T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ESAS İDEAL BÖLGELERİ VE EUCLİD BÖLGELERİ

YÜKSEK LİSANS TEZİ

Reyhan KARADELİOĞLU

Enstitü Anabilim Dalı : MATEMATİK

Tez Danışmanı : Doç. Dr. Refik KESKİN

Haziran 2006

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ESAS İDEAL BÖLGELERİ ve EUCLİD BÖLGELERİ

YÜKSEK LİSANS TEZİ

Reyhan KARADELİOĞLU

Enstitü Anabilim Dalı : MATEMATİK

Bu tez 22 / 06 / 2006 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Doç. Dr. Refik KESKİN	**Doç. Dr. Murat TOSUN**	**Doç. Dr. İbrahim OKUR**
Jüri Başkanı	**Üye**	**Üye**

TEŞEKKÜR

Değerli hocam Doç. Dr. Refik KESKİN'e, tez çalışmamız boyunca beni sabırla dinlediği, bilgi ve birikimini paylaştığı ve verdiği destek için, dostum olmasından onur duyduğum Araş. Gör. Bahar DEMİRTÜRK'e, fikir ve önerilerini paylaştığı için, beni bugüne getiren, hiçbir fedakarlıktan çekinmeyen ve haklarını ödememin mümkün olmadığını çok iyi bildiğim, annem ve babamla ağabeyim Hakan ve kardeşim Emel'e şükranlarımı sunarım.

Reyhan KARADELİOĞLU

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

$a \mid b$	: a böler b
$a \nmid b$	: a bölmez b
$a \sim b$	: a ilgili b
$a \not\sim b$	: a ilgili değil b
$\langle a \rangle$	: a'nın ürettiği ideal
$\langle a,b \rangle$	: a ve b'nin ürettiği ideal
D/I	: Bölüm ideali
$\widetilde{D}$	: Birim elemanlar ve sıfırın oluşturduğu küme
$\mathbb{Q}$	: Rasyonel sayılar kümesi
$\mathbb{R}$	: Reel sayılar kümesi
U(D)	: D'nin birim elemanlarının kümesi
$\mathbb{Z}$	: Tam sayılar kümesi
$\subset$	: Alt küme
$\Rightarrow$	: İse
$\Leftrightarrow$	: Ancak ve ancak
$\left(\frac{m}{p}\right)$	: Legendre sembolü
$[\![\ ]\!]$	: Tam değer
p$\|\|a$	: p tam böler a

ÖZET

Anahtar Kelimeler: Tamlık bölgesi, Euclid bölgesi, Esas ideal bölgesi, Tek türlü parçalanmalı bölge.

Bu tez 4 bölümden oluşmaktadır. Birinci bölüm halka teorisiyle ilgili temel kavramları kapsamaktadır. İkinci bölümde tamlık bölgeleri ve esas ideal bölgeleri incelenmiştir. Üçüncü bölümde m karesiz tam sayı olmak üzere $m \not\equiv 1 \pmod 4$ ise, $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ ve $m \equiv 1 \pmod 4$ ise $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ tamlık bölgeleri incelenmiştir. Bu tamlık bölgelerinin Euclid bölgesi olması için gerekli ve yeterli şartlar verilmiştir. Ayrıca $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{-19}}{2}\right)$ tamlık bölgesinin esas ideal bölgesi olduğu fakat Euclid bölgesi olmadığı gösterilmiştir. Son bölüm tek türlü parçalanmalı bölgelerle ilgilidir. Ayrıca m'nin hangi değerleri için yukarıdaki tamlık bölgelerinin tek türlü parçalanmalı bölge olduğu incelenmiştir. Son olarak tek türlü parçalanmalı bölgeler kullanılarak bazı Diophant denklemleri çözülmüştür.

PRINCIPAL IDEAL DOMAINS AND EUCLID DOMAINS

SUMMARY

Keywords: Integral domain, Euclid domain, Principle ideal domain, Unique factorization domain

This thesis consists of four chapters. First chapter covers the fundamental concept of ring theory. In the chapter 2, integral domains and principical ideal domains are investigated. In the chapter 3, the integral domains $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ and $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ are studied. A necessary and sufficient condition for the above integral domains to be an Euclidean domain is given. Morever, it is shown that $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{-19}}{2}\right)$ is a principical ideal domain but not an Euclidean domain. The last chapter is related to unique factorization domains. In this chapter, we show that the above integral domains are unique factorization domains for some values of m. Lastly we used the unique factorization domains in order to solve some Diophant equations.

BÖLÜM 1. GİRİŞ

1.1 Temel Tanımlar ve Teoremler

Tanım 1.1.1: $R \neq \varnothing$ bir küme ve $.,+$ R'de tanımlı iki işlem olsun. Aşağıdaki şartlar sağlanıyorsa, R'ye bir halka denir ve R halkası bazen $(R,.,+)$ ile gösterilir:

1) $(R,+)$ bir değişmeli gruptur.

2) $(R,.)$ bir yarı gruptur (Yani $a,b \in R$ ise $a.b \in R$ ve $a(bc) = (ab)c$ 'dir.).

3) $a.(b+c) = a.b + a.c$ (.'nın + üzerine soldan dağılma özelliği vardır.)

$a.b$ yerine genellikle ab yazılır. $(R,+)$'nın birim (etkisiz) elemanı 0 ile gösterilir ve halkanın sıfır elemanı olarak adlandırılır. a'nın +'ya göre tersini $-a$ ile göstereceğiz ve $a+(-b)$ yerine de $a-b$ yazacağız.

Teorem 1.1.2: $(R,+,.)$ bir halka olsun. $(R,+,.)$ halkası aşağıdaki özellikleri sağlar:

1) $a.0 = 0.a = 0$

2) $a.(-b) = -ab = (-a).b$

3) $(-a).(-b) = ab$

4) $a(b-c) = ab - ac$

5) $(b-c)a = ba - ca$

İspat: 1) $a.0 = a(0+0) = a.0 + a.0$, $a.0$'ın tersini her iki tarafa eklersek,

$$-a.0 + a.0 = a.0 + a.0 + (-a).0$$

buluruz. Bu durumda $0 = a.0 + 0 = a.0$ elde edilir. Benzer şekilde $0.a = 0$ olduğu gösterilir.

2) $a.(-b)=-ab$ olduğunu göstermek için $ab+\left(a\left(-b\right)\right)=0$ olduğunu görmek yeterlidir. $ab+a.(-b)=a.\left(b+\left(-b\right)\right)=a.0=0$ olup, ab'nin tersi $-ab$ elemanı $a.\left(-b\right)$ olur. Yani $-ab=a\left(-b\right)$'dir.

3) 2. özellik yardımıyla, $\left(-a\right).\left(-b\right)=-a.\left(-b\right)=-\left(ab\right)=ab$ elde edilir.

4) $a\left(b-c\right)=a.\left(b+\left(-c\right)\right)=ab+\left(-ac\right)=ab-ac$ olur.

5) $\left(b-c\right).a=\left(b+\left(-c\right)\right).a=ba+\left(-ca\right)=ba-ca$ bulunur.

Örnek 1.1.3: $\left(\mathbb{Z},+,.\right)$ ve $\left(\mathbb{Q},+,.\right)$ birer halkadır.

Örnek 1.1.4: R=$\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}:a,b,c,d\in\mathbb{R}\right\}$ kümesinde + ve . işlemleri,

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

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}.\begin{pmatrix}a* & b*\\ c* & d*\end{pmatrix}=\begin{pmatrix}aa*+bc* & ab*+bd*\\ ca*+dc* & cb*+dd*\end{pmatrix}$$

olarak tanımlanırsa $\left(R,+,.\right)$ bir halkadır. $M_{2\times2}\left(R\right)$'nin sıfır elemanı $\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$ ve $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ matrisinin +'ya göre tersi $\begin{pmatrix}-a & -b\\ -c & -d\end{pmatrix}$'dir.

Tanım 1.1.5: $\left(R,+,.\right)$ bir halka ve $a,b\in R$ olsun. $a.b=0$ iken $a=0$ veya $b=0$ oluyorsa R'ye sıfır bölensiz halka denir.

Sıfır bölensiz bir halkada kısaltma yapılabilir. Yani $\left(R,+,.\right)$ sıfır bölensiz bir halka olsun. Eğer $ab=ac$ ve $a\neq0$ ise $b=c$'dir ($ba=ca$ ve $a\neq0$ ise $b=c$'dir.). $\mathbb{Z}$ tam sayılar kümesi olmak üzere $\left(\mathbb{Z},+,.\right)$ bir sıfır bölensiz halkadır. Ayrıca p asal ise $\mathbb{Z}_p=\left\{\bar{0},\bar{1},...,\overline{p-1}\right\}$ sıfır bölensiz bir halkadır. Fakat $\mathbb{Z}_{10}=\left\{\bar{0},\bar{1},\bar{2},...,\bar{9}\right\}$ sıfır bölensiz bir halka değildir. Çünkü $\bar{2}.\bar{5}=\overline{10}=\bar{0}$'dir.

Tanım 1.1.6: $p, m \in \mathbb{Z}$ olmak üzere $p^2 \mid m$ olacak biçimde bir p asal sayısı yoksa m'ye karesiz tamsayı denir.

BÖLÜM 2. TAMLIK BÖLGELERİ

2.1. Tamlık Bölgeleri

Tanım 2.1.1: Çarpma işlemine göre birim elemana sahip, sıfır böleni olmayan değişmeli halkaya tamlık bölgesi denir.

D tamlık bölgesi olsun. Her $a \in D$, $a \neq 0$ için $a.b = 1$ olacak biçimde $b \in D$ varsa D'ye cisim denir.

Örnek 2.1.2: Tamsayılar halkası $\mathbb{Z} = \{0, \mp 1, \mp 2, ...\}$ bir tamlık bölgesidir.

Örnek 2.1.3: $\mathbb{Z} + \mathbb{Z}i = \{a + bi : a, b \in \mathbb{Z}\}$ bir tamlık bölgesidir. $\mathbb{Z} + \mathbb{Z}i$'ye Gauss tamsayılar halkası denir. $\mathbb{Z} + \mathbb{Z}i$'nin elemanlarına da Gauss tamsayıları denir.

Örnek 2.1.4: $w = \left(-1 + \sqrt{-3}\right)\Big/2$, birimin küp kökü olmak üzere, $\mathbb{Z} + \mathbb{Z}w = \{a + bw : a, b \in \mathbb{Z}\}$ bir tamlık bölgesidir. $\mathbb{Z} + \mathbb{Z}w$'nın elemanları Einstein tamsayıları ve $\mathbb{Z} + \mathbb{Z}w$ Einstein Bölgesi olarak adlandırılır. $w^3 = 1$ denkleminin diğer kompleks küp kökü $w^2 = \overline{w} = \left(-1 + \sqrt{-3}\right)/2$'dir. Burada $\sqrt{-3} = \sqrt{3}i$'dir.

$$w^2 = (\frac{-1+\sqrt{-3}}{2})(\frac{-1+\sqrt{-3}}{2}) = \frac{1-\sqrt{-3}-\sqrt{-3}-3}{4} = \frac{-2-2\sqrt{-3}}{4} = \frac{-1-\sqrt{-3}}{2} = \overline{w}$$

ve

$$-w-1 = -(\frac{-1+\sqrt{-3}}{2}) - 1 = \frac{1-\sqrt{-3}-2}{2} = \frac{-1-\sqrt{-3}}{2} = w^2$$

olduğundan $w^2 = -w - 1$'dir. Aynı zamanda, $\mathbb{Z} + \mathbb{Z}w = \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{-3}}{2})$ olarak yazılacaktır.

Örnek 2.1.5: m karesiz pozitif veya negatif bir tamsayı olmak üzere, $\mathbb{Z} + \mathbb{Z}\sqrt{m} = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$ bir tamlık bölgesidir.

Örnek 2.1.6: m karesiz ve $m \equiv 1 (\mathrm{mod}\, 4)$ bir tamsayı olmak üzere

$$\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{m}}{2}) = \{a + b(\frac{1+\sqrt{m}}{2}) : a, b \in \mathbb{Z}\}$$

bir tamlık bölgesidir. Eğer $m \not\equiv 1 (\mathrm{mod}\, 4)$ olursa $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{m}}{2})$ çarpmaya göre kapalı olmadığından tamlık bölgesi değildir. Çünkü

$$\frac{1+\sqrt{m}}{2}, 1 - \frac{1+\sqrt{m}}{2} \in \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{m}}{2})$$

alırsak

$$(\frac{1+\sqrt{m}}{2})(1 - \frac{1+\sqrt{m}}{2}) = (\frac{1+\sqrt{m}}{2})(\frac{1-\sqrt{m}}{2}) = \frac{1-m}{4} \notin \mathbb{Z}$$

dir. $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{m}}{2})$ tamlık bölgesinin elemanlarını $x \equiv y (\mathrm{mod}\, 2)$ ve $x, y \in \mathbb{Z}$ olmak üzere $\frac{1}{2}(x + y\sqrt{m})$ formunda yazabileceğimize dikkat edelim. Çünkü $x \equiv y (\mathrm{mod}\, 2)$ ise $x - y = 2k$ olacak şekilde $k \in \mathbb{Z}$ vardır. Buradan $x = y + 2k$ ve

$$\frac{1}{2}(x + y\sqrt{m}) = \frac{1}{2}(y + 2k + y\sqrt{m}) = k + y(\frac{1+\sqrt{m}}{2}) \in \mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{m}}{2})$$

elde edilir. Açıkça $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ bölgesi $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{m}}{2})$ bölgesinin bir alt bölgesidir.

Örnek 2.1.7: F cisim olmak üzere $F[x]$ polinomlar halkası bir tamlık bölgesidir.

Örnek 2.1.8: Katsayıları tamsayı olan polinomlar halkası $\mathbb{Z}[x]$ bir tamlık bölgesidir.

Örnek 2.1.9: D bir tamlık bölgesi olmak üzere $D[x]$ polinomlar halkası bir tamlık bölgesidir.

Tamlık Bölgesinin Özellikleri

D bir tamlık bölgesi olsun. D bölgesi aşağıdaki özellikleri sağlar:

(a) D'nin birim elemanı tektir.

(b) D'nin soldan kısaltma kuralı vardır. Yani $a,b,c \in D$ olmak üzere

$$ab = ac, a \neq 0 \Rightarrow b = c$$

dir. D'nin sağdan kısaltma kuralı vardır. Yani $a,b,c \in D$ olmak üzere

$$ac = bc, c \neq 0 \Rightarrow a = b$$

dir.

Tanım 2.1.10: a ve b, D tamlık bölgesinin iki elemanı olsun. Eğer $b = ac$ olacak şekilde $c \in D$ elemanı varsa a elemanına b'nin böleni denir. Eğer a, b'nin böleni ise bu durum $a \mid b$ ile gösterilir. Eğer a, b'nin böleni değilse bu durum $a \nmid b$ ile gösterilir.

Örnek 2.1.11: $\mathbb{Z}+\mathbb{Z}i$'de $2 = (1+i)(1-i)$ olduğundan $1+i \mid 2$'dir.

Örnek 2.1.12: $\mathbb{Z}[x]$'de $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$ olduğundan

$$x^2 + x + 1 \mid x^4 + x^2 + 1$$

elde edilir.

Örnek 2.1.13: $\mathbb{Z}+\mathbb{Z}w$'da $3 = (1-w)^2(1+w)$ olduğundan

$$(1-w)^2 \mid 3$$

elde edilir. $w = \dfrac{-1+\sqrt{-3}}{2}$ ise

$$(1-w)^2(1+w) = (1-(\frac{-1+\sqrt{-3}}{2})^2(1+\frac{-1+\sqrt{-3}}{2})$$

$$= (\frac{3-\sqrt{-3}}{2})^2(\frac{1+\sqrt{-3}}{2})$$

$$= \frac{3-3\sqrt{-3}}{2}.\frac{1+\sqrt{-3}}{2}$$

$$= \frac{3-3\sqrt{-3}+3\sqrt{-3}+9}{4} = \frac{12}{4} = 3$$

olduğundan $(1-w^2) \mid 3$ olur.

Örnek 2.1.14: $\mathbb{Z}+\mathbb{Z}\sqrt{2}$ 'de $\frac{3}{2+\sqrt{2}} = 3-\frac{3}{2}\sqrt{2} \notin \mathbb{Z}+\mathbb{Z}\sqrt{2}$ olduğundan $2+\sqrt{2} \nmid 3$ yazılabilir.

Bölenlerin Özellikleri

D tamlık bölgesi ve $a,b,c \in D$ olsun. Bu durumda

(a) $a \mid a$ (yansıma özelliği)

(b) $a \mid b$ ve $b \mid c$ ise $a \mid c$ (geçişme özelliği)

(c) $a \mid b$ ve $a \mid c$ ise $\forall x, y \in D$ için $a \mid bx+cy$

(d) $a \mid b$ ise $ac \mid bc$

(e) $ac \mid bc$ ve $c \neq 0$ ise $a \mid b$

(f) $1 \mid a$

(g) $a \mid 0$

(h) $0 \mid a$ ise $a = 0$

özellikleri geçerlidir.

Tanım 2.1.15: D tamlık bölgesi olmak üzere, $a \mid 1$ ise $a \in D$ elemanına birim denir. D tamlık bölgesinin birimlerinin kümesi U(D) ile gösterilir.

a birim ise $ab = 1$ olan $b \in D$ vardır. b elemanına a'nın tersi denir ve b elemanı a^{-1} ile gösterilir.

Birimlerin Özellikleri

D bir tamlık bölgesi olsun. Bu durumda

(a) $\mp 1 \in U(D)$

(b) $a \in U(D)$ ise $-a \in U(D)$

(c) $a \in U(D)$ ise $a^{-1} \in U(D)$

(d) $a \in U(D)$ ve $b \in U(D)$ ise $ab \in U(D)$

(e) $a \in U(D)$ ise $\forall n \in \mathbb{Z}$ için $\mp a^n \in U(D)$

özellikleri doğrudur.

İspat: (a) $\mp 1 \in U(D)$ olduğu açıktır.

(b) $a \in U(D)$ olsun. Dolayısıyla $ab = 1$ olacak şekilde $b \in D$ vardır. Buradan $(-a)(-b) = 1$ ise $-a \mid 1$ elde edilir. Yani $-a \in U(D)$ olur.

(c) $a \in U(D)$ ise $a.a^{-1} = 1$'dir. Öyleyse $a^{-1} \mid 1$ olduğundan $a^{-1} \in U(D)$ olur.

(d) $a, b \in D$ ise $ax = by = 1$ olacak şekilde $x, y \in D$ vardır. Öyleyse

$$(ab)yx = (aby)x = a(by)x = a.1.x = ax = 1$$

dir. Dolayısıyla $ab \mid 1$'dir. Yani $ab \in U(D)$ olur.

(e) $a \in U(D)$ ise $ab = 1$ olacak şekilde $b \in D$ vardır. $\forall n \in \mathbb{Z}$ için $a^n.b^n = 1$ $((-a^n).(-b^n) = 1)$ demektir ki, bu da $\mp a^n \in U(D)$ olduğunu gösterir.

Örnek 2.1.16: (a) $\mathbb{Z} + \mathbb{Z}i$'nin birimi i olduğundan $i \in U(\mathbb{Z} + \mathbb{Z}i)$'dir.

(b) $\mathbb{Z} + \mathbb{Z}w$'nın birimi w olduğundan $w \in U(\mathbb{Z} + \mathbb{Z}w)$ dır (Örnek 2.1.4).

Teorem 2.1.17: D bir tamlık bölgesi ise U(D) çarpmaya göre değişmeli gruptur.

İspat: Birimin 4. özelliğinden, U(D) çarpmaya göre kapalıdır. D tamlık bölgesi olduğundan U(D)'nin elemanları çarpma işlemine göre değişmeli ve birleşmelidir.

Birimlerin (a) özelliğine göre, U(D) birim elemana sahiptir ve birim elemanı 1'dir. Birimlerin (c) özelliğine göre, U(D)'nin her elemanının çarpmaya göre bir ters elemanı vardır. Sonuç olarak U(D) çarpma işlemine göre değişmeli gruptur.

Örnek 2.1.18: (a) $U(\mathbb{Z}) = \{1,-1\}$ 'dir.

(b) $U(\mathbb{Z}+\mathbb{Z}i) = \{1,-1,i,-i\}$ 'dir.

(c) F cisim olmak üzere $U(F[x]) = F \setminus \{0\}$ 'dır.

(d) $U(\mathbb{Z}[x]) = \{1,-1\}$ 'dir.

(e) $\forall n \in \mathbb{Z}$ için $\mp(1+\sqrt{2})^n \in U(\mathbb{Z}+\mathbb{Z}\sqrt{2})$ 'dir.

Tanım 2.1.19: D tamlık bölgesinin sıfırdan farklı a ve b elemanlarından her biri diğerini bölüyorsa bu elemanlara ilgili denir. Eğer a ve b ilgili ise $a \sim b$; ilgili değilse $a \nsim b$ yazılır.

Özellikler

D tamlık bölgesi olmak üzere $a,b,c \in D^* = D \setminus \{0\}$ olsun. Bu durumda aşağıdaki özellikler doğrudur.

(a) $a \sim a$ 'dır.

(b) $a \sim b \Rightarrow b \sim a$ 'dır.

(c) $a \sim b$ ve $b \sim c \Rightarrow a \sim c$ 'dir.

(d) $a \sim b \Leftrightarrow ab^{-1} \in U(D)$ 'dir.

(e) $a \sim 1 \Leftrightarrow a$ birimdir.

Örnek 2.1.20: (a) $\mathbb{Z}$ 'de $a \sim b \Leftrightarrow a = \mp b$, yani $|a| = |b|$ 'dir.

(b) $\mathbb{Z}+\mathbb{Z}i$ 'de $\dfrac{1+i}{1-i} = i \in U(\mathbb{Z}+\mathbb{Z}i)$ olduğundan $1+i \sim 1-i$ 'dir.

(c) $\mathbb{Z}+\mathbb{Z}\sqrt{2}$ 'de $\dfrac{1+3\sqrt{2}}{5-2\sqrt{2}} = 1+\sqrt{2} \in U(\mathbb{Z}+\mathbb{Z}\sqrt{2})$ olduğundan $1+3\sqrt{2} \sim 5-2\sqrt{2}$ 'dir.

2.2. İndirgenemezler ve Asallar

Tanım 2.2.1: D tamlık bölgesi ve $a \in D$ olsun. Eğer $a = bc$ iken b veya c'den biri birim oluyorsa a elemanına indirgenemezdir denir.

Örnek 2.2.2: 2 elemanı $\mathbb{Z}$ de indirgenemezdir. $a,b \in \mathbb{Z}$, $2 = a.b$ ise $a = \mp 1$ veya $b = \mp 1$'dir.

Örnek 2.2.3: 2 elemanı $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$'de indirgenemezdir.

Çözüm: $a,b,c,d \in \mathbb{Z}$ için $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ olduğunu varsayalım. Bu denklemin her iki tarafının modülünü alırsak

$$4 = (a^2 + 5b^2)(c^2 + 5d^2)$$

elde ederiz. Bu durumda $a^2 + 5b^2$, 4'ü bölen bir pozitif tamsayıdır ve $a^2 + 5b^2 = 1,2$ ya da 4 olmalıdır. Dolayısıyla $(a,b) = (\mp 1, 0)$ ya da $(a,b) = (\mp 2, 0)$'dır. Yani

$$a + b\sqrt{-5} = \mp 1 \text{ ya da } a + b\sqrt{-5} = \mp 2$$

dir.

$a + b\sqrt{-5} = \mp 1$ ise $a + b\sqrt{-5}$ elemanı $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$'in birimidir. Diğer taraftan, $a + b\sqrt{-5} = \mp 2$ için $c + d\sqrt{-5} = \dfrac{2}{a + b\sqrt{-5}} = \dfrac{2}{\mp 2} = \mp 1$ elde edilir. Öyleyse, $c + d\sqrt{-5}$ elemanı $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$'de birim olur. Sonuç olarak 2 elemanı, $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$'de indirgenemezdir.

Örnek 2.2.4: $7 + \sqrt{-5}$ elemanı $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$'de indirgenemez değildir. Çünkü $7 + \sqrt{-5} = (1 + \sqrt{-5})(2 - \sqrt{-5})$ olur. Ayrıca $1 + \sqrt{-5}$ ve $2 - \sqrt{-5}$ elemanları $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$'de birim değildir.

Tanım 2.2.5: $a,b \in D$ olmak üzere $p \in D, p \neq 0$ ve p birim olmasın. Eğer $p \mid ab$ iken $p \mid a$ veya $p \mid b$ ise p'ye D'nin bir asal elemanı denir.

Örnek 2.2.6: 2 sayısı $\mathbb{Z}$ 'de asaldır.

$a,b \in \mathbb{Z}$ için $2 \mid ab$ olduğunu varsayalım. Öyleyse ab çifttir. İki tek sayının çarpımı tek olduğundan a ve b'den en az biri çift olmalıdır. Yani $2 \mid a$ veya $2 \mid b$ 'dir. Bu da 2'nin asal olduğunu gösterir.

Örnek 2.2.7: 2, $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ 'de asal değildir. Çünkü $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$ olmasına rağmen $2 \nmid (1 \mp \sqrt{-5})$ 'dir.

Örnek 2.2.8: 1+i, $\mathbb{Z}+\mathbb{Z}i$ 'de asaldır.

Çözüm: Bunu göstermek için $a,b,c,d \in \mathbb{Z}$ olmak üzere $1+i \mid (a+bi)(c+di)$ olduğunu varsayalım. Bu durumda $(a+bi)(c+di) = (1+i)(x+yi)$ olacak şekilde x ve y tamsayıları vardır. Bu denklemin her iki tarafının modülünü alırsak, $(a^2+b^2)(c^2+d^2) = 2(x^2+y^2)$ elde edilir. Bu durumda $2 \mid (a^2+b^2)(c^2+d^2)$ ve 2, $\mathbb{Z}$ 'de asal olduğundan $2 \mid (a^2+b^2)$ veya $2 \mid (c^2+d^2)$ olur.

$2 \mid (a^2+b^2)$ olduğunu varsayalım. Burada a ve b'den her ikisi de çifttir ya da her ikisi de tektir. r,s$\in \mathbb{Z}$ için $a=2r$ ve $b=2s$ alırsak

$$a+bi = 2(r+si) = (1+i)(r+s+(-r+s)i)$$

elde edilir. Buradan $1+i \mid a+bi$ 'dir. Eğer $a=2k+1$ ve $b=2t+1$ alırsak

$$a+bi = 2(k+t)+1+i = (1+i)(k+t-ki-ti+1)$$

olur. Buradan $1+i \mid a+bi$ elde edilir. Dolayısıyla 1+i, $\mathbb{Z}+\mathbb{Z}i$ 'de asaldır.

Teorem 2.2.9: Herhangi bir tamlık bölgesinde bir asal eleman indirgenemezdir.

İspat: $p \in D$ asal eleman olsun. $a,b \in D$ için $p=ab$ olduğunu varsayalım. $ab = p.1$ olduğundan $p \mid ab$ 'dir ve p asal olduğundan $p \mid a$ veya $p \mid b$ 'dir. $p \mid a$ olsun. Öyleyse $a = px$ olan $x \in D$ vardır. $p=ab$ olduğundan $a \neq 0$ 'dır. $a = abx$ ve

$a \neq 0$ olduğundan 1=bx olur. Yani b birimdir. Benzer şekilde eğer $p \mid b$ ise, a birim olur. Öyleyse, p elemanı D'nin indirgenemez elemanıdır.

Bu teoremin tersi doğru değildir. 2 elemanı $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ 'de indirgenemezdir, fakat asal değildir. Bunu görmek için Örnek 2.2.3 ve Örnek 2.2.7'ye bakılabilir.

2.3. İdealler

Tanım 2.3.1: D'nin boştan farklı I altkümesi aşağıdaki iki özelliğe sahipse I'ya D tamlık bölgesinin ideali denir.

(i) $a \in I, b \in I$ ise $ab \in I$ 'dir.
(ii) $a \in I, r \in D$ ise $ar \in I$ 'dir.

Açıktır ki, $a_1, a_2, ..., a_n \in I$ ise $r_1, r_2, ..., r_n \in D$ için $r_1a_1 + r_2a_2 + ... + r_na_n \in I$ olur. Özellikle $a \in I$ ve $b \in I$ ise $-a \in I$ ve $a-b \in I$ 'dır. Öyleyse $0 \in I$ 'dır ve $1 \in I$ ise $I = D$ olur.

Örnek 2.3.2: $\{a_1, a_2, ..., a_n\}$ D tamlık bölgesinin elemanları ise $a_1, a_2, ..., a_n$ 'nin sonlu lineer kombinasyonlarının kümesi $\{\sum_{i=1}^{n} r_i a_i : r_1, r_2, ..., r_n \in D\}$ D'nin bir idealidir. Bu ideal $\langle a_1, ..., a_n \rangle$ ile gösterilir ve $\langle a_1, ..., a_n \rangle$'ye, $a_1, a_2, ..., a_n$ elemanları tarafından üretilen ideal denir.

Tanım 2.3.3: $I = \langle a \rangle$ olacak şekilde bir $a \in D$ elemanı varsa D tamlık bölgesinin I idealine esas ideal denir. a elemanına da I'nın üreticisi denir.

D bir tamlık bölgesi ise $a \in D$ elemanı tarafından üretilen $\langle a \rangle$ esas ideali $\{ra : r \in D\}$ şeklinde bir kümedir. Açıkça $\langle 0 \rangle$ esas ideali tek elemanlı $\{0\}$ kümesine ve $\langle 1 \rangle$ esas ideali D tamlık bölgesine eşittir. Yani $\langle 0 \rangle = \{0\}$ ve $\langle 1 \rangle$ = D'dir.

Teorem 2.3.4: D tamlık bölgesi ve $a,b \in D$ olsun. Bu takdirde $\langle a \rangle \subset \langle b \rangle \Leftrightarrow b \mid a$'dır.

İspat: $\Rightarrow$: $a \in \langle a \rangle \subset \langle b \rangle$ ise $a \in \langle b \rangle$'dir. Öyleyse $a = bx$ olacak şekilde $x \in D$ vardır. Buradan $b \mid a$ elde edilir.

$\Leftarrow$: $b \mid a$ ise $a = bx$ olacak şekilde $x \in D$ vardır. Ayrıca $y \in \langle a \rangle$ ise $y = ak$ olacak şekilde $k \in D$ vardır. Dolayısıyla $y = bxk$ ve $y \in \langle b \rangle$ olur. Bu ise $\langle a \rangle \subset \langle b \rangle$ demektir.

Tanım 2.3.5: Bir D tamlık bölgesinin $\langle 0 \rangle$ ve $\langle 1 \rangle$'den farklı I idealine, D'nin öz ideali denir.

Örnek 2.3.6: Bir pozitif k tamsayısı için $k\mathbb{Z} = \{0, \mp k, \mp 2k, ...\}$ kümesi $\mathbb{Z}$'nin bir idealidir. Gerçekten $k\mathbb{Z}$, k tarafından üretilen bir esas idealdir, yani

$$k\mathbb{Z} = \langle k \rangle$$

dir.

Örnek 2.3.7: $I = \{ f(x) \in \mathbb{Z} : f(0) = 0 \}$ olsun. Bu durumda I, $\mathbb{Z}[x]$'in idealidir ve $I = \langle x \rangle$'dir.

Örnek 2.3.8: $J = \{ f(x) \in \mathbb{Z}[x] : f(0) \equiv 0 (\mathrm{mod}\, 2) \}$ olsun. Bu durumda J, $\mathbb{Z}[x]$'in bir idealidir ve $J = \langle 2, x \rangle$'dir. Bununla beraber J esas ideal değildir.

Teorem 2.3.9: D tamlık bölgesi ve $a,b \in D^* = D \setminus \{0\}$ olsun. Bu durumda

$$\langle a \rangle = \langle b \rangle \Leftrightarrow a \sim b$$

dir.

İspat: $\Leftarrow$: $a \sim b$ ise $a \mid b$ ve $b \mid a$'dır. $a \mid b$ ise önceki teoreme göre $\langle b \rangle \subset \langle a \rangle$'dir. $b \mid a$ ise $\langle a \rangle \subset \langle b \rangle$'dir. Dolayısıyla $\langle a \rangle = \langle b \rangle$'dir.

$\Leftarrow$: $\langle a \rangle = \langle b \rangle$ ise $\langle a \rangle \subset \langle b \rangle \subset \langle a \rangle$ olup, $a \mid b$ ve $b \mid a$ elde edilir. Bu ise $a \sim b$ ile gösterilir.

2.4. Esas İdeal Bölgeleri

Tanım 2.4.1: D tamlık bölgesindeki her ideal esas ideal ise bu D bölgesine esas ideal bölgesi denir.

Teorem 2.4.2: $\mathbb{Z}$ bir esas ideal bölgesidir.

İspat: $\mathbb{Z}$'nin bir ideali I olsun. $I = \{0\}$ ise $I = \langle 0 \rangle$ bir esas idealdir. $I \neq \{0\}$ olduğunu varsayalım. Öyleyse I'nın sıfırdan farklı bir a elemanı vardır. a ve $-a$'nın her ikisi de I'ya ait olduğundan $a > 0$ kabul edebiliriz. Böylece I en az bir pozitif tamsayı içerir. I'daki en küçük pozitif tamsayının m olduğunu kabul edelim. $a \in I$ olsun. a'yı m'ye bölersek $q, r \in \mathbb{Z}$ için $a = mq + r$, $0 \leq r < m$ elde ederiz. $a \in I$ ve $m \in I$ olduğundan $r = a - mq \in I$ olur. $r \neq 0$ olursa $r < m$ olması m'nin en küçük olması ile çelişir. $r = 0$ olmalıdır. $r = 0$ ise $a = mq \Rightarrow a \in \langle m \rangle$'dir. Dolayısıyla $I \subset \langle m \rangle$ olur. Ayrıca $m \in I$ olduğundan $\langle m \rangle \subset I$'dır. Sonuç olarak $I = \langle m \rangle = m\mathbb{Z}$'dir.

Teorem 2.4.3: Esas ideal bölgesinde bir indirgenemez eleman asaldır.

İspat: D esas ideal bölgesinde p bir indirgenemez eleman olsun. $a, b \in D$ olmak üzere $p \mid ab$ olduğunu varsayalım. $p \nmid a$ durumu için D'nin $\langle p, a \rangle$ ideali I olsun. D bir esas ideal bölgesi olduğundan $I = \langle c \rangle$ olacak şekilde bir $c \in D$ elemanı vardır. $a \in I$ ve $p \in I$ olduğundan $c \mid a$ ve $c \mid p$ olur. Eğer $p \mid c$ ise $c \mid a$ olduğundan $p \mid a$ bulunur. Bu $p \nmid a$ ile çelişir. Öyleyse $p \nmid c$'dir. $c \mid p$ ise $p = cx$ olacak şekilde

$x \in D$ vardır. p indirgenemez olduğundan ya c ya da x birim olmalıdır. x birim olamaz. Çünkü bu durumda $p \mid c$ olur. Dolayısıyla c birimdir. O halde $cd = 1$ olacak şekilde $d \in D$ vardır. $I = \langle c \rangle = \langle p, a \rangle$ olduğundan $c \in \langle a, p \rangle$'dir. Öyleyse

$$c = xa + yp$$

olan $x, y \in D$ vardır. Buradan $1 = cd = dxa + dyp$ ve $b = (dx)ab + (bdy)p$ elde edilir. $p \mid p$ ve $p \mid ab$ olduğundan $p \mid (dx)ab + (bdy)p$'dir. Öyleyse $p \mid b$ bulunur. Yani $p \mid ab$ iken $p \mid a$ veya $p \mid b$ olur. Bu ise p'nin asal eleman olması demektir.

Teorem 2.4.4: Esas ideal bölgesindeki bir a elemanı indirgenemezdir $\Leftrightarrow$ a asaldır.

İspat: Teorem 2.2.9 ve Teorem 2.4.3'ün sonucudur.

Örnek 2.4.5: Bölüm 2.2'de 2'nin $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$'de indirgenemez olduğunu, fakat $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$'de asal olmadığını gösterdik. Teorem 2.4.4'e göre $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ tamlık bölgesi bir esas ideal bölgesi değildir. Gerçekten $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$'in $\langle 2, 1+\sqrt{-5} \rangle$ ideali esas ideal değildir. Bunu direkt olarak görebiliriz. Tam tersini kabul edelim. $\langle 2, 1+\sqrt{-5} \rangle$ ideali bir esas ideal olsun. Bu demektir ki, bir $\alpha \in \mathbb{Z}+\mathbb{Z}\sqrt{-5}$ için $\langle 2, 1+\sqrt{-5} \rangle = \langle \alpha \rangle$'dir. Buradan $2 \in \langle \alpha \rangle$ ve $1+\sqrt{-5} \in \langle \alpha \rangle$ olur. Öyleyse

$$\alpha \mid 2 \text{ ve } \alpha \mid 1+\sqrt{-5}$$

dir. $\alpha \mid 2$ ve $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$'de 2 indirgenemez olduğundan $\alpha \sim 1$ ya da $\alpha \sim 2$ olmalıdır. $\alpha \sim 2$ ise $\frac{1+\sqrt{-5}}{2} = \frac{1}{2} + \frac{\sqrt{-5}}{2} \notin \mathbb{Z}+\mathbb{Z}\sqrt{-5}$ olduğundan $2 \mid 1+\sqrt{-5}$ olması mümkün değildir. Öyleyse $\alpha \sim 1$'dir ve $\langle 2, 1+\sqrt{-5} \rangle = \langle 1 \rangle$'dir. $\langle 2, 1+\sqrt{-5} \rangle = \langle 1 \rangle$ ifadesi bize, 1'in $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$'den katsayılarla 2 ve $1+\sqrt{-5}$'in bir lineer kombinasyonu olduğunu gösterir. Yani

$$1 = (x + y\sqrt{-5}).2 + (z + w\sqrt{-5})(1+\sqrt{-5})$$

olacak şekilde $x, y, z, w \in \mathbb{Z}$ vardır. Katsayıların eşitliğinden,

$$1 = 2x + z - 5w, 0 = 2y + z + w$$

elde ederiz. Bu denklemlerin farkını alırsak

$$1 = 2(x - y - 3w)$$

buluruz. Bu mümkün değildir. Çünkü sağ taraf çift sol taraf tek tamsayıdır. Öyleyse $\left\langle 2, 1+\sqrt{-5} \right\rangle$ ideali $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ 'de esas ideal değildir.

Tanım 2.4.6: D bir esas ideal bölgesi ve $\{a_1,...,a_n\}$ D'nin elemanlarının bir kümesi olsun. Bu durumda $\langle a_1,...,a_n \rangle$ ideali bir esas idealdir. Bu idealin bir üreticisi $a_1, a_2,..., a_n$ 'nin bir en büyük ortak böleni olarak adlandırılır.

2.5. Asal İdealler ve Maksimal İdealler

Tanım 2.5.1: D tamlık bölgesinin bir I ideali için $M \subseteq I \subseteq D$ olduğunda, $I = M$ veya $I = D$ ise M öz idealine maksimal ideal denir.

Örnek 2.5.2: $\langle x^2+1 \rangle$ ideali R[x]'de maksimaldir. Bunu göstermek için

$$\langle x^2+1 \rangle \subset I \subset R[x]$$

olmak üzere R[x]'in bir idealinin I olduğunu kabul edelim. $\langle x^2+1 \rangle \subset I$ ve $\langle x^2+1 \rangle \neq I$ olduğundan $f(x) \in I$ ve $f(x) \notin \langle x^2+1 \rangle$ olacak biçimde bir $f(x) \in R[x]$ vardır. f(x) polinomunu (x^2+1)'e bölersek

$$f(x) = (x^2+1)q(x) + r(x),\ r(x) \neq 0,\ der(r(x)) < 2$$

elde edilir. $a, b \in R$, a ve b'nin her ikisi birden sıfır olmamak üzere $r(x) = ax + b$ olur. $a^2x^2 - b^2 = (ax+b)(ax-b)$ ve $a^2(x^2+1) \in I$ 'dır. Böylece

$$a^2 + b^2 = (a^2(x^2+1) - (a^2x^2 - b^2) \in I$$

elde edilir. Yani I ideali sıfırdan farklı gerçek sayıları içeriyorsa R[x]'in birimini içeriyor demektir. Bu da $I = R[x]$ olduğunu gösterir. Bu ise çelişkidir. Öyleyse böyle bir I ideali yoktur. Sonuç olarak $\langle x^2+1 \rangle$, R[x]'in maksimal idealidir.

Örnek 2.5.3: $\langle 5 \rangle$, $\mathbb{Z}+\mathbb{Z}i$ 'nin maksimal ideali değildir.

Çözüm: $\langle 5\rangle \subset \langle 1+2i\rangle \subset \mathbb{Z}+\mathbb{Z}i$ 'dir. $\langle 5\rangle \subset \langle 1+2i\rangle$ olduğunu göstermek için $1+2i \mid 5$ olduğunu görmek yeterlidir. Ayrıca $5 \nmid 1+2i$ olduğundan $\langle 5\rangle \neq \langle 1+2i\rangle$ 'dir.

Teorem 2.5.4: D tamlık bölgesi olsun. $a \neq 0$ ve $a \notin U(D)$ olmak üzere $a \in D$ olsun. Bu durumda $\langle a\rangle$ ideali D'nin maksimal ideali ise, a elemanı D'de indirgenemezdir.

İspat: a, D'nin indirgenemez elemanı olmasın. O zaman a elemanı ne sıfır ne de birim olamadığından indirgenebilirdir. Öyleyse $b \in D$ ve $c \in D$ için $a = bc$ 'dir ve hem b hem de c sıfır ya da birim değildir. Bu durumda $\langle a\rangle \subset \langle b\rangle \subset D$ ise $\langle a\rangle$ maksimal ideal değildir. Sonuç olarak $\langle a\rangle$ maksimal ideal ise a elemanı indirgenemezdir.

Örnek 2.5.5: (a) $\langle x\rangle \subset \langle 2, x\rangle \subset \mathbb{Z}[x]$ olduğunda; x, $\mathbb{Z}[x]$'in indirgenemez elemanıdır. Bununla beraber $\langle x\rangle$, $\mathbb{Z}[x]$'in maksimal ideali değildir.

(b) $1+\sqrt{-5}$ elemanı $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ 'in indirgenemez elemanıdır.

$$\langle 1+\sqrt{-5}\rangle \subset \langle 2, 1+\sqrt{-5}\rangle \subset \mathbb{Z}+\mathbb{Z}\sqrt{-5}$$

olduğundan $\langle 1+\sqrt{-5}\rangle$ ideali maksimal ideal değildir.

Teorem 2.5.4'ün tersi esas ideal bölgesinde doğrudur.

Teorem 2.5.6: D bir esas ideal bölgesi olsun. $a \neq 0$, $a \notin U(D)$ olmak üzere $a \in D$ olsun. Bu durumda

$\langle a\rangle$, D'nin maksimal idealidir $\Leftrightarrow$ a elemanı D'de indirgenemezdir.

İspat: Teorem 2.5.4'ü göz önüne alırsak sadece tek yönü göstermek yeterli olacaktır. a indirgenemez olsun. Fakat $\langle a\rangle$ maksimal ideal olmasın. O zaman $\langle a\rangle \subset I \subset D$

olacak biçimde D'den ve $\langle a \rangle$'dan farklı bir I ideali vardır. D esas ideal bölgesi olduğundan $\langle b \rangle = I$ olacak biçimde bir $b \in D$ vardır. Böylece

$$\langle a \rangle \subset \langle b \rangle \subset D$$

bulunur. $\langle b \rangle$ ideali D'den faklı olduğundan b elemanı birim olamaz. $a \in \langle b \rangle$ olduğundan $a = bc$ olacak biçimde bir $c \in D$ vardır. $\langle a \rangle \neq \langle b \rangle$ olduğundan c'de birim olamaz. $a = bc$ ve b ile c birim olmadığından bu durum a'nın indirgenemez olmasıyla çelişir. Şu halde kabulümüz yanlıştır. Yani a indirgenemez ise $\langle a \rangle$ ideali maksimal idealdir.

Teorem 2.5.7: D bir tamlık bölgesi ve D'nin bir ideali I olsun. D/I bir cisimdir $\Leftrightarrow$ I maksimal bir idealdir.

İspat: D/I bir cisim ve $I \subset J \subseteq D$ olmak üzere D'nin I'dan farklı bir ideali J olsun. Bu takdirde $b \notin I$ olmak üzere $b \in J$ vardır. Böylece $b+I$, D/I'nın sıfırdan farklı bir elemanıdır. D/I bir cisim olduğundan $(b+I)(c+I) = 1+I$ olacak biçimde bir c+I $\in$ D/I elemanı vardır. Bu $bc+I = 1+I$ ve $bc-1 \in I \subset J$ olmasını gerektirir. Böylece $1 = bc-(bc-1) \in J$ olup $J = \langle 1 \rangle = D$ elde edilir. Bu durum I'nın maksimal olduğunu ispatlar.

Şimdi I'nın maksimal olduğunu kabul edelim. D/I'nın bir cisim olduğunu göstermek için sadece $b+I \neq 0+I$ elemanının çarpmaya göre tersinin var olduğu gösterilmelidir. Çünkü cismin diğer özellikleri açıkça sağlanmaktadır. $b+I \neq 0+I$ olduğundan $b \notin I$'dır.

$$B = \{x \in D : y \in D \text{ ve } w \in I \text{ için } x = by + w\}$$

kümesini göz önüne alalım. $I \subset B$ ve B'nin bir ideal olduğunu görmek kolaydır. I maksimal olduğundan $B = D$ olmalıdır. Böylece $1 \in I$, yani $y' \in D$ ve $w' \in I$ için $1 = by' + w'$ olması demektir. Bu durumda;

$$(b+I).(y'+I) = by'+I = 1-w'+I = 1+I$$

elde edilir. Öyleyse $(b+I)^{-1}$ vardır ve $(b+I)^{-1} = y'+I$'dır.

Tanım 2.5.8: D bir tamlık bölgesi ve P bir öz ideal olsun. $a,b \in D$ ve $ab \in P$ iken $a \in P$ veya $b \in P$ ise P'ye asal ideal denir.

Örnek 2.5.9: $x \mp i \in \mathbb{C}[x]$, $(x+i)(x-i) = x^2 + 1 \in I$, fakat $x \mp i \notin I$ olduğundan $I = \langle x^2 + 1 \rangle$ esas ideali, $\mathbb{C}[x]$'in bir asal ideali değildir.

Örnek 2.5.10: $\mathbb{Z} + \mathbb{Z}i$'nin asal ideali $I = \langle 1+i \rangle$'dir. Bunu göstermek için $(a+bi)(c+di) \in \langle 1+i \rangle$ olmak üzere $a+bi, c+di \in \mathbb{Z} + \mathbb{Z}i$ olsun. Bu durumda;

$$(a+bi)(c+di) = (1+i)(x+yi)$$

olacak şekilde $x+yi \in \mathbb{Z} + \mathbb{Z}i$ vardır. Reel ve sanal kısımları eşitlersek

$$ac - bd = x - y \text{ ve } ad + bc = x + y$$

elde ederiz. Bu iki denklemi toplarsak

$$ac + ad + bc - bd = 2x$$

ve böylece

$$(a+b)(c+d) = ac + ad + bc - bd + 2bd = 2x + 2bd \equiv 0 \pmod 2$$

bulunur. Dolayısıyla $a+b$ veya $c+d$ çifttir. Genelliği bozmadan $a+b$'nin çift olduğunu kabul edebiliriz. Böylece $a+b = 2u$ ve $a-b = 2v$ olacak şekilde $u,v \in \mathbb{Z}$ vardır. $a+b = 2u$ ve $a-b = 2v$ olduğundan $a = u+v$, $b = u-v$ bulunur. Bu durumda $a+bi = (u+v)+(u-v)i = (1+i)(u-vi)$ ve böylece $a+bi \in \langle 1+i \rangle$ elde edilir. Bu da $\langle 1+i \rangle$'nin asal ideal olduğunu gösterir.

Teorem 2.5.11: D bir tamlık bölgesi, $a \neq 0$ ve $a \notin U(D)$ olsun. Bu takdirde ,

$\langle a \rangle$, D'nin asal idealidir $\Leftrightarrow$ a elmanı D'de asaldır.

İspat: $\langle a \rangle$ ideali D'nin asal ideali olsun. $b,c \in D$ olmak üzere $a \mid bc$ olsun. Dolayısıyla $bc \in \langle a \rangle$'dir. $\langle a \rangle$ asal ideal olduğundan $b \in \langle a \rangle$ veya $c \in \langle a \rangle$ olmalıdır. Yani $a \mid b$ veya $a \mid c$'dir. Bu a'nın asal olduğunu gösterir.

Şimdi D de a'nın asal olduğunu kabul edelim. $b,c \in D$ olmak üzere $bc \in \langle a \rangle$ olsun. Böylece $bc = ad$ olacak şekilde $d \in D$ vardır. Yani $a \mid bc$'dir. a asal olduğundan $a \mid b$ veya $a \mid c$'dir. Genelliği bozmadan $a \mid b$ kabul edelim. Böylece $b = ae$ olacak şekilde $e \in D$ vardır. Öyleyse $b \in \langle a \rangle$'dir. Bu da $\langle a \rangle$'nın asal ideal olduğunu ispatlar.

Teorem 2.5.12: D bir tamlık bölgesi ve D'nin bir ideali I olsun. Bu durumda

D/I tamlık bölgesidir $\Leftrightarrow$ I asaldır.

İspat: D/I bir tamlık bölgesi ve $a,b \in D$ olmak üzere $ab \in I$ olsun. O zaman $(a+I)(b+I) = ab+I = 0+I$'dır ve $0+I$, D/I tamlık bölgesinin sıfır elemanıdır. D/I tamlık bölgesi olduğundan $b+I = 0+I$ veya $a+I = 0+I$'dır. Yani ya $a \in I$ ya da $b \in I$'dır. Öyleyse I asaldır.

Şimdi D'nin asal idealinin I olduğunu kabul edelim. D'nin öz ideali I olduğundan D/I; $1+I$ birimli, değişmeli bir halkadır. $a+I \in D/I$ ve $b+I \in D/I$ olmak üzere $(a+I)(b+I) = 0+I$ olduğunu varsayalım. O zaman $ab+I = I$, yani $ab \in I$'dır. I asal olduğundan ya $a \in I$ ya da $b \in I$'dır. Yani $a+I = 0+I$ veya $b+I = 0+I$'dır. Öyleyse D/I sıfır bölenlerine sahip değildir.

Teorem 2.5.13: D bir tamlık bölgesi ve D'nin maksimal ideali I olsun. Bu durumda I, D'nin asal idealidir.

İspat: D'nin maksimal ideali I olsun. O zaman Teorem 2.5.7'ye göre D/I bir cisimdir. Her cisim bir tamlık bölgesi olduğundan, D/I bir tamlık bölgesidir. Bu durumda Teorem 2.5.12'ye göre I, D'nin asal idealidir.

Aşağıdaki örnek, Teorem 2.5.13'ün tersinin genelde doğru olmadığını gösteriyor.

Örnek 2.5.14: $\mathbb{Z}[x]$'in asal ideali $\langle x \rangle$'dir. Fakat $\langle x \rangle$, $\mathbb{Z}[x]$'in maksimal ideali değildir.

Esas ideal bölgesinde Teorem 2.5.13'ün tersi doğrudur.

Teorem 2.5.15: D bir esas ideal bölgesi ve D'nin öz ideali I olsun. Bu durumda

I maksimaldir $\Leftrightarrow$ I asaldır.

İspat: Teorem 2.5.13'den dolayı sadece I asal ideal ise I'nın maksimal ideal olduğunu göstermek yeterlidir. D'nin asal ideali I olsun, fakat I maksimal olmasın. Bu durumda $I \subset J \subset D$ olacak şekilde bir J ideali vardır. D bir esas ideal bölgesi olduğundan $a,b \in D$ için $I = \langle a \rangle$ ve $J = \langle b \rangle$'dir. $\langle a \rangle \subset \langle b \rangle$ olduğundan $c \in D$ için $a = bc$ olacak biçimde $c \in D$ vardır. $bc = a \in \langle a \rangle = I$ ve I asal olduğundan ya $b \in I$ ya da $c \in I$ olmalıdır. $b \in I$ ise $J = \langle b \rangle \subseteq I \subset J$'dir. Bu ise çelişkidir. Bu yüzden $c \in I$ olmalıdır. $c \in I$ ve $I = \langle a \rangle$ olduğundan $c = ad$ olacak biçimde $d \in D$ vardır. Böylece $a = bc = bad$ olur. Burada $a \neq 0$ olduğundan $bd = 1$'dir. Dolayısıyla b birimdir ve $J = \langle b \rangle = D \supset J$ elde edilir. Bu bir çelişkidir. Öyleyse I maksimaldir.

BÖLÜM 3. EUCLİD BÖLGELERİ

3.1. Euclid Bölgeleri

Euclid bölgelerini tanımlamak için önce Euclid fonksiyonunu tanımlayacağız.

Tanım 3.1.1: D bir tamlık bölgesi olsun. $\phi : D \to \mathbb{Z}$ fonksiyonu aşağıdaki iki özelliğe sahipse ϕ 'ye bir Euclid fonksiyonu denir.

(3.1) $\forall a,b \in D$ ve $b \neq 0$ için $\phi(ab) \geq \phi(a)$ 'dir. … (3.1.1)

(3.2) $b \neq 0$ ve $a,b \in D$ ise $a = qb + r$ ve $\phi(r) < \phi(b)$
olacak şekilde $q,r \in D$ vardır. … (3.1.2)

Örnek 3.1.2: $a \in \mathbb{Z}$ olmak üzere $\phi(a) = |a|$, $\mathbb{Z}$ üzerinde bir Euclid fonksiyonudur.

Çözüm: (a) $\forall a,b \in \mathbb{Z}$ ve $b \neq 0$ için $\phi(ab) = |ab| = |a||b| \geq |a| = \phi(a)$ 'dır.

(b) $b \neq 0$ ise $a = bq + r$, $0 \leq r < |b|$ yani $0 \leq \phi(r) < \phi(b)$ 'dir.

Örnek 3.1.3: F bir cisim olmak üzere $D = F[x]$ olsun. D, F cisminden alınan katsayılar ile x'i içeren polinom bölgesidir. $P(x) \in D$ olsun. Bu durumda;

$$\phi(P(x)) = \begin{cases} der(P(x)), & P(x) \neq 0 \\ -1, & P(x) = 0 \end{cases}$$

fonksiyonu D üzerinde bir Euclid fonksiyonudur.

Teorem 3.1.4: D bir tamlık bölgesi ve $\phi : D \to \mathbb{Z}$ bir Euclid fonksiyonu olsun. Bu durumda

(a) $a \sim b \Rightarrow \phi(a) = \phi(b)$,

(b) $a \mid b$ ve $\phi(a) = \phi(b) \Rightarrow a \sim b$,

(c) $a \in U(D) \Leftrightarrow \phi(a) = \phi(1)$**,**

(d) $a \neq 0 \Rightarrow \phi(a) > \phi(0)$

dir.

İspat: (a) $a \sim b$ olsun. Dolayısıyla $a = ub$ olacak şekilde $u \in U(D)$ vardır. Bu durumda (3.1.1)'e göre $\phi(a) = \phi(ub) \geq \phi(b)$'dir. $u \in U(D)$ olduğundan $u^{-1} \in U(D)$ ve $b = u^{-1}a$'dır. O halde tekrar (3.1.1)'e göre $\phi(b) = \phi(u^{-1}a) \geq \phi(a)$'dır. Bu iki eşitlikten $\phi(a) = \phi(b)$ elde edilir.

(b) (3.1.2)'ye göre $a = qb + r$ ve $\phi(r) < \phi(b) = \phi(a)$ olacak şekilde $q, r \in D$ vardır. Eğer $a \mid b$ ise $a \mid a - qb$ olduğundan $a \mid r$ olur. $a \mid r$ ise $u \in D$ için $r = au$'dur. (3.1.1)'e göre $\phi(r) = \phi(au) \geq \phi(a)$ olur ki bu bir çelişkidir. Bu yüzden $r = 0$ olur. Bu $a = qb$ demektir. Dolayısıyla $b \mid a$'dır. Fakat $a \mid b$ idi. Buradan $a \sim b$ bulunur.

(c) (a) şıkkına göre, $a \in U(D)$ ise $a \sim 1$'dir. Öyleyse $\phi(a) = \phi(1)$ olur. (b) şıkkına göre, $1 \mid a$ ve $\phi(1) = \phi(a)$ ise $1 \sim a$'dır. Buradan $a \in U(D)$ bulunur.

(d) (3.1.2)'ye göre $0 = qa + r$, $\phi(r) < \phi(a)$ olacak şekilde $q, r \in D$ vardır. $r \neq 0$ olduğunu varsayalım. Bu durumda $q \neq 0$ ve (3.1.1)'e göre $\phi(r) = \phi(-q(a)) \geq \phi(a)$ olur. Bu ise çelişkidir. Bu yüzden $r = 0$ ve $\phi(0) < \phi(a)$'dır.

Tanım 3.1.5: D bir tamlık bölgesi olsun. D tamlık bölgesi ϕ Euclid fonksiyonuna sahipse D ye ϕ ile ilgili Euclid bölgesi denir.

ϕ Euclid fonksiyonu ile ilgili Euclid bölgesi D ise ϕ'yi belirtmek gerekmez. Biz D'yi kısaca Euclid bölgesi olarak adlandıracağız.

Teorem 3.1.6: Euclid bölgesi bir esas ideal bölgesidir.

İspat: D bir Euclid bölgesi olsun. Böylece D, bir ϕ Euclid fonksiyonuna sahiptir. I, D'de bir ideal olsun. $I = \{0\}$ ise $I = \langle 0 \rangle$ bir esas idealdir. $I \neq \{0\}$ olsun.

$$S = \{\phi(x) \mid x \in I, x \neq 0\}$$

olsun. $I \neq \{0\}$ olduğundan S boş kümeden farklıdır. Euclid fonksiyonunun 4. özelliğine göre S alttan sınırlıdır. İyi sıralama ilkesine göre tam sayıların alttan sınırlı bir kümesi bir en küçük elemana sahiptir. O halde S bir en küçük elemana sahiptir. Bu eleman $\phi(a)$, $(a \in I, a \neq 0)$ olsun. $b \in I$ ise ϕ Euclid fonksiyonu olduğundan $b = aq + r$, $\phi(r) < \phi(a)$ olacak şekilde $q, r \in D$ vardır. I bir ideal, $b \in I$ ve $a \in I$ olduğundan $r = b - aq \in I$ bulunur. $r \neq 0$ ise $\phi(r) \in S$ olur (Çünkü $r \in I$). Böylece $\phi(a) \leq \phi(r)$ elde edilir. Fakat bu çelişkidir. Şu halde $r = 0$ olmalıdır. Dolayısıyla $b = aq$ ve buradan $b \in \langle a \rangle$ elde edilir. Yani $I \subset \langle a \rangle$ olur. $a \in I$ ise $\langle a \rangle \subset I$ olduğu açıktır. Şu halde $I = \langle a \rangle$'dır. Bu da D'de ki her idealin esas ideal olması, yani D'nin esas ideal bölgesi olması demektir.

$\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-19}}{2}\right)$ tamlık bölgesi bir esas ideal bölgesidir. Aksine bu bölge Euclid bölgesi değildir. Bu, Örnek 3.3.16'da gösterilecektir. O halde Teorem 3.1.6'nın tersi doğru değildir.

3.2. Euclid Bölgesi Örnekleri

Teorem 3.2.1: (a) $\mathbb{Z}$ bir Euclid bölgesidir.
(b) F bir cisim olsun. F[x] bir Euclid bölgesidir.

Teorem 3.1.6 ve Teorem 3.2.1'den $\mathbb{Z}$ ve F[x]'in esas ideal bölgeleri olduğu görülür.

Tanım 3.2.2: m karesiz bir tamsayı olsun. $\forall r,s \in \mathbb{Q}$ için ϕ_m fonksiyonu

$$\phi_m : \mathbb{Q}\left(\sqrt{m}\right) \to \mathbb{Q}\,,\ \phi_m(r+s\sqrt{m}) = \left|r^2 - ms^2\right|$$

şeklinde tanımlanır. İlerde $\phi_m(\alpha)$'yı kolaylık sağlaması açısından N(α) ile göstereceğiz. ϕ_m'nin özellikleri aşağıdaki önerme ile verilir.

Önerme 3.2.3: m karesiz tamsayı olsun.

(a) $m \not\equiv 1 \pmod 4$ ise $\phi_m : \mathbb{Z}+\mathbb{Z}\sqrt{m} \to \mathbb{N}\cup\{0\}$ bir Euclid fonksiyonudur.

(b) $m \equiv 1 \pmod 4$ ise $\phi_m : \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) \to \mathbb{N}\cup\{0\}$ bir Euclid fonksiyonudur.

(c) $\alpha \in \mathbb{Q}(\sqrt{m})$ olsun. Bu durumda $\phi_m(\alpha)=0 \Leftrightarrow \alpha = 0$ 'dır.

(d) $\forall \alpha,\beta \in \mathbb{Q}\left(\sqrt{m}\right)$ için $\phi_m(\alpha\beta) = \phi_m(\alpha).\phi_m(\beta)$ 'dır.

(e) $\beta \neq 0$ ile $\forall \alpha,\beta \in \mathbb{Z}+\mathbb{Z}\sqrt{m}$ için $\phi_m(\alpha\beta) \geq \phi_m(\alpha)$ 'dır.

(f) Eğer $m \equiv 1 \pmod 4$ ise $\forall \alpha,\beta \in \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$, $\beta \neq 0$ için $\phi_m(\alpha\beta) \geq \phi_m(\alpha)$ 'dır.

İspat: (a) $\alpha \in \mathbb{Z}+\mathbb{Z}\sqrt{m}$, yani $x,y \in \mathbb{Z}$ için $\alpha = x+y\sqrt{m}$ olsun. Bu durumda, $x^2 - my^2 \in \mathbb{Z}$ ve $\left|x^2-my^2\right| \geq 0$, yani $\phi_m(\alpha) = \phi_m(x+y\sqrt{m}) = \left|x^2-my^2\right| \in \mathbb{N}\cup\{0\}$ 'dır.

(b) Eğer $m \equiv 1 \pmod 4$ ise $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ bir tamlık bölgesidir.

$$\alpha \in \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$$

yani $x,y \in \mathbb{Z}$ için $\alpha = x+y\left(\frac{1+\sqrt{m}}{2}\right) = (x+\frac{y}{2})+\frac{y}{2}\sqrt{m}$ 'dir. Bu durumda

$$\phi_m(\alpha)=\phi_m((x+\frac{y}{2})+\frac{y}{2}\sqrt{m})=\left|\left(x+\frac{y}{2}\right)^2-m\left(\frac{y}{2}\right)^2\right|$$

$$=\left|x^2+xy+\frac{1}{4}(1-m)y^2\right|\in\mathbb{N}\cup\{0\}$$

dır. Çünkü $\frac{1}{4}(1-m)\in\mathbb{Z}$ 'dır.

(d) $\alpha\in\mathbb{Q}\left(\sqrt{m}\right)$, yani $r,s\in\mathbb{Q}$ için $\alpha=r+s\sqrt{m}$ olsun. O zaman m karesiz olduğundan

$$\phi_m(\alpha)=0\Leftrightarrow\phi_m(r+s\sqrt{m})=0$$

$$\Leftrightarrow\left|r^2-ms^2\right|=0$$

$$\Leftrightarrow r^2=ms^2$$

$$\Leftrightarrow r=s=0$$

$$\Leftrightarrow r+s\sqrt{m}=0\Leftrightarrow\alpha=0$$

(d) $\alpha,\beta\in\mathbb{Q}\left(\sqrt{m}\right)$ olsun. O zaman $x,y,u,v\in\mathbb{Q}$ için

$$\alpha=x+y\sqrt{m}\ \text{ ve }\quad\beta=u+v\sqrt{m}$$

dir. Buradan

$$\phi_m(\alpha\beta)=\phi_m((x+y\sqrt{m})(u+v\sqrt{m}))$$

$$=\phi_m((xu+myv)+(xv+yu)\sqrt{m})$$

$$=\left|(xu+myv)^2-m(xv+yu)^2\right|$$

$$=\left|x^2u^2+m^2y^2v^2-mx^2v^2-my^2u^2\right|$$

$$=\phi_m(\alpha).\phi_m(\beta)$$

bulunur.

(e) $\alpha, \beta \in \mathbb{Z}+\mathbb{Z}\sqrt{m}$, $\beta \neq 0$ olsun. (c) maddesine göre, $\phi_m(\beta) \neq 0$'dır. Bu durumda (a) maddesine göre, $\phi_m(\alpha) \geq 0$ ve $\phi_m(\beta) \geq 1$ elde ederiz. (d) maddesine göre, $\phi_m(\alpha\beta) = \phi_m(\alpha).\phi_m(\beta) \geq \phi_m(\alpha)$'dır.

(f) (a) maddesinde (b)'yi kullanırsak istenen elde edilir.

Teorem 3.2.4: m karesiz tamsayı olsun. Bu durumda $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ tamlık bölgesi ϕ_m'li Euclid bölgesidir $\Leftrightarrow$ $\forall x, y \in \mathbb{Q}$ için

$$\phi_m((x+y\sqrt{m})-(a+b\sqrt{m})) < 1 \quad \ldots (3.2.1)$$

olacak şekilde $a, b \in \mathbb{Z}$ vardır.

İspat: $\Rightarrow$: İlk olarak $\mathbb{Z}+\mathbb{Z}\sqrt{m}$'nin ϕ_m'li Euclid bölgesi olduğunu varsayalım. $x, y \in \mathbb{Q}$ olsun. Bu durumda $r, s, t \in \mathbb{Z}$, $t \neq 0$ için $x+y\sqrt{m} = (r+s\sqrt{m})/t$'dir. $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ üzerinde Euclid fonksiyonu ϕ_m'nin varlığından

$$r+s\sqrt{m} = t(a+b\sqrt{m})+(c+d\sqrt{m}),\ \phi_m(c+d\sqrt{m}) < \phi_m(t)$$

olacak şekilde $a+b\sqrt{m}$, $c+d\sqrt{m} \in \mathbb{Z}+\mathbb{Z}\sqrt{m}$ vardır. Lemma 3.2.4 (d)'ye göre,

$$\begin{aligned}
\phi_m((x+y\sqrt{m})-(a+b\sqrt{m})) &= \phi_m\left(\frac{r+s\sqrt{m}}{t}-\left(a+b\sqrt{m}\right)\right) \\
&= \phi_m\left(\frac{r+s\sqrt{m}-t(a+b\sqrt{m})}{t}\right) \\
&= \phi_m\left(\frac{c+d\sqrt{m}}{t}\right) \\
&= \frac{\phi_m(c+d\sqrt{m})}{\phi_m(t)} < 1
\end{aligned}$$

bulunur.

$\Leftarrow$: (3.2.1)'in sağlandığını varsayalım. $\mathbb{Z}+\mathbb{Z}\sqrt{m}$'nin ϕ_m'li Euclid bölgesi olduğunu göstermek için (3.1.1) ve (3.1.2)'nin varlığını göstermeliyiz. (3.1.1) eşitsizliği

Önerme 3.2.3, (e) özelliği göz önüne alınarak bulunur. Şimdi (3.1.2)'yi göstereceğiz. $t+u\sqrt{m}\neq 0$, $r+s\sqrt{m}$, $t+u\sqrt{m}\in\mathbb{Z}+\mathbb{Z}\sqrt{m}$ olsun. Bu durumda

$$\frac{r+s\sqrt{m}}{t+u\sqrt{m}}=x+y\sqrt{m},\ t+u\sqrt{m}\neq 0$$

ise

$$x=\frac{rt-msu}{t^2-mu^2}\in\mathbb{Q}\ \text{ ve }\ y=\frac{st-ru}{t^2-mu^2}\in\mathbb{Q}$$

elde edilir.

$t^2-mu^2=0$ olsun. Dolayısıyla $u\neq 0$'dır. Çünkü $u=0$ ise $t=0$ olur. Bu durumda $t+u\sqrt{m}=0$ bulunur. $u\neq 0$ ve $t^2-mu^2=0$ ise $m=\frac{t^2}{u^2}$, yani $\sqrt{m}=\frac{t}{u}$ elde edilir. m karesiz olduğundan $\sqrt{m}$ rasyonel sayı olamaz. Şu halde $t^2-mu^2\neq 0$ olmalıdır.

(3.1.1)'e göre, $\phi_m((x+y\sqrt{m})-(a+b\sqrt{m}))<1$ olacak şekilde $a+b\sqrt{m}\in\mathbb{Z}+\mathbb{Z}\sqrt{m}$ vardır. $c=r-at-bum\in\mathbb{Z}$ ve $d=s-au-bt\in\mathbb{Z}$ olarak alınırsa

$$c+d\sqrt{m}=(r+s\sqrt{m})-(a+b\sqrt{m})(t+u\sqrt{m})\in\mathbb{Z}+\mathbb{Z}\sqrt{m}$$

olur. Buradan

$$r+s\sqrt{m}=(a+b\sqrt{m})(t+u\sqrt{m})+(c+d\sqrt{m})$$

ve Önerme 3.2.3, (d)'den,

$$\begin{aligned}\phi_m(c+d\sqrt{m})&=\phi_m\left((r+s\sqrt{m})-(a+b\sqrt{m})(t+u\sqrt{m})\right)\\&=\phi_m\left((x+y\sqrt{m})(t+u\sqrt{m})-(a+b\sqrt{m})(t+u\sqrt{m})\right)\\&=\phi_m\left((t+u\sqrt{m})\left((x+y\sqrt{m})-(a+b\sqrt{m})\right)\right)\\&=\phi_m(t+u\sqrt{m})\phi_m\left((x+y\sqrt{m})-(a+b\sqrt{m})\right)\\&<\phi_m(t+u\sqrt{m})\end{aligned}$$

elde edilir. Bu da (3.1.2)'nin ispatını tamamlar.

Önerme 3.2.5: $s>0$ olmak üzere $\frac{r}{s}\neq 0$ bir rasyonel sayı olsun. Bu durumda bir $c\in\mathbb{Z}$ tamsayı $\left|\frac{r}{s}-c\right|\leq\frac{1}{2}$ olacak biçimde vardır.

İspat: r tamsayısı s'ye bölünerek $r=sq+t$, $0\leq t<s$ biçiminde yazılabilir. Bu durumda $\frac{r}{s}=q+\frac{t}{s}=q+t^*$, $0\leq t^*<1$ olarak yazılabilir. Eğer $t^*\leq\frac{1}{2}$ ise

$$\left|\frac{r}{s}-q\right|=|t^*|\leq\frac{1}{2}$$

elde edilir. Eğer $\frac{1}{2}<t^*<1$ ise $\frac{r}{s}=q+1+t^*-1$ olup $|t^*-1|<\frac{1}{2}$ olduğu görülür. Böylece $\left|\frac{r}{s}-(q+1)\right|=|t^*-1|<\frac{1}{2}$ bulunur. Sonuç olarak $\left|\frac{r}{s}-c\right|\leq\frac{1}{2}$ olacak biçimde bir c tamsayısı vardır.

Teorem 3.2.6: m bir negatif karesiz tamsayı olsun. Bu durumda $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ tamlık bölgesi ϕ_m'li bir Euclid bölgesidir $\Leftrightarrow$ $m=-1$ veya $m=-2$'dir.

İspat: $\Leftarrow$: İlk olarak $\mathbb{Z}+\mathbb{Z}\sqrt{m}$'nin $m=-1$ ve $m=-2$ için ϕ_m'li bir Euclid bölgesi olduğunu görelim: $x,y\in\mathbb{Q}$ olsun. Önceki önermeye göre $|x-a|\leq\frac{1}{2}$, $|y-b|\leq\frac{1}{2}$ olacak şekilde $a,b\in\mathbb{Z}$ vardır. Bu durumda

$$\begin{aligned}\phi_m\left((x+y\sqrt{m})-(a+b\sqrt{m})\right)&=\phi_m\left((x-a)+(y-b)\sqrt{m}\right)\\&=\left|(x-a)^2-m(y-b)^2\right|\\&\leq|x-a|^2+|m||y-b|^2\\&\leq\frac{1}{4}+2.\frac{1}{4}=\frac{3}{4}<1\end{aligned}$$

bulunur. Teorem 3.2.5'den dolayı $\mathbb{Z}+\mathbb{Z}\sqrt{m}$, $m=-1$ veya $m=-2$ için ϕ_m'li Euclid bölgesidir.

$\Rightarrow$: Şimdi $\mathbb{Z}+\mathbb{Z}\sqrt{m}$, ϕ_m 'li Euclid bölgesi olsun. Bu durumda Teorem 3.2.5'e göre,

$$\phi_m\left(\left(\frac{1}{2}+\frac{1}{2}\sqrt{m}\right)-\left(a+b\sqrt{m}\right)\right)<1$$

olacak şekilde $a,b\in\mathbb{Z}$ vardır. Yani ($-m=|m|$ olduğundan)

$$\left(\frac{1}{2}-a\right)^2+|m|\left(\frac{1}{2}-b\right)^2<1$$

dir. Fakat herhangi bir x tamsayısı için $\left|\frac{1}{2}-x\right|\geq\frac{1}{2}$, $\left(\frac{1}{2}-x\right)^2\geq\frac{1}{4}$ olduğundan $\frac{1}{4}+|m|.\frac{1}{4}<1$ ve buradan da $\frac{|m|}{4}<1-\frac{1}{4}=\frac{3}{4}$ bulunur. Bu ise $|m|<3$ olduğunu gösterir. Böylece $m=-1$ veya $m=-2$ bulunur.

Örnek 3.2.7: (i) $m=-1$ olmak üzere $\mathbb{Z}+\mathbb{Z}i$ 'de $2+i\neq 0$ için

$$\phi_{-1}\left((4+5i)(2+i)\right)=\phi_{-1}(3+14i)=205 \text{ ve } \phi_{-1}(4+5i)=41$$

dir. Buradan

$$\phi_{-1}\left((4+5i)(2+i)\right)\geq\phi_{-1}(4+5i) \qquad \ldots(3.2.2)$$

elde edilir. Diğer taraftan

$$\frac{4+5i}{\underset{(2-i)}{2+i}}=\frac{8+6i+5}{5}=\frac{13}{5}+\frac{6}{5}i=3+\left(-\frac{2}{5}\right)+\left(1+\frac{1}{5}\right)i=(3+i)+\left(-\frac{2}{5}+\frac{1}{5}i\right)$$

bulunur. Böylece $4+5i=(2+i)(3+i)+(-1)$ elde edilir. $\phi_{-1}(-1)=1$ ve $\phi_{-1}(2+i)=5$ olduğundan

$$\phi_{-1}(-1)<\phi_{-1}(2+i) \qquad \ldots(3.2.3)$$

dir.

(ii) $m=-2$ olmak üzere $\mathbb{Z}+\mathbb{Z}\sqrt{2}i$ 'de $4+5\sqrt{2}i=(3+2\sqrt{2}i)(...)+(...)$ dir. Şimdi (3.2.1) sağlansın. $r=4$, $s=5$ için $r+s\sqrt{2}i=4+5\sqrt{2}i$ ve $t=3$, $u=2$ için $t+u\sqrt{2}i=3+2\sqrt{2}i$ alalım. Öyleyse

$$x+y\sqrt{2}i=\frac{4+5\sqrt{2}i}{\underset{(3-2\sqrt{2}i)}{3+2\sqrt{2}i}}=\frac{32+7\sqrt{2}i}{17}$$

dir. Böylece $x=\frac{32}{17}$ ve $y=\frac{7}{17}$ elde edilir. Burada $x=2+\frac{-2}{17}$ ve $y=0+\frac{7}{17}$ yazılabilir. Dolayısıyla $a=2$ ve $b=0$ elde edilir. Buradan

$$c+d\sqrt{2}i=r+s\sqrt{2}i-(a+b\sqrt{2}i)(t+u\sqrt{2}i)=4+5\sqrt{2}i-(2+0\sqrt{2}i)(3+2\sqrt{2}i)$$
$$=-2+\sqrt{2}i$$

bulunur. Şimdi bulduğumuz değerleri $r+s\sqrt{2}i=(a+b\sqrt{2}i)(t+u\sqrt{2}i)+(c+d\sqrt{2}i)$ ifadesinde yerleştirirsek

$$4+5\sqrt{2}i=2(3+2\sqrt{2}i)+(-2+\sqrt{2}i)$$

elde ederiz. Burada $\phi_{-2}(-2+\sqrt{2}i)=|4+2|=6$ ve $\phi_{-2}(3+2\sqrt{2}i)=|9+8|=17$ 'dir. Sonuç olarak $\phi_{-2}(-2+\sqrt{2}i)<\phi_{-2}(3+2\sqrt{2}i)$ bulunur.

(iii) $m=-2$ olmak üzere $\mathbb{Z}+\mathbb{Z}\sqrt{2}i$'de $3+\sqrt{2}i\neq 0$ için

$$\frac{4+7\sqrt{2}i}{\underset{(3-\sqrt{2}i)}{3+\sqrt{2}i}}=\frac{(4+7\sqrt{2}i)(3-\sqrt{2}i)}{11}=\frac{26+17\sqrt{2}i}{11}=\frac{26}{11}+\frac{17}{11}\sqrt{2}i$$
$$=\left(2+\frac{4}{11}\right)+\left(2-\frac{5}{11}\right)\sqrt{2}i=\left(2+2\sqrt{2}i\right)+\left(\frac{4-5\sqrt{2}i}{11}\right)$$

dir. Buradan

$$4+7\sqrt{2}i=\left(3+\sqrt{2}i\right)\left(2+\sqrt{2}i\right)+\left(3+\sqrt{2}i\right)\left(\frac{4-5\sqrt{2}i}{11}\right)$$

ve

$$4+7\sqrt{2}i=\left(3+\sqrt{2}i\right)\left(2+2\sqrt{2}i\right)+\left(2-\sqrt{2}i\right)$$

elde edilir.

(iv) $m=-1$ olmak üzere $\mathbb{Z}+\mathbb{Z}i$'de $3+i\neq 0$ için

$$\frac{4+7i}{3+i}=\frac{(4+7i)(3-i)}{10}=\frac{19+17i}{10}=\frac{19}{10}+\frac{17}{10}i=\left(2-\frac{1}{10}\right)+\left(2-\frac{3}{10}\right)i$$

$$=(2+2i)+\left(-\frac{1}{10}-\frac{3}{10}i\right)$$

bulunur. Böylece

$$4+7i=(3+i)(2+2i)+(3+i)\left(-\frac{1}{10}-\frac{3}{10}i\right)$$

ve

$$4+7i=(3+i)(2+2i)+(-i)$$

elde edilir.

Teorem 3.2.4'ün ispatına benzer bir yolla aşağıdaki sonucu ispatlayabiliriz.

Teorem 3.2.8: $m\equiv 1(\bmod 4)$ ve m karesiz tamsayı olsun. Bu durumda $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$, ϕ_m li Euclid bölgesidir $\Leftrightarrow$ $\forall x,y\in\mathbb{Q}$ için

$$\phi_m\left(\left(x+y\sqrt{m}\right)-\left(a+b\left(\frac{1+\sqrt{m}}{2}\right)\right)\right)<1$$

olacak şekilde $a,b\in\mathbb{Z}$ vardır.

$m\equiv 1(\bmod 4)$ olmak üzere Teorem 3.2.6'de kesin olarak belirlediğimiz gibi, Teorem 3.2.8'dan ϕ_m'li Euclid bölgesi olan $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ tamlık bölgesindeki negatif karesiz tamsayıları da belirleyebiliriz.

Teorem 3.2.9: m negatif karesiz tamsayısı için $m\equiv 1(\bmod 4)$ olsun. Bu durumda $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ tamlık bölgesi ϕ_m'li Euclid bölgesidir $\Leftrightarrow$ $m=-3$, -7, -11'dir.

İspat: $\Leftarrow$: $m \equiv 1 \pmod 4$ olduğundan $x, y \in \mathbb{Q}$ ise $\left| \left(x - a - \frac{1}{2}b \right)^2 - m\left(y - \frac{1}{2}b \right)^2 \right| < 1$ olacak şekilde a ve b tamsayılarının varlığı gösterilmelidir. Önerme 3.2.6'ya göre $|2y - b| \le \frac{1}{2}$ ve $\left| x - a - \frac{1}{2}b \right| \le \frac{1}{2}$ olacak şekilde a ve b tamsayıları vardır. $m = -3, -7, -11$ için

$$\left| \left(x - a - \frac{1}{2}b \right)^2 - m\left(y - \frac{1}{2}b \right)^2 \right| \le \left(x - a - \frac{1}{2}b \right)^2 + |m|\left(y - \frac{1}{2}b \right)^2 \le \frac{1}{4} + \frac{11}{16} = \frac{15}{16} < 1$$

elde edilir.

$\Rightarrow$: $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2} \right)$ tamlık bölgesi ise önceki teoreme göre her $x, y \in \mathbb{Q}$ için

$$\left| \left(x - a - \frac{1}{2}b \right)^2 - m\left(y - \frac{1}{2}b \right)^2 \right| < 1$$

olacak biçimde a ve b tamsayıları vardır. Dolayısıyla $x = \frac{1}{4}$, $y = \frac{1}{4}$ için

$$\left| \left(\frac{1}{4} - a - \frac{1}{2}b \right)^2 - m\left(\frac{1}{4} - \frac{1}{2}b \right)^2 \right| < 1$$

olacak biçimde a ve b tamsayıları vardır. Buradan

$$\left[\frac{1}{2}\left(\frac{1}{2} - 2a - b \right)^2 + |m|\left[\frac{1}{2}\left(\frac{1}{2} - b \right)^2 \right] \right] < 1$$

ve böylece

$$\frac{1}{4}\left[\left(\frac{1}{2} - 2a - b \right)^2 + |m|\left(\frac{1}{2} - b \right)^2 \right] < 1$$

bulunur. Diğer taraftan $\left| \frac{1}{2} - 2a - b \right| \ge \frac{1}{2}$ ve $\left| \frac{1}{2} - b \right| \ge \frac{1}{2}$ olduğundan

$$\frac{1}{4}\left[\left(\frac{1}{2} - 2a - b \right)^2 + |m|\left(\frac{1}{2} - b \right)^2 \right] \ge \frac{1}{4}\left[\frac{1}{4} + |m|\frac{1}{4} \right] = \frac{1}{16}\left(1 + |m| \right)$$

yazılabilir. Böylece $\frac{1}{16}(1+|m|)<1$, yani $11+|m|<16$ bulunur. $|m|<15$ ve $m\equiv 1(\bmod 4)$ olduğu göz önüne alınırsa $m=-3$, -7, -11 elde edilir. Dolayısıyla teorem ispatlanmış olur.

Teorem 3.2.10: $m\equiv 2,3(\bmod 4)$ ve m pozitif karesiz bir tamsayı olsun. Bu durumda $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ tamlık bölgesi ϕ_m'li Euclid bölgesidir $\Leftrightarrow$ $m=2$, 3, 6, 7, 11, 19, 57'dir [4].

Teorem 3.2.11: $m\equiv 1(\bmod 4)$ ve m pozitif karesiz bir tamsayı olsun. Bu durumda $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ tamlık bölgesi ϕ_m'li Euclid bölgesidir $\Leftrightarrow$ $m=5$, 13, 17, 21, 29, 33, 37, 41, 73'tür [4].

Teorem 3.2.10'un özel bir durumu olan aşağıdaki teoremi ispat edeceğiz.

Teorem 3.2.12: $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ tamlık bölgesi m = 2, 3, 6 için ϕ_m'li Euclid bölgesidir.

İspat: m = 2, 3, 6 ve $x,y\in\mathbb{Q}$ olsun. Önerme 3.2.5'e göre,

$$|x-a|\le\frac{1}{2},\ |y-b|\le\frac{1}{2}$$

olacak şekilde a ve b tamsayıları vardır.

$x\ge 0$ ve $y\ge 0$ için $|x-y|>\max\{|x|,|y|\}$ alalım. $x>y$ kabul edelim.

$$\begin{aligned} x>y &\Rightarrow |x|>|y| \text{ ve } |x-y|=x-y \\ &\Rightarrow |x-y|>|x| \\ &\Rightarrow x-y>x \\ &\Rightarrow y<0 \end{aligned}$$

olur. Bu ise olamaz. Öyleyse, $|x-y|\le\max\{|x|,|y|\}$'dir.

$(x-a)^2\ge 0$ ve $m(y-b)^2\ge 0$ olduğundan

$$\left|(x-a)^2 - m(y-b)^2\right| \le \max\left\{|x-a|^2, m|y-b|^2\right\}$$

dir. $|x-a|^2 \le \frac{1}{4}$ ve $m|y-b|^2 \le \frac{3}{4}$ veya $m|y-b|^2 \le \frac{2}{4}$ olduğundan

$$\left|(x-a)^2 - m(y-b)^2\right| \le \max\left\{|x-a|^2, m|y-b|^2\right\} \le \frac{3}{4}$$

elde edilir. Buradan

$$\phi_m\left(\left(x+y\sqrt{m}\right)-\left(a+b\sqrt{m}\right)\right) = \left|(x-a)^2 - m(y-b)^2\right| < 1$$

bulunur. Teorem 3.2.4'den istenen sonuç elde edilir.

$m=6$ için $\mathbb{Z}+\mathbb{Z}\sqrt{6}$, ϕ_6'lı Euclid bölgesi olmasın. Bu durumda Teorem 3.2.4'e göre, $\forall x, y \in \mathbb{Z}$ için $\phi_6\left(\left(r+s\sqrt{6}\right)-\left(x+y\sqrt{6}\right)\right) \ge 1$ olacak şekilde $r, s \in \mathbb{Q}$ vardır. Yani $\forall x, y \in \mathbb{Z}$ için $\left|(r-x)^2 - 6(s-y)^2\right| \ge 1$ olmalıdır. Biz

$$0 \le \varepsilon_1 r + u_1 \le \frac{1}{2} \text{ olacak şekilde } \varepsilon_1 = \mp 1 \text{ ve } u_1 \in \mathbb{Z}$$

ve

$$0 \le \varepsilon_2 s + u_2 \le \frac{1}{2} \text{ olacak şekilde } \varepsilon_2 = \mp 1 \text{ ve } u_2 \in \mathbb{Z}$$

seçebiliriz.

$$r_1 = \varepsilon_1 r + u_1 \in \mathbb{Q},\ x_1 = \varepsilon_1 x + u_1 \in \mathbb{Z}$$

$$s_2 = \varepsilon_2 s + u_2 \in \mathbb{Q},\ y_1 = \varepsilon_2 y + u_2 \in \mathbb{Z}$$

olarak alınırsa

$$0 \le r_1 \le \frac{1}{2},\ 0 \le s_1 \le \frac{1}{2} \qquad \ldots (3.2.6)$$

ve böylece her $x, y \in \mathbb{Z}$ için

$$\left|(r_1 - x_1)^2 - 6(s_1 - y_1)^2\right| \ge 1 \qquad \ldots (3.2.7)$$

bulunur. $(x_1, y_1) = (0,0)$, $(1,0)$, $(-1,0)$ alınırsa ve bu değerler (3.2.7)'de yerine yazılırsa

$$\begin{cases} \left|r_1^2 - 6s_1^2\right| \geq 1 \\ \left|(1-r_1)^2 - 6s_1^2\right| \geq 1 \\ \left|(1+r_1)^2 - 6s_1^2\right| \geq 1 \end{cases} \quad \ldots (3.2.8)$$

bulunur. (3.2.6)'dan,

$$\begin{cases} -\frac{3}{2} \leq r_1^2 - 6s_1^2 \leq \frac{1}{4} \\ -\frac{5}{4} \leq (1-r_1)^2 - 6s_1^2 \leq 1 \\ -\frac{1}{2} \leq (1+r_1)^2 - 6s_1^2 \leq 1 \end{cases} \quad \ldots (3.2.9)$$

elde edilir. (3.2.8) ve (3.2.9)'dan,

$$-\frac{3}{2} \leq r_1^2 - 6s_1^2 \leq -1 \quad \ldots (3.2.10)$$

$$\text{(i) } (1-r_1)^2 - 6s_1^2 = 1 \text{ veya (ii) } -\frac{5}{4} \leq (1-r_1)^2 - 6s_1^2 \leq -1 \quad \ldots (3.2.11)$$

ve

$$1 \leq (1+r_1)^2 - 6s_1^2 \leq \frac{9}{4} \quad \ldots (3.2.12)$$

elde edilir. (3.2.10) ve (3.2.12)'den

$$1 \leq 1 + 2r_1 + \left(r_1^2 - 6s_1^2\right) \leq 2r_1$$

yani $r_1 \geq \frac{1}{2}$ elde ederiz. Fakat $r_1 \leq \frac{1}{2}$'dir. Öyleyse $r_1 = \frac{1}{2}$ olmalıdır. Bu durumda (3.2.11) (i)'den $\frac{1}{4} - 6s_1^2 = 1$ olur ki, bu mümkün değildir ve (3.2.11) (ii)'den $\frac{1}{4} - 6s_1^2 \leq -1$, yani $s_1^2 \geq \frac{5}{24}$ olur. Fakat (3.2.12)'den $6s_1^2 \leq (1+r_1)^2 - 1 = \frac{5}{4}$ olur; bu $s_1^2 \geq \frac{5}{24}$, yani $s_1^2 = \frac{5}{24}$ ($s_1 = \sqrt{\frac{5}{24}} \notin \mathbb{Q}$) demektir ki, bu mümkün değildir. Bu da $\mathbb{Z} + \mathbb{Z}\sqrt{6}$'nın ϕ_6'lı Euclid bölgesi olduğunu gösterir.

Önceki teoremlerin sonucu olarak aşağıdaki teorem verilebilir.

Teorem 3.2.13: $m \not\equiv 1 \pmod 4$ ise $K_m = \mathbb{Z} + \mathbb{Z}\sqrt{m}$ ve $m \equiv 1 \pmod 4$ ise $K_m = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ olmak üzere K_m tamlık bölgesinin Euclid bölgesi olması için gerekli ve yeterli şart m = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 73 olmasıdır.

3.3. Euclid Bölgesi Olmayan Bölgeler

Burada ϕ_m fonksiyonuna göre Euclid bölgesi olmayan $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ için m'nin bazı değerlerini vereceğiz.

Teorem 3.3.1: m pozitif karesiz tamsayı olsun. $\left(\frac{m}{p}\right) = \left(\frac{m}{q}\right) = -1$ olacak şekilde birbirinden farklı p ve q asalları mevcut ve

$$pt + qu = m,\ p \nmid t,\ q \nmid u$$

olacak şekilde t ve u pozitif tam sayıları ile

$$r^2 \equiv pt \pmod m$$

olacak şekilde bir r tamsayısı varsa $\mathbb{Z} + \mathbb{Z}\sqrt{m}$, ϕ_m'li Euclid bölgesi değildir.

İspat: $\mathbb{Z} + \mathbb{Z}\sqrt{m}$, ϕ_m'li Euclid bölgesi olsun. Bu durumda

$$r\sqrt{m} = m\gamma + \delta,\ \phi_m(\delta) < \phi_m(m)$$

olacak şekilde $\gamma, \delta \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ vardır. $\gamma = x + y\sqrt{m}$ alınırsa,

$$\phi_m\left(r\sqrt{m} - m\left(x + y\sqrt{m}\right)\right) < \phi_m(m)$$

yani $\left|m^2x^2 - m(r - my)^2\right| < m^2$ elde edilir. Öyleyse

$$\left|mx^2 - (my - r)^2\right| < m$$

olur. Böylece

$$mx^2 - (my - r)^2 = mx^2 - m^2y^2 + 2myr - r^2$$

$$\equiv -r^2 \pmod{m}$$

$$\equiv -pt \pmod{m}$$

ve $0 < pt < pt + qu = m$ olduğundan

$$mx^2 - (my - r)^2 = -pt \text{ veya } mx^2 - (my - r)^2 = m - pt$$

olmalıdır. Dolayısıyla $X = x$, $Y = my - r$ ise

$$mX^2 - Y^2 = -pt \text{ veya } mX^2 - Y^2 = qu$$

olur. $mX^2 - Y^2 = -pt$ olsun. $\left(\frac{m}{p}\right) = -1$ olduğundan $p \nmid m$'dir. Biliyoruz ki, p asal sayı iken $p^k \mid m$ ve $p^{k+1} \nmid m$ ise k sayısına, $p^e \mid m$ şartını sağlayan e $(e \geq 0)$ sayılarının en büyüğüdür denir ve bu durum $p^k \| m$ ile gösterilir. Şimdi $p \nmid t$ olduğunda $p \| -pt$ olduğunu görelim. $p \nmid t$ iken $p \nmid -pt$ ise $p^{k+1} \| -pt$ olacak şekilde k > 0 vardır. Öyleyse $-pt = p^{k+1}.x$ olacak şekilde $x \in \mathbb{Z}$ vardır. Buradan $-t = p^k x$ ise $p^k \mid t$ olur. Böylece $p \mid t$ elde edilir. Bu ise çelişkidir. Dolayısıyla, $p \nmid t$ iken $p \| -pt$ olur. Bu yüzden $p \nmid X$ ve $p \nmid Y$'dir. Ayrıca

$$\left(\frac{m}{p}\right) = \left(\frac{mX^2}{p}\right) = \left(\frac{Y^2}{p}\right) = 1$$

olduğundan bu $\left(\frac{m}{p}\right) = -1$ olmasıyla çelişir. Bu ise $\mathbb{Z} + \mathbb{Z}\sqrt{m}$'nin ϕ_m fonksiyonuna göre Euclid bölgesi olmadığını gösterir.

Şimdi $mX^2 - Y^2 = qu$ olsun. $\left(\frac{m}{q}\right) = -1$ olduğundan $q \nmid m$ elde edilir. Öyleyse $q \nmid u$ olduğundan $q \| qu$ olur. Bu yüzden $p \nmid X$ ve $p \nmid Y$'dir. Bu

$$\left(\frac{m}{q}\right) = \left(\frac{mX^2}{q}\right) = \left(\frac{Y^2}{q}\right) = 1$$

olmasını gerektirir. Bu ise $\left(\frac{m}{q}\right) = -1$ olması ile çelişir. Bu da $\mathbb{Z} + \mathbb{Z}\sqrt{m}$'nin ϕ_m'li Euclid bölgesi olmadığını gösterir.

Aşağıda $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ yi ϕ_m'li Euclid bölgesi yapmayan bazı m değerlerini belirlemek için Teorem 3.3.1'i kullanacağız.

Teorem 3.3.2: $\mathbb{Z}+\mathbb{Z}\sqrt{m}$, $m=23$, 47, 59, 83 için ϕ_m'li Euclid bölgesi değildir.

İspat: Teorem 3.3.1'den aşağıdaki tablo oluşur.

m	p	q	t	u	r
23	3	5	1	4	7
47	3	5	4	7	23
59	3	7	15	2	24
83	3	5	1	16	13

Örnek 3.3.3: m = 23, t = 1, p = 3, u = 4, q = 5, ve r = 7 değerleri için

$$\left(\frac{m}{p}\right)=\left(\frac{23}{3}\right)=\left(\frac{2}{3}\right)=-1$$

ve

$$\left(\frac{m}{q}\right)=\left(\frac{23}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)(-1)^{\frac{5-1}{2}}=\left(\frac{2}{3}\right)=-1$$

bulunur. Ayrıca $pt+qu=3.1+5.4=23=m$, $3\nmid 1$ ve $5\nmid 4$ 'tür. Burada

$$7^2\equiv 3(\mathrm{mod}\,23)$$
$$\downarrow$$
$$\text{p.t} = 3.1 = 3$$

olduğu görülür. Öyleyse $\mathbb{Z}+\mathbb{Z}\sqrt{23}$, ϕ_{23}'lü Euclid bölgesi değildir.

Önerme 3.3.4: $|a|<n$ olmak üzere $a\equiv b(\mathrm{mod}\,n)$ ise

$$a=b-n\left[\!\left[\frac{b}{n}\right]\!\right] \text{ veya } a=b-n\left[\!\left[1+\frac{b}{n}\right]\!\right]$$

dir.

İspat: $a \equiv b \pmod{n}$ ise $a = b + nk$ olacak şekilde $k \in \mathbb{Z}$ vardır. Buradan $k = \frac{a-b}{n} = \frac{a}{n} - \frac{b}{n}$ olur.

$$|a| < n \Rightarrow \left|\frac{a}{n}\right| < 1 \Rightarrow -1 < \frac{a}{n} < 1 \Rightarrow \left[\!\left[\frac{a}{n}\right]\!\right] = 0 \text{ veya } \left[\!\left[\frac{a}{n}\right]\!\right] = -1$$

dir.

$$\frac{a}{n} = k + \frac{b}{n} \Rightarrow \left[\!\left[\frac{a}{n}\right]\!\right] = \left[\!\left[k + \frac{b}{n}\right]\!\right] = k + \left[\!\left[\frac{b}{n}\right]\!\right]$$

$$\Rightarrow k = \left[\!\left[\frac{a}{n}\right]\!\right] - \left[\!\left[\frac{b}{n}\right]\!\right]$$

$$\left[\!\left[\frac{a}{n}\right]\!\right] = 0 \Rightarrow k = -\left[\!\left[\frac{b}{n}\right]\!\right] \text{ ve } \left[\!\left[\frac{a}{n}\right]\!\right] = -1 \Rightarrow k = -\left(1 + \left[\!\left[\frac{b}{n}\right]\!\right]\right)$$

dir. Öyleyse $a = b - n\left[\!\left[\frac{b}{n}\right]\!\right]$ veya $a = b - n\left[\!\left[1 + \frac{b}{n}\right]\!\right]$ elde edilir.

Teorem 3.3.5: $m \equiv 1 \pmod{4}$ olmak üzere m bir pozitif karesiz tamsayı olsun. $\left(\frac{m}{p}\right) = \left(\frac{m}{q}\right) = -1$ olacak şekilde birbirinden farklı p ve q asal sayıları ve

$$p \,\|\, (m-1)r^2 - 4m\left[\!\left[\frac{(m-1)r^2}{4m}\right]\!\right],$$

$$q \,\|\, (m-1)r^2 - 4m\left[\!\left[\frac{(m-1)r^2}{4m}\right]\!\right] - 4m$$

olacak şekilde r tek tamsayısı varsa $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ ϕ_m'li Euclid bölgesi değildir.

İspat: m ve r her ikisi de tek olduğundan $\frac{m-r}{2} \in \mathbb{Z}$'dir. Bu yüzden

$$\frac{m + r\sqrt{m}}{2} = \frac{m-r}{2} + r\left(\frac{1+\sqrt{m}}{2}\right) \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$$

olur. $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ ϕ_m'li Euclid bölgesi olsun. Bu durumda

$$\frac{m+r\sqrt{m}}{2}=m\gamma+\delta\ ,\ \phi_m(\delta)<\phi_m(m)$$

olacak şekilde $\gamma,\delta\in\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ elemanları vardır. Böylece $\gamma=x+y\left(\frac{1+\sqrt{m}}{2}\right)$ olarak alınırsa

$$\phi_m\left(\frac{m+r\sqrt{m}}{2}-m\left(x+y\left(\frac{1+\sqrt{m}}{2}\right)\right)\right)<\phi_m(m)$$

bulunur. Buradan

$$\left|\left(\frac{m}{2}-m-\frac{my}{2}\right)^2-m\left(\frac{r}{2}-\frac{my}{2}\right)^2\right|<m^2$$

olur. Burada eşitsizliğin her iki yanı $\frac{4}{m}$ ile çarpılırsa

$$\left|m(1-2x-y)^2-(r-my)^2\right|<4m$$

elde edilir. $X=1-2x-y$ ve $Y=r-my$ alınırsa

$$\left|mX^2-Y^2\right|<4m$$

bulunur. $m\equiv 1(\bmod 4)$ ve her u, v tamsayısı için $(u+2v)^2\equiv u^2(\bmod 4)$ olduğundan

$$(X+2x)^2\equiv X^2(\bmod 4)\Rightarrow X^2\equiv(1-y^2)(\bmod 4)$$

elde edilir. Ayrıca $Y^2=r^2-2rmy+m^2y^2$ ve $r^2\equiv 1(\bmod 4)$ olduğundan

$$Y^2\equiv 1-2ry+y^2(\bmod 4)$$

bulunur. $r\equiv 1(\bmod 4)$ ise $Y^2\equiv 1-2y+y^2\equiv(1-y)^2(\bmod 4)$'dir. $r\equiv 3(\bmod 4)$ ise $Y^2\equiv 1-6y+y^2\equiv 1-2y+y^2\equiv(1-y)^2(\bmod 4)$ olur. Sonuç olarak

$$mX^2-Y^2\equiv(1-y)^2-(1-y)^2\equiv 0(\bmod 4)$$

elde edilir. Ayrıca

$$mX^2-Y^2\equiv -Y^2\equiv -r^2(\bmod m)$$

dir. $m\equiv 1(\bmod 4)$ ise $4\mid m-1$'dir. Buradan $4\mid(m-1)r^2$ olur, yani $(m-1)r^2\equiv 0(\bmod 4)$'tür. $mX^2-Y^2\equiv 0(\bmod 4)$ ise $mX^2-Y^2\equiv(m-1)r^2(\bmod 4)$

elde edilir. Yine $mX^2 - Y^2 \equiv -r^2 \pmod{m}$ ve $-r^2 \equiv (m-1)r^2 \pmod{m}$ ve $(4,m)=1$ olduğundan

$$mX^2 - Y^2 \equiv (m-1)r^2 \pmod{4m}$$

elde edilir. Böylece Önerme 3.3.4'e göre

$$mX^2 - Y^2 = (m-1)r^2 - 4m\left[\!\left[\frac{(m-1)r^2}{4m}\right]\!\right]$$

veya

$$mX^2 - Y^2 = (m-1)r^2 - 4m\left[\!\left[\frac{(m-1)r^2}{4m}\right]\!\right] - 4m$$

bulunur. İlk durumdan $p \,||\, mX^2 - Y^2$'dir. $\left(\frac{m}{p}\right) = -1$ olduğundan $p \nmid m$'dir. Bu $p \nmid X$ ve $p \nmid Y$ olması demektir. Bu durumda

$$\left(\frac{m}{p}\right) = \left(\frac{mX^2}{p}\right) = \left(\frac{Y^2}{p}\right) = 1$$

elde edilir. Bu durum $\left(\frac{m}{p}\right) = -1$ olması ile çelişir. İkinci durum için de benzer işlemler yapılır.

Şimdi $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{53}}{2}\right)$'nin ϕ_{53}'lü Euclid bölgesi olmadığını göstermek için Teorem 3.3.5'i kullanıyoruz.

Teorem 3.3.6: $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{53}}{2}\right)$, ϕ_{53}'lü Euclid bölgesi değildir.

İspat: m =53, q = 19, p = 5 ve r = 29 değerleri için yukarıdaki teoremi kullanıyoruz:

$$\left(\frac{m}{p}\right) = \left(\frac{53}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right).(-1)^{\frac{5-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$$

$$\left(\frac{m}{q}\right) = \left(\frac{53}{19}\right) = \left(\frac{15}{19}\right) = \left(\frac{3}{19}\right).\left(\frac{5}{19}\right) = \left(\frac{19}{3}\right).(-1)^{\frac{19-1}{2}\cdot\frac{3-1}{2}}\left(\frac{19}{5}\right).(-1)^{\frac{19-1}{2}\cdot\frac{5-1}{2}}$$

$$= \left(\frac{1}{3}\right).(-1).\left(\frac{4}{5}\right) = (-1)\left(\frac{2}{5}\right)^2 = (-1).1 = -1$$

$$(m-1)r^2 - 4m\left[\!\left[\frac{(m-1)r^2}{4m}\right]\!\right] = 52 - 29^2 - 4.53.\left[\!\left[\frac{52.29^2}{4.53}\right]\!\right]$$

$$= 43732 - 212.206 = 60 = 2^3.3.5$$

$$= 43732 - 43672 = -152 = -19.2^3$$

bulunur. Buradan $5 \| 2^3.3.5$ ve $19 \| -19.2^3$ elde edilir. Öyleyse $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{53}}{2}\right)$, ϕ_{53} 'lü Euclid bölgesi değildir.

Teorem 3.2.9'un bir sonucu $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-19}}{2}\right)$ bölgesinin ϕ_{-19}'lu Euclid bölgesi olmamasıdır. Bu bölge diğer fonksiyonlarla da Euclid bölgesi değildir. $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-19}}{2}\right)$ bölgesinin evrensel yan bölene sahip olmadığını ve ayrıca bir fonksiyonla Euclid bölgesi olmadığını göstereceğiz.

Şimdi evrensel yan böleni tanımlıyoruz. Bir D tamlık bölgesi için

$$\widetilde{D} = U(D) \cup \{0\}$$

olarak tanımlanır. Bu durumda $D - \widetilde{D} = \varnothing$ olması için gerekli ve yeterli şart D'nin bir cisim olmasıdır.

Tanım 3.3.7: D bir tamlık bölgesi olsun ve D bir cisim olmasın. $u \in D - \widetilde{D}$ olsun. Her $x \in D$ için $u \mid x - z$ olacak şekilde bir $z \in \widetilde{D}$ mevcut ise u'ya bir evrensel yan bölen denir.

Teorem 3.3.8: D cisim olmayan bir tamlık bölgesi olsun. D evrensel yan bölene sahip değilse D, Euclid bölgesi değildir.

İspat: D, Euclid fonksiyonu ϕ ile Euclid bölgesi olsun ve evrensel yan bölene sahip olmasın.

$$S = \{\phi(v) : v \in D - \widetilde{D}\}$$

ile tanımlı tamsayıların altkümesini göz önüne alalım. D cisim olmadığından $D - \widetilde{D} \neq \varnothing$ ve S boş kümeden farklıdır. Euclid fonksiyonunun 4. özelliğine göre S alttan sınırlıdır. Bu durumda S en az bir $\phi(u)$ $(u \in D - \widetilde{D})$ elemanına sahiptir. D, ϕ ile Euclid bölgesi olduğundan $x \in D$ için

$$x = uy + z \text{ ve } \phi(z) < \phi(u)$$

olacak şekilde $y, z \in D$ vardır.

$$z = 0 \Rightarrow x = uy \text{ ve } u \mid x$$

ve

$$z \neq 0 \Rightarrow \phi(z) < \phi(u)$$

olduğundan $z \notin D - \widetilde{D}$, yani $z \in U(D)$'dir.

Her iki durumda $u \mid x - z$ olan $z \in \widetilde{D}$ vardır. Bu ise u'nun evrensel yan bölen olduğunu gösterir. Bu bir çelişkidir.

$m \equiv 2,3 \pmod 4$ olmak üzere m karesiz tamsayı ise $\mathbb{Z} + \mathbb{Z}\sqrt{m}$, $m = -1$ ve $m = -2$ için ϕ_m'li Euclid bölgesidir ve $m < -2$ (Teorem 3.2.6) için ϕ_m'li Euclid bölgesi değildir. Şimdi $\mathbb{Z} + \mathbb{Z}\sqrt{m}$'nin $m < -2$ olmak üzere bir fonksiyonla Euclid bölgesi olmadığını göstermek için Teorem 3.3.8'i kullanacağız.

Örnek 3.3.9: p asal ve $m \leq -(p+1)$ olmak üzere m bir tamsayı olsun. $\mathbb{Z} + \mathbb{Z}\sqrt{m}$'de p'nin indirgenemez olduğunu gösteriniz.

Çözüm: p asal olsun. m negatif tamsayısı $m \leq -(p+1)$ şartını sağlasın. $\mathbb{Z} + \mathbb{Z}\sqrt{m}$'de p'nin indirgenebilir olduğunu varsayalım. Bu durumda

$$a + b\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m} \text{ ve } c + d\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$$

elemanları vardır ve $a + b\sqrt{m}, c + d\sqrt{m} \notin U(\mathbb{Z} + \mathbb{Z}\sqrt{m})$ olmak üzere

$$p = (a + b\sqrt{m})(c + d\sqrt{m})$$

dir. Her iki tarafın modülünü alırsak,

$$p^2 = \left(a^2 - mb^2\right)\left(c^2 - md^2\right)$$

elde ederiz. $a^2 - mb^2$ ve $c^2 - md^2$ sayıları pozitif tamsayılardır ve p asaldır. Dolayısıyla $a^2 - mb^2 = 1$, $a^2 - mb^2 = p$ veya $a^2 - mb^2 = p^2$'dir.

Eğer $a^2 - mb^2 = 1$ ise $\left(a + b\sqrt{m}\right)\left(a - b\sqrt{m}\right) = 1$'dir. $a + b\sqrt{m} \in U(\mathbb{Z} + \mathbb{Z}\sqrt{m})$ olur. Bu olamaz.

Eğer $a^2 - mb^2 = p^2$ ise $c^2 - mb^2 = 1$'dir. Buradan $\left(c + d\sqrt{m}\right)\left(c - d\sqrt{m}\right) = 1$ olur. Böylece $c + d\sqrt{m} \in U(\mathbb{Z} + \mathbb{Z}\sqrt{m})$ olur. Bu yine olamaz.

Eğer $a^2 - mb^2 = p$ ise p karesiz olduğundan $b \neq 0$ dır. Öyleyse

$$p = a^2 - mb^2 \geq -mb^2 \geq (p+1)b^2 \geq p + 1 > p$$

elde edilir. Bu bir çelişkidir. Öyleyse $\mathbb{Z} + \mathbb{Z}\sqrt{m}$'de p indirgenemezdir.

Örnek 3.3.10: a) m bir tamsayı olmak üzere $m < -1$ için $U(\mathbb{Z} + \mathbb{Z}\sqrt{m}) = \{\mp 1\}$ ve $m = -1$ için $U\left(\mathbb{Z} + \mathbb{Z}i\right) = \pm 1, \pm i$ olduğunu gösteriniz.

b) $m < 0$ ve $m \equiv 1 \pmod 4$ olsun. Bu durumda $m \neq -3$ ise $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$'nin birimleri ± 1'dir. $m = -3$ ise birimler ± 1, $\pm\left(\frac{-1+\sqrt{-3}}{2}\right)$ ve $\pm\left(\frac{-1-\sqrt{-3}}{2}\right)$'dir.

Çözüm: a) $m < -1$ ve $m \in \mathbb{Z}$ olmak üzere $\alpha \in U(\mathbb{Z} + \mathbb{Z}\sqrt{m})$ olsun. Bu durumda $\alpha.\beta = 1$ olacak şekilde $\alpha = a + b\sqrt{m}$ ve $\beta = c + d\sqrt{m}$ elemanları vardır. Yani $(a + b\sqrt{m})(c + d\sqrt{m}) = 1$'dir. Buradan

$$(ac + bdm) + (ad + bc)\sqrt{m} = 1$$

bulunur. $m < -1$, $\sqrt{m} \in \mathbb{R} - \mathbb{Q}$ olduğundan $ac + bdm = 1$ ve $ad + bc = 0$'dır.Yani

$$\left(a^2 - mb^2\right)\left(c^2 - md^2\right) = \left(ac + bdm\right)^2 - m\left(ad + bc\right)^2 = 1$$

dir. $m<-1$ olduğundan a^2-mb^2 sayısı 1'i bölen bir pozitif tamsayıdır. Bu yüzden $a^2-mb^2=1$ olur. $b\neq 0$ ise $m<-1$ olduğundan

$$1=a^2-mb^2\geq -mb^2>b^2\geq 1$$

olur ki, bu bir çelişkidir. Bu yüzden $b=0$ ve $a=\mp 1$'dir. Bu ise $\alpha=\mp 1$ demektir. Şu halde

$$U(\mathbb{Z}+\mathbb{Z}\sqrt{m})\subseteq\{-1,1\}$$

dir. $\mp 1\in U(\mathbb{Z}+\mathbb{Z}\sqrt{m})$ olduğu açıktır. Yani $\{-1,1\}\subseteq U(\mathbb{Z}+\mathbb{Z}\sqrt{m})$'dir. Öyleyse

$$U(\mathbb{Z}+\mathbb{Z}\sqrt{m})=\{\mp 1\}$$

dir. $a+bi\in\mathbb{Z}+\mathbb{Z}i$ birim olsun. $(a+bi)(c+di)=1$ olacak şekilde $c+di\in\mathbb{Z}+\mathbb{Z}i$ vardır. Öyleyse $(a^2+b^2)(c^2+d^2)=1$'dir. $a^2+b^2=1$ ise $a=0$, $b=\pm 1$ veya $a=\pm 1$, $b=0$ bulunur. Buradan $a+bi=\pm 1$ veya $\pm i$ birimleri elde edilir.

b) $m=-3$ için $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right)$ de $x=a+b\left(\frac{1+\sqrt{-3}}{2}\right)$ birim olsun. Bu durumda $1=\left(a+b\left(\frac{1+\sqrt{-3}}{2}\right)\right)\left(c+d\left(\frac{1+\sqrt{-3}}{2}\right)\right)$ olur. Her iki tarafın normunu alırsak

$$1=\left[\left(a+\frac{b}{2}\right)^2+\frac{3b^2}{4}\right]\left[\left(c+\frac{d}{2}\right)^2+\frac{3d^2}{4}\right]$$

elde edilir. Buradan

$$1=\left(a+\frac{b}{2}\right)^2+\frac{3b^2}{4}=a^2+\frac{b^2}{4}+ab+\frac{3b^2}{4}$$

olur. Yani $a^2+ab+b^2=1$ bulunur. $b\geq 2$ olsun. Öyleyse $b^2\geq 4$ ve $\frac{3b^2}{4}\geq 3$ olur. Buradan

$$\left(a+\frac{b}{2}\right)^2=1-\frac{3b^2}{4}<0$$

elde edilir. Bu olamaz. Bu durumda $b<2$ olmalıdır. $b=\pm 1$ veya $b=0$'dır. Tüm birimler;

$b=1\Rightarrow a^2+a=0\Rightarrow a=0$ veya $a=-1\Rightarrow x=\frac{1+\sqrt{-3}}{2}$ veya $x=\frac{-1+\sqrt{-3}}{2}$,

$b=-1 \Rightarrow a^2-a=0 \Rightarrow a=0$ veya $a=1 \Rightarrow x=\dfrac{-1-\sqrt{-3}}{2}$ veya $x=\dfrac{1-\sqrt{-3}}{2}$,

$$b=0 \Rightarrow a^2=1 \Rightarrow a=\pm 1 \Rightarrow x=\pm 1$$

olarak bulunur.

$m\neq -3$ için $\mathbb{Z}+\mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right)$'de $x=a+b\left(\dfrac{1+\sqrt{m}}{2}\right)$ birim olsun. Bu durumda $m\leq -7$ ve $1=\left(a+b\left(\dfrac{1+\sqrt{m}}{2}\right)\right)\left(c+d\left(\dfrac{1+\sqrt{m}}{2}\right)\right)$ olur. Her iki tarafın normunu alırsak,

$$1=\left[\left(a+\frac{b}{2}\right)^2-\frac{mb^2}{4}\right]\left[\left(c+\frac{d}{2}\right)^2-\frac{md^2}{4}\right] \Rightarrow 1=\left(a+\frac{b}{2}\right)^2-\frac{mb^2}{4}$$

olur. Diğer taraftan $-m\geq 7$'dir. Yani $\dfrac{-mb^2}{4}\geq\dfrac{7b^2}{4}>1$'dir. Dolayısıyla $b\neq 0$ için $\dfrac{-mb^2}{4}>1$ ile $1=\left(a+\dfrac{b}{2}\right)^2-\dfrac{mb^2}{4}$ çelişir. $b=0$ olmalıdır. $b=0$ ise, $a^2=1$ ve $a=\pm 1$ olur. Öyleyse $x=\pm 1$ elde edilir.

Teorem 3.3.11: $m\equiv 2,3\pmod 4$ ve $m<-2$ olmak üzere m negatif karesiz tamsayı olsun. Bu durumda $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ Euclid bölgesi değildir.

İspat: $D=\mathbb{Z}+\mathbb{Z}\sqrt{m}$ olsun. Yukarıdaki örneğe göre $m<-2$ için $U(D)=\{-1,1\}$ olduğundan $\widetilde{D}=\{-1,0,1\}$'dir. D de bir evrensel yan bölen u olsun. Bu durumda u, $2-1$, $2-0$, $2+1$ değerlerinden birini bölmelidir, yani 1, 2, 3 sayılarından birini bölmelidir. Fakat evrensel yan bölen birim değildir, yani u sayısı için $u\nmid 1$'dir. Bu yüzden $u\mid 2$ veya $u\mid 3$ olur. $m\equiv 2,3\pmod 4$ ve $m<-2$ olduğundan $m\leq -5$'tir. Yukarıdaki örneğe göre 2 ve 3'ün her ikisi de D'de indirgenemezdir. Burada mümkün olan evrensel yan bölenler 2, -2, 3 ve -3'tür. Evrensel yan bölen tanımına göre her $x\in D$ için $u\mid x-z$ olacak şekilde bir $z\in\widetilde{D}$ vardır. $x=\sqrt{m}\in\mathbb{Z}+\mathbb{Z}\sqrt{m}$

alalım. u=2, -2, 3, -3 sayılarından hiçbiri $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ 'nin elemanları olan $\sqrt{m}-1$, $\sqrt{m}$, $\sqrt{m}+1$ 'den birini bölmez.

Örneğin $2\mid\sqrt{m}$ olsun. $\sqrt{m}=2.x$ olacak şekilde $x\in\mathbb{Z}+\mathbb{Z}\sqrt{m}$ vardır. Dolayısıyla $a,b\in\mathbb{Z}$ için $x=a+b\sqrt{m}$ olmak üzere $\sqrt{m}=2(a+b\sqrt{m})$ 'dir. Buradan $2a=0$ ve $2b=1$ elde edilir. Ama $a+b\sqrt{m}=0+\frac{1}{2}\sqrt{m}\notin\mathbb{Z}+\mathbb{Z}\sqrt{m}$ olur. Dolayısıyla $2\nmid\sqrt{m}$ olur. Öyleyse $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ 'nin evrensel yan böleni yoktur. Bu yüzden Teorem 3.3.8'e göre D Euclid bölgesi değildir.

Teorem 3.3.13'ü ispatlamak için aşağıdaki örneği verelim.

Örnek 3.3.12: p asal olsun. $m\equiv 1(\bmod 4)$ ve $m\le -(4p+1)$ olmak üzere m karesiz bir tamsayı olsun. Bu takdirde $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ 'de p elemanı indirgenemezdir.

Çözüm: p asal olsun. $m\equiv 1(\bmod 4)$ ve $m\le -(4p+1)$ olmak üzere m karesiz bir tamsayı olsun. $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ 'de p'nin indirgenebilir olduğunu varsayalım. Bu durumda $p=\left[a+b\left(\frac{1+\sqrt{m}}{2}\right)\right]\left[c+d\left(\frac{1+\sqrt{m}}{2}\right)\right]$ olacak biçimde

$$a+b\left(\frac{1+\sqrt{m}}{2}\right)\in\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) \text{ ve } c+d\left(\frac{1+\sqrt{m}}{2}\right)\in\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$$

elemanları vardır ve $a+b\left(\frac{1+\sqrt{m}}{2}\right),c+d\left(\frac{1+\sqrt{m}}{2}\right)\notin U\left(\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)\right)$ 'dir. Her iki tarafın modülünü alırsak,

$$p^2=\left(\left(a+\frac{b}{2}\right)^2-\frac{mb^2}{4}\right)\left(\left(c+\frac{d}{2}\right)^2-\frac{md^2}{4}\right)$$

elde ederiz. $\left(a+\frac{b}{2}\right)^2-\frac{mb^2}{4}$ ve $\left(c+\frac{d}{2}\right)^2-\frac{md^2}{4}$ sayıları pozitiftir ve p asaldır. Dolayısıyla

$$\left(a+\frac{b}{2}\right)^2-\frac{mb^2}{4}=1,\ \left(a+\frac{b}{2}\right)^2-\frac{mb^2}{4}=p \text{ veya } \left(a+\frac{b}{2}\right)^2-\frac{mb^2}{4}=p^2$$

dir. Eğer $\left(a+\frac{b}{2}\right)^2-\frac{mb^2}{4}=1$ ise $\left(\left(a+\frac{b}{2}\right)-\frac{b\sqrt{m}}{2}\right)\left(\left(a+\frac{b}{2}\right)+\frac{b\sqrt{m}}{2}\right)=1$ ve böylece

$$a+b\left(\frac{1+\sqrt{m}}{2}\right)\in U\left(\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)\right)$$

olur. Bu bir çelişkidir. Eğer $\left(a+\frac{b}{2}\right)^2-\frac{mb^2}{4}=p^2$ ise $\left(c+\frac{d}{2}\right)^2-\frac{md^2}{4}=1$ ve böylece $\left(\left(c+\frac{d}{2}\right)-\frac{d\sqrt{m}}{2}\right)\left(\left(c+\frac{d}{2}\right)+\frac{d\sqrt{m}}{2}\right)=1$ olur. Buradan

$$c+d\left(\frac{1+\sqrt{m}}{2}\right)\in U\left(\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)\right)$$

bulunur. Bu da çelişkidir. $\left(a+\frac{b}{2}\right)^2-\frac{mb^2}{4}=p$ ise p tam kare olamayacağından $b\neq 0$ olmalıdır. Ayrıca

$$p=\left(a+\frac{b}{2}\right)^2-\frac{mb^2}{4}\geq-\frac{mb^2}{4}\geq(4p+1)\frac{b^2}{4}=\left(p+\frac{1}{4}\right)b^2\geq p+\frac{1}{4}>p$$

dır. Bu ise çelişkidir. Öyleyse $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$'de p elemanı indirgenemezdir.

Teorem 3.3.13: $m\equiv 1(\bmod 4)$ ve $m<-11$ olmak üzere m bir negatif karesiz tamsayı olsun. Bu durumda $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$, Euclid bölgesi değildir.

İspat: $D=\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ olsun. $m\neq -3$ olduğundan $U(D)=\{-1,1\}$ 'dir. Öyleyse $\widetilde{D}=\{-1,0,1\}$ olur. D de bir evrensel yan bölen u olsun. Bu durumda u, $2-1$, $2-0$, $2+1$ sayılarından birini bölmelidir. Yani u sayısı 1, 2 veya 3 sayılarından birini bölmelidir. u birim olmadığından u sayısı 2 veya 3'ü böler. $m\leq -15$ olduğundan yukarıdaki örneğe göre 2 ve 3'ün her ikisi de $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$'de indirgenemezdir. Bu yüzden sadece mümkün olan yan bölenler 2, -2, 3 veya -3'tür. Evrensel yan bölen tanımına göre her $x\in D$ için $u\mid x-z$ olacak şekilde bir $z\in\widetilde{D}$ vardır.

$$x=\frac{1}{2}(1+\sqrt{m})\in\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$$

alalım. u=2, -2, 3, -3 bölenlerinden biri $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$'nin

$$\frac{1}{2}\left(-1+\sqrt{m}\right)=\frac{1}{2}\left(1+\sqrt{m}\right)-1,\ \frac{1}{2}\left(1+\sqrt{m}\right),\ \frac{1}{2}\left(3+\sqrt{m}\right)=\frac{1}{2}\left(1+\sqrt{m}\right)+1$$

elemanlarından birini bölmelidir. Fakat u bu elemanlardan hiç birini bölmez. Öyleyse böyle evrensel yan bölenler yoktur. Bu yüzden Teorem 3.3.8'e göre D, Euclid bölgesi değildir.

Her esas ideal bölgesinin Euclid bölgesi olması gerekmediğini göstermek için aşağıdaki normu tanımlıyoruz.

Tanım 3.3.14: D tamlık bölgesi ve $N:D\to\mathbb{Z}$ bir Euclid fonksiyonu olsun. Ayrıca $x\in D$ için $N(x)\geq 0$ ve $x\neq 0$ ise $N(x)>0$ olsun.

Eğer her $a,b\in D$ için $b\mid a$ veya $s,t\in D$ elemanları $0<N(sa-tb)<N(b)$ olacak biçimde mevcut ise N'ye bir Dedekind Hasse normu denir.

Önerme 3.3.15: D bir tamlık bölgesi olsun. D tamlık bölgesi esas ideal bölgesidir $\Leftrightarrow$ D bir Dedekind Hasse normuna sahiptir.

İspat: $\Leftarrow$: D bir Dedekind Hasse normuna sahip ve $I \neq \{0\}$ ideali D'nin bir ideali olsun. $S = \{N(x) \mid x \neq 0, x \in I\}$ ise $S \subseteq \mathbb{N}$ ve $S \neq \varnothing$'dir. $b \in I$ olmak üzere $N(b)$, S'nin en küçük elemanı olsun. $a \neq 0$ ve $a \in I$ ise $\langle a,b \rangle \subset I$'dır. $N(b)$'nin tanımına göre $b \mid a$'dır. Dolayısıyla $a = bx$ olacak biçimde bir $x \in D$ vardır. Buradan $a \in \langle b \rangle$ bulunur. Böylece $I \subset \langle b \rangle$ olur. $b \in I$ olduğundan $\langle b \rangle \subset I$'dır. Bu ise $I = \langle b \rangle$ olduğunu gösterir.

$\Rightarrow$: Bu kısmın ispatı için [8] nolu kaynağa bakılabilir.

Örnek 3.3.16: $D = \mathbb{Z} + \mathbb{Z}\left(\left(1+\sqrt{-19}\right)/2\right)$ kuadratik tamsayı halkası olsun. D üzerinde tanımlı

$$N\left(a + b\frac{\left(1+\sqrt{-19}\right)}{2}\right) = a^2 + ab + 5b^2$$

normun Dedekind Hasse normu olduğunu gösterip, Önerme 3.3.15'e göre D'nin esas ideal bölgesi olduğunu göstereceğiz.

Çözüm: D'nin sıfırdan farklı elemanları α, β ve $\beta \nmid \alpha$ olsun. Bu durumda

$$0 < N(s\alpha - t\beta) < N(\beta)$$

olacak biçimde $s,t \in D$ elemanlarının mevcut olduğunu gösterelim. Bunun için $0 < N\left(\frac{\alpha}{\beta}s - t\right) < 1$ olduğunu göstermek yeterlidir. $c > 0$ ve $(a,b,c) = 1$ olmak üzere $\frac{\alpha}{\beta} = \frac{a + b\sqrt{-19}}{c}$ olsun. $\beta \nmid \alpha$ olduğundan $c > 1$'dir. $(a,b,c) = 1$ olduğundan $ax + by + cz = 1$ olacak biçimde $x, y, z \in \mathbb{Z}$ vardır. Önerme 3.2.6'ya göre

$$\left|\frac{ay - 19bx}{c} - q\right| \leq \frac{1}{2}$$

olacak biçimde bir $q \in \mathbb{Z}$ vardır. $s = y + x\sqrt{-19}$, $t = q - z\sqrt{-19}$ olsun. Eğer $c \geq 5$ ise

$$\frac{(ay-19bx-cq)^2+19(ax+by+cz)^2}{c^2} \le \frac{\frac{c^2}{4}+19}{c^2} = \frac{1}{4}+\frac{19}{c^2} < 1$$

elde edilir. Bu ise $0 < N\left(\frac{\alpha}{\beta}s-t\right) < 1$ olduğunu gösterir. $c=2$ olsun. Bu durumda a ve b tamsayılarından biri tek diğeri çifttir. Çünkü $\frac{\alpha}{\beta} \notin \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{-19}}{2}\right)$'dir. $s=1$ ve $t=\frac{(a-1)+b\sqrt{-19}}{2}$ alınırsa

$$0 < N\left(\frac{\alpha}{\beta}s-t\right) = N\left(\frac{a+b\sqrt{-19}}{2}-\frac{(a-1)+b\sqrt{-19}}{2}\right) = \frac{1}{2} < 1$$

bulunur. $c=3$ olsun. Şimdi $3 \nmid a^2+19b^2$ olduğunu gösterelim. $3 \mid a^2+19b^2$ olduğunu kabul edelim. $3 \mid 18b^2$ olduğundan $3 \mid a^2+19b^2-18b^2$, yani $3 \mid a^2+b^2$ elde edilir. Bu ise $3 \mid a$ ve $3 \mid b$ olduğunu gösterir. $c=3$ olduğundan bu durum $(a,b,c)=1$ olmasıyla çelişir. Şu halde $3 \nmid a^2+19b^2$ olur. Dolayısıyla

$$a^2+19b^2 = 3q+r,\ 1 \le r \le 2$$

olacak biçimde q ve r tamsayıları vardır. Bu takdirde $s=a-b\sqrt{-19}$ ve $t=q$ alınırsa

$$N\left(\frac{\alpha}{\beta}s-t\right) = N\left(\frac{a+b\sqrt{-19}}{c}.\left(a-b\sqrt{-19}\right)-q\right) = N\left(\frac{a^2+19b^2}{c}-q\right)$$

$$= N\left(\frac{3q+r}{3}-q\right) = N\left(q+\frac{r}{3}-q\right) = N\left(\frac{r}{3}\right) = \frac{r^2}{9} \le \frac{4}{9} < 1$$

bulunur. Son olarak $c=4$ olduğunu varsayalım. Bu durumda da a ve b tamsayılarının her ikisi de çift olamaz. a ve b tamsayılarından biri tek diğeri çift olsun. Bu ise a^2+19b^2 tamsayısının tek tamsayı olduğunu gösterir. Şu halde $0 < r < 4$ olmak üzere $a^2+19b^2 = 4q+r$ olacak biçimde q ve r tamsayıları vardır. Bu durumda $s=a-b\sqrt{-19}$ ve $t=q$ alınırsa $N\left(\frac{\alpha}{\beta}s-t\right) < 1$ olduğu görülür. a ve b tamsayılarının ikisi de tek ise $a^2+19b^2 = 1+3(\mathrm{mod}\,8)$ yazılabilir. Bu durumda

$a^2+19b^2=8q+4$ olacak biçimde $q\in\mathbb{Z}$ vardır. Böylece $s=\frac{a-b\sqrt{-19}}{2}$ ve $t=q$ alınırsa $0<N\left(\frac{\alpha}{\beta}s-t\right)<1$ elde edilir.

Şu halde daima $0<N\left(\frac{\alpha}{\beta}s-t\right)<1$ olacak biçimde $s,t\in D$ elemanları mevcuttur. Bu ise N normunun bir Dedekind Hasse normu olduğunu gösterir. Önerme 3.3.15'e göre D bir esas ideal bölgesi olur.

BÖLÜM 4. TEK TÜRLÜ PARÇALANMALI BÖLGELER

4.1 Tek Türlü Parçalanmalı Bölgeler

Teorem 4.1.1: $m \equiv 1 \pmod 4$ ise $K_m = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ ve $m \not\equiv 1 \pmod 4$ ise $K_m = \mathbb{Z} + \mathbb{Z}\sqrt{m}$ olsun. Bu durumda K_m'de sıfırdan farklı, birim olmayan her bir eleman indirgenemezdir veya indirgenemez elemanların çarpımı biçiminde yazılabilir.

İspat: α indirgenemez ise ispat biter. Şimdi n üzerinden tümevarımla ispat yapalım. $n \geq 2$ olmak üzere P(n) önermesi şöyle tanımlansın; α, K_m'de sıfırdan farklı, birim olmayan bir eleman ve $N(\alpha) \leq n$ ise α indirgenemez olsun veya α, indirgenemez elemanların çarpımı biçiminde yazılsın.

$n = 2$ olsun. $N(\alpha) \leq 2$ olur. $N(\alpha)$ birim olmadığından $N(\alpha) = 2$'dir. α indirgenemez olmasın. Bu durumda $\alpha = \beta\gamma$ olarak yazılabilir. Öyleyse

$$N(\alpha) = N(\beta).N(\gamma) \geq 2.2 = 4$$

tür. Bu ise olamaz. Şu halde α indirgenemezdir. Yani $n = 2$ için ifade doğru olur.

Teorem n için doğru olsun. Yani α sıfırdan farklı ve birim olmayan $N(\alpha) \leq n$ şartını sağlayan bir eleman ise α, ya indirgenemez ya da indirgenemez elemanların çarpımı biçiminde olsun.

Şimdi iddianın (n+1) için doğru olduğunu gösterelim. α sıfırdan farklı, birim olmayan bir eleman ve $N(\alpha) \leq n+1$ olsun. $N(\alpha) \leq n$ ise tümevarım kabulüne göre

iddia doğrudur. O zaman $n < N(\alpha) \le n+1$ kabul edelim. α indirgenemez ise ispat biter. Şu halde α indirgenemez olmasın. $\alpha = \beta\gamma$ olup, $N(\alpha) = N(\beta).N(\gamma) = n+1$ olduğundan $N(\beta) \le n$ ve $N(\gamma) \le n$ olur. Tümevarım kabulüne göre β ve γ elemanları ya indirgenemezdir ya da indirgenemez elemanların çarpımı biçimindedir. Böylece α'nın indirgenemez elemanların çarpımı biçiminde yazıldığı görülür.

Tanım 4.1.2: K_m aşağıdaki özelliği sağlıyorsa, K_m'ye tek türlü parçalanmalı bölge denir. $\alpha_1,...,\alpha_r$, $\beta_1,...,\beta_s$ indirgenemez elemanlar ve ε birim olmak üzere

$$\alpha_1\alpha_2...\alpha_r = \varepsilon\beta_1\beta_2...\beta_s$$

olsun. Bu durumda $r = s$'dir ve $\sigma : \{1,2,...,r\} \to \{1,2,...,r\}$ bir permütasyon (birebir, örten dönüşüm) olmak üzere, α_i sayısı $\beta_{\sigma(i)}$ sayısı ile ilgidir.

Örnek 4.1.3: K_{-13} tek türlü parçalanmalı bölge değildir.

Çözüm: $1-\sqrt{-13}, 1+\sqrt{-13} \in K_{-13}$ için

$$\left(1-\sqrt{-13}\right).\left(1+\sqrt{-13}\right) = 14 = 2.7$$

dir. $1-\sqrt{-13}$ indirgenemez olmasın.

$$1-\sqrt{-13} = \left(a+b\sqrt{-13}\right).\left(c+d\sqrt{-13}\right)$$

olacak şekilde birimden farklı $a+b\sqrt{-13}, c+d\sqrt{-13} \in K_{-13}$ vardır. Her iki tarafın normunu alırsak $14 = \left(a^2+13b^2\right)\left(c^2+13d^2\right)$ olur. $a^2+13b^2 = 2$ ve $c^2+13d^2 = 7$ olmalıdır. Fakat iki eşitliğin de çözümü yoktur. Öyleyse $1-\sqrt{-13}$ indirgenemezdir. Benzer şekilde $1+\sqrt{-13}$ sayısının da indirgenemez olduğu gösterilir. Şimdi 2 indirgenemez olmasın. Dolayısıyla $2 = \left(a+b\sqrt{-13}\right)\left(c+d\sqrt{-13}\right)$ olacak şekilde birimden farklı $a+b\sqrt{-13}, c+d\sqrt{-13} \in K_{-13}$ elemanları vardır. Her iki tarafın normunu alırsak $4 = \left(a^2+13b^2\right)\left(c^2+13d^2\right)$ olur. Dolayısıyla $a^2+13b^2 = 2$ ve

$c^2+13d^2=2$ olmalıdır. Fakat iki eşitliğin de çözümü yoktur. Öyleyse 2 indirgenemezdir. Benzer şekilde 7'nin de indirgenemez olduğu görülür. Sonuç olarak 2, 7, $1+\sqrt{-13}$ ve $1-\sqrt{-13}$ indirgenemez elemanlardır.

Şimdi $2\sim 1+\sqrt{-13}$ olsun. Bu durumda $2\,|\,1+\sqrt{-13}$ ise $1+\sqrt{-13}=2(a+b\sqrt{-13})$ olur. Böylece $1=2a$ ve $1=2b$ elde edilir. Bu ise $a,b\in\mathbb{Z}$ olması ile çelişir. Dolayısıyla $2\nsim 1+\sqrt{-13}$'tür. Şimdi $2\sim 1-\sqrt{-13}$ olsun. $2\,|\,1-\sqrt{-13}$ ise

$$1-\sqrt{-13}=2(a+b\sqrt{-13})$$

dir. Öyleyse $1=2a$ ve $-1=2b$'dir. Bu ise $a,b\in\mathbb{Z}$ olması ile çelişir. Dolayısıyla $2\nsim 1-\sqrt{-13}$'tür. Öyleyse K_{-13} tek türlü parçalanmalı bölge değildir.

Teorem 4.1.4: K_m tek türlü parçalanmalı bölgedir $\Leftrightarrow$ K_m'nin her indirgenemez elemanı asaldır [2].

Sonuç 4.1.5: K_m bir esas ideal bölgesi ise K_m tek türlü parçalanmalı bölgedir.

İspat: π, K_m'de indirgenemez bir eleman ise Teorem 2.4.3'e göre, π asaldır. Teorem 4.1.4'e göre K_m tek türlü parçalanmalı bölgedir.

Teorem 4.1.6: K_m tek türlü parçalanmalı bölge olsun. $\alpha,\beta\in K_m$ olmak üzere α ve β'nın birimden başka ortak böleni olmasın. Eğer n pozitif tamsayısı için $\alpha\beta=\varepsilon\gamma^n$ eşitliğini sağlayan bir $\gamma\in K_m$ varsa

$$\alpha=\varepsilon_1\gamma_1^n$$

$$\beta=\varepsilon_2\gamma_2^n$$

olacak biçimde ε_1, ε_2 birimleri ve $\gamma_1,\gamma_2\in K_m$ elemanları vardır [2].

Teorem 4.1.7: a ve b sıfırdan farklı tamsayılar ve $(a,b)=c$ olsun. $\alpha \mid a$ ve $\alpha \mid b$ olacak biçimde $\alpha \in K_m$ varsa $\alpha \mid c$'dir. Özel olarak a ve b aralarında asal ise a ve b'nin K_m'de birimden başka ortak asal böleni yoktur.

İspat: $(a,b)=c$ ise $ar+bs=c$ olacak biçimde r ve s tamsayıları vardır. $\alpha \mid a$ ve $\alpha \mid b$ ise $\alpha \mid ar+bs$'dir. Diğer bir deyişle $\alpha \mid c$'dir. Özel olarak a ve b aralarında asal ise $c=1$'dir ve $\alpha \mid c$ olduğundan α birim olur.

Örnek 4.1.8: K_{-47} tek türlü parçalanmalı bölge değildir.

Çözüm: Önce K_{-47}'de 2'nin indirgenemez olduğunu görelim.

$2=\left(\frac{a+b\sqrt{-47}}{2}\right)\left(\frac{c+d\sqrt{-47}}{2}\right)=\alpha\beta$ olsun. Buradan $4=\left(\frac{a^2+47b^2}{4}\right)\left(\frac{c^2+47d^2}{4}\right)$ olur. $2=\alpha\beta$ ise $4=N(\alpha).N(\beta)$'dir. Eğer $N(\alpha)=1$ ise α birimdir. Eğer $N(\alpha)=2$ ise $\frac{a^2+47b^2}{4}=2$ ve böylece $a^2+47b^2=8$ bulunur. $b\neq 0$ ise $8=a^2+47b^2\geq 47$ veya $b=0$ ise $a^2=8$'dir. Bu iki durum içinde çözüm yoktur. Öyleyse 2 indirgenemezdir. Ayrıca $2\mid\left(\frac{1+\sqrt{-47}}{2}\right)\left(\frac{1-\sqrt{-47}}{2}\right)$'dir. Fakat $2\nmid\left(\frac{1+\sqrt{-47}}{2}\right)$ ve $2\nmid\left(\frac{1-\sqrt{-47}}{2}\right)$'dir. Dolayısıyla 2 asal değildir. Teorem 4.1.4'e göre K_{-47} tek türlü parçalanmalı bölge değildir.

Teorem 4.1.9: $m<0$ ise K_m tek türlü parçalanmalı bölgedir $\Leftrightarrow$ m, -1, -2, -3, -7, -11, -19, -43, -67 veya -163 sayılarından biridir $[2]$.

Teorem 4.1.10: $2\leq m<100$ olmak üzere m'nin 38 değeri için K_m tek türlü parçalanmalı bölgedir. Bunlar, 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33,

37, 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97'dir [2].

Önerme 4.1.11: a) α, K_m'nin bir elemanı olsun. α'nın normu asal ise α indirgenemezdir.

b) K_m tek türlü parçalanmalı bölge ve $N(\alpha)$ asal ise α asaldır.

İspat: a) $N(\alpha)$ asal olsun. α'nın indirgenemez olmadığını kabul edelim. Bu durumda β ve γ birimden farklı elemanlar olmak üzere $\alpha = \beta\gamma$ biçiminde yazılabilir. Buradan $N(\alpha) = N(\beta)N(\gamma)$ elde edilir. β ve γ birimden farklı olduğundan $N(\beta) > 1$ ve $N(\gamma) > 1$'dir. Bu ise $N(\alpha)$'nın asal sayı olması ile çelişir.

b) $N(\alpha)$ asal ise (a) şıkkına göre α indirgenemezdir ve Teorem 4.1.4'e göre α asal eleman olur.

Örnek 4.1.12: a) $\mathbb{Z}+\mathbb{Z}i$'de $N(1+2i)=5$ olduğundan $1+2i$ asaldır.

b) $\mathbb{Z}+\mathbb{Z}\sqrt{2}i$'de $N\left(1+\sqrt{2}i\right)=3$ olduğundan $1+\sqrt{2}i$ asaldır.

Önerme 4.1.13: a) K_m tek türlü parçalanmalı bölge, $\alpha \in K_m$, $\alpha \neq 0$ ve α birim olmasın. Bu takdirde $\pi \mid \alpha$ olan bir π asal elemanı vardır.

b) K_m tek türlü parçalanmalı bölge olsun. α ve β'nın birimden başka ortak böleni yoktur $\Leftrightarrow$ α ve β'nın hiçbir asal böleni yoktur.

İspat: a) İspatı açıktır.

b) $\Rightarrow$: α ve β'nın birimden başka ortak böleni yoksa α ve β'nın ortak asal böleni olmadığı açıktır.

$\Leftarrow$: α ve β'nın ortak asal böleni olmasın. Şimdi α ve β'nın birimden farklı bir γ ortak böleninin mevcut olduğunu kabul edelim. γ birimden farklı olduğundan (a) şıkkına göre, α'nın bir π asal böleni vardır. Dolayısıyla $\pi \mid \alpha$ ve $\pi \mid \beta$ olur. Bu ise hipotezle çelişir.

Teorem 4.1.14: K_m tek türlü parçalanmalı bölge ise K_m bir esas ideal bölgesidir [1], [7].

İspat: Bu teoremin ispatı için Dedekind bölge tanımına, [1] nolu kaynağın 194. sayfasına ve [7] nolu kaynağın 143. sayfasına bakılabilir.

Tek türlü parçalanmalı bölgelerle ilgili teoremler kullanılarak bazı Diophant denklemleri çözülebilir. Bununla ilgili birkaç örnek verelim.

Örnek 4.1.15: $x^2+2=y^3$ denkleminin çözümleri $x=5$, $y=3$ ve $x=-5$, $y=3$ olduğunu gösteriniz.

Çözüm: $x^2+2=y^3$ ise $\left(x+\sqrt{2}i\right)\left(x-\sqrt{2}i\right)=y^3$'tür. Şimdi $x+\sqrt{2}i$ ve $x-\sqrt{2}i$'nin bir ortak böleni α olsun. $\alpha \mid x+\sqrt{2}i$ ve $\alpha \mid x-\sqrt{2}i$ olduğundan $\alpha \mid 2\sqrt{2}i$ olur. $x^2+2=y^3$ olduğundan x tek olmalıdır. Aksine x çift ise $x^2+2 \equiv 2 \pmod 4$, yani $y^3 \equiv 2 \pmod 4$ olur. Hâlbuki $a \in \mathbb{Z}$ ise $a^3 \equiv 0,1,3 \pmod 4$ olduğu açıktır. Dolayısıyla x tektir. $\alpha \mid 2\sqrt{2}i$ ise $N(\alpha) \mid 8$'dir. Eğer $N(\alpha)>1$ ise, $N(\alpha)$ çift olur. $\alpha \mid x+\sqrt{2}i$ ise $N(\alpha) \mid x^2+2$ olur. Bu ise $N(\alpha)$ çift ve x^2+2 tek olduğundan mümkün değildir. Şu halde $N(\alpha)=1$'dir. Yani α birimdir. Böylece $x+\sqrt{2}i$ ve $x-\sqrt{2}i$'nin birimden başka ortak böleni yoktur. Teorem 4.1.6'ya göre, $x+\sqrt{2}i=\varepsilon\lambda^3$ olacak biçimde ε birimi ve $\lambda \in \mathbb{Z}+\mathbb{Z}\sqrt{2}i$ vardır. $\mathbb{Z}+\mathbb{Z}\sqrt{2}i$'nin birimleri ± 1 ve $(-1)^3=-1$ olduğundan

$$x+\sqrt{2}i=\left(a+b\sqrt{2}i\right)^3$$

olarak yazılabilir. Buradan

$$x+\sqrt{2}i=\left(a+b\sqrt{2}i\right)^3=a^3+3a^2b\sqrt{2}i-6ab^2-2b^3\sqrt{2}i$$

elde edilir. Burada reel ve sanal kısımları eşitlersek, $x=a\left(a^2-6b^2\right)$ buluruz. $1=b\left(3a^2-2b^2\right)$ ve $a,b\in\mathbb{Z}$ olduğundan $b=\pm1$'dir. Eğer $b=-1$ ise $3a^2-2=-1$ bulunur. Böylece $a^2=1/3$'tür. Fakat $a\in\mathbb{Z}$ olduğundan çözüm yoktur. Eğer $b=1$ ise $3a^2-2=1$'dir. Buradan $a=\pm1$ olur. Böylece $x=\pm5$ bulunur. Burada $y^3=x^2+2$ olduğundan $y=3$'tür. Sonuç olarak $(x,y)=(\pm5,3)$ bulunur.

Örnek 4.1.16: $x^2+1=y^3$ denklemini çözünüz.

Çözüm: $x^2+1=y^3$ olsun. $(x+i)(x-i)=y^3$'tür. $x^2\equiv0,1\pmod4$ olduğundan $x^2+1\equiv1,2\pmod4$ olur. Herhangi bir y tamsayısı için $y^3\equiv0,1,3\pmod4$ olduğundan $y^3\equiv1\pmod4$ olmalıdır. Bu ise $y\equiv1\pmod4$ olduğunu gösterir. Dolayısıyla y tektir. Şimdi π sayısı $x+i$ ve $x-i$'nin ortak asal böleni olsun. $\pi\mid x+i$ ve $\pi\mid x-i$ olduğundan $\pi\mid2x$ olur. Dolayısıyla $\pi\mid x$ veya $\pi\mid2$ olmalıdır. $\pi\mid x$ olsun. $\pi\mid x+i$ olduğundan $\pi\mid i$ olur. Bu olamaz. Şu halde $\pi\mid2$'dir. $\pi\mid2$ ise π sayısı asal ve $2=(1+i)(1-i)$ olduğundan $\pi\mid1+i$ veya $\pi\mid1-i$ olmalıdır. Her iki durumda da $N(\pi)=2$ olduğu görülür. $\pi\mid1+i$ olduğundan $N(\pi)\mid N(x+i)$'dir. Yani $2\mid x^2+1$ olur. Bu ise $2\mid y^3$, yani $2\mid y$ olmasını gerektirir. Bu olamaz. Şu halde $x+i$ ve $x-i$'nin birimden başka ortak böleni yoktur. Teorem 4.1.6'ya göre $x+i=\varepsilon(c+di)^3$ olacak biçimde ε birimi ve $c+di\in\mathbb{Z}+\mathbb{Z}i$ vardır. $\mathbb{Z}+\mathbb{Z}i$'nin birimleri ±1 ve $\pm i$'dir. $(-1)^3=-1$, $i^3=-i$ ve $(-i)^3=i$ olduğundan $x+i=(a+bi)^3$ olarak yazılabilir. Buradan

$$x+i=(a+bi)^3=a^3+3a^2(bi)+3a(bi)^2+(bi)^3=\left(a^3-3ab^2\right)+\left(3a^2b-b^3\right)i$$

elde edilir. Reel ve sanal kısımları eşitlersek, $x = a\left(a^2 - 3b^2\right)$ ve $1 = b\left(3a^2 - b^2\right)$ olur. İkinci eşitlikten $b = 1$ ve $3a^2 - b^2 = 1$ bulunur. Fakat $3a^2 = 2$ olamaz. Buradan çözüm yoktur. $b = -1$ ve $3a^2 - b^2 = -1$ ise, $3a^2 = 0$ olur. Öyleyse $a = 0$ elde edilir. Buradan $x = 0$; $y = 1$ bulunur.

Örnek 4.1.17: $x^2 + 11 = y^3$ denkleminin çözümlerini bulunuz.

Çözüm: $x^2 + 11 = y^3$ ise x çifttir. x'i tek kabul edelim. Bu durumda $x^2 + 11 = 4 (\mathrm{mod}\, 8)$'dir. Herhangi bir y tamsayısı için $y^3 \not\equiv 4 \left(\mathrm{mod}\, 8\right)$ olduğundan bu bir çelişkidir. Şu halde x çifttir. $11 \mid x$ ise $11 \mid y$ olur ve $121 \mid y^3 - x^2$ bulunur. Bu ise $y^3 - x^2 = 11$ olması ile çelişir. Öyleyse $11 \nmid x$ olur.

$m \equiv 1 (\mathrm{mod}\, 4)$ ise K_m'de elemanlar $a + b\left(\dfrac{1+\sqrt{m}}{2}\right)$ biçimindedir. $-11 \equiv 1 (\mathrm{mod}\, 4)$'tür.

x çift olsun. Bu durumda

$$x + \sqrt{-11} = x - 1 + 2\left(\frac{1+\sqrt{-11}}{2}\right) \text{ ve } x - \sqrt{-11} = x - 1 + (-2)\left(\frac{1+\sqrt{-11}}{2}\right)$$

olarak yazılabilir. Dolayısıyla $x + \sqrt{-11}$, $x - \sqrt{-11} \in K_{-11}$'dir. Buradan

$$(x + \sqrt{-11})(x - \sqrt{-11}) = x^2 + 11 = y^3$$

olur. $x + \sqrt{-11}$ ve $x - \sqrt{-11}$'in ortak asal böleni α olsun. Bu durumda $\alpha \mid x + \sqrt{-11}$ ve $\alpha \mid x - \sqrt{-11}$'dir. Böylece $\alpha \mid 2\sqrt{-11}$ ve 2 ile $\sqrt{-11}$ asal olduğundan $\alpha = \pm 2$ ve $\alpha = \pm\sqrt{-11}$ olmalıdır. Fakat x çift ve $2 \nmid \sqrt{-11}$ olduğundan $\alpha = \pm 2$ olamaz. $\alpha = \pm\sqrt{-11}$ ise $\alpha \mid x$'tir. Buradan $11 \mid x$ elde edilir. Bu ise mümkün değildir. Bu durumda $x + \sqrt{-11}$ ve $x - \sqrt{-11}$ sayılarının birimden başka ortak böleni yoktur. Öyleyse Teorem 4.1.6'ya göre $x + \sqrt{-11} = \varepsilon\lambda^3$ olacak şekilde ε birimiyle $\lambda \in K_{-11}$ vardır. K_{-11}'in birimleri ± 1 ve $(\pm 1)^3 = \pm 1$ olduğundan $x + \sqrt{-11} = \lambda^3$ olur. Öyleyse

$$x + \sqrt{-11} = \left[a + b\left(\frac{1+\sqrt{-11}}{2}\right)\right]^3 = \frac{\left(2a + b + b\sqrt{-11}\right)^3}{8}$$

$$=\left(a^3-4b^3-\frac{15}{2}ab^2+\frac{3}{2}a^2b\right)+\left(\frac{3}{2}a^2b+\frac{3}{2}ab^2-b^3\right)\sqrt{-11}$$

dir. Buradan $x=a^3-4b^3-\frac{15}{2}ab^2+\frac{3}{2}a^2b$ ve $1=\frac{3}{2}a^2b+\frac{3}{2}ab^2-b^3$ elde edilir. İkinci eşitlikten $2=b\left(3a^2+3ab-2b^2\right)$ bulunur. Dolayısıyla $b\mid 2$'dir. Böylece $b=\pm 1$ veya $b=\pm 2$ olur. Eğer $b=1$ ise $2=3a^2+3a-2$'dir. Öyleyse $4=3a\left(a+1\right)$'dir ve $3\nmid 4$ olduğundan bu olamaz. Eğer $b=-1$ ise $2=-3a^2+3a+2$ ve böylece $0=3a\left(1-a\right)$ bulunur. Buradan $a=0$ veya $a=1$ olur. Buradaki çözümler $a=0$ ise $x=4$ ve $a=1$ ise $x=-4$'tür. Eğer $b=2$ ise $2=6a^2+12a-16$ ve böylece $a^2+2a-3=0$ olur. Öyleyse $a=-3$ veya $a=1$ bulunur. Buradaki çözümler $a=-3$ ise $x=58$ ve $a=1$ ise $x=-58$'dir. Eğer $b=-2$ ise $2=-6a^2+12a+16$ ve $-7=3a\left(2-a\right)$ olur. Fakat $3\nmid 7$ olduğundan çözüm yoktur. Bulunan x değerleri için tüm çözümler;

$x=\pm 4$ için $y^3=x^2+11=27$ ise $y=3$ ve $x=\pm 58$ için $y^3=3375$ ise $y=15$ olarak bulunur.

BÖLÜM 5. SONUÇLAR VE ÖNERİLER

Bu çalışmada m karesiz bir tamsayı, $m \equiv 1 \pmod 4$ ise $K_m = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ ve $m \not\equiv 1 \pmod 4$ ise $K_m = \mathbb{Z} + \mathbb{Z}\sqrt{m}$ olmak üzere K_m tamlık bölgesi ele alınmış ve K_m'nin Euclid bölgesi olması için gerekli ve yeterli şartlar verilmiştir. Özellikle, K_m'nin m = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 73 değerleri için Euclid bölgesi olduğu ve m'nin diğer değerleri için Euclid bölgesi olmadığı gösterilmiştir. Ayrıca tezin son bölümünde tek türlü parçalanmalı bölgeler ele alınmıştır. m'nin bazı değerleri için K_m'nin tek türlü parçalanmalı bölge olduğu ispatsız olarak verilmiştir. Tek türlü parçalanmalı bölgeler bazı Diophant denklemlerin çözümünde kolaylık sağlamaktadır. Bu nedenle Diophant denklemlerinin çözümüyle ilgilenmek isteyenler için tek türlü parçalanmalı bölgeler önem taşımaktadır. Ayrıca bu çalışma , cebirsel sayılar teorisiyle uğraşmak isteyenler için de bir basamak olma özelliği taşımaktadır. Konuyla ilgilenmek isteyenlere [1] ve [10] numaralı kaynaklar tavsiye edilebilir.

KAYNAKLAR

[1] ALACA, Ş., WILLIAMS, K. S., Introductory Algebraic Number Theory, Cambrıdge University Press, 2004.

[2] HAROLD, M. STARK, An Introduction to Number Theory, The MIT Press, 1987.

[3] NİVEN, I., ZUCKERMAN, S., MONTGOMERY, H. L., An Introduction to the Theory of Numbers, fifth ed., John Willey, 1991.

[4] CHATLAND, H., DAVENPORT, H., Euclid's Algorithm in Real Quadratic Fields, Canadian Journal of Mathematics 2 (1950), 289-296.

[5] CLARK, D. A., A Quadratic Field which is Euclidean but not norm-Euclidean, Manuscripta Mathematica 83 (1994), 327-330.

[6] ADLER, A., COURY, J. E., The Theory of Numbers, Jones and Bertlett Publischers, 1995.

[7] MOLLIN, R. A., Algebric Number Theory, Chapman and Holl / CRC Press, 1999.

[8] DUMMIT, D. S., FOOTE, R. M., Abstract Algebra, New York Wiley, 1999.

[9] HARDY, G. H., WRIGHT, E. M., An Introduction to the Theory of Numbers, Oxford University Pres, 1965.

[10] STEWART, I., TALL D., Algebric Number Theory and Fermat's Last Theorem, AK Peters, Ltd, 2001.

ÖZGEÇMİŞ

1978 yılında Almanya'da doğdu. İlk ve orta öğrenimini Tokat'ın Zile ilçesinde tamamladı. 1996 yılında Hacettepe Üniversitesi Eğitim Fakültesi Matematik Öğretmenliği Bölümü'nde lisans öğrenimine başladı. 2001 yılında bölümünden mezun oldu. Aynı yıl Bitlis'in Tatvan ilçesinde öğretmenlik görevine başladı. 2004 yılında Adapazarı Şehit Üsteğmen Selçuk Esedoğlu Lisesine tayin oldu. Halen aynı lisede öğretmenlik yapmaktadır.