following theorem for θ_n:

2.14. Theorem Let $k \geq 0$ be an integer. Then,

$$\theta_{2k+1} \cong \mathbb{Z}[x] / \langle 3^k x, 3^{k+1}, x^2 - 3x + 3 \rangle$$

Proof. Since

$$(1-w)^{2k+1} = (1-w)(1-w)^{2k} = (1-w)(-3w)^k$$

we have $\langle (1-w)^{2k+1} \rangle = \langle 3^k (1-w) \rangle$. By (8), the elements of θ_{2k+1} are the equivalence classes $[a + bw]$ with $0 \leq a < 3^{k+1}$ and $0 \leq b < 3^k$ whence θ_{2k+1} has 3^{2k+1} elements.

Let $I = \langle 3^k x, 3^{k+1}, x^2 - 3x + 3 \rangle$. Then,

$$\mathbb{Z}[x]/I = \{[c + dx] : 0 \le c < 3^{k+1}, 0 \le d < 3^k\}$$

i.e it has the same number elements as θ_{2k+1}

Let $\psi : \mathbb{Z}[x] \to \theta_{2k+1}$ be defined by $\psi(p(x)) = [p(1-w)]$. Clearly it is an epimorphism. Since $\psi(3^k x) = [3^k(1-w)] = [0]$, $3^k x \in Ker\ \psi$. Also since both 3^{k+1} and $x^2 - 3x + 3$ in $Ker\ \psi$, we see that $I \subseteq Ker\ \psi$. On the other hand let $p(x) \in Ker\ \psi$. Since $x^2 - 3x + 3$ is monic, we can write $p(x) = (x^2 - 3x + 3)q(x) + r(x)$ where $q(x), r(x) \in \mathbb{Z}[x]$ and $r(x) = r_0 + r_1(1-x)$. Since $r(x) \in Ker\ \psi$, $r_0 + r_1 w \in \langle 3^k(1-w) \rangle$ say $r_0 + r_1 w = 3^k(1-w)(\gamma_1 + \gamma_2 w)$. Thus, we get $r(x) = 3^{k+1}\gamma_2 + 3^k(\gamma_1 - 2\gamma_2)x \in I$. Therefore $p(x) \in I$ and so $Ker\ \psi = I$. Then, it is followed the required result.

Acknowledgements

We would like to thank Prof. Dr. Greg Dresden for his helpful discussions.

REFERENCES

Dresden G. and Dymacek W.M. (2005). Finding factors of factor rings over the Gaussian integers, *The American Mathematical Monthly*, 112(7), 602-611.

Gallian J. A. (1990). *Contemporary Abstract Algebra.*, Houghton Mi- in.

Misaghian M, (2009). Factor rings and their decompositionsof an imaginary extension of the ring of integers, *International Mathematical Forum*, 4 (42), 2075-2086.

Alkam O, Osba E. A., (2010). On Eisenstein integers modulo n, *International Mathematical Forum*, 5(22), 1075-1082.

***