



UZEM | ONDOKUZ MAYIS ÜNİVERSİTESİ
UZAKTAN EĞİTİM MERKEZİ



1

Ondokuz Mayıs Üniversitesi
Fen Edebiyat Fakültesi
Matematik Bölümü
Dijital Ders Platformu

Cebir 2

Tamlik Bölgesinde Aritmetik

Prof. Dr. Şenol EREN

Ders 11

Tanım 5.17 R bir tamlık bölgesi olsun. $d: R \rightarrow \mathbb{Z}$ fonksiyonu aşağıdaki özellikleri sağlarsa R 'ye Eulid Bölgesi denir ve kısaca EB ile gösterilir.

i) $\forall x \in R$ için $d(x) \geq 0$

ii) $d(x) = 0 \iff x = 0_R$

iii) $\forall x, y \in R$ için $d(xy) = d(x) \cdot d(y)$

iv) $\forall x, y \in R, y \neq 0_R$ için $x = qy + r, 0 \leq d(r) < d(y)$ olacak şekilde $\exists q, r \in R$ bulunabilir.

Tanım 5.18 d fonksiyonu i-ii-iii sağlarsa Garpımsal norm, (iv) özelliğindedir bölme algoritması veya Eulid algoritması denir.

Örnek 5.19 \mathbb{Z} bir E.B dir. $d: \mathbb{Z} \rightarrow \mathbb{Z}$ $a \in \mathbb{Z}$ için $d(a) = |a|$ fonksiyonu alınırsa

$\forall a \in \mathbb{Z}$ için $d(a) = |a| \geq 0$, $d(a) = |a| = 0 \Leftrightarrow a = 0$

$\forall a, b \in \mathbb{Z}$ için $d(ab) = |a \cdot b| = |a| \cdot |b| = d(a)d(b)$ ve

$\forall a, b \in \mathbb{Z}$, $b \neq 0$ olmak üzere $a = bq + r$, $0 \leq r < |b|$ yani $0 \leq d(r) < d(b)$ olacak şekilde $\exists q, r \in \mathbb{Z}$ bulunabilir.

Örnek 5.20 F cisim ise $F[x]$ E.B dir. F cisim olduğundan T.B dir. F TB ise $F[x]$ T.B dir.

$$d: F[x] \rightarrow \mathbb{Z} \quad d(f) = \begin{cases} 2^{d^0 f}, & f \neq 0 \text{ ise} \\ 0, & f = 0 \text{ ise} \end{cases}$$

şeklinde tanımlanan d fonksiyonu i-ii-iii-iv şartlarını sağlar (gösteriniz)

Teorem 5.21 R bir EB ise TIB dir.

İspat: R bir EB ve I R 'nin bir ideali olsun.

$I = (0)$ ise I temel idealdir. $I \neq (0)$ olsun. I idealinde sıfırdan farklı $d(a)$ en küçük tam sayı olacak şekilde bir $a \in I$ alalım. $(a) \subset I$ dir. Tersine $\forall x \in I$ için R EB olduğundan $x = qa + r$, $0 \leq d(r) < d(a)$ olacak şekilde $\exists q, r \in R$ vardır. $r \neq 0$ ise $r = x - qa \in I$ olacağından $d(r) < d(a)$ olması a 'nın seçimi ile çelişir. $r = 0$ olup $x = qa \in (a)$ bulunur. $I \subset (a)$ olur.

Buradan $I = (a)$ olup I temel idealdir.

Sonuç 5.22 R EB ise TAG dir.

Tanım 5.23 $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ TB'ne Gauss Tam Sayılar Bölgesi denir.

Teorem 5.24 $\mathbb{Z}[i]$ Bölgesi EB dir.

İspat: $d: \mathbb{Z}[i] \rightarrow \mathbb{Z}$ $d(a+bi) = |a+bi|^2 = a^2+b^2$ ile tanımlayalım.

i) $\forall a+bi \in \mathbb{Z}[i]$, $d(a+bi) = a^2+b^2 \geq 0$ dir.

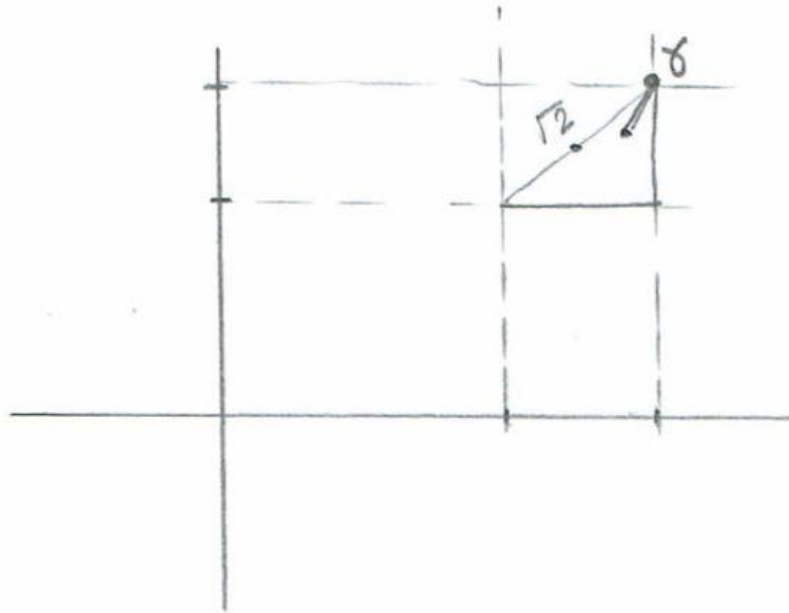
ii) $d(a+bi) = 0 \iff a^2+b^2 = 0 \iff a=b=0$ dir.

iii) $\forall a+bi, c+id \in \mathbb{Z}[i]$ için $d[(a+bi) \cdot (c+id)] = d[(ac-bd)+i(ad+bc)]$
 $= (ac-bd)^2 + (ad+bc)^2 = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$
 $= a^2(c^2+d^2) + b^2(c^2+d^2)$
 $= (a^2+b^2)(c^2+d^2)$
 $= d(a+bi) \cdot d(c+id)$ bulunur.

iv) $\alpha, \beta \in \mathbb{Z}[i]$ ve $\beta \neq 0$ olsun. $\frac{\alpha}{\beta} \in \mathbb{C}$ olup düzlemde bir noktaya karşılık gelir. Bu noktanın kenarına veya içine düştüğü birim kareyi düşünelim. $\frac{\alpha}{\beta}$ ya en yakın olan köşe $\gamma \in \mathbb{Z}[i]$ olsun.

$$\left| \frac{\alpha}{\beta} - \gamma \right| \leq \frac{\sqrt{2}}{2} \Rightarrow \left| \frac{\alpha}{\beta} - \gamma \right|^2 \leq \frac{1}{2} \Rightarrow |\alpha - \beta\gamma|^2 \leq \frac{1}{2}|\beta|^2 < |\beta|^2$$

olup $d(\alpha - \beta\gamma) < d(\beta)$ olur. $\alpha - \beta\gamma = \delta \in \mathbb{Z}[i]$ dersek $\alpha = \beta\gamma + \delta$ ve $d(\delta) < d(\beta)$ olacak şekilde $\exists \gamma, \delta \in \mathbb{Z}[i]$ vardır.



Sonuç 5.25 $\mathbb{Z}[i]$ EB olduğundan TİB ve TAG dir.

Teorem 5.26 $\mathbb{Z}[i]$ de $a+bi | c+di \Rightarrow \mathbb{Z}$ de $d(a+bi) | d(c+di)$ dir.

İspat: $a+bi | c+di \Rightarrow c+di = (a+bi)(e+fi)$, $e+fi \in \mathbb{Z}[i]$
 Buradan $d(c+di) = d[(a+bi)(e+fi)] = d(a+bi)d(e+fi)$
 olup $d(a+bi) | d(c+di)$ bulunur.

Teorem 5.27 $d(a+bi)$, \mathbb{Z} 'de asalsa $a+bi$, $\mathbb{Z}[i]$ 'de asaldır.

İspat: $a+bi$ asal olmasa $a+bi = (r+si)(u+vi)$
 ($r+si, u+vi \in \mathbb{Z}[i]$) şeklinde asiker olmayan bir
 çarpımlara ayrılır. $r+si, u+vi \neq 1, \bar{i}$ aritmetik birimlerinden
 farklıdır. O halde $d(a+bi) = d(r+si)d(u+vi)$ olup
 $d(r+si) > 1$, $d(u+vi) > 1$ olup $d(a+bi)$ sayısının asal olmasıyla
 çelişir. Şu halde $a+bi$, $\mathbb{Z}[i]$ 'de asal olmak zorundadır.

Örnek 5.28 $5 \in \mathbb{Z}[i]$ -yi asal çarpanlarını bulalım.

$a+bi \mid 5$ olsun $d(a+bi) = a^2+b^2 \mid 25$ $a^2+b^2 \rightarrow 1, 5, 25$ olabilir.

$a^2+b^2 = 1$ v 25 ise $a+bi$, 5'in asikar bölenidir.

$$a^2+b^2 = 5 \Rightarrow a^2=4, b^2=1 \Rightarrow a = \pm 2, b = \pm 1$$

$$a^2=1, b^2=4 \Rightarrow a = \pm 1, b = \pm 2$$

$a+bi$ için $\pm(2+i)$, $\pm(2-i)$, $\pm(1+2i)$, $\pm(1-2i)$ sayıları

söz konusu olur. $5 = (2+i)(2-i)$

$d(2+i) = 5$ asal olduğundan $2+i$, $\mathbb{Z}[i]$ de asaldır.

$\pm(1+2i)$ ve $\pm(1-2i)$ $2+i$ ile ilgilidir.

Örnek 5.29 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ TB-i TAG değildir.

$\forall \alpha = a + b\sqrt{-5}$ elemanı için $d(\alpha) = a^2 + 5b^2$ ile $d: \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{Z}$ fonksiyonu bir çarpımsal normdur. (Gösteriniz)

$9 = 3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ olduğundan 3, $2 + \sqrt{-5}$, $2 - \sqrt{-5}$ elemanları $\mathbb{Z}[\sqrt{-5}]$ indirgenemezdir.

$\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ için $\alpha \cdot \beta = 3 \Rightarrow d(\alpha)d(\beta) = 9$, $d(\alpha) = 1, 3, 9$ olabilir. $d(\alpha) = 1 \vee 9$ ise asikor bölendir.

$d(\alpha) = 3 = a^2 + 5b^2$, olacak şekilde $a, b \in \mathbb{Z}$ yoktur.

3 indirgenemezdir. Benzer şekilde $2 + \sqrt{-5}$ ve $2 - \sqrt{-5}$ 'inde indirgenemez olduğu gösterilebilir.

Örnek 5.30 $\mathbb{Z}[i\sqrt{5}]$ halkasında 3 asal değildir.

$$3 \mid (1+i\sqrt{5})(1-i\sqrt{5}) = 6 \Rightarrow 3 \mid 1+i\sqrt{5} \vee 3 \mid 1-i\sqrt{5} \text{ olmalı}$$

$$3 \mid 1+i\sqrt{5} \text{ olsun } 1+i\sqrt{5} = 3(a+bi\sqrt{5}) \Rightarrow 1 = 3a \Rightarrow$$

$$a = \frac{1}{3} \in \mathbb{Z} \text{ ilişkisi elde edilir. } 3 \nmid 1+i\sqrt{5} \text{ dir.}$$

Benzer şekilde $3 \nmid 1-i\sqrt{5}$ olduğunda gösterilebilir.

0 halde $3 = 3+0i\sqrt{5}$, $\mathbb{Z}[i\sqrt{5}]$ de asal değildir.



UZEM | ONDOKUZ MAYIS ÜNİVERSİTESİ
UZAKTAN EĞİTİM MERKEZİ



Ondokuz Mayıs Üniversitesi
Fen Edebiyat Fakültesi
Matematik Bölümü
Dijital Ders Platformu

Teşekkürler

Prof. Dr. Şenol EREN

Cebir II

Ders 11