

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

**BACHET DİYOFANT DENKLEMİNİN CEBİRSEL
SAYILAR TEORİSİ İLE ÇÖZÜMÜ**

YÜKSEK LİSANS TEZİ

Ahmet Şamil ÖZMEN

Enstitü Anabilim Dalı : MATEMATİK
Enstitü Bilim Dalı : CEBİR VE SAYILAR TEORİSİ
Tez Danışmanı : Prof. Dr. Refik KESKİN

Haziran 2019

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

**BACHET DİYOFANT DENKLEMİNİN CEBİRSEL
SAYILAR TEORİSİ İLE ÇÖZÜMÜ**

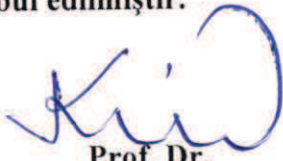
YÜKSEK LİSANS TEZİ

Ahmet Şamil ÖZMEN

Enstitü Anabilim Dalı : Matematik

Enstitü Bilim Dalı : Cebir ve Sayılar Teorisi

Bu tez 21.06.2019 tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.



Prof. Dr.
Refik KESKİN
Jüri Başkanı



Prof. Dr.
Gökhan SOYDAN
Üye



Doç. Dr.
Murat GÜZELTEPE
Üye

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.



Ahmet Şamil ÖZMEN

24.06.2019

TEŞEKKÜR

Lisans ve yüksek lisans eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteğini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen, teşvik eden, aynı titizlikte beni yönlendiren değerli danışman hocam Prof. Dr. Refik KESKİN'e teşekkürlerimi sunarım.

Ayrıca bu çalışma kaynak kitap temini için destek veren Sakarya Üniversitesi Bilimsel Araştırma Projeleri (BAP) Komisyon Başkanlığına (Proje No: 2018-50-01-015) teşekkür ederim.

İÇİNDEKİLER

TEŞEKKÜR	i
İÇİNDEKİLER	ii
SİMGELER VE KISALTMALAR LİSTESİ	iii
TABLolar LİSTESİ	v
ÖZET	vi
SUMMARY	vii
 BÖLÜM 1.	
GİRİŞ	1
 BÖLÜM 2.	
CEBİRSEL TAMSAYILAR	22
 BÖLÜM 3.	
DEDEKİND BÖLGELERİ	70
 BÖLÜM 4.	
BACHET DENKLEMİNİN ÇÖZÜMÜ	109
 BÖLÜM 5.	
SONUÇ VE ÖNERİLER	131
 KAYNAKLAR	132
ÖZGEÇMİŞ	133

SİMGELER VE KISALTMALAR LİSTESİ

A^B	: A tamlık bölgesinin B tamlık bölgesindeki tam kapanışı
$\mathbb{C}$	: Kompleks sayılar kümesi
$\text{der}_K(\alpha)$	: α cebirsel sayısının K 'daki derecesi
$D(\alpha)$	: α cebirsel sayısının diskriminantı
$d(K)$	: K cebirsel sayı cisminin diskriminantı
$D(w_1, \dots, w_n)$	: $w_1, \dots, w_n$ elemanlarının diskriminantı
$e_K(P)$	: P idealinin K 'daki dallanma indeksi
$\text{cis}_K(\alpha)$	: α cebirsel sayısının K 'daki cisim polinomu
$g_K(p)$	: p asal sayısının K 'daki parçalanma sayısı
$H(K)$	: K cebirsel sayı cisminin ideal sınıf grubu
$h(K)$	: K cebirsel sayı cisminin sınıf sayısı
$I(K)$	: O_K 'nın bütün kesir ideallerinin grubu
$K(\alpha)$	: K cismine α cebirsel sayısı eklenerek elde edilen genişleme
$K[x]$	: K 'dan katsayılı x 'e değişkenine bağlı polinomlar kümesi
M_K	: K cebirsel sayı cismi için Minkowski sınırı
$N(I)$	: I idealinin normu
O_K	: K cebirsel sayı cisminin cebirsel tamsayılar halkası
Ω	: $\mathbb{C}$ cismindeki bütün cebirsel tamsayıların kümesi
$U(D)$	: D tamlık bölgesindeki birimsel elemanların kümesi
$P(K)$	: O_K 'nın bütün esas ideallerinin kümesi
$\mathbb{Q}$	: Rasyonel sayılar kümesi

$\mathbb{Z}$: Tamsayılar (Rasyonel tamsayılar) kümesi
 $\mathbb{Z}^+$: Pozitif tamsayılar kümesi



TABLÖLAR LİSTESİ

Tablo 3.1. $2 \leq m \leq 40$, m karesiz, $O_{\mathbb{Q}(\sqrt{m})}$ 'nin temel birimi	103
Tablo 3.2. $-30 < k < 0$, k karesiz, $H\left(\mathbb{Q}(\sqrt{k})\right)$ 'nin ideal sınıf grupları	106
Tablo 3.3. $2 \leq k < 100$, k karesiz, $H\left(\mathbb{Q}(\sqrt{k})\right)$ 'nin temel birimi	107
Tablo 4.1. $-20 \leq k < 0$ olmak üzere $y^2 = x^3 + k$ 'nin $(x, y) \in \mathbb{Z}^2$ çözümleri	130
Tablo 4.2. $0 < k \leq 20$ olmak üzere $y^2 = x^3 + k$ 'nin $(x, y) \in \mathbb{Z}^2$ çözümleri	131

ÖZET

Anahtar kelimeler: Cebirsel sayılar, Cebirsel sayı cisimleri, Dedekind bölgeleri, Cebirsel tamsayılar halkası, Kesir idealleri, Temel birim, Sınıf sayısı, Bachet denklemi

Bu çalışma beş bölümden oluşmaktadır. Birinci bölümde halka, ideal, tamlık bölgeleri ve Noetherian bölgeleri ile ilgili bazı tanım ve teoremler verilmiştir.

İkinci bölümde cebirsel sayılar, cebirsel sayı cisimleri ve cebirsel cisim genişlemeleri incelenmiştir.

Üçüncü bölümde Dedekind bölgelesi, kesir ideali, temel birim ve sınıf sayısı tanımları yapılmıştır. Dedekind bölgelerinde idealler için en büyük ortak bölen ve en küçük ortak kat tanımları verilmiştir. Daha sonra en büyük ortak bölen ve en küçük ortak kat ile ilgili teoremler ispatlanmıştır.

Dördüncü bölümde Bachet denklemlerinin çözümünün olup olmadığı, varsa bu çözümlerin neler olduğu araştırılmıştır.

Beşinci bölüm, sonuç ve önerilerden oluşmaktadır.

SOLUTION OF BACHET DIOPHANTINE EQUATION WITH ALGEBRAIC NUMBERS THEORY

SUMMARY

Keywords: Algebraic numbers, Algebraic number fields, Dedekind domains, Ring of algebraic integers, Fractional ideals, Fundamental unit, Class number, Bachet equation

This study consists of five parts. In the first part, some definitions and theorems related to rings, ideals, integral domains and Noetherian domains are given.

In the second part, algebraic numbers, algebraic number fields and algebraic field extensions are examined.

In the third part, definitions of Dedekind domain, fractional ideal, fundamental unit and class number are given. The greatest common divisor and the least common multiple of two ideals are given. Later, some theorems concerning the greatest common divisor and the least common multiple are proved.

In the fourth part, the solutions of the Bachet equations are examined. And if they have solutions, these solutions are given.

The fifth part consists of conclusions and recommendations.

BÖLÜM 1. GİRİŞ

Tanım 1.1. Boştan farklı bir D kümesinde $+$ ve $\cdot$ iki tane ikili işlem olsun. D kümesi aşağıdaki şartları sağlıyorsa D 'ye bir halka denir ve bu $(D, +, \cdot)$ ile gösterilir.

- a. $(D, +)$ bir değişmeli gruptur.
- b. Her $a, b, c \in D$ için $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ dir.
- c. Her $a, b, c \in D$ için $a \cdot (b + c) = a \cdot b + a \cdot c$ ve $(a + b) \cdot c = a \cdot c + b \cdot c$ dir.

Bundan sonra $a \cdot b$ yerine ab yazılacaktır.

Tanım 1.2. $(D, +, \cdot)$ bir halka olsun.

- a. Her $a \in D$ için $1a = a1 = a$ olacak biçimde $1 \in D$ elemanı varsa 1 elemanına D 'nin birim elemanı denir ve bu durumda D 'ye birim elemanlı halka denir.
- b. Her $a, b \in D$ için $ab = ba$ ise D 'ye değişmeli halka denir.
- c. $a, b \in D$ olmak üzere $ab = 0$ iken $a = 0$ veya $b = 0$ oluyorsa D 'ye sıfır bölensiz halka denir.

Tanım 1.3. Bir D halkasının boştan farklı bir alt kümesi S olsun. S kümesi D deki $+$ ve $\cdot$ ikili işlemlerine göre bir halka ise, S 'ye D 'nin bir alt halkası denir.

Tanım 1.4. D bir halka ve $a, b \in D$ olsun. $b = ac$ olacak biçimde bir $c \in D$ elemanı varsa a böler b denir ve $a | b$ olarak yazılır.

Örnek 1.1. $\mathbb{Z} + \mathbb{Z}\sqrt{-1}$ 'de $2 = (1 + \sqrt{-1})(1 - \sqrt{-1})$ olduğundan $1 + \sqrt{-1} \mid 2$ olur.

Örnek 1.2. $\mathbb{Z}[x]$ 'de $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$ olduğundan $x^2 + x + 1 \mid x^4 + x^2 + 1$ olur.

Örnek 1.3. $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ 'de $\frac{3}{2 + \sqrt{2}} = 3 - \frac{3}{2}\sqrt{2} \notin \mathbb{Z} + \mathbb{Z}\sqrt{2}$ olduğundan $2 + \sqrt{2} \nmid 3$ dir.

Tanım 1.5. D birim elemanlı bir halka ve $a \in D$ sıfırdan farklı bir eleman olsun. $ab = 1$ olacak biçimde bir $b \in D$ elemanı varsa, yani $a \mid 1$ ise, a 'ya bir birim veya birimsel eleman denir. Ayrıca buradaki b 'ye a 'nın tersi denir ve $b = a^{-1}$ ile gösterilir. D 'nin birimlerinin kümesi $U(D)$ ile gösterilir.

Örnek 1.4. $\mathbb{Z}$ tamsayılar halkası olmak üzere $U(\mathbb{Z}) = \{+1, -1\}$ 'dir.

Örnek 1.5. F bir cisim olmak üzere $U(F[x]) = F \setminus \{0\}$ 'dir.

Tanım 1.6. D bir halka ve $a, b \in D$ olsun. $a \mid b$ ve $b \mid a$ ise a ile b ilgilidir veya bağdaşıktır denir ve bu durum $a \sim b$ olarak yazılır.

Tanım 1.7. D birim elemanlı, değişmeli ve sıfır bölensiz bir halka olsun. Bu takdirde D 'ye bir tamlık bölgesi denir. Bir D tamlık bölgesinde, her $a \in D, a \neq 0$ için $ab = 1$ olacak biçimde $b \in D$ mevcut ise, yani D 'nin sıfırdan farklı her elemanının tersi var ise, D 'ye bir cisim denir.

Örnek 1.6. m tam kare olmayan pozitif veya negatif bir tamsayı olmak üzere $\mathbb{Z} + \mathbb{Z}\sqrt{m} = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$ bir tamlık bölgesidir. $\sqrt{m}$ sayısı $x^2 - m$ indirgenemez kuadratik polinomunun bir köküdür.

Örnek 1.7. m tam kare olmayan pozitif veya negatif bir tamsayı ve $m \equiv 1 \pmod{4}$ olmak üzere $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) = \left\{a + b\left(\frac{1+\sqrt{m}}{2}\right) \mid a, b \in \mathbb{Z}\right\}$ bir tamlık bölgesidir. $m \equiv 0, 2, 3 \pmod{4}$ ise

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

olacağından $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ bir tamlık bölgesi değildir. $\frac{1+\sqrt{m}}{2}$ sayısı

$x^2 - x + \frac{1-m}{4} = 0$ indirgenemez kuadratik polinomunun bir köküdür. Bu yüzden

$\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ 'ye bir kuadratik bölge denir. Ayrıca $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ 'nin

elemanları x, y tamsayılar ve $x \equiv y \pmod{2}$ olmak üzere $\frac{x+y\sqrt{m}}{2}$ biçiminde yazılabilirler.

Örnek 1.8. D bir tamlık bölgesi olsun. $D[x]$ polinomlar halkası bir tamlık bölgesidir. Dolayısıyla $\mathbb{Z}[x]$ 'de bir tamlık bölgesidir.

Tanım 1.8. D bir tamlık bölgesi ve $a \in D$ sıfırdan farklı, birim olmayan bir eleman olsun. $a = bc$ ($b, c \in D$) iken b veya c 'den biri birim oluyorsa a 'ya D 'de indirgenemez eleman denir.

Örnek 1.10. $\mathbb{Z}$ 'de 2 elemanı indirgenemezdir. Çünkü $a, b \in \mathbb{Z}$ için $2 = ab$ ise ya $a = \pm 1$ ya da $b = \pm 1$ olur.

Örnek 1.11. $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ 'de 2 elemanı indirgenemezdir. Bunu gösterelim. $a, b, c, d \in \mathbb{Z}$ için $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ olsun. Buradan $4 = (a^2 + 5b^2)(c^2 + 5d^2)$ elde edilir. O halde $a^2 + 5b^2$ sayısı 4 'ün bir pozitif tamsayı bölenidir. Dolayısıyla $a^2 + 5b^2$ sayısı 1, 2 veya 4 sayılarından birine eşittir. Buradan $(a, b) = (\pm 1, 0)$ veya $(a, b) = (\pm 2, 0)$ olur. O zaman $a + b\sqrt{-5} = \pm 1$ veya $a + b\sqrt{-5} = \pm 2$ olur. $a + b\sqrt{-5} = \pm 1$ ise $a + b\sqrt{-5}$ elemanı $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ 'in bir birimi olur. $a + b\sqrt{-5} = \pm 2$ ise

$$c + d\sqrt{-5} = \frac{2}{a + b\sqrt{-5}} = \frac{2}{\pm 2} = \pm 1$$

olacağından $c + d\sqrt{-5}$ elemanı $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ 'in bir birimi olur. Dolayısıyla 2 elemanı $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ 'de indirgenemezdir.

Örnek 1.12. $P(x) = x^4 + 1$ polinomu $\mathbb{Q}[x]$ 'de indirgenemezdir. Bunu gösterelim. $P(x)$ polinomunun reel sayılarda kökü olmadığından birinci dereceden çarpanı yoktur. $P(x)$ 'in $\mathbb{Q}[x]$ 'de ikinci dereceden çarpanı olduğunu kabul edelim. O zaman $a, b, c, d \in \mathbb{Q}$ olmak üzere

$$P(x) = (x^2 + ax + b)(x^2 + cx + d)$$

olarak yazılabilir. Buradan

$$a + c = 0, ac + b + d = 0, ad + bc = 0, bd = 1$$

elde edilir. $ad+bc=0$ olduğundan $abd+b^2c=0$ olur. $bd=1$ ve $a=-c$ olduğu kullanılırsa $b^2=1$ bulunur. O halde $b=1, d=1$ veya $b=-1, d=-1$ elde edilir. İkinci ve birinci ifadelerden $b+d=-ac=a^2$ olur. Buradan $a^2=\pm 2$ elde edilir. a rasyonel sayı olduğundan bu mümkün değildir. O halde $P(x)$, $\mathbb{Q}[x]$ 'de indirgenemezdir.

Örnek 1.13. $x^2-\sqrt{2}x+1$ polinomu $\mathbb{Q}(\sqrt{2})[x]$ 'de indirgenemezdir. Bunu gösterelim. Tersine $x^2-\sqrt{2}x+1$ polinomunun $\mathbb{Q}(\sqrt{2})[x]$ 'de indirgenebilir olduğunu kabul edelim. O zaman $x^2-\sqrt{2}x+1=0$ 'ın $\mathbb{Q}(\sqrt{2})$ 'de bir kökü vardır. Yani

$$(\alpha + \beta\sqrt{2})^2 - \sqrt{2}(\alpha + \beta\sqrt{2}) + 1 = 0$$

olacak biçimde bir $\alpha + \beta\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ vardır. Buradan

$$(a^2 + 2b^2 - 2b + 1) + (2ab - a)\sqrt{2} = 0$$

elde edilir. $\sqrt{2}$ irrasyonel olduğundan

$$a^2 + 2b^2 - 2b + 1 = 0, \quad 2ab - a = 0$$

eşitlikleri elde edilir. İkinci ifadeden $a=0$ veya $b=\frac{1}{2}$ olmalıdır. $a=0$ ise birinci ifadeden $2b^2 - 2b + 1 = 0$ elde edilir. Fakat $2b^2 - 2b + 1 = 0$ 'ın reel kökü olmadığından bu, $b \in \mathbb{Q}$ olması ile çelişir. $b=\frac{1}{2}$ ise birinci ifadeden $a^2 + \frac{1}{2} = 0$ elde edilir. Fakat bu $a \in \mathbb{Q}$ olması ile çelişir. Dolayısıyla $x^2-\sqrt{2}x+1$ polinomu $\mathbb{Q}(\sqrt{2})[x]$ 'de indirgenemezdir.

Örnek 1.14. $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ 'de $7 + \sqrt{-5}$ elemanı indirgenebilirdir. Çünkü

$$7 + \sqrt{-5} = (1 + \sqrt{-5})(2 - \sqrt{-5})$$

olup $1 + \sqrt{-5}$ ve $2 - \sqrt{-5}$ elemanlarının ikisi de $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ 'de birim değildir.

Tanım 1.9. D bir tamlık bölgesi ve $p \in D$ sıfırdan farklı, birim olmayan bir eleman olsun. $p \mid ab$ ($a, b \in D$) iken $p \mid a$ veya $p \mid b$ oluyorsa p 'ye D 'de asal eleman denir.

Örnek 1.15. $\mathbb{Z}$ 'de 2 elemanı asaldır. $a, b \in \mathbb{Z}$ için $2 \mid ab$ olsun. O halde ab bir çift tamsayıdır. a ve b 'nin ikisi de tek olursa ab tek olacağından, a veya b 'den en az biri çifttir. Yani $2 \mid a$ veya $2 \mid b$ elde edilir. O halde 2 asaldır.

Örnek 1.16. $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ 'de 2 elemanı asal değildir. Çünkü $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ olmasına rağmen $2 \nmid 1 \pm \sqrt{-5}$ 'dir.

Örnek 1.17. $\mathbb{Z} + \mathbb{Z}\sqrt{-1}$ 'de $1 + \sqrt{-1}$ elemanı asaldır. Bunu gösterelim. $a, b, c, d \in \mathbb{Z}$ için $1 + \sqrt{-1} \mid (a + b\sqrt{-1})(c + d\sqrt{-1})$ olsun. O zaman

$$(a + b\sqrt{-1})(c + d\sqrt{-1}) = (1 + \sqrt{-1})(x + y\sqrt{-1})$$

olacak biçimde $x, y \in \mathbb{Z}$ vardır. Buradan

$$(a^2 + b^2)(c^2 + d^2) = 2(x^2 + y^2)$$

elde edilir. O halde $2 \mid (a^2 + b^2)(c^2 + d^2)$ olur. 2 elemanı $\mathbb{Z}$ 'de asal olduğundan, $2 \mid (a^2 + b^2)$ veya $2 \mid (c^2 + d^2)$ 'dir. Genelliği bozmaksızın $2 \mid (a^2 + b^2)$ olsun. O halde a ve b 'nin ya ikisi de tektir ya da ikisi de çifttir. a ve b 'nin ikisi de tek ise $a = 2r + 1$, $b = 2s + 1$ olan r, s tamsayıları vardır. Böylece

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

elde edilir. Yani $1 + \sqrt{-1} \mid a + b\sqrt{-1}$ olur. a ve b 'nin ikisi de çift ise $a = 2r$, $b = 2s$ olan r, s tamsayıları vardır. Böylece

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

elde edilir. Yani $1 + \sqrt{-1} \mid a + b\sqrt{-1}$ olur. Dolayısıyla $1 + \sqrt{-1}$ elemanı $\mathbb{Z} + \mathbb{Z}\sqrt{-1}$ 'de asaldır.

Tanım 1.10. D bir tamlık bölgesi olsun. D 'nin kesir cismi

$$F = \{ ab^{-1} \mid a, b \in D, b \neq 0 \}$$

ile tanımlanır [3]. Kesir cismi hakkında detaylı bilgi için [5] nolu kaynağa bakılabilir.

Tanım 1.11. Bir D değişmeli halkasının boştan farklı bir alt kümesi I olsun. Aşağıdaki şartlar sağlanıyorsa I 'ya bir ideal denir.

- a. Her $a, b \in I$ için $a - b \in I$ dır.
- b. Her $r \in D$ ve $a \in I$ için $ra \in I$ dır.

Örnek 1.18. Bir D değişmeli halkasında her $x \in D$ elemanı bir ideal üretir. x tarafından üretilen ideal $\langle x \rangle$ ile gösterilir ve

$$\langle x \rangle = xD = \{ xa \mid a \in D \}$$

olarak tanımlanır. Şimdi ideal şartlarının sağlandığını gösterelim.

$a, b \in \langle x \rangle$ olsun. Bu takdirde $a = xm, b = xn$ olacak biçimde $m, n \in D$ vardır. O zaman $a - b = xm - xn = x(m - n)$ olur. $m - n \in D$ olduğundan $x(m - n) \in xD = \langle x \rangle$ dır. Yani $a - b \in \langle x \rangle$ elde edilir.

$r \in D$ ve $a \in \langle x \rangle$ olsun. $a = xm$ olacak biçimde $m \in D$ vardır. O zaman $ra = ar = xm(r) = x(mr)$ olur. $mr \in D$ olduğundan $x(mr) \in xD = \langle x \rangle$ 'dir. Yani $ra \in \langle x \rangle$ elde edilir

O halde $\langle x \rangle$, D 'nin bir idealidir. D halkasında, toplama işleminin etkisiz elemanı $0 \in D$ dir. 0 tarafından üretilen ideal, D 'nin sadece 0 elemanını içeren ve başka elemanı olmayan bir alt kümesidir. 1 tarafından üretilen ideal ise $\langle 1 \rangle = \{1a \mid a \in D\} = \{a \mid a \in D\} = D$ olur. Ayrıca $r \in \langle x \rangle$ ise $r = xa$, $a \in D$ olacağından $x \mid r$ 'dir.

Tanım 1.12. D bir tamlık bölgesi olsun. A ve B 'ler D 'nin idealleri olsun.

a. A ile B 'nin toplamı $A+B$ ile gösterilir ve $A+B = \{a+b \mid a \in A, b \in B\}$ olarak tanımlanır.

b. A ile B 'nin çarpımı AB ile gösterilir ve

$$AB = \left\{ \sum_{j=1}^n x_j y_j \mid x_j \in A, y_j \in B, 1 \leq j \leq n, n \text{ sabit değil} \right\}$$

olarak tanımlanır.

c. $x_1, x_2, \dots, x_n \in D$ ise $x_1, x_2, \dots, x_n$ 'ler tarafından üretilen ideal

$$\langle x_1, x_2, \dots, x_n \rangle = \left\{ x_1 a_1 + x_2 a_2 + \dots + x_n a_n \mid a_j \in D \text{ keyfi}, 1 \leq j \leq n \right\}$$

olarak tanımlanır.

$\langle x_1, x_2, \dots, x_n \rangle$ ideali $x_1, x_2, \dots, x_n$ elemanlarını içeren en küçük idealdir. Diğer yandan $A+B$ ve AB 'nin birer ideal olduğunu görmek kolaydır. A ve B ideallerse $A \cap B$ 'de bir idealdir.

Bu verilen tanımlara göre ideallerle ilgili aşağıdaki özellikler geçerlidir. A, B, C 'ler D 'nin idealleri olmak üzere

a. $A(B+C) = AB+AC$ ve $(B+C)A = BA+CA$

b. $(A+B)+C = A+(B+C)$

ve $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n \in D$ olmak üzere

c.
$$\langle x_1, x_2, \dots, x_n \rangle \langle y_1, y_2, \dots, y_n \rangle = \langle x_1 y_1, x_2 y_1, \dots, x_n y_1, x_1 y_2, x_2 y_2, \dots, x_n y_2, \dots, x_1 y_m, x_2 y_m, \dots, x_n y_m \rangle$$

d. $x, y \in D$ elemanları tarafından üretilen esas ideallerin çarpımı

$$\langle x \rangle \langle y \rangle = \langle x, y \rangle$$

dir.

Tanım 1.13. D bir tamlık bölgesi olsun. I , D 'nin bir ideali olsun. $I = \langle x \rangle$ olacak biçimde bir $x \in D$ varsa I 'ya bir esas ideal denir. D tamlık bölgesinin her ideali bir esas ideal ise D 'ye esas ideal bölgesi denir.

Örnek 1.19. $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ 'de $a + b\sqrt{-5} \in \langle 2, 1 + \sqrt{-5} \rangle$ olmasının gerek ve yeter koşulu $a \equiv b \pmod{2}$ olmasıdır. Yani

$$\langle 2, 1 + \sqrt{-5} \rangle = \{ u + v\sqrt{-5} \mid u, v \in \mathbb{Z}, u \equiv v \pmod{2} \}$$

dir. Bunu gösterelim. Önce $a \equiv b \pmod{2}$ olsun. O halde $a = b + 2c$ olan $c \in \mathbb{Z}$ vardır. Böylece

$$a + b\sqrt{-5} = b + 2c + b\sqrt{-5} = c(2) + b(1 + \sqrt{-5}) \in \langle 2, 1 + \sqrt{-5} \rangle$$

elde edilir. Şimdi $a + b\sqrt{-5} \in \langle 2, 1 + \sqrt{-5} \rangle$ olsun. O zaman $x, y, z, w \in \mathbb{Z}$ için

$$\begin{aligned} a + b\sqrt{-5} &= (x + y\sqrt{-5})2 + (z + w\sqrt{-5})(1 + \sqrt{-5}) \\ &= (2x + z - 5w) + (2y + z + w)\sqrt{-5} \end{aligned}$$

olur. Buradan $a = 2x + z - 5w$, $b = 2y + z + w$ olduğu görülür. O halde

$$a \equiv 2x + z - 5w \equiv z - 5w \equiv z + w \equiv 2y + z + w \equiv b \pmod{2}$$

olduğu görülür. Yani $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ 'de

$$\langle 2, 1 + \sqrt{-5} \rangle = \left\{ u + v\sqrt{-5} \mid u, v \in \mathbb{Z}, u \equiv v \pmod{2} \right\}$$

dir.

Teorem 1.1. D bir halka ve $u \in D$ olsun. Bu takdirde $\langle u \rangle = D$ olması için gerek ve yeter koşul $u \in U(D)$ olmasıdır [1].

Teorem 1.2. D bir halka ve $a, b \in D \setminus \{0\}$ olsun. Bu takdirde $\langle a \rangle = \langle b \rangle$ olması için gerek ve yeter koşul $a = \varepsilon b$ olacak biçimde bir $\varepsilon \in U(D)$ olmasıdır. [1].

Teorem 1.3. $\mathbb{Z}$ bir esas ideal bölgesidir [1].

Tanım 1.14. Bir D halkasının boştan farklı bir alt kümesi M olsun. Aşağıdaki şartlar sağlanıyorsa M 'ye bir maksimal ideal denir.

- a. $M \neq D$ dir.
- b. $M \subset I$ olacak biçimdeki D 'nin her I ideali için ya $I = M$ ya da $I = D$ dir.

Tanım 1.15. Bir D halkasının bir ideali P ve $P \neq D$ olsun. Her $a, b \in D$ için $ab \in P$ iken $a \in P$ ya da $b \in P$ elde ediliyorsa P 'ye bir asal ideal denir.

Örnek 1.20. $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ ’de $\langle 2, 1 + \sqrt{-5} \rangle$ ideali asaldır. Bunu gösterelim.

Örnek 1.19’da

$\langle 2, 1 + \sqrt{-5} \rangle = \{u + v\sqrt{-5} \mid u, v \in \mathbb{Z}, u \equiv v \pmod{2}\}$ olduğunu göstermiştik.

$$\alpha = a + b\sqrt{-5} \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}, \beta = c + d\sqrt{-5} \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$$

olmak üzere $\alpha\beta \in \langle 2, 1 + \sqrt{-5} \rangle$ olsun. Burada

$$\alpha\beta = (a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5}$$

dir. Örnek 1.19’a göre $ac - 5bd \equiv ad + bc \pmod{2}$ olur. Ayrıca

$$(a - b)(c - d) = ac - bc - ad + bd \equiv (ad + bc + 5bd) - bc - ad + bd \equiv 0 \pmod{2}$$

elde edilir. O halde ya $a - b \equiv 0 \pmod{2}$ ya da $c - d \equiv 0 \pmod{2}$ olur. Yani ya

$a \equiv b \pmod{2}$ ya da $c \equiv d \pmod{2}$ olur. O zaman Örnek 1.19’a göre dolayısı ya

$\alpha = a + b\sqrt{-5} \in \langle 2, 1 + \sqrt{-5} \rangle$ ya da $\beta = c + d\sqrt{-5} \in \langle 2, 1 + \sqrt{-5} \rangle$ elde edilir.

Dolayısıyla $\langle 2, 1 + \sqrt{-5} \rangle$ ideali asaldır.

Teorem 1.4. D bir tamlık bölgesi olsun. Bu takdirde D ’nin her asal elemanı indirgenemezdir.

İspat. $p \in D$ bir asal eleman ve $a, b \in D$ için $p = ab$ olsun. $ab = p \cdot 1$ olduğundan $p \mid ab$ elde edilir. p asal olduğundan $p \mid a$ veya $p \mid b$ olur. $p \mid a$ ise $a = pp'$ olacak biçimde $p' \in D$ vardır. Böylece $p = ab = pp'b = p(p'b)$ olur. Yani $1 = p'b$ elde edilir. Bu da b ’nin birim olduğunu gösterir. $p \mid b$ ise $b = pp''$ olacak biçimde $p'' \in D$ vardır. Böylece $p = ab = app'' = p(ap'')$ olur. Yani $1 = ap''$ elde edilir. Bu da a ’nin

birim olduğunu gösterir. O halde a veya b 'den biri birimdir. Dolayısıyla p indirgenemezdir.

Örnek 1.21. Teorem 1.1'in tersi her zaman doğru değildir. Buna örnek verelim. $\mathbb{Z} + \mathbb{Z}(\sqrt{-5})$ 'de $1 + \sqrt{-5} \in \mathbb{Z} + \mathbb{Z}(\sqrt{-5})$ olsun. $1 + \sqrt{-5}$ indirgenemezdir. Bunu gösterelim. $a, b, c, d \in \mathbb{Z}$ olmak üzere $1 + \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5})$ olsun.

Buradan

$$6 = (a^2 + 5b^2)(c^2 + 5d^2)$$

elde edilir. O halde $a^2 + 5b^2$ sayısı 6'nın bir pozitif tamsayı bölenidir. O zaman $a^2 + 5b^2$ sayısı 1, 2, 3 veya 6 olabilir. $a^2 + 5b^2 = 2$ ve $a^2 + 5b^2 = 3$ eşitliklerinin tamsayılarda çözümü yoktur. O halde $a^2 + 5b^2$ sayısı 1 veya 6 olabilir. $a^2 + 5b^2 = 1$ ise $a = \pm 1$ böylece $a + b\sqrt{-5} = \pm 1$ olur. Yani $a + b\sqrt{-5}$ bir birimdir. $a^2 + 5b^2 = 6$ ise $c^2 + 5d^2 = 1$ olacağından $c + d\sqrt{-5}$ bir birim olur. Dolayısıyla $1 + \sqrt{-5}$ indirgenemezdir. Şimdi $1 + \sqrt{-5}$ 'in asal olmadığını gösterelim.

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$$

olduğu açıktır. Buradan $1 + \sqrt{-5} \mid 2 \cdot 3$ elde edilir. $1 + \sqrt{-5}$ 'in asal eleman ise ya $1 + \sqrt{-5} \mid 2$ ya da $1 + \sqrt{-5} \mid 3$ olmalıdır. Fakat normlara geçerse, $6 \nmid 4$ ve $6 \nmid 9$ olacağından $1 + \sqrt{-5} \nmid 2$ ve $1 + \sqrt{-5} \nmid 3$ olur. O halde $1 + \sqrt{-5}$ asal değildir.

Teorem 1.5. D bir esas ideal bölgesi olsun. Bu takdirde D 'nin her indirgenemez elemanı asaldır.

İspat. $p \in D$ indirgenemez eleman ve $a, b \in D$ için $p \mid ab$ olsun. $p \mid a$ ise istenilen elde edilir. $p \nmid a$ olsun. $I = \{px + ay \mid x, y \in D\}$ olsun. I 'nin D 'de bir ideal olduğu

gösterilebilir. D bir esas ideal bölgesi olduğundan $I = \langle c \rangle$ olacak biçimde bir $c \in D$ vardır. $a \in I$ ve $p \in I$ olduğundan $c|a$ ve $c|p$ olur. $c|p$ ve p indirgenemez olduğundan ya $c \sim p$ ya da c 'nin bir birim olduğu elde edilir. $c \sim p$ ise $c|a$ olduğundan $p|a$ olur ki bu çelişkidir. O halde c bir birimdir. O zaman $cd=1$ olacak biçimde bir $d \in D$ vardır. Ayrıca $c \in \langle p, a \rangle$ olduğundan $c = xp + ya$ olacak biçimde $x, y \in D$ vardır. O halde $1 = cd = xad + ypd$ elde edilir. Buradan $b = xadb + ypdb$ olur. Bu ise $b = (dx)ab + (bdy)p$ olarak yazılabilir. $p|p$ ve $p|ab$ olduğundan $p|b$ elde edilir. Dolayısıyla ya $p|a$ ya da $p|b$ olur. Yani p asaldır.

Teorem 1.6. D bir tamlık bölgesi olsun. $p \in D$, $p \neq 0$, $p \notin U(D)$ olsun. $\langle p \rangle$, D de asal ideal ise p , D 'de asal elemandır. Tersine p asal eleman ise $\langle p \rangle$ ideali asal idealdir.

İspat. $\langle p \rangle$ asal ideal olsun. $a, b \in D$ için $p|ab$ olsun. O halde $ab = pp'$ olacak biçimde $p' \in D$ vardır. O zaman $ab \in \langle p \rangle$ olur. $\langle p \rangle$ asal ideal olduğundan ya $a \in \langle p \rangle$ ya da $b \in \langle p \rangle$ olmalıdır. O halde ya $p|a$ ya da $p|b$ elde edilir. Dolayısıyla p asaldır. Diğer yandan p asal eleman ise $\langle p \rangle$ 'nin asal ideal olduğunu görmek kolaydır.

Teorem 1.7. D bir tamlık bölgesi olsun. $a \in D$, $a \neq 0$, $a \notin U(D)$ olsun. Eğer $\langle a \rangle$, D 'de maksimal ideal ise a , D 'de indirgenemez elemandır.

İspat. $\langle a \rangle$ maksimal ideal olsun. $b, c \in D$ olmak üzere $a = bc$ olsun. O zaman $\langle a \rangle \subset \langle b \rangle$ olur. b birim ise istenilen elde edilir. b birim olmasın. O halde $\langle b \rangle \neq D$

olur. $\langle a \rangle$ maksimal ideal olduğundan $\langle a \rangle = \langle b \rangle$ elde edilir. $b \in \langle b \rangle = \langle a \rangle$ olduğundan $b = aa'$ olacak biçimde $a' \in D$ vardır. O halde $a = bc = aa'c = a(a'c)$ dir. Yani $1 = a'c$ elde edilir. O zaman c birim olur. Dolayısıyla a indirgenemezdir.

Teorem 1.8. D bir esas ideal bölgesi olsun. $a \in D$, $a \neq 0$, $a \notin U(D)$ olsun. a , D de indirgenemez eleman ise $\langle a \rangle$, D 'de maksimal idealdir.

İspat. a indirgenemez olsun ve $\langle a \rangle \subset M \subset D$, $M \neq D$ olsun. $\langle a \rangle = M$ olduğunu gösterelim. D bir esas ideal bölgesi olduğundan $M = \langle b \rangle$ olacak biçimde bir $b \in D$ vardır. $a \in M$ ve $M = \langle b \rangle$ olduğundan $a \in \langle b \rangle$ olur. Yani $a = bc$ olacak biçimde bir $c \in D$ vardır. a indirgenemez olduğundan b veya c birimdir. $D \neq M = \langle b \rangle$ olduğundan b birim olamaz. O halde c birimdir. Dolayısıyla $\langle a \rangle = \langle bc \rangle = \langle b \rangle = M$ olur. Yani $\langle a \rangle$ maksimal idealdir.

Teorem 1.9. D bir tamlık bölgesi ve $M \subset D$, $M \neq D$ bir ideal olsun. Bu takdirde M maksimal idealdir. $\Leftrightarrow a \notin M$ ise $1 = ax_0 + y_0$ olan $y_0 \in M$, $x_0 \in D$ vardır.

İspat. $\Rightarrow$: M maksimal ideal olsun. $a \notin M$ alalım. $M^* = \{ax + y \mid y \in M, x \in D\}$ olsun. M^* kümesi D 'nin bir idealidir ve $M \subset M^*$ 'dir. Ayrıca $a \in M^*$, $a \notin M$ olduğundan $M \neq M^*$ 'dir. M maksimal olduğundan $M^* = D$ elde edilir. O halde $1 \in D = M^*$ dir. Dolayısıyla $1 = ax_0 + y_0$ olan $y_0 \in M$, $x_0 \in D$ vardır.

$\Leftarrow$: $a \notin M$ ise $1 = ax_0 + y_0$ olan $y_0 \in M$, $x_0 \in D$ mevcut olsun. L bir ideal ve $M \subset L$ olsun. $L \neq M$ ise $L = D$ olduğunu göstermek yeterlidir. $L \neq M$ olsun. O halde bir $a \in L$ elemanı $a \notin M$ olacak biçimde vardır. $a \notin M$ olduğundan

$1 = ax_0 + y_0$ olan $y_0 \in M$, $x_0 \in D$ vardır. $y_0 \in M$ ve $M \subset L$ olduğundan $y_0 \in L$ olur. O halde $a \in L$, $y_0 \in L$ olduğundan $ax_0 + y_0 \in L$ 'dir. Yani $1 \in L$ elde edilir. O zaman $L = D$ olur. Dolayısıyla M maksimal idealdir.

Teorem 1.10. D bir tamlık bölgesi ve $I \subset D$ bir ideal olsun. Bu takdirde

1. I 'nin asal ideal olması için gerek ve yeter koşul D/I 'nin tamlık bölgesi olmasıdır.
2. I 'nin maksimal ideal olması için gerek ve yeter koşul D/I 'nin cisim olmasıdır [1].

Teorem 1.11. D bir tamlık bölgesi olsun. $M \subset D$ bir maksimal ideal ise M asal idealdir.

İspat. M bir maksimal ideal ve $ab \in M$ olsun. $a \in M$ ise istenilen elde edilir. $a \notin M$ olsun. O halde $1 = ax_0 + y_0$ olan $y_0 \in M$, $x_0 \in D$ vardır. Buradan $b = abx_0 + by_0$ olur. $y_0 \in M$ ve $ab \in M$ olduğundan $abx_0 + by_0 = b \in M$ elde edilir. Dolayısıyla M asal idealdir.

Örnek 1.22. Tamlık bölgelerinde asal idealin maksimal olması gerekmez. Buna bir örnek verelim. $\mathbb{Z}[x]$ 'de $\langle x \rangle$ bir asal idealdir. Bunu gösterelim. m ve n negatif olmayan tamsayılar,

$$p(x) = a_0 + a_1x + \dots + a_mx^m \in \mathbb{Z}[x], q(x) = b_0 + b_1x + \dots + b_nx^n \in \mathbb{Z}[x]$$

olmak üzere $p(x)q(x) \in \langle x \rangle$ olsun. O zaman $p(x)q(x) = xh(x)$ olacak biçimde $h(x) = c_0 + c_1x + \dots + c_kx^k \in \mathbb{Z}[x]$, $k \in \mathbb{Z}^+ \cup \{0\}$ vardır. O halde

$$(a_0 + a_1x + \dots + a_mx^m)(b_0 + b_1x + \dots + b_nx^n) = x(c_0 + c_1x + \dots + c_kx^k)$$

elde edilir. Burada katsayılar eşitlenirse

$$a_0b_0 = 0$$

olur. O halde ya $a_0 = 0$ ya da $b_0 = 0$ elde edilir. $a_0 = 0$ ise

$$p(x) = a_1x + \dots + a_mx^m = x(a_1 + \dots + a_mx^{m-1}) \in \langle x \rangle$$

olur. $b_0 = 0$ ise

$$q(x) = b_1x + \dots + b_nx^n = x(b_1 + \dots + b_nx^{n-1}) \in \langle x \rangle$$

olur. Sonuç olarak $\langle x \rangle$ bir asal idealdir. Fakat $\langle x \rangle \subset \langle 2, x \rangle \subset \mathbb{Z}[x]$ olmasına rağmen $\langle x \rangle \neq \langle 2, x \rangle$ ve $\langle 2, x \rangle \neq \mathbb{Z}[x]$ olduğundan $\langle x \rangle$ ideali $\mathbb{Z}[x]$ 'de maksimal değildir.

Teorem 1.12. D bir esas ideal bölgesi olsun. $P \subset D$ bir asal ideal ise P maksimal idealdir.

İspat. P asal ideal olsun. D esas ideal bölgesi olduğundan $P = \langle p \rangle$ olacak biçimde $p \in D$ vardır. P asal ideal olduğundan Teorem 1.6'ye göre p asal elemandır. O halde p indirgenemez elemandır. Teorem 1.8'e göre $\langle p \rangle$ maksimal idealdir. Yani P maksimal idealdir.

Teorem 1.13. D bir tamlık bölgesi, $a \in D$ ve $\langle a \rangle$ maksimal ideal olsun. $a \nmid b$ ise $1 = bx + ay$ olacak biçimde $x, y \in D$ vardır.

İspat. $\langle a \rangle$ maksimal ve $a \nmid b$ olsun. O zaman $b \notin \langle a \rangle$ olur. $\langle a \rangle$ maksimal olduğundan $1 = bx + y_0$ olan $y_0 \in \langle a \rangle$, $x \in D$ vardır. $y_0 \in \langle a \rangle$ ise $y_0 = ay$ olan $y \in D$ vardır. Böylece $1 = bx + ay$, $x \in D$, $y \in D$ elde edilir.

Teorem 1.14. D bir esas ideal bölgesi, $a \in D$ indirgenemez eleman olsun. $a \nmid b$ ise $1 = bx + ay$ olacak biçimde $x, y \in D$ vardır.

İspat. a indirgenemez olsun. Teorem 1.8'e göre $\langle a \rangle$ ideali maksimaldir. $a \nmid b$ olsun. O halde Teorem 1.13'e göre $1 = bx + ay$ olan $x, y \in D$ vardır.

Bu teoremin sonucu olarak aşağıdaki teorem verilebilir.

Teorem 1.15. K bir cisim, $p(x) \in K[x]$ indirgenemez polinom olsun. $p(x) \nmid q(x)$ ise

$$1 = p(x)p_0(x) + g(x)g_0(x)$$

olacak biçimde $p_0(x), g_0(x) \in K[x]$ vardır.

Teorem 1.16. $f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in \mathbb{Z}[x]$ bir monik polinomu için $p \mid a_1, \dots, p \mid a_{n-1}, p \mid a_n, p^2 \nmid a_n$ olacak biçimde bir p asal sayısı varsa $f(x)$ polinomu $\mathbb{Z}[x]$ 'de indirgenemezdir. Bu kritere Eisenstein indirgenemezlik kriteri denir.

Teorem 1.17. A ve D tamlık bölgeleri ve $D \subseteq A$ olsun. P , A 'da asal ideal ve $P \cap D \neq \{0\}$, $P \cap D \neq D$ olsun. Bu takdirde $P \cap D$, D 'de bir asal idealdir [1].

Tanım 1.16. D bir tamlık bölgesi olsun. D kümesinde aşağıdaki iki şartı sağlayan bir $\phi: D \rightarrow \mathbb{Z}$ dönüşümü var ise D 'ye bir Öklid bölgesi denir.

- a. Her $a, b \in D, a \neq 0$ için $\phi(ab) > \phi(b)$ 'dir.
- b. $a, b \in D, b \neq 0$ ise $a = qb + r$, $\phi(r) < \phi(b)$ olacak biçimde $q, r \in D$ vardır [1].

Teorem 1.18. D bir Öklid bölgesi olsun. Bu takdirde D bir esas ideal bölgesidir[1].

Teorem 1.19. $\mathbb{Z}$ bir Öklid bölgesidir [1].

Teorem 1.20. F bir cisim olsun. Bu takdirde $F[x]$ bir Öklid bölgesidir [1].

Tanım 1.17. Bir tamlık bölgesinde ideallerin sonsuz bir dizisi $\{I_n \mid n=1,2,\dots\}$ olsun. Eğer

$$I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$$

ise bu $\{I_n \mid n=1,2,\dots\}$ dizisine bir artan ideal zinciri denir. Eğer

$$I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$$

ise bu zincire kesin artan ideal zinciri denir.

Tanım 1.18. Bir tamlık bölgesinde artan bir ideal zinciri

$$I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$$

olsun. Her $n \geq n_0$ için

$$I_n = I_{n_0}$$

olacak biçimde bir n_0 tamsayısı varsa bu zincire sonludur denir.

Tanım 1.19. D bir tamlık bölgesi olsun. D 'deki her artan ideal zinciri sonlu ise, yani D 'de kesin artan bir ideal zinciri mevcut değil ise D 'ye artan zincir koşulunu sağlar denir.

Tanım 1.20. Bir D tamlık bölgesi artan zincir koşulunu sağlasın. Bu takdirde D ye bir Noetherian bölgesi denir.

Örnek 1.23. $\mathbb{Z}$ bir Noetherian bölgesidir. Aksine $\mathbb{Z}$ 'nin bir Noetherian bölgesi olmadığını kabul edelim. O halde $\mathbb{Z}$ artan zincir koşulunu sağlamaz. Yani $\mathbb{Z}$ 'de en azından bir tane kesin artan ideal zinciri mevcuttur. Bu kesin artan ideal zinciri $I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$ olsun. $\mathbb{Z}$ bir esas ideal bölgesi olduğundan $I_1 = \langle m_1 \rangle, I_2 = \langle m_2 \rangle$ olacak biçimde $m_1, m_2 \in \mathbb{Z}$ vardır. $I_1 \subset I_2$ olduğundan $m_2 \mid m_1$ dir. m_1 tamsayısının sonlu sayıda böleni olacağından $I_1 \subset I$ olacak biçimde sonlu sayıda I ideali vardır. Dolayısıyla $I_1 \subset I_2 \subset I_3 \subset I_4 \subset \dots$ olacak biçimde sonsuz sayıda $I_k (k=1,2,\dots)$ idealinin var olması mümkün değildir. O halde $\mathbb{Z}$ bir Noetherian bölgesidir.

Teorem 1.21. D bir tamlık bölgesi olsun. Bu takdirde D 'nin Noetherian bölgesi olmasının gerek ve yeter koşulu D 'nin her idealinin sonlu üretilmiş olmasıdır[1].

Teorem 1.22. D bir esas ideal bölgesi olsun. Bu takdirde D bir Noetherian bölgesidir.

İspat. D bir esas ideal bölgesi ise D 'deki her ideal esas idealdir dolayısıyla sonlu üretilmiştir. Teorem 1.21'ye göre D bir Noetherian bölgesidir.

Örnek 1.24. Teorem 1.18'e göre Öklid bölgeleri birer esas ideal bölgesi olduğundan Teorem 1.23 kullanılırsa her Öklid bölgesi bir Noetherian bölgesi olduğu görülür.

Tanım 1.21. D bir tamlık bölgesi olsun. D 'deki ideallerin boştan farklı bir kümesi S olsun. D 'deki her S kümesi, S 'deki diğer hiçbir ideal tarafından tam kapsanılmayan bir ideale sahip ise D 'ye maksimal koşulunu sağlar denir. Yani S kümesinde öyle bir I ideali vardır öyle ki $I \subseteq J$ olan her $J \in S$ ideali için $J = I$ olur.

Teorem 1.23. D bir tamlık bölgesi olsun. Bu takdirde D 'nin Noetherian bölgesi olmasının gerek ve yeter koşulu D 'nin maksimal koşulunu sağlamasıdır[1].

Teorem 1.24. D bir tamlık bölgesi olsun fakat bir cisim olmasın. D Noetherian ise D 'de indirgenemez olan elemanlar vardır[1].

Tanım 1.22. D bir tamlık bölgesi olsun. D 'deki sıfırdan farklı, birim olmayan her eleman, D 'deki indirgenemez elemanların sonlu bir çarpımı biçiminde ifade edilebiliyorsa D 'ye bir çarpanlarına ayrılabilir bölge denir.

Teorem 1.25. D bir Noetherian bölgesi olsun. Bu takdirde D bir çarpanlarına ayrılabilir bölgedir[1].

Teorem 1.26. D bir esas ideal bölgesi olsun. Bu takdirde D bir çarpanlarına ayrılabilir bölgedir.

İspat. D bir esas ideal bölgesi olsun. Teorem 1.23'e göre D bir Noetherian bölgedir ve Teorem 1.25'e göre D bir çarpanlarına ayrılabilir bölgedir.

Tanım 1.23. D bir çarpanlarına ayrılabilir bölge olsun. Kabul edelim ki, D 'nin sıfırdan farklı, birim olmayan her a elemanı, D 'nin indirgenemez elemanlarının çarpımı biçiminde tek türlü olarak yazılabilir. Bu durumda D 'ye tek türlü çarpanlarına ayrılabilen bölge denir. a 'nın indirgenemez elemanların tek türlü çarpımı biçiminde yazılması şu anlamdadır: $\pi_1, \pi_2, \dots, \pi_r, \pi_1^*, \pi_2^*, \dots, \pi_s^*$ 'ler indirgenemez elemanlar olmak üzere $a = \pi_1 \pi_2 \dots \pi_r = \pi_1^* \pi_2^* \dots \pi_s^*$ ise $r = s$ 'dir ve $\sigma: \{1, 2, \dots, r\} \rightarrow \{1, 2, \dots, s\}$ permutasyonu $\pi_j \sim \pi_{\sigma(j)}^*$, $1 \leq j \leq r$ olacak biçimde vardır.

Teorem 1.27. D bir esas ideal bölgesi olsun. Bu takdirde D bir tek türlü çarpanlarına ayrılabilen bölgedir [1].

Teorem 1.28. D bir tek türlü çarpanlarına ayrılabilen bölge olsun. D 'nin bir a elemanı olsun. Bu takdirde a 'nın indirgenemez olmasının gerek ve yeter koşulu a 'nın asal olmasıdır [1].

BÖLÜM 2. CEBİRSEL TAMSAYILAR

Tanım 2.1. A ve B tamlık bölgeleri ve $A \subseteq B$ olsun. Bir $b \in B$ elemanı, $a_0, a_1, \dots, a_{n-1} \in A$ olmak üzere

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$$

monik (başkatsayısı 1 olan) polinom denklemini sağlıyor ise b 'ye A üzerinde integraldir veya tamdır denir [1].

Her $a \in A$ elemanı $x - a \in A[x]$ 'in bir kökü olduğundan her $a \in A$ elemanı A üzerinde tamdır.

Tanım 2.2. $\mathbb{Z}$ üzerinde tam olan bir kompleks sayıya bir cebirsel tamsayı denir[1].

Örnek 2.1. $\sqrt[3]{2} - \sqrt[3]{4}$ bir cebirsel tamsayıdır çünkü $x^3 + 6x + 2 = 0$ denklemini sağlar.

Örnek 2.2. $\frac{1}{3} \left(1 + 10^{\frac{1}{3}} + 10^{\frac{2}{3}} \right)$ bir cebirsel tamsayıdır. Bunu gösterelim.

$$\alpha = \frac{1}{3} \left(1 + 10^{\frac{1}{3}} + 10^{\frac{2}{3}} \right)$$

olsun. O zaman $3\alpha - 1 = 10^{\frac{1}{3}} + 10^{\frac{2}{3}}$ olur. Her iki tarafın küpü alınırsa,

$$27\alpha^3 - 27\alpha^2 + 9\alpha - 1 = 110 + 30\left(10^{\frac{1}{3}} + 10^{\frac{2}{3}}\right)$$

olur. $3\alpha - 1 = 10^{\frac{1}{3}} + 10^{\frac{2}{3}}$ olduğu kullanılırsa

$$27\alpha^3 - 27\alpha^2 + 9\alpha - 1 = 80 + 90\alpha$$

elde edilir. Böylece $\alpha^3 - \alpha^2 - 3\alpha - 3 = 0$ olur. O halde α sayısı $x^3 - x^2 - 3x - 3 \in \mathbb{Z}[x]$ monik polinomunun bir köküdür. Dolayısıyla α bir cebirsel tamsayıdır.

Örnek 2.3. $\frac{10^{\frac{2}{3}} - 1}{\sqrt{-3}}$ bir cebirsel tamsayıdır. Bunu gösterelim.

$$\alpha = \frac{10^{\frac{2}{3}} - 1}{\sqrt{-3}}$$

olsun. O zaman $1 + \alpha\sqrt{-3} = 10^{\frac{2}{3}}$ olur. Her iki tarafın küpü alınırsa,

$$(1 - 9\alpha^2) + 3\sqrt{-3}(\alpha - \alpha^3) = 100$$

olur. Böylece $\sqrt{-3}(\alpha - \alpha^3) = 33 + 3\alpha^2$ elde edilir. Her iki tarafın karesi alınırsa,

$$-3(\alpha^2 - 2\alpha^4 + \alpha^6) = 1089 + 198\alpha^2 + 9\alpha^4$$

elde edilir. Böylece $\alpha^6 + \alpha^4 + 67\alpha^2 + 363 = 0$ olur. O halde α sayısı $x^6 + x^4 + 67x^2 + 363 \in \mathbb{Z}[x]$ monik polinomunun bir köküdür. Dolayısıyla α bir cebirsel tamsayıdır.

Örnek 2.4. $\frac{1}{\sqrt{2}}$ bir cebirsel tamsayı değildir. Bunu gösterelim. Tersine $\frac{1}{\sqrt{2}}$ 'nin

bir cebirsel tamsayı olduğunu kabul edelim. Bu takdirde

$$\left(\frac{1}{\sqrt{2}}\right)^n + a_{n-1}\left(\frac{1}{\sqrt{2}}\right)^{n-1} + \dots + a_1x + a_0 = 0$$

olacak biçimde bir n pozitif tamsayısı ve $a_0, a_1, \dots, a_{n-1}$ tamsayıları vardır. Bu eşitliğin her iki tarafı $(\sqrt{2})^n$ ile çarpılırsa

$$1 + a_{n-1}\sqrt{2} + a_{n-2}(\sqrt{2})^2 + \dots + a_1x(\sqrt{2})^{n-1} + a_0(\sqrt{2})^n = 0$$

elde edilir. Dolayısıyla

$$(1 + 2a_{n-2} + 4a_{n-4} + \dots) + \sqrt{2}(a_{n-1} + 2a_{n-3} + \dots) = 0$$

olur. $a_{n-1} + 2a_{n-3} + \dots \neq 0$ ise

$$\sqrt{2} = \frac{-(1 + 2a_{n-2} + 4a_{n-4} + \dots)}{a_{n-1} + 2a_{n-3} + \dots}$$

elde edilir ki bu ifade iki tamsayının bölümü olduğundan bir rasyonel sayı olur. Bu ise mümkün değildir. Dolayısıyla $a_{n-1} + 2a_{n-3} + \dots = 0$ olur. Buradan

$1 + 2a_{n-2} + 4a_{n-4} + \dots = 0$ elde edilir. $1 + 2a_{n-2} + 4a_{n-4} + \dots$ tamsayısı tek bir tamsayı

olduğundan bu da bir çelişkidir. O halde $\frac{1}{\sqrt{2}}$ cebirsel tamsayı değildir.

Tanım 2.3. A ve B tamlık bölgeleri ve $A \subseteq B$ olsun. A bir cisim ve $b \in B$ elemanı A üzerinde tam olsun. Bu takdirde b 'ye A üzerinde cebirseldir denir [1].

Tanım 2.4. $\mathbb{Q}$ üzerinde cebirsel olan kompleks sayıya bir cebirsel sayı denir [1].

Örnek 2.5. $\frac{1}{\sqrt{2}}$ bir cebirsel sayıdır çünkü $x^2 - \frac{1}{2} = 0$ denklemini sağlar.

Tanım 2.5. A ve B tamlık bölgeleri ve $A \subseteq B$ olsun. Her $b \in B$ elemanı A üzerinde tam ise B 'ye A üzerinde tamdır denir [1].

Örnek 2.6. m tamkare olmayan bir tamsayı olmak üzere $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ kuadratik bölgesi $\mathbb{Z}$ üzerinde tamdır. Çünkü her $u + v\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ elemanı, $-2u \in \mathbb{Z}$ ve $u^2 - mv^2 \in \mathbb{Z}$ olmak üzere

$$x^2 - 2ux + u^2 - mv^2 = 0$$

denklemini sağladığından, $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ 'nin her $u + v\sqrt{m}$ elemanı $\mathbb{Z}$ üzerinde tamdır.

Örnek 2.7. m tamkare olmayan bir tamsayı ve $m \equiv 1 \pmod{4}$ olsun.

$\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ kuadratik bölgesi $\mathbb{Z}$ üzerinde tamdır. Çünkü her

$\alpha = u + v\left(\frac{1+\sqrt{m}}{2}\right) \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ elemanı $(-2u + v) \in \mathbb{Z}$ ve

$u^2 + uv + \frac{1}{4}(1-m^2)v^2 \in \mathbb{Z}$ olmak üzere

$$x^2 - (2u - v)x + u^2 + uv + \frac{1}{4}(1-m^2)v^2 = 0$$

denklemini sağlar. O halde $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ 'nin her $u + v\left(\frac{1+\sqrt{m}}{2}\right)$ elemanı $\mathbb{Z}$ üzerinde tamdır.

Örnek 2.8. A ve B tamlık bölgeleri ve $A \subseteq B$ olsun. $a \in A$ olsun. $b \in B$ elemanı A üzerinde tam olsun. ab 'nin de A üzerinde tam olduğunu gösterelim. $b \in B$, A üzerinde tam olduğundan

$$b^n + a_{n-1}b^{n-1} + \dots + a_1b + a_0 = 0$$

olacak biçimde $a_0, a_1, \dots, a_{n-1} \in A$ elemanları vardır. $a \in A$ olsun. O zaman $ab \in B$ dir. Yukarıdaki polinomun her iki tarafı a^n ile çarpılırsa

$$(ab)^n + a_{n-1}a(ab)^{n-1} + \dots + a_1a^{n-1}(ab) + a_0a^n = 0$$

olur. Burada $a_{n-1}a, \dots, a_1a^{n-1}, a_0a^n \in A$ olduğundan ab 'nin de A üzerinde tam olduğu görülür.

Teorem 2.1. $A \subseteq B \subseteq C$ tamlık bölgeleri olsun. Bir $c \in C$ elemanı A üzerinde tam ise c elemanı B üzerinde de tamdır [1].

İspat. $c \in C$ elemanı, A üzerinde tam olduğundan

$$c^n + a_{n-1}c^{n-1} + \dots + a_1c + a_0 = 0$$

olacak biçimde $a_0, a_1, \dots, a_{n-1} \in A$ vardır. $A \subseteq B$ olduğundan $a_0, a_1, \dots, a_{n-1} \in B$ olur. Böylece c elemanı B üzerinde de tamdır.

Teorem 2.2. $A \subseteq B \subseteq C$ tamlık bölgeleri olsun. C bölgesi A üzerinde tam ise C bölgesi B üzerinde de tamdır [1].

İspat. $c \in C$ olsun. C bölgesi A üzerinde tam olduğundan, c elemanı A üzerinde tamdır. Teorem 2.1'e göre c elemanı B üzerinde de tamdır. c keyfi ve c elemanı B üzerinde tam olduğundan C bölgesi B üzerinde tamdır.

Teorem 2.3. A ve B tamlik bölgeleri ve $A \subseteq B$ olsun. b_1, b_2 elemanları A üzerinde tam olsun. Bu takdirde $b_1 + b_2$, $b_1 - b_2$, $b_1 b_2$ elemanları da A üzerinde tamdır [1].

Sonuç 2.1. A ve B tamlik bölgeleri ve $A \subseteq B$ olsun. B 'nin A üzerinde tam olan bütün elemanlarının kümesi B 'nin A 'yı içeren bir alt bölgesidir [1].

Sonuç 2.2. Tüm cebirsel tamsayıların kümesi bir tamlik bölgesidir. Bu küme Ω ile gösterilir [1].

Teorem 2.4. $A \subseteq B \subseteq C$ tamlik bölgeleri olsun. B bölgesi A üzerinde tam ve $c \in C$ elemanı B üzerinde tam ise c elemanı A üzerinde tamdır [1].

Teorem 2.5. $A \subseteq B \subseteq C$ tamlik bölgeleri olsun. C bölgesi B üzerinde tam ve B bölgesi A üzerinde tam ise C bölgesi A üzerinde tamdır [1].

Tanım 2.6. A ve B tamlik bölgeleri ve $A \subseteq B$ olsun. B 'nin A üzerinde tam olan tüm elemanlarını içeren alt bölgesine, A 'nın B 'deki integral kapanışı veya tam kapanışı denir ve A^B ile gösterilir [1].

Teorem 2.6. A ve B tamlik bölgeleri ve $A \subseteq B$ olsun. Bu takdirde A 'nın B 'deki tam kapanışı A^B ;

$$A \subseteq A^B \subseteq B$$

şartını sağlayan bir tamlik bölgesidir. Ayrıca her A tamlik bölgesi için $A^A = A$ olduğu açıktır [1].

Teorem 2.7. D bir tek türlü çarpanlarına ayrılabilen bölge olsun. D 'nin kesir cismi F olsun. Bu takdirde $c \in F$ elemanının D üzerinde tam olabilmesinin gerek ve yeter koşulu $c \in D$ olmasıdır [1].

İspat. $\Rightarrow$: $c \in D$ ise c elemanı $x - c = 0$ denklemini sağlar. O halde c elemanı D üzerinde tamdır.

$\Leftarrow$: $c \in F$ elemanı D üzerinde tam olsun. O zaman c elemanı, $a_0, a_1, \dots, a_{n-1} \in A$ olmak üzere

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$$

biçiminde bir polinom denklemini sağlar. $c \in F$ olduğundan, $r \in D$, $s \in D$, $s \neq 0$, $(r, s) = 1$ olmak üzere c 'yi $c = \frac{r}{s}$ biçiminde ifade edebiliriz. O zaman

$$r^n + a_{n-1}r^{n-1}s + \dots + a_1rs^{n-1} + a_0s^n = 0$$

olur. s elemanı D 'nin bir birimi değil ise s 'yi bölen bir p asal sayısı vardır. $r^n + a_{n-1}r^{n-1}s + \dots + a_1rs^{n-1} + a_0s^n = 0$ denkleminde $p \mid r^n$ elde edilir ve p asal olduğundan $p \mid r$ olur. Bu ise $(r, s) = 1$ olması ile çelişir. Dolayısıyla s bir birim olmak zorundadır ve $c = rs^{-1} \in D$ olur.

Teorem 2.8. $\mathbb{Q} \cap \Omega = \mathbb{Z}$ 'dir [1].

İspat. $\mathbb{Z}$ bir tek türlü çarpanlarına ayrılabilen bölge olduğundan, Teorem 2.7'de $D = \mathbb{Z}$ alınırsa $F = \mathbb{Q}$ olur. Böylece

$$c \in \mathbb{Q} \cap \Omega \Leftrightarrow c \in \mathbb{Z}$$

elde edilir. Dolayısıyla $\mathbb{Q} \cap \Omega = \mathbb{Z}$ 'dir.

Tanım 2.7. D bir tamlık bölgesi olsun. D 'nin kesir cismi F olsun. F 'nin D üzerinde tam olan bütün elemanlarının kümesi D 'nin kendisi ise, yani $D^F = D$ ise, D 'ye integralce kapalıdır veya tam kapalıdır denir [1].

Teorem 2.9. D bir tek türlü çarpanlarına ayrılabilir bölge olsun. Bu takdirde D tam kapalıdır [1].

İspat. D 'nin kesir cismi F olsun. Teorem 2.4'e göre $D^F = D$ olur. Yani D tam kapalıdır.

Örnek 2.9. $\mathbb{Z} + \mathbb{Z}\sqrt{-3}$ tam kapalı değildir. $\mathbb{Z} + \mathbb{Z}\sqrt{-3}$ 'ün kesir cismi $\mathbb{Q}(\sqrt{-3}) = \{x + y\sqrt{-3} \mid x, y \in \mathbb{Q}\}$ 'dir. $\alpha = \frac{1}{2}(1 + \sqrt{-3})$ olsun. $\alpha \in \mathbb{Q}(\sqrt{-3})$ 'dür fakat $\alpha \notin \mathbb{Z} + \mathbb{Z}\sqrt{-3}$ 'dir. Ayrıca α , $\mathbb{Z}$ üzerinde tamdır çünkü $\alpha^2 - \alpha + 1 = 0$ denklemini sağlar. Dolayısıyla α , $\mathbb{Z}$ üzerinde tamdır. Böylece $\mathbb{Z} + \mathbb{Z}\sqrt{-3}$ tam kapalı olmadığı görülür. Ayrıca Teorem 2.9'a göre $\mathbb{Z} + \mathbb{Z}\sqrt{-3}$ 'ün bir tek türlü çarpanlarına ayrılabilir bölge olmadığı da elde edilir. Buna örnek verelim. 4 elemanı $\mathbb{Z} + \mathbb{Z}\sqrt{-3}$ 'de 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ indirgenemez elemanlar olmak üzere

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

biçiminde, indirgenemez elemanların iki farklı çarpımı olarak yazılabilir. Çünkü burada 2 ne $1 + \sqrt{-3}$ ne de $1 - \sqrt{-3}$ ile ilgilidir.

Teorem 2.10. Her cebirsel sayı, a bir cebirsel tamsayı, b de sıfırdan farklı bir rasyonel tamsayı olmak üzere $\frac{a}{b}$ biçimindedir [1].

İspat. c bir cebirsel sayı olsun. Bu takdirde

$$c^n + a_{n-1}c^{n-1} + \dots + a_1c + a_0 = 0$$

olacak biçimde $a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}$ vardır. $a_0, a_1, \dots, a_{n-1}$ 'lerin paydalarının en küçük ortak katı b olsun. O halde $b \in \mathbb{Z}$ ve her $i = 0, 1, 2, \dots, n-1$ için $ba_i \in \mathbb{Z}$ olur. Böylece

$$(bc)^n + (ba_{n-1})(bc)^{n-1} + \dots + (b^{n-1}a_1)(bc) + (b^na_0) = 0$$

elde edilir. Bu ise bc 'nin $\mathbb{Z}$ 'deki bir monik polinomun kökü olduğunu gösterir. Dolayısıyla bc 'de bir cebirsel tamsayıdır. $bc = a$ olsun. Bu takdirde $c = \frac{a}{b}$ olur. a bir cebirsel tamsayı ve $b \in \mathbb{Z}$ 'dir.

$\mathbb{C}$ kompleks sayılar cisminin bir alt cismi K olsun. $\alpha \in \mathbb{C}$ elemanı K üzerinde cebirsel olsun. α , K 'da cebirsel olduğundan $g(\alpha) = 0$ olacak biçimde sıfır polinomu olmayan bir $g(x) \in K[x]$ polinomu vardır. $K[x]$ 'de α elemanını kök kabul eden bütün polinomların kümesi $I_K(\alpha)$ olsun. Yani

$$I_K(\alpha) = \{f(x) \in K[x] \mid f(\alpha) = 0\}$$

olsun. $I_K(\alpha)$ 'nın sıfır polinomunu içerdiği açıktır. Ayrıca $I_K(\alpha)$, $K[x]$ 'in bir idealidir ve $g(x) \in I_K(\alpha)$ olduğundan $I_K(\alpha) \neq \langle 0 \rangle$ olur. K bir cisim olduğundan Teorem 1.20'e göre $K[x]$ bir Öklid bölgesidir. Dolayısıyla Teorem 1.18'e göre $K[x]$ bir esas ideal bölgesidir. O zaman

$$I_K(\alpha) = \langle p(x) \rangle$$

olacak biçimde bir $p(x) \in K[x]$ polinomu vardır. Bu $p(x)$ polinomu tek türlü belirlidir. $p_1(x) \in K[x]$ polinomu $I_K(\alpha)$ 'yı üreten başka bir polinom ise

$$I_K(\alpha) = \langle p_1(x) \rangle$$

olur. Böylece $\langle p(x) \rangle = \langle p_1(x) \rangle$ elde edilir. O halde Teorem 1.3'e göre $u(x) \in K[x]$ bir birim olmak üzere

$$p_1(x) = u(x)p(x)$$

olur. Ayrıca Örnek 1.9'a göre

$$U(K[x]) = K^*$$

olduğundan

$$u(x) \in K^*$$

elde edilir. Böylece $p(x)$ polinomu monik polinom olarak kabul edilebilir. O zaman $I_K(\alpha) = \langle p(x) \rangle$ ifadesindeki $p(x)$ polinomu tek türlü belirli olur.

Tanım 2.8. $\mathbb{C}$ 'nin bir alt cismi K olsun. $\alpha \in \mathbb{C}$ elemanı K üzerinde cebirsel olsun. Bu takdirde

$$I_K(\alpha) = \langle p(x) \rangle$$

olacak biçimde tek türlü belirli monik bir $p(x) \in K[x]$ polinomu vardır. Bu $p(x)$ polinomuna α 'nın K 'daki minimal polinomu denir ve bu polinom $\text{ind}_K(\alpha)$ ile gösterilir [1].

Tanım 2.9. $\mathbb{C}$ 'nin bir alt cismi K olsun. $\alpha \in \mathbb{C}$ elemanı K üzerinde cebirsel olsun. Bu takdirde α 'nın K 'daki derecesi $\text{der}_K(\alpha)$ diye yazılır ve

$$\text{der}_K(\alpha) = \text{der}(\text{ind}_K(\alpha))$$

olarak tanımlanır. $K = \mathbb{Q}$ ise $\text{der}_{\mathbb{Q}}(\alpha)$ yerine $\text{der}(\alpha)$ yazılır [1].

Teorem 2.11. $\mathbb{C}$ 'nin bir alt cismi K olsun. $\alpha \in \mathbb{C}$ elemanı K üzerinde cebirsel olsun. Bu takdirde $\text{ind}_K(\alpha)$ elemanı $K[x]$ 'de indirgenemezdir [1].

Örnek 2.9. $\alpha = (1+i)/\sqrt{2} \in \mathbb{C}$ sayısı $x^4 + 1 \in \mathbb{Q}[x]$ polinomunun bir köküdür. $x^4 + 1$ polinomu monik ve $\mathbb{Q}[x]$ 'de indirgenemez olduğundan

$$\text{ind}_{\mathbb{Q}}\left(\frac{1+i}{\sqrt{2}}\right) = x^4 + 1 \text{ ve } \text{der}\left(\frac{1+i}{\sqrt{2}}\right) = 4$$

elde edilir.

Örnek 2.10. $K = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ cismi olsun. $\alpha = (1+i)/\sqrt{2} \in \mathbb{C}$ olsun. Bu takdirde α sayısı $x^2 - \sqrt{2}x + 1 \in K[x]$ polinomunun bir köküdür. $x^2 - \sqrt{2}x + 1$ polinomu monik ve $K[x]$ 'de indirgenemez olduğundan

$$\text{ind}_{\mathbb{Q}(\sqrt{2})}\left(\frac{1+i}{\sqrt{2}}\right) = x^2 - \sqrt{2}x + 1 \text{ ve } \text{der}_{\mathbb{Q}(\sqrt{2})}\left(\frac{1+i}{\sqrt{2}}\right) = 2$$

elde edilir.

Örnek 2.11. $K = \mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$ cismi olsun. $\alpha = (1+i)/\sqrt{2} \in \mathbb{C}$ olsun. Bu takdirde α sayısı $x^2 - \sqrt{-1} \in \mathbb{Q}(\sqrt{-1})[x]$ polinomunun bir köküdür. $x^2 - \sqrt{-1}$ polinomunun iki kökü $\pm(1+i)/\sqrt{2} \notin \mathbb{Q}(\sqrt{-1})$ olduğundan $x^2 - \sqrt{-1}$ polinomu $\mathbb{Q}(\sqrt{-1})[x]$ 'de indirgenemezdir. O halde

$$\text{ind}_{\mathbb{Q}(\sqrt{-1})}\left(\frac{1+i}{\sqrt{2}}\right) = x^2 - \sqrt{-1} \text{ ve } \text{der}_{\mathbb{Q}(\sqrt{-1})}\left(\frac{1+i}{\sqrt{2}}\right) = 2$$

elde edilir.

Örnek 2.12. $K = \mathbb{Q}(\sqrt{-2}) = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Q}\}$ cismi olsun.

$\alpha = (1+i)/\sqrt{2} \in \mathbb{C}$ olsun. . Bu takdirde α sayısı $x^2 - \sqrt{-2}x - 1 \in \mathbb{Q}(\sqrt{-2})[x]$ polinomunun bir köküdür. $x^2 - \sqrt{-2}x - 1$ polinomunun iki kökü $(\sqrt{-2} \pm \sqrt{2})/2 \notin \mathbb{Q}(\sqrt{-2})$ olduğundan $x^2 - \sqrt{-2}x - 1$ polinomu $\mathbb{Q}(\sqrt{-2})[x]$ 'de indirgenemezdir. O halde

$$\text{ind}_{\mathbb{Q}(\sqrt{-2})}\left(\frac{1+i}{\sqrt{2}}\right) = x^2 - \sqrt{-2}x - 1 \text{ ve } \text{der}_{\mathbb{Q}(\sqrt{-2})}\left(\frac{1+i}{\sqrt{2}}\right) = 2$$

elde edilir.

Tanım 2.10. $\alpha \in \mathbb{C}$ sayısı $\mathbb{C}$ 'nin bir K alt cismi üzerinde cebirsel olsun. α 'nın K 'daki eşlenikleri, $\text{ind}_K(\alpha)$ 'nın $\mathbb{C}$ 'deki kökleridir [1].

Örnek 2.13. Örnek 2.8'e göre $\text{ind}_{\mathbb{Q}}((1+i)/\sqrt{2}) = x^4 + 1$ idi.

$$x^4 + 1 = \left(x - \left(\frac{1+i}{\sqrt{2}}\right)\right) \left(x - \left(\frac{1-i}{\sqrt{2}}\right)\right) \left(x - \left(\frac{-1+i}{\sqrt{2}}\right)\right) \left(x - \left(\frac{-1-i}{\sqrt{2}}\right)\right)$$

olduğundan $(1+i)/\sqrt{2}$ 'nin $\mathbb{Q}$ 'daki eşlenikleri

$$\frac{1+i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}}, \frac{-1+i}{\sqrt{2}}, \frac{-1-i}{\sqrt{2}}$$

dir.

Örnek 2.14. Örnek 2.9'e göre $\text{ind}_{\mathbb{Q}(\sqrt{2})}((1+i)/\sqrt{2}) = x^2 - \sqrt{2}x + 1$ idi.

$$x^2 - \sqrt{2}x + 1 = \left(x - \left(\frac{1+i}{\sqrt{2}}\right)\right) \left(x - \left(\frac{1-i}{\sqrt{2}}\right)\right)$$

olduğundan $(1+i)/\sqrt{2}$ 'nin $\mathbb{Q}(\sqrt{2})$ 'daki eşlenikleri

$$\frac{1+i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}}$$

dir.

Teorem 2.12. $\mathbb{C}$ 'nin bir alt cismi K olsun. $\alpha \in \mathbb{C}$ sayısı K üzerinde cebirsel olsun. Bu takdirde α 'nın K 'daki eşlenikleri birbirlerinden farklıdır [1].

Teorem 2.13. α bir cebirsel tamsayı ise α 'nın $\mathbb{Q}$ 'daki eşlenikleri de birer cebirsel tamsayıdır [1].

Örnek 2.15. $\alpha = \sqrt[3]{2} - \sqrt[3]{4}$ olsun. O zaman

$$\alpha^3 = 2 - 6\sqrt[3]{2} + 6\sqrt[3]{4} - 4 = -2 - 6(\sqrt[3]{2} - \sqrt[3]{4}) = -2 - 6\alpha$$

olur. Yani α sayısı $x^3 + 6x + 2 \in \mathbb{Z}[x]$ monik kübik polinomunun bir köküdür.

Dolayısıyla α bir cebirsel tamsayıdır. $x^3 + 6x + 2$ polinomu Eisenstein indirgenemezlik kriterine göre $\mathbb{Z}[x]$ 'de indirgenemezdir. Dolayısıyla

$$\text{ind}_{\mathbb{Q}}(\alpha) = x^3 + 6x + 2$$

olur. $\text{ind}_{\mathbb{Q}}(\alpha)$ 'nın diğer iki kökü ise, w birim elemanın bir kompleks küp kökü olmak üzere

$$\alpha' = w\sqrt[3]{2} - w^2\sqrt[3]{4}, \alpha'' = w^2\sqrt[3]{2} - w\sqrt[3]{4}$$

dir. Dolayısıyla α' ve α'' de birer cebirsel tamsayıdır.

Teorem 2.14. α bir cebirsel tamsayı ise $\text{ind}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$ 'dir [1].

Tanım 2.11. $\mathbb{Q}[x]$ 'de indirgenemez olan bir kuadratik $x^2 + ax + b \in \mathbb{Q}[x]$ polinomunun bir $\alpha \in \mathbb{C}$ kökünü $\mathbb{Q}$ 'ya ekleyerek elde edilen $\mathbb{Q}(\alpha)$ cismindeki cebirsel tamsayıları belirleyelim. Burada $\mathbb{Q}(\alpha)$, $\mathbb{C}$ 'nin hem $\mathbb{Q}$ 'yu hem de α 'yı içeren en küçük alt cisimidir. Ayrıca $x^2 + ax + b$ polinomu $\mathbb{Q}[x]$ 'de indirgenemez olduğundan $\alpha \notin \mathbb{Q}$ 'dur. Açıkça görülür ki,

$$\mathbb{Q}(\alpha) = \left\{ \frac{a_0 + a_1\alpha + \dots + a_m\alpha^m}{b_0 + b_1\alpha + \dots + b_n\alpha^n} \mid \begin{array}{l} m, n \in \mathbb{Z}^+ \cup \{0\}, a_0, a_1, \dots, a_m, b_0, b_1, \dots, b_n \in \mathbb{Q} \\ b_0 + b_1\alpha + \dots + b_n\alpha^n \neq 0 \end{array} \right\}$$

dir. $\alpha^2 = -b - a\alpha$ olduğundan $c_k, d_k \in \mathbb{Q}$ olmak üzere $\alpha^k = c_k + d_k\alpha$ ($k = 2, 3, \dots$) elde edilir. Dolayısıyla

$$\mathbb{Q}(\alpha) = \left\{ \frac{e_0 + e_1\alpha}{f_0 + f_1\alpha} \mid e_0, e_1, f_0, f_1 \in \mathbb{Q}, (f_0, f_1) \neq (0, 0) \right\}$$

dır. $(f_0, f_1) \neq (0, 0)$ olduğundan $f_0^2 - af_0f_1 + bf_1^2 \neq 0$ 'dır ve

$$\frac{e_0 + e_1\alpha}{f_0 + f_1\alpha} = \left(\frac{e_0f_0 - ae_0f_1 + be_1f_1}{f_0^2 - af_0f_1 + bf_1^2} \right) + \left(\frac{e_1f_0 - e_0f_1}{f_0^2 - af_0f_1 + bf_1^2} \right) \alpha$$

olur. Böylece $\alpha^2 + a\alpha + b = 0$ olmak üzere

$$\mathbb{Q}(\alpha) = \{x + y\alpha \mid x, y \in \mathbb{Q}\}$$

elde edilir. $\mathbb{Q}(\alpha)$ cisminde bir kuadratik cisim veya $\mathbb{Q}$ 'nun bir kuadratik genişlemesi veya ikinci dereceden genişlemesi denir.

Teorem 2.15. K bir kuadratik cisim olsun. Bu takdirde $K = \mathbb{Q}(\sqrt{m})$ olacak biçimde tek türlü belirli bir karesiz m tamsayısı vardır [1].

Teorem 2.16. K bir kuadratik cisim olsun. $K = \mathbb{Q}(\sqrt{m})$ olacak biçimde tek türlü belirli karesiz tamsayı m olsun. Bu takdirde K ’daki cebirsel tamsayıların kümesi O_K ;

$$O_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m} & , \quad m \equiv 2,3 \pmod{4} \text{ ise} \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) & , \quad m \equiv 1 \pmod{4} \text{ ise} \end{cases}$$

ile verilir [1].

Tanım 2.12. m karesiz bir tamsayı olmak üzere $K = \mathbb{Q}(\sqrt{m})$ kuadratik cismine, $K \subseteq \mathbb{R}$ ise reel kuadratik cisim, $K \not\subseteq \mathbb{R}$ ise sanal kuadratik cisim denir. Yani $m > 0$ ise K reeldir, $m < 0$ ise K sanaldır [1].

Teorem 2.17. K bir sanal kuadratik cisim olsun. Bu takdirde, w birim elemanın bir kompleks küp kökü olmak üzere

$$U(O_K) = \begin{cases} \{\pm 1, \pm i\} \simeq \mathbb{Z}_4 & , \quad K = \mathbb{Q}(\sqrt{-1}) \text{ ise} \\ \{\pm 1, \pm w, \pm w^2\} \simeq \mathbb{Z}_6 & , \quad K = \mathbb{Q}(\sqrt{-3}) \text{ ise} \\ \{\pm 1\} \simeq \mathbb{Z}_2 & , \quad \text{diğer durumlar} \end{cases}$$

dir [1].

Tanım 2.13. $\mathbb{C}$ ’nin bir alt cismi K ve $\alpha \in \mathbb{C}$ olsun. $\mathbb{C}$ ’nin hem K ’yı hem de α yı içeren bütün F alt cisimlerinin arakesiti $K(\alpha)$ olsun. Yani

$$K(\alpha) = \bigcap_{\substack{F \\ \alpha \in F \\ K \subseteq F \subseteq \mathbb{C}}} F$$

olsun. Bu kesişim boştan farklıdır. Çünkü $\mathbb{C}$ kompleks sayılar kümesi zaten hem K yı hem de α 'yı içeren böyle bir cisimdir. $\mathbb{C}$ 'nin alt cisimlerinin kesişimi yine $\mathbb{C}$ 'nin bir alt cismi olacağından, $K(\alpha)$ kesişim cismi, hem K 'yı hem de α 'yı içeren en küçük cisimdir. $K(\alpha)$ 'nın K 'ya tek bir α elemanının eklenmesi ile elde edildiğini söylemiştik. Şimdi L , $\mathbb{C}$ 'nin bir alt cismi olsun. $L = K(\alpha)$ olacak biçimde bir $\alpha \in \mathbb{C}$ varsa, L 'ye K 'nın bir basit genişlemesi denir. Açıkça görülür ki, $\alpha \in K$ ise $K(\alpha) = K$ olur. $K \subseteq \mathbb{C}$ ve $\alpha \in \mathbb{C}$ için

$$L = \left\{ \frac{b_0 + b_1\alpha + \dots + b_k\alpha^k}{c_0 + c_1\alpha + \dots + c_h\alpha^h} \mid \begin{array}{l} k, h \in \mathbb{N} \cup \{0\}, b_0, b_1, \dots, b_k, c_0, c_1, \dots, c_h \in K \\ c_0 + c_1\alpha + \dots + c_h\alpha^h \neq 0 \end{array} \right\}$$

olsun. Bu takdirde L kümesi, $\mathbb{C}$ 'nin hem K 'yı hem de α 'yı içeren bir alt cismidir. Ayrıca $\mathbb{C}$ 'nin hem K 'yı hem de α 'yı içeren her alt cismi L 'nin bütün elemanlarını içermek zorundadır. Dolayısıyla L , $\mathbb{C}$ 'nin hem K 'yı hem de α 'yı içeren en küçük alt cismidir. Yani $L = K(\alpha)$ 'dır [1].

$\alpha \in \mathbb{C}$ sayısı K 'da cebirsel ve α 'nın K 'daki minimal polinomunun derecesi n olsun. Yukarıdaki tanıma göre, $K(\alpha)$ 'nın her β elemanı

$$f(x) = b_0 + b_1x + \dots + b_kx^k \in K[x], g(x) = c_0 + c_1x + \dots + c_hx^h \in K[x], g(\alpha) \neq 0$$

olmak üzere

$$\beta = \frac{f(x)}{g(x)}$$

biçimindedir. Bu ise $\text{ind}_K(\alpha) \nmid g(x)$ demektir ve $\text{ind}_K(\alpha)$, $K[x]$ 'de indirgenemez olduğundan

$$\langle \text{ind}_K(\alpha), g(x) \rangle = K[x]$$

olur. Dolayısıyla Teorem 1.15'den dolayı

$$m(x)\text{ind}_K(\alpha) + n(x)g(x) = 1$$

olacak biçimde $m(x), n(x) \in K[x]$ polinomları vardır. α sayısı $\text{irr}_K(\alpha)$ 'nın bir kökü olduğundan

$$n(\alpha)g(\alpha) = 1$$

elde edilir. Buradan

$$\frac{1}{g(\alpha)} = n(\alpha)$$

olur. Dolayısıyla

$$\beta = \frac{f(\alpha)}{g(\alpha)} = f(\alpha)n(\alpha)$$

olduğu görülür. Dolayısıyla, $K(\alpha)$ 'nın her β elemanı, α 'nın K 'dan katsayılı bir polinomu olarak ifade edilebilir. Yani l negatif olmayan bir tamsayı ve $d_0, d_1, \dots, d_l \in K$ olmak üzere

$$\beta = d_0 + d_1\alpha + \dots + d_l\alpha^l$$

biçimindedir.

$$h(x) = d_0 + d_1x + \dots + d_lx^l \in K[x]$$

olsun. O zaman $\beta = h(\alpha)$ olur. K bir cisim olduğundan $h(x)$ 'i $\text{ind}_K(\alpha)$ 'ya bölebiliriz. Böylece $u(x) \in K[x]$, $v(x) \in K[x]$ polinomlar olmak üzere

$$h(x) = u(x)\text{ind}_K(\alpha) + v(x), \deg(v(x)) < \deg(\text{ind}_K(\alpha)) = n$$

olarak yazılabilir. $\text{ind}_K(\alpha)$ 'nın bir kökü α olduğundan

$$h(\alpha) = v(\alpha)$$

dolayısıyla

$$\beta = v(\alpha)$$

elde edilir. Sonuç olarak $K(\alpha)$ 'nın her elemanı, $a_0, a_1, \dots, a_{n-1} \in K$ ve $n = \text{der}(\text{ind}_K(\alpha))$ olmak üzere

$$a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$$

biçimindedir. Böylece aşağıdaki teoremin ispatı verilmiş olur.

Teorem 2.18. $\mathbb{C}$ 'nin bir alt cismi K olsun. $\alpha \in \mathbb{C}$ sayısı K 'da cebirsel olsun. $n = \text{der}(\text{ind}_K(\alpha))$ olsun. Bu takdirde

$$K(\alpha) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in K\}$$

dir [1].

Teorem 2.19. $\mathbb{C}$ 'nin bir alt cismi K olsun. $\alpha \in \mathbb{C}$ sayısı K 'da cebirsel olsun ve α nın derecesi $\text{der}_K(\alpha) = \text{der}(\text{ind}_K(\alpha)) = n$ olsun. $K(\alpha)$ genişlemesinin K üzerinde derecesi $[K(\alpha):K]$ olarak yazılır ve

$$[K(\alpha):K] = n$$

olarak tanımlanır [1].

Örnek 2.16. m karesiz bir tamsayı olsun. Bu takdirde $\sqrt{m} \in \mathbb{C}$ sayısı $x^2 - m \in \mathbb{Q}[x]$ polinomunun bir köküdür. m karesiz olduğundan $\pm\sqrt{m} \notin \mathbb{Q}$ 'dur.

Böylece $x^2 - m = (x + \sqrt{m})(x - \sqrt{m})$ olduğundan $x^2 - m$ polinomu $\mathbb{Q}[x]$ 'de indirgenemezdir. Dolayısıyla

$$\text{ind}_{\mathbb{Q}}(\sqrt{m}) = x^2 - m$$

olur. Teorem 2.18'e göre

$$\mathbb{Q}(\sqrt{m}) = \{a_0 + a_1\sqrt{m} \mid a_0, a_1 \in \mathbb{Q}\}$$

olur. Buradan

$$[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$$

elde edilir. Yani $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}$ 'nin bir kuadratik genişlemesidir.

Örnek 2.17. $\alpha = (5 + \sqrt{17})^{1/3} + (5 - \sqrt{17})^{1/3} \in \mathbb{R}$ olsun. Bu takdirde

$$\begin{aligned} \alpha^3 &= (5 + \sqrt{17}) + 3(5 + \sqrt{17})^{2/3}(5 - \sqrt{17})^{1/3} + 3(5 + \sqrt{17})^{1/3}(5 - \sqrt{17})^{2/3} + (5 - \sqrt{17}) \\ &= 10 + 3(5 + \sqrt{17})^{1/3}(5 - \sqrt{17})^{1/3} \left[(5 + \sqrt{17})^{1/3} + (5 - \sqrt{17})^{1/3} \right] \\ &= 10 + 3 \left[(5 + \sqrt{17})(5 - \sqrt{17}) \right]^{1/3} \alpha \\ &= 10 + 3 \cdot 8^{1/3} \alpha \\ &= 10 + 6\alpha \end{aligned}$$

olur. Yani α sayısı $x^3 - 6x - 10 \in \mathbb{Z}[x]$ monik polinomunun bir köküdür. Dolayısıyla α sayısı bir cebirsel tamsayıdır. Ayrıca $x^3 - 6x - 10$ polinomu Eisenstein indirgenemezlik kriterine göre indirgenemezdir. O zaman

$$\text{ind}_{\mathbb{Q}}(\alpha) = x^3 - 6x - 10$$

olur. Dolayısıyla Teorem 2.18'den dolayı

$$\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$$

ve

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

elde edilir. Yani $\mathbb{Q}(\alpha)$, $\mathbb{Q}$ 'nin bir kübik genişlemesidir.

Tanım 2.14. $\mathbb{C}$ 'nin bir alt cismi olan K 'ya, sonlu sayıda $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{C}$ ($k \geq 2$) elemanını eklemeye elde edilen cismi $K(\alpha_1, \alpha_2, \dots, \alpha_k)$ ile göstereceğiz. $K(\alpha_1, \alpha_2, \dots, \alpha_k)$ cismi, $\mathbb{C}$ 'nin hem K 'yı hem de α_i 'leri içeren en küçük alt cismidir. Yani $K(\alpha_1, \alpha_2, \dots, \alpha_k)$ cismi, $\mathbb{C}$ 'nin hem K 'yı hem de α_i 'leri içeren bütün alt cisimlerinin arakesitidir. $K(\alpha_1, \alpha_2, \dots, \alpha_k)$ cisminde K 'nın bir çoklu genişlemesi denir. $\alpha_1, \alpha_2, \dots, \alpha_k$ 'ların sırasının bir önemi olmadığı aşıkardır. $K(\alpha_1, \alpha_2, \dots, \alpha_k)$ cismi, peşpeşe k tane tekli ekleme olarak da kabul edilebilir. Yani

$$\begin{aligned} K(\alpha_1, \alpha_2) &= K(\alpha_1)(\alpha_2) \\ K(\alpha_1, \alpha_2, \alpha_3) &= K(\alpha_1, \alpha_2)(\alpha_3) \\ &\vdots \\ K(\alpha_1, \alpha_2, \dots, \alpha_k) &= K(\alpha_1, \alpha_2, \dots, \alpha_{k-1})(\alpha_k) \end{aligned}$$

olarak görülebilir [1].

Teorem 2.20. $\mathbb{C}$ 'nin bir alt cismi K olsun. $\alpha \in \mathbb{C}$ ve $\beta \in \mathbb{C}$ elemanları K 'da cebirsel olsun. Bu takdirde

$$K(\alpha, \beta) = K(\gamma)$$

olacak biçimde K 'da cebirsel olan bir $\gamma \in \mathbb{C}$ elemanı vardır [1].

İspat. $p(x) = \text{ind}_K(\alpha)$ ve $q(x) = \text{ind}_K(\beta)$ olsun. O zaman $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m$ 'ler α 'nın K 'daki eşlenikleri ve $\beta_1 = \beta, \beta_2, \dots, \beta_n$ 'ler β 'nın K 'daki eşlenikleri olmak üzere

$$p(x) = (x - \alpha_1) \dots (x - \alpha_m) \in K[x], \quad q(x) = (x - \beta_1) \dots (x - \beta_n) \in K[x]$$

dir. Teorem 2.12'ye göre tüm α_i 'lerin ($i=1,2,\dots,m$) farklı olduğunu ve β_j 'lerin ($j=1,2,\dots,n$) farklı olduğunu biliyoruz.

$$S = \left\{ \frac{\alpha_r - \alpha_s}{\beta_t - \alpha_u} \mid r, s = 1, 2, \dots, m; t, u = 1, 2, \dots, n; t \neq u \right\}$$

olsun. S kümesi sonlu sayıda kompleks sayıdan oluşur. S 'nin tüm elemanlarından farklı olan bir c sayısı seçelim. Böylece c 'nin seçilimi ile birlikte mn tane

$$\alpha_i + c\beta_j \quad (i=1,2,\dots,m; j=1,2,\dots,n)$$

elemanlarının hepsi de farklı olur. $\gamma = \alpha_1 + c\beta_1 = \alpha + c\beta$ ve $K_1 = K(\gamma)$ olsun.

Ayrıca

$$p_1(x) = p(\gamma - cx) \in K_1[x]$$

olsun. O zaman

$$p_1(\beta) = p(\gamma - c\beta) = p(\alpha) = 0$$

bulunur. $q(\beta) = 0$ olduğundan β sayısının hem $p_1(x)$ 'in hem de $q(x)$ 'in bir ortak kökü olduğu görülür. Şimdi $p_1(x)$ ve $q(x)$ 'in başka ortak kökü olmadığını gösterelim. $\lambda \in \mathbb{C}$ elemanı $\lambda \neq \beta$ olmak üzere $p_1(x)$ ve $q(x)$ 'in bir ortak kökü olsun. λ elemanı $q(x)$ 'in $\beta = \beta_1$ 'den farklı bir kökü olduğu için $\lambda = \beta_j$ olacak biçimde bir $j \in \{2, 3, \dots, n\}$ vardır. O zaman $p(\gamma - c\beta_j) = p_1(\beta_j) = 0$ olur. O halde $\gamma - c\beta_j$ elemanı $p(x)$ 'in bir köküdür. Dolayısıyla $\gamma - c\beta_j$ elemanı $\alpha_1, \alpha_2, \dots, \alpha_m$ lerden birine eşit olmalıdır, bu α_k ($k \in \{1, 2, \dots, m\}$) olsun. O halde

$$\alpha_k + c\beta_j = \gamma = \alpha_1 + c\beta_1$$

elde edilir. Buradan

$$c = \frac{\alpha_1 - \alpha_k}{\beta_j - \beta_1}$$

olur ki bu c 'nin seçimi ile çelişir. Dolayısıyla $p_1(x)$ ve $q(x)$ 'in β 'dan başka ortak kökü yoktur. Şimdi $h(x) = \text{irr}_{K_1}(\beta)$ olsun. O zaman $h(x) \mid p_1(x)$ ve $h(x) \mid q(x)$ bulunur. $p_1(x)$ ve $q(x)$ 'in $\mathbb{C}$ 'de sadece bir tane ortak kökü olduğundan $\deg h(x) = 1$ olur. Dolayısıyla bir $\delta \in K_1$ elemanı için $h(x) = x + \delta$ olur. Ayrıca $0 = h(\beta) = \beta + \delta$ olduğundan $\beta = -\delta \in K_1$ elde edilir. Böylece

$$K(\alpha, \beta) \subseteq K_1 = K(\gamma)$$

olduğu gösterilmiş olur. Ayrıca $\gamma = \alpha + c\beta \in K(\alpha, \beta)$ olduğundan

$$K(\gamma) \subseteq K(\alpha, \beta)$$

elde edilir. Dolayısıyla

$$K(\alpha, \beta) = K(\gamma)$$

olur.

Teorem 2.21. $\mathbb{C}$ 'nin bir alt cismi K olsun. $\alpha_1, \alpha_2, \dots, \alpha_n$ 'ler K 'da cebirsel olsun. Bu takdirde

$$K(\alpha_1, \alpha_2, \dots, \alpha_n) = K(\alpha)$$

olacak biçimde K 'da cebirsel olan bir $\alpha \in \mathbb{C}$ elemanı vardır [1].

Eğer K , $\mathbb{C}$ 'nin bir alt cismi ve $\alpha \in \mathbb{C}$, $\beta \in \mathbb{C}$ elemanları K 'da cebirsel ise $K(\alpha, \beta) = K(\gamma)$ olacak biçimdeki K 'da cebirsel olan $\gamma \in \mathbb{C}$ elemanının nasıl bulunacağı Teorem 2.20'nin ispatından elde edilir. Tek yapılması gereken, α_i 'ler α nın eşleniklerini, β_i 'ler de β 'nin eşleniklerini tarar iken $\alpha_i + c\beta_i$ 'lerin hepsini de birbirinden farklı yapacak bir c rasyonel sayısı bulmak. Böylece $K(\alpha, \beta) = K(\alpha + c\beta)$ olur.

Örnek 2.18. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ cismini basit bir genişleme olarak gösterelim. $\sqrt{2}$ 'nin $\mathbb{Q}$ 'daki eşlenikleri $\sqrt{2}$ ve $-\sqrt{2}$ 'dir. $\sqrt{3}$ 'ün $\mathbb{Q}$ 'daki eşlenikleri $\sqrt{3}$ ve $-\sqrt{3}$ 'tür. Teorem 2.20'nin ispatındaki $c=1$ alınır; $\sqrt{2} + \sqrt{3}$, $\sqrt{2} - \sqrt{3}$, $-\sqrt{2} + \sqrt{3}$ ve $-\sqrt{2} - \sqrt{3}$ elemanlarının hepside birbirinden farklıdır. Böylece Teorem 2.20'ye göre $\mathbb{Q}(-\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ elde edilir. Şimdi $\sqrt{2} + \sqrt{3}$ 'ün bir cebirsel tamsayı olduğunu gösterelim. $\alpha = \sqrt{2} + \sqrt{3}$ olsun. Buradan,

$$\alpha^2 = 5 + 2\sqrt{6}$$

$$\alpha^2 - 5 = 2\sqrt{6}$$

$$\alpha^4 - 10\alpha^2 + 25 = 24$$

elde edilir. Dolayısıyla α sayısı

$$f(x) = x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$$

monik kuartik polinomunun bir köküdür. O halde α bir cebirsel tamsayıdır. Son olarak $f(x)$ polinomunun $\mathbb{Z}[x]$ 'de indirgenemez olduğunu gösterelim.

$f(\pm 1) = -8 \neq 0$ olduğundan $f(x)$ 'in $\mathbb{Z}[x]$ 'de hiç lineer çarpanı yoktur.

Dolayısıyla $f(x)$ 'in $\mathbb{Z}[x]$ 'de çarpanlara ayrılışı, eğer varsa, $\mathbb{Z}[x]$ 'deki iki kuadratik polinomun çarpımı biçiminde olmalıdır. O zaman $a, b, c, d \in \mathbb{Z}$ olmak üzere

$$x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

biçiminde çarpanlarına ayrılsın. Katsayıları eşitlesek;

$$a + c = 0, b + ac + d = -10, bc + ad = 0 \text{ ve } bd = 1$$

elde edilir. İlk ifadeden $c = -a$, son ifadeden de $b = d = \pm 1$ 'dir. Yani $b + d = \pm 2$ elde edilir. O zaman ikinci ifade $a^2 = 8$ veya $a^2 = 12$ olur ki bu ise tamsayılarda mümkün değildir. Dolayısıyla $f(x)$ polinomu $\mathbb{Z}[x]$ 'de dolayısıyla da $\mathbb{Q}[x]$ 'de indirgenemezdir. Sonuç olarak

$$\text{ind}_{\mathbb{Q}}(\sqrt{2} + \sqrt{3}) = x^4 - 10x^2 + 1$$

ve

$$\left[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q} \right] = \left[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q} \right] = 4$$

olduğu görülür.

Teorem 2.22. $\mathbb{C}$ 'nin bir alt cismi K olsun. $\alpha \in \mathbb{C}$ sayısı K 'da cebirsel olsun. Bu takdirde $K(\alpha)$ 'nın her β elemanı K 'da cebirseldir. Ayrıca β 'nin K 'daki derecesi, α 'nın K 'daki derecesinden küçük veya eşittir. Yani $\text{der}_K(\beta) \leq \text{der}_K(\alpha)$ dır [1].

Tanım 2.15. $\mathbb{Q}$ rasyonel sayılar cismine, $\alpha_1, \alpha_2, \dots, \alpha_n$ 'ler cebirsel sayılarının eklenmesiyle oluşturulan $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n)$ biçimindeki $\mathbb{C}$ 'nin alt cismine bir cebirsel sayı cismi denir [1].

Teorem 2.23. K bir cebirsel sayı cismi ise $K = \mathbb{Q}(\theta)$ olacak biçimde bir θ cebirsel sayısı vardır [1].

İspat. Teorem 2.18'de $K = \mathbb{Q}$ alınırsa istenilen elde edilir.

Teorem 2.24. K bir cebirsel sayı cismi ise $K = \mathbb{Q}(\theta)$ olacak biçimde bir θ cebirsel tamsayısı vardır [1].

İspat. K bir cebirsel sayı cismi olsun. Teorem 2.23'e göre $K = \mathbb{Q}(\phi)$ olacak biçimde bir ϕ cebirsel sayısı vardır. Teorem 2.10'a göre, θ bir cebirsel tamsayı ve b

de sıfırdan farklı bir rasyonel tamsayı olmak üzere $\phi = \frac{\theta}{b}$ biçiminde yazılabilir.

Böylece

$$K = \mathbb{Q}(\phi) = \mathbb{Q}\left(\frac{\theta}{b}\right) = \mathbb{Q}(\theta)$$

olur.

Teorem 2.25. K bir cebirsel sayı cismi olsun. θ bir cebirsel sayı olmak üzere $K = \mathbb{Q}(\theta)$ olsun. $\text{ind}_{\mathbb{Q}}(\theta) = n$ olsun. Bu takdirde K 'nin her elemanı $c_0, c_1, \dots, c_{n-1} \in \mathbb{Q}$ olmak üzere

$$c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1}$$

biçiminde tek türlü olarak ifade edilebilir. Ayrıca $c_0, c_1, \dots, c_{n-1} \in \mathbb{Q}$ olmak üzere $c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1}$ biçimindeki her ifade K 'nin bir elemanıdır [1].

İspat. Teorem 2.18'de $K = \mathbb{Q}$ alınırsa istenilen elde edilir.

Tanım 2.16. K cebirsel sayı cisminde bulunan bütün cebirsel tamsayıların kümesi O_K ile gösterilir. Yani $O_K = \Omega \cap K$ dır [1].

Teorem 2.26. K bir cebirsel sayı cismi olsun. Bu takdirde O_K bir tamlık bölgesidir[1].

İspat. Sonuç 2.2'den dolayı Ω 'nın bir tamlık bölgesi olduğu bilinmektedir ve $\Omega \subseteq \mathbb{C}$ 'dir. Ayrıca K bir cisim ve $K \subseteq \mathbb{C}$ 'dir. O halde $O_K = \Omega \cap K$ bir tamlık bölgesidir.

Tanım 2.17. O_K 'ya K cebirsel sayı cisminin tamsayılar halkası denir [1].

Teorem 2.27. K bir cebirsel sayı cismi olsun. Bu takdirde O_K 'nın kesir cismi K olur[1].

İspat. O_K 'nın kesir cismi F ve $\alpha \in F$ olsun. O zaman $b \in O_K$, $c \in O_K$, $c \neq 0$ olmak üzere $\alpha = \frac{b}{c}$ biçimindedir. $O_K \subseteq K$ olduğundan $b \in K$, $c \in K$ 'dır. K bir cisim olduğundan $\alpha = \frac{b}{c} \in K$ olur. O halde $F \subseteq K$ elde edilir.

Şimdi $\alpha \in K$ olsun. Teorem 2.10'a göre, b bir cebirsel tamsayı ve c 'de sıfırdan farklı bir rasyonel sayı olmak üzere $\alpha = \frac{b}{c}$ biçimindedir. $b = \alpha c \in K$ olduğu açıktır.

Böylece $b \in O_K$ olur. Dolayısıyla $\alpha = \frac{b}{c} \in F$ 'dir. O halde $K \subseteq F$ elde edilir. Sonuç olarak $K = F$ olduğu görülür. Yani O_K 'nın kesir cismi K 'dır.

Teorem 2.28. K bir cebirsel sayı cismi olsun. Bu takdirde O_K tam kapalıdır [1].

İspat. Teorem 2.27'ye göre O_K 'nın kesir cismi K 'dır. $\beta \in K$ elemanı O_K üzerinde tam olsun. $\beta \in O_K$ olduğunu gösterelim. O_K , $\mathbb{Z}$ üzerinde tam olduğundan, Teorem 2.4'e göre, β elemanı $\mathbb{Z}$ üzerinde tamdır. Yani β elemanı K 'da bir cebirsel tamsayıdır. O zaman $\beta \in O_K$ olur. O halde O_K tam kapalıdır.

Teorem 2.29. K bir cebirsel sayı cismi olsun. Bu takdirde O_K 'nın sıfırdan farklı her ideali sıfırdan farklı bir rasyonel tamsayı içerir [1].

İspat. $I \neq \{0\}$, O_K 'nin bir ideali olsun. $\alpha \in I, \alpha \neq 0$ seçelim. $\alpha \in I \subseteq O_K$ olduğundan α bir cebirsel tamsayıdır. $\text{ind}_{\mathbb{Q}}(\alpha) = x^n + b_1x^{n-1} + \dots + b_n$ olsun. $b_n \neq 0$ olduğunu gösterelim. $n=1$ ise $\text{ind}_{\mathbb{Q}}(\alpha) = x + b_1$ olur. Yani $\alpha + b_1 = 0$ elde edilir. Dolayısıyla $b_1 = -\alpha \neq 0$ 'dır. $n \geq 2$ ise Teorem 2.11'e göre $\text{irr}_{\mathbb{Q}}(\alpha)$ polinomu $\mathbb{Q}[x]$ de indirgenemez olduğundan $b_n \neq 0$ 'dir. α bir cebirsel tamsayı olduğundan Teorem 2.14'e göre $\text{ind}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$ 'dir. O zaman $b_1, b_2, \dots, b_n \in \mathbb{Z}$ olur. Dolayısıyla

$$b_n = -\alpha^n - b_1\alpha^{n-1} - \dots - b_{n-1}\alpha \in I$$

elde edilir. Yani b_n sıfırdan farklı bir rasyonel tamsayıdır ve I 'nin bir elemanıdır.

Teorem 2.30. K bir cebirsel sayı cismi olsun. I , O_K 'nin sıfırdan farklı bir ideali olsun. Bu takdirde $K = \mathbb{Q}(\gamma)$ olacak biçimde bir $\gamma \in I$ vardır [1].

İspat. Teorem 2.2'ye göre $K = \mathbb{Q}(\theta)$ olacak biçimde bir $\theta \in O_K$ vardır. Teorem 2.7'ye göre bir $c \in \mathbb{Z} \cap I$, $c \neq 0$ rasyonel tamsayısı vardır. $\gamma = c\theta$ olsun. $\theta \in O_K$ ve $c \in I$ olduğundan $\gamma \in I$ olur. Ayrıca $c \in \mathbb{Z} - \{0\}$ olduğundan $K = \mathbb{Q}(\theta) = \mathbb{Q}(c\gamma) = \mathbb{Q}(\gamma)$ elde edilir. Yani $K = \mathbb{Q}(\gamma)$ olan bir $\gamma \in I$ vardır.

Teorem 2.31. K bir cebirsel sayı cismi ve K 'nin $\mathbb{Q}$ 'daki derecesi n olsun. Bu takdirde tam olarak n tane farklı $\sigma_k : K \rightarrow \mathbb{C}$ ($k=1, 2, \dots, n$) monomorfizması (birebir homomorfizması) vardır [1].

İspat. Teorem 2.23'e göre $K = \mathbb{Q}(\theta)$ olacak biçimde bir θ cebirsel sayısı vardır. $p(x) = \text{ind}_{\mathbb{Q}}(\theta)$ olsun. Bu takdirde

$$\deg p(x) = \deg(\text{ind}_{\mathbb{Q}}(\theta)) = [\mathbb{Q}(\theta) : \mathbb{Q}] = n$$

olur. O zaman Teorem 2.12'ye göre θ 'nın $\mathbb{Q}$ 'da n farklı eşleniği vardır ve bunlar $\theta_1 = \theta, \theta_2, \dots, \theta_n$ olsun. O zaman

$$p(x) = (x - \theta_1)(x - \theta_2) \dots (x - \theta_n)$$

olur. Teorem 2.25'ye göre, K 'nın her α elemanı, $a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}$ olmak üzere $\alpha = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$ biçiminde tek türlü olarak ifade edilebilir. Böylece $k = 1, 2, \dots, n$ için

$$\sigma_k : K \rightarrow \mathbb{C}$$

$$\sigma_k(a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}) = a_0 + a_1\theta_k + \dots + a_{n-1}\theta_k^{n-1}$$

ile tanımlayabiliriz.

Şimdi σ_k ($k = 1, 2, \dots, n$)'ların birer cisim homomorfizması olduğunu gösterelim.

Önce σ_k ($k = 1, 2, \dots, n$)'ların toplamsal olduğunu gösterelim. O zaman $a_0, a_1, \dots, a_{n-1}, b_0, b_1, \dots, b_{n-1} \in \mathbb{Q}$ olmak üzere

$$\alpha = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}, \quad \beta = b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1}$$

biçiminde yazılabilir. Böylece

$$\alpha + \beta = (a_0 + b_0) + (a_1 + b_1)\theta + \dots + (a_{n-1} + b_{n-1})\theta^{n-1}$$

elde edilir. Dolayısıyla

$$\begin{aligned} \sigma_k(\alpha + \beta) &= (a_0 + b_0) + (a_1 + b_1)\theta_k + \dots + (a_{n-1} + b_{n-1})\theta_k^{n-1} \\ &= (a_0 + a_1\theta_k + \dots + a_{n-1}\theta_k^{n-1}) + (b_0 + b_1\theta_k + \dots + b_{n-1}\theta_k^{n-1}) \\ &= \sigma_k(\alpha) + \sigma_k(\beta) \end{aligned}$$

olur. Yani σ_k toplamsaldır.

Şimdi σ_k ($k = 1, 2, \dots, n$)'ların çarpımsal olduğunu gösterelim. Aynı gösterim ile

$$f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in \mathbb{Q}[x], \quad g(x) = b_0 + b_1x + \dots + b_{n-1}x^{n-1} \in \mathbb{Q}[x]$$

olsun. Böylece

$$f(\theta) = \alpha, \quad g(\theta) = \beta$$

olur. $\mathbb{Q}[x]$ 'de $f(x)g(x)$ polinomunu $p(x)$ polinomuna bölersek

$$f(x)g(x) = p(x)q(x) + r(x), \quad \deg r(x) < \deg p(x) = n$$

olacak biçimde bir $q(x) \in \mathbb{Q}[x]$ bölümü ve bir $r(x) \in \mathbb{Q}[x]$ kalanı elde edilir.

$$p(\theta) = 0 \text{ olduğundan}$$

$$\alpha\beta = f(\theta)g(\theta) = p(\theta)q(\theta) + r(\theta) = r(\theta)$$

olur. Ayrıca $p(\theta_k) = 0$ olduğundan

$$\sigma_k(\alpha\beta) = \sigma_k(r(\theta)) = \sigma_k(r(\theta_k)) = p(\theta_k)q(\theta_k) + r(\theta_k) = f(\theta_k)g(\theta_k) = \sigma_k(\alpha)\sigma_k(\beta)$$

elde edilir. Yani σ_k çarpımsaldır. Böylece σ_k ($k=1,2,\dots,n$)'ların birer homomorfizma olduğunu göstermiş olduk.

Şimdi σ_k ($k=1,2,\dots,n$)'ların birebir olduğunu gösterelim.

$$\alpha = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1} \in K \quad \text{ve} \quad \beta = b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1} \in K \quad \text{olmak üzere}$$

$$\sigma_k(\alpha) = \sigma_k(\beta) \text{ olsun. O zaman}$$

$$\begin{aligned} a_0 + a_1\theta_k + \dots + a_{n-1}\theta_k^{n-1} &= b_0 + b_1\theta_k + \dots + b_{n-1}\theta_k^{n-1} \\ (a_0 - b_0) + (a_1 - b_1)\theta_k + \dots + (a_{n-1} - b_{n-1})\theta_k^{n-1} &= 0 \end{aligned}$$

olur. Yani θ_k 'nın

$$(a_0 - b_0) + (a_1 - b_1)x + \dots + (a_{n-1} - b_{n-1})x^{n-1} \in \mathbb{Q}[x]$$

polinomunun bir kökü olduğu görülür. Bu polinomun derecesi n 'den küçüktür. Ayrıca $\text{der}\left(\text{ind}_{\mathbb{Q}}(\theta_k)\right) = \text{der } p(x) = n$ olduğu biliniyor. O halde yukarıdaki bu polinom sıfır polinomu olmalıdır. Böylece

$$a_0 - b_0 = 0, a_1 - b_1 = 0, \dots, a_{n-1} - b_{n-1} = 0$$

dır. Buradan

$$a_0 = b_0, a_1 = b_1, \dots, a_{n-1} = b_{n-1}$$

olur. O zaman

$$\alpha = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1} = b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1} = \beta$$

elde edilir. Yani σ_k birebirdir. O halde σ_k ($k=1,2,\dots,n$)'lar birer birebir homomorfizma olduklarından birer monomorfizmadır.

Şimdi K 'dan $\mathbb{C}$ 'ye $\sigma_1, \sigma_2, \dots, \sigma_n$ 'den başka monomorfizma olmadığını gösterelim.

$\lambda: K \rightarrow \mathbb{C}$ bir monomorfizma olsun. O zaman

$$p(\lambda(\theta)) = \lambda(p(\theta)) = \lambda(0) = 0$$

olur. Yani $\lambda(\theta)$, $p(x)$ 'in bir köküdür ve $p(x)$ 'in kökleri θ 'nın eşlenikleri olduğundan

$$\lambda(\theta) = \theta_k$$

olacak biçimde bir $k \in \{1, 2, \dots, n\}$ vardır. O zaman

$$\lambda(\theta) = \sigma_k(\theta)$$

yazılabilir. Böylece her $a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}$ için

$$\lambda(a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}) = a_0 + a_1\theta_k + \dots + a_{n-1}\theta_k^{n-1} = \sigma_k(a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1})$$

olur. Bu da $\lambda = \sigma_k$ olduğunu gösterir. Sonuç olarak $\{\sigma_k \mid k=1, 2, \dots, n\}$ kümesi K dan $\mathbb{C}$ 'ye bütün monomorfizmaları içerir.

$k = 1, 2, \dots, n$ için

$$\begin{aligned}\sigma_k(K) &= \sigma_k(\mathbb{Q}(\theta)) \\ &= \left\{ \sigma_k(a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}) \mid a_0, a_1, \dots, a_{n-1} \in \mathbb{Q} \right\} \\ &= \left\{ a_0 + a_1\theta_k + \dots + a_{n-1}\theta_k^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in \mathbb{Q} \right\} \\ &= \mathbb{Q}(\theta_k)\end{aligned}$$

elde edilir. Yani $\sigma_k : \mathbb{Q}(\theta) \rightarrow \mathbb{Q}(\theta_k)$ birer izomorfizmadır. Dolayısıyla tüm $\mathbb{Q}(\theta_k)$ ($k = 1, 2, \dots, n$) cisimleri izomorfiktir.

Tanım 2.18. K bir cebirsel sayı cismi olsun. $K = \mathbb{Q}(\theta)$ biçimindeki sayı θ olsun.

$$\theta_1 = \theta, \theta_2, \dots, \theta_n$$

ler θ 'nın $\mathbb{Q}$ 'daki eşlenikleri olsun. Bu takdirde

$$\mathbb{Q}(\theta_1) = \mathbb{Q}(\theta) = K, \mathbb{Q}(\theta_2), \dots, \mathbb{Q}(\theta_n)$$

cisimlerine K 'nın eşlenik cisimleri denir [1].

Teorem 2.32. K bir cebirsel sayı cismi olsun. $K = \mathbb{Q}(\theta)$ biçimindeki bir cebirsel sayı θ olsun. $\theta_1 = \theta, \theta_2, \dots, \theta_n$ 'ler θ 'nın $\mathbb{Q}$ 'daki eşlenikleri olsun. $K = \mathbb{Q}(\phi)$ biçimindeki başka bir cebirsel sayı ϕ olsun. $c_0, c_1, \dots, c_{n-1} \in \mathbb{Q}$ olmak üzere

$$\phi = c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1}$$

olsun. $k = 1, 2, \dots, n$ için

$$\phi_k = c_0 + c_1\theta_k + \dots + c_{n-1}\theta_k^{n-1}$$

olsun. Böylece $\phi_1 = \phi$ olur. Bu takdirde $\phi_1, \phi_2, \dots, \phi_n$ 'ler ϕ 'nin $\mathbb{Q}$ 'daki eşlenikleridir ve

$$\mathbb{Q}(\theta_k) = \mathbb{Q}(\phi_k) \quad (k=1,2,\dots,n)$$

dir [1].

Tanım 2.19. K bir cebirsel sayı cismi ve K 'nin $\mathbb{Q}$ 'daki derecesi n olsun.

$\theta \in O_K$ için $K = \mathbb{Q}(\theta)$ olsun. $\theta_1 = \theta, \theta_2, \dots, \theta_n$ 'ler θ 'nın $\mathbb{Q}$ 'daki eşlenikleri olsun.

$\alpha \in K$ için tek türlü belirli $c_0, c_1, \dots, c_{n-1}$ rasyonel sayıları

$$\alpha = c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1}$$

olacak biçimde vardır. $k=1,2,\dots,n$ için

$$\alpha_k = c_0 + c_1\theta_k + \dots + c_{n-1}\theta_k^{n-1} \in \mathbb{Q}(\theta_k)$$

olsun. Bu $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ cebirsel sayılarına α 'nın K eşlenikleri denir. α 'nın

K eşlenikleri α 'ya $\sigma_k : K \rightarrow \mathbb{C} \quad (k=1,2,\dots,n)$ monomorfizmaları uygulanarak elde edilir. $k=1,2,\dots,n$ için $\sigma_k(\alpha) = \alpha_k \in \mathbb{Q}(\theta_k)$ 'dir [1].

Örnek 2.19. $\theta = \sqrt{2} + \sqrt{3}$ olmak üzere $K = \mathbb{Q}(\theta)$ olsun. Örnek 2.18'den dolayı $\text{ind}_{\mathbb{Q}}(\theta) = x^4 - 10x^2 + 1$ olduğu biliniyor.

$$x^4 - 10x^2 + 1 = (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3})$$

olduğundan, θ 'nın eşlenikleri

$$\theta_1 = \sqrt{2} + \sqrt{3}, \theta_2 = \sqrt{2} - \sqrt{3}, \theta_3 = -\sqrt{2} + \sqrt{3}, \theta_4 = -\sqrt{2} - \sqrt{3}$$

olur. $\alpha = 2\sqrt{3}$ sayısını ele alalım. O zaman Örnek 2.18'e göre

$$\alpha \in \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\theta) = K$$

olur. Dolayısıyla $\alpha = a + b\theta + c\theta^2 + d\theta^3$ olacak biçimde $a, b, c, d \in \mathbb{Q}$ vardır.

$$\begin{aligned}
2\sqrt{3} &= a + b(\sqrt{2} + \sqrt{3}) + c(\sqrt{2} + \sqrt{3})^2 + d(\sqrt{2} + \sqrt{3})^3 \\
&= (a + 5c) + (b + 11d)\sqrt{2} + (b + 9d)\sqrt{3} + 2c\sqrt{6}
\end{aligned}$$

ifadesinden $a + 5c = 0$, $b + 11d = 0$, $b + 9d = 2$, $2c = 0$ olur. Yani $a = 0$, $b = 11$, $c = 0$, $d = -1$ elde edilir. Böylece

$$\alpha = 11\theta - \theta^3$$

olur. O halde α 'nın K eşlenikleri

$$\alpha_1 = \alpha = 11\theta - \theta^3 = 2\sqrt{3}$$

$$\alpha_2 = 11\theta_2 - \theta_2^3 = -2\sqrt{3}$$

$$\alpha_3 = 11\theta_3 - \theta_3^3 = 2\sqrt{3}$$

$$\alpha_4 = 11\theta_4 - \theta_4^3 = -2\sqrt{3}$$

olarak bulunur.

Tanım 2.20. K derecesi n olan bir cebirsel sayı cismi olsun. $\alpha \in K$ olsun. $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ 'ler α 'nın K eşlenikleri olsun. Bu takdirde α 'nın K üzerindeki cisim polinomu

$$\text{cis}_K(\alpha) = \prod_{k=1}^n (x - \alpha_k)$$

olarak tanımlanır. $\text{cis}_K(\alpha) \in \mathbb{C}[x]$ olduğu açıktır [1].

Teorem 2.33. K derecesi n olan bir cebirsel sayı cismi olsun. $\alpha \in K$ alalım. Bu takdirde $\text{cis}_K(\alpha) \in \mathbb{Q}[x]$ 'dir [1].

Örnek 2.20. $x^3 + 11x + 4 \in \mathbb{Z}[x]$ kübik polinomu indirgenemezdir. Bu polinomun üç kökü $\theta_1 = \theta, \theta_2, \theta_3$ olsun. Bu köklerden birisi reeldir, diğer ikisi reel değildir ve biri diğerinin kompleks eşleniğidir. $K = \mathbb{Q}(\theta)$ olsun. Böylece

$$[K : \mathbb{Q}] = \deg(\text{ind}_{\mathbb{Q}}(\theta)) = \deg(x^3 + 11x + 4) = 3$$

olur. $\alpha = \frac{\theta + \theta^2}{2} \in K$ olsun. $\text{cis}_K(\alpha)$ 'yı bulalım.

$$\text{cis}_K(\alpha) = \left(x - \left(\frac{\theta_1 + \theta_1^2}{2} \right) \right) \left(x - \left(\frac{\theta_2 + \theta_2^2}{2} \right) \right) \left(x - \left(\frac{\theta_3 + \theta_3^2}{2} \right) \right)$$

dir. $\text{cis}_K(\alpha) = x^3 + a_2x^2 + a_1x + a_0$ dersek;

$$a_2 = -\frac{(\theta_1 + \theta_1^2)}{2} - \frac{(\theta_2 + \theta_2^2)}{2} - \frac{(\theta_3 + \theta_3^2)}{2} = -\frac{1}{2}(\theta_1 + \theta_2 + \theta_3) - \frac{1}{2}(\theta_1^2 + \theta_2^2 + \theta_3^2)$$

$$\begin{aligned} a_1 &= \frac{1}{4} \left((\theta_1 + \theta_1^2)(\theta_2 + \theta_2^2) + (\theta_2 + \theta_2^2)(\theta_3 + \theta_3^2) + (\theta_3 + \theta_3^2)(\theta_1 + \theta_1^2) \right) \\ &= \frac{1}{4} \left((\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1) + (\theta_1\theta_2^2 + \theta_1^2\theta_2 + \theta_2\theta_3^2 + \theta_2^2\theta_3 + \theta_3\theta_1^2 + \theta_3^2\theta_1) \right. \\ &\quad \left. + (\theta_1^2\theta_2^2 + \theta_2^2\theta_3^2 + \theta_3^2\theta_1^2) \right) \end{aligned}$$

$$\begin{aligned} a_0 &= -\frac{1}{8}(\theta_1 + \theta_1^2)(\theta_2 + \theta_2^2)(\theta_3 + \theta_3^2) \\ &= -\frac{1}{8}\theta_1\theta_2\theta_3(1 + \theta_1)(1 + \theta_2)(1 + \theta_3) \\ &= -\frac{1}{8}\theta_1\theta_2\theta_3(1 + (\theta_1 + \theta_2 + \theta_3) + (\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1) + \theta_1\theta_2\theta_3) \end{aligned}$$

olur. Ayrıca

$$x^3 + 11x + 4 = (x - \theta_1)(x - \theta_2)(x - \theta_3)$$

idi. Buradan

$$\theta_1 + \theta_2 + \theta_3 = 0$$

$$\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1 = 11$$

$$\theta_1\theta_2\theta_3 = -4$$

elde edilir. Bunlar kullanılarak

$$\begin{aligned}\theta_1^2 + \theta_2^2 + \theta_3^2 &= (\theta_1 + \theta_2 + \theta_3)^2 - 2(\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1) = -22 \\ \theta_1^2\theta_2^2 + \theta_2^2\theta_3^2 + \theta_3^2\theta_1^2 &= (\theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1)^2 - 2\theta_1\theta_2\theta_3(\theta_1 + \theta_2 + \theta_3) = 121 \\ \theta_1\theta_2^2 + \theta_1^2\theta_2 + \theta_2\theta_3^2 + \theta_2^2\theta_3 + \theta_3\theta_1^2 + \theta_3^2\theta_1 &= \theta_1\theta_2(\theta_2 + \theta_1) + \theta_2\theta_3(\theta_3 + \theta_2) \\ &\quad + \theta_3\theta_1(\theta_1 + \theta_3) = -3\theta_1\theta_2\theta_3 = 12\end{aligned}$$

bulunur. Dolayısıyla

$$a_2 = 11, a_1 = 36, a_0 = 4$$

dir. Dolayısıyla

$$\text{cis}_K(\alpha) = x^3 + 11x^2 + 36x + 4$$

olacağından $\alpha \in O_K$ olduğu görülür.

Teorem 2.34. K derecesi n olan bir cebirsel sayı cismi olsun. $\alpha \in K$ olsun. Bu takdirde s pozitif tamsayısı

$$s = \frac{n}{\text{der}(\text{ind}_{\mathbb{Q}}(\alpha))}$$

olmak üzere s tamsayısı

$$\text{cis}_K(\alpha) = (\text{ind}_{\mathbb{Q}}(\alpha))^s$$

olacak biçimde vardır [1].

Teorem 2.35. K bir cebirsel sayı cismi ve $\alpha \in O_K$ olsun. Bu takdirde α 'nın K eşlenikleri birer cebirsel tamsayıdır [1].

Teorem 2.36. K bir cebirsel sayı cismi ve $\alpha \in K$ olsun. Bu takdirde α 'nın K eşleniklerinin hepsinin eşit olmasının gerek ve yeter koşulu $\alpha \in \mathbb{Q}$ olmasıdır [1].

Teorem 2.37. K bir cebirsel sayı cismi ve $\alpha \in K$ olsun. Bu takdirde α 'nın K eşleniklerinin hepsinin farklı olmasının gerek ve yeter koşulu $K = \mathbb{Q}(\alpha)$ olmasıdır [1].

Tanım 2.21. K derecesi n olan bir cebirsel sayı cismi olsun. $w_1, w_2, \dots, w_n$ 'ler K cisminin n tane elemanı olsun. σ_k ($k=1, 2, \dots, n$) ile K 'dan $\mathbb{C}$ 'ye tanımlı n farklı monomorfizma gösterilsin. $i=1, 2, \dots, n$ için

$$w_i^{(1)} = \sigma_1(w_i) = w_i, \quad w_i^{(2)} = \sigma_2(w_i), \quad \dots, \quad w_i^{(n)} = \sigma_n(w_i)$$

ile w_i 'nin K eşlenikleri gösterilsin. Bu takdirde $\{w_1, w_2, \dots, w_n\}$ 'nin diskriminantı

$$D(w_1, w_2, \dots, w_n) = \begin{vmatrix} w_1^{(1)} & w_2^{(1)} & \dots & w_n^{(1)} \\ w_1^{(2)} & w_2^{(2)} & \dots & w_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ w_1^{(n)} & w_2^{(n)} & \dots & w_n^{(n)} \end{vmatrix}^2$$

olarak tanımlanır [1].

Örnek 2.21. $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ olsun. $w_1 = 1$, $w_2 = \sqrt{2}$, $w_3 = \sqrt{3}$, $w_4 = \sqrt{2} + \sqrt{3}$ seçelim. Örnek 2.18'den dolayı K 'nın bir kuadratik cisim olduğu biliniyor. K 'dan $\mathbb{C}$ 'ye tanımlı dört monomorfizma, $a, b, c, d \in \mathbb{Q}$ olmak üzere

$$\begin{aligned}
\sigma_1(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) &= a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \\
\sigma_2(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) &= a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6} \\
\sigma_3(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) &= a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6} \\
\sigma_4(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) &= a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}
\end{aligned}$$

ile verilir. Böylece

$$D(1, \sqrt{2}, \sqrt{3}, \sqrt{2} + \sqrt{3}) = \begin{vmatrix} 1 & +\sqrt{2} & +\sqrt{3} & +\sqrt{2} + \sqrt{3} \\ 1 & +\sqrt{2} & -\sqrt{3} & +\sqrt{2} - \sqrt{3} \\ 1 & -\sqrt{2} & +\sqrt{3} & -\sqrt{2} + \sqrt{3} \\ 1 & -\sqrt{2} & -\sqrt{3} & -\sqrt{2} - \sqrt{3} \end{vmatrix}^2$$

olur. Diskriminantın dördüncü sütunu, ikinci ve üçüncü sütunların toplamı olduğundan

$$D(1, \sqrt{2}, \sqrt{3}, \sqrt{2} + \sqrt{3}) = 0$$

elde edilir.

Tanım 2.22. K derecesi n olan bir cebirsel sayı cismi olsun. $\alpha \in K$ olsun. Bu takdirde α 'nin diskriminantı olan $D(\alpha)$,

$$D(\alpha) = D(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$$

olarak tanımlanır [1].

Teorem 2.38. K derecesi n olan bir cebirsel sayı cismi olsun. $\alpha \in K$ olsun. Bu takdirde $\alpha^{(1)} = \alpha, \alpha^{(2)}, \dots, \alpha^{(n)}$ 'ler α 'nın K eşlenikleri olmak üzere

$$D(\alpha) = \prod_{1 \leq i < j \leq n} (\alpha^{(i)} - \alpha^{(j)})^2$$

dir [1].

Tanım 2.23. $n \in \mathbb{N}$ ve $a_n \neq 0$ olmak üzere

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{C}[x]$$

olsun. $f(x)$ 'in kökleri $x_1, x_2, \dots, x_n$ 'ler olsun. $f(x)$ polinomunun diskriminantı

$$\text{disk}(f(x)) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in \mathbb{C}$$

sayısıdır. Bu tanıma göre $f(x)$ 'in bir katlı köke sahip olmasının gerek ve yeter koşulu $\text{disk}(f(x)) = 0$ olmasıdır [1].

Teorem 2.39. K derecesi n olan bir cebirsel sayı cismi ve $\alpha \in K$ olsun. Bu takdirde

$$D(\alpha) = \text{disk}(\text{cis}_K(x))$$

dır [1].

Örnek 2.22. $K = \mathbb{Q}(\sqrt[3]{2})$ ve $\alpha = \sqrt[3]{2}$ olsun. Bu takdirde α 'nın eşlenikleri

$w = (-1 + \sqrt{-3})/2$ olmak üzere $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = w\sqrt[3]{2}$, $\alpha_3 = w^2\sqrt[3]{2}$ olur. O zaman

$$\alpha_1 - \alpha_2 = (1 - w)\sqrt[3]{2}$$

$$\alpha_2 - \alpha_3 = w(1 - w)\sqrt[3]{2}$$

$$\alpha_3 - \alpha_1 = w^2(1 - w)\sqrt[3]{2}$$

olur. Böylece

$$(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) = (1 - w)^3 2$$

olduğu görülür. Ayrıca

$$(1-w)^3 = 1-3w+3w^2-w^3 = -3(w-w^2)$$

dır. Buradan

$$(1-w)^6 = 3^2(w-w^2)^2 = 3^2(w^2+w-2) = -3^2$$

olur. Böylece

$$D(\alpha) = \left((\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \right)^2 = (1-w)^6 2^2 = -2^2 3^2$$

elde edilir.

Teorem 2.40. K derecesi n olan bir cebirsel sayı cismi olsun. $\alpha \in K$ olsun. Bu takdirde $K = \mathbb{Q}(\alpha)$ olmasının gerek ve yeter koşulu $D(\alpha) \neq 0$ olmasıdır [1].

Teorem 2.41. K derecesi n olan bir cebirsel sayı cismi olsun.

- a. Eğer $w_1, w_2, \dots, w_n \in K$ ise $D(w_1, w_2, \dots, w_n) \in \mathbb{Q}$ olur.
- b. Eğer $w_1, w_2, \dots, w_n \in O_K$ ise $D(w_1, w_2, \dots, w_n) \in \mathbb{Z}$ olur.
- c. $w_1, w_2, \dots, w_n \in K$ olsun. Bu takdirde $D(w_1, w_2, \dots, w_n) \neq 0$ olmasının gerek ve yeter koşulu $w_1, w_2, \dots, w_n$ 'lerin $\mathbb{Q}$ 'da lineer bağımsız olmasıdır [1].

Teorem 2.42. K derecesi n olan bir cebirsel sayı cismi olsun. O_K 'nin sıfırdan farklı bir ideali I olsun. Bu takdirde

$$D(\mu_1, \mu_2, \dots, \mu_n) \neq 0$$

olacak biçimde $\mu_1, \mu_2, \dots, \mu_n \in I$ vardır [1].

Teorem 2.43. K derecesi n olan bir cebirsel sayı cismi olsun. O_K 'nin sıfırdan farklı bir ideali I olsun. Bu takdirde, I 'nin $\mu_1, \mu_2, \dots, \mu_n$ elemanları vardır ve I 'nin her α elemanı, $x_1, x_2, \dots, x_n \in \mathbb{Z}$ olmak üzere

$$\alpha = x_1\mu_1 + x_2\mu_2 + \dots + x_n\mu_n$$

biçiminde tek türlü olarak ifade edilebilir [1].

Teorem 2.44. K bir cebirsel sayı cismi olsun. Bu takdirde O_K Noetherian bölgesidir [1].

Tanım 2.24. K derecesi n olan bir cebirsel sayı cismi olsun. I ideali O_K 'nin sıfırdan farklı bir ideali olsun. I 'nin elemanlarından oluşan bir $\{\mu_1, \mu_2, \dots, \mu_n\}$ kümesi için, her $\alpha \in I$ elemanı

$$\alpha = x_1\mu_1 + x_2\mu_2 + \dots + x_n\mu_n \quad (x_1, x_2, \dots, x_n \in \mathbb{Z})$$

biçiminde tek türlü olarak ifade edilebilecek biçimde mevcut ise $\{\mu_1, \mu_2, \dots, \mu_n\}$ 'ye I ideali için bir taban denir [1].

Teorem 2.45. K derecesi n olan bir cebirsel sayı cismi olsun. O_K 'nin sıfırdan farklı bir ideali I olsun.

a. $\{\mu_1, \mu_2, \dots, \mu_n\}$ ve $\{\lambda_1, \lambda_2, \dots, \lambda_n\}$ 'ler I için iki taban olsun. Bu takdirde

$$D(\mu_1, \mu_2, \dots, \mu_n) = D(\lambda_1, \lambda_2, \dots, \lambda_n) \text{ 'dir. Ayrıca } c_{ij} \quad (i, j = 1, 2, \dots, n)$$

rasyonel sayıları $\det(c_{ij}) = \pm 1$ biçimindeki rasyonel tamsayılar olmak üzere

$$1 \leq i \leq n \text{ için } \mu_i = \sum_{j=1}^n c_{ij} \lambda_j \text{ olacak biçimde vardır.}$$

- b. $\{\mu_1, \mu_2, \dots, \mu_n\}$ 'ler I için bir taban ve $\lambda_1, \lambda_2, \dots, \lambda_n \in I$ için $D(\mu_1, \mu_2, \dots, \mu_n) = D(\lambda_1, \lambda_2, \dots, \lambda_n)$ olsun. Bu takdirde $\{\lambda_1, \lambda_2, \dots, \lambda_n\}$ 'ler de I için bir tabandır [1].

Örnek 2.23. $K = \mathbb{Q}(\sqrt{7})$ olsun. O zaman Teorem 2.16'ya göre $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{7} = \{a + b\sqrt{7} \mid a, b \in \mathbb{Z}\}$ olur. O_K 'nin $2 + \sqrt{7}$ tarafından üretilen ideali I olsun. Bu takdirde

$$\begin{aligned} I &= \{(a + b\sqrt{7})(2 + \sqrt{7}) \mid a, b \in \mathbb{Z}\} = \{a(2 + \sqrt{7}) + b(7 + 2\sqrt{7}) \mid a, b \in \mathbb{Z}\} \\ &= (2 + \sqrt{7})\mathbb{Z} + (7 + 2\sqrt{7})\mathbb{Z} \end{aligned}$$

olur. Yani $\{2 + \sqrt{7}, 7 + 2\sqrt{7}\}$, I 'nin bir tabanıdır. Ayrıca basit bir düzenleme ile

$$\begin{aligned} I &= \{(a + b\sqrt{7})(2 + \sqrt{7}) \mid a, b \in \mathbb{Z}\} = \{(2a + 7b) + (a + 2b)\sqrt{7} \mid a, b \in \mathbb{Z}\} \\ &= \{(2(c - 2b) + 7b) + c\sqrt{7} \mid b, c \in \mathbb{Z}\} = \{3b + c(2 + \sqrt{7}) \mid b, c \in \mathbb{Z}\} \\ &= 3\mathbb{Z} + (2 + \sqrt{7})\mathbb{Z} \end{aligned}$$

elde edilir. Yani $\{3, 2 + \sqrt{7}\}$, I 'nin bir tabanıdır.

Tanım 2.25. K derecesi n olan bir cebirsel sayı cismi olsun. O_K 'nin sıfırdan farklı bir ideali I olsun. $\{\mu_1, \mu_2, \dots, \mu_n\}$ 'ler I 'nin bir tabanı olsun. Bu takdirde I idealinin diskriminantı olan $D(I)$;

$$D(I) = D(\mu_1, \mu_2, \dots, \mu_n)$$

ile verilen sıfırdan farklı tamsayıdır [1].

Örnek 2.24. Örnek 3.23.'deki I idealinin diskriminantını hesaplayalım. $\{3, 2+\sqrt{7}\}$, I için bir taban olduğundan

$$D(I) = D(3, 2+\sqrt{7}) = \begin{vmatrix} 3 & 2+\sqrt{7} \\ 3 & 2-\sqrt{7} \end{vmatrix}^2 = (3(2+\sqrt{7}) - 3(2-\sqrt{7}))^2 = (-6\sqrt{7})^2 = 252$$

elde edilir.

Teorem 2.46. m karesiz bir tamsayı olmak üzere $K = \mathbb{Q}(\sqrt{m})$ bir kuadratik cisim olsun.

- a.** $m \equiv 2, 3 \pmod{4}$ olsun. $a, b, c \in \mathbb{Z}$ ve $a \neq 0, c \neq 0$ olsun. Bu takdirde $\{a, b+c\sqrt{m}\}$ kümesinin $\langle a, b+c\sqrt{m} \rangle$ ideali için bir taban olmasının gerek ve yeter koşulu $c \mid a$, $c \mid b$, $ac \mid b^2 - mc^2$ olmasıdır.
- b.** $m \equiv 1 \pmod{4}$ olsun. $a, b, c \in \mathbb{Z}$ ve $a \neq 0, c \neq 0$ ve $b \equiv c \pmod{2}$ olsun. Bu takdirde $\left\{a, \frac{b+c\sqrt{m}}{2}\right\}$ kümesinin $\left\langle a, \frac{b+c\sqrt{m}}{2} \right\rangle$ ideali için bir taban olmasının gerek ve yeter koşulu $c \mid a$, $c \mid b$, $4ac \mid b^2 - mc^2$ olmasıdır [1].

Teorem 2.47. Bir K cebirsel sayı cisminin tamsayılar halkası olan O_K 'nin bir asal ideali P olsun. Bu takdirde P ideali O_K 'nin bir maksimal idealidir.

İspat. M , O_K 'nin $P \neq M$, $M \neq O_K$ ve $P \subset M \subset O_K$ şartlarını sağlayan bir ideali olsun. $P \cap \mathbb{Z} \subset M \cap \mathbb{Z}$ olduğu açıktır. Teorem 2.29'a göre O_K 'nin P ideali sıfırdan farklı olduğundan $c \neq 0$ rasyonel tamsayısı $c \in P$ olacak biçimde vardır. Şu halde $P \cap \mathbb{Z} \neq \{0\}$ olur. $P \neq O_K$ olduğundan $1 \notin P$ ve buradan $P \cap \mathbb{Z} \neq \mathbb{Z}$ olur. Benzer biçimde $M \neq O_K$ olduğundan $1 \notin M$ ve buradan $M \cap \mathbb{Z} \neq \mathbb{Z}$ 'dir. Ayrıca Teorem 1.17'ye göre $P \cap \mathbb{Z}$, $\mathbb{Z}$ 'nin bir asal idealidir. Fakat Teorem 1.3'e göre $\mathbb{Z}$ bir esas

ideal bölgesi idi. O halde Teorem 1.6'ya göre $P \cap \mathbb{Z} = \langle p \rangle$ olacak biçimde bir $p \in \mathbb{Z}$ asal sayısı vardır. Böylece

$$\langle p \rangle = P \cap \mathbb{Z} \subset M \cap \mathbb{Z} \subset \mathbb{Z}$$

elde edilir. Teorem 1.12'ye göre $\langle p \rangle$ ideali $\mathbb{Z}$ 'de maksimaldir. Böylece

$$P \cap \mathbb{Z} = M \cap \mathbb{Z} = \langle p \rangle$$

elde edilir. $P \neq M$ olduğundan bir $\alpha \in M$, $\alpha \notin P$ elemanı vardır. $\alpha \in O_K$ olduğundan

$$\alpha^k + a_{k-1}\alpha^{k-1} + \dots + a_1\alpha + a_0 = 0$$

olacak biçimde bir $k \in \mathbb{Z}^+$ ve $a_0, a_1, \dots, a_{k-1} \in \mathbb{Z}$ vardır. O halde $0 \in P$ olduğundan

$$\alpha^k + a_{k-1}\alpha^{k-1} + \dots + a_1\alpha + a_0 \in P$$

olur. $b_0, b_1, \dots, b_{m-1} \in \mathbb{Z}$ olmak üzere

$$\alpha^m + b_{m-1}\alpha^{m-1} + \dots + b_1\alpha + b_0 \in P \quad (1)$$

olan en küçük pozitif tamsayı m olsun. Ayrıca $\alpha \in M$ olduğundan

$$\alpha^m + b_{m-1}\alpha^{m-1} + \dots + b_1\alpha = \alpha(\alpha^{m-1} + b_{m-1}\alpha^{m-2} + \dots + b_1) \in M$$

olduğu açıktır. $P \subset M$ ve M bir ideal olduğundan

$$(\alpha^m + b_{m-1}\alpha^{m-1} + \dots + b_1\alpha + b_0) - (\alpha^m + b_{m-1}\alpha^{m-1} + \dots + b_1\alpha) \in M$$

olur. Yani $b_0 \in M$ 'dir. Fakat $b_0 \in \mathbb{Z}$ idi. Böylece

$$b_0 \in M \cap \mathbb{Z} = P \cap \mathbb{Z}$$

dolayısıyla $b_0 \in P$ elde edilir. $\alpha^m + b_{m-1}\alpha^{m-1} + \dots + b_1\alpha + b_0 \in P$ ifadesinden

$$\alpha^m + b_{m-1}\alpha^{m-1} + \dots + b_1\alpha \in P \quad (2)$$

elde edilir. $m=1$ ise (1)'den dolayı $\alpha + b_0 \in P$ ve böylece $\alpha + b_0 - b_0 \in P$ yani $\alpha \in P$ olur. Bu olamaz. O halde $m \geq 2$ 'dir. (2)'ye göre

$$\alpha(\alpha^{m-1} + b_{m-1}\alpha^{m-2} + \dots + b_1) \in P$$

olur. P asal ideal ve $\alpha \notin P$ olduğundan

$$\alpha^{m-1} + b_{m-1}\alpha^{m-2} + \dots + b_1 \in P$$

elde edilir. Burada $m \geq 2$ olduğundan $m-1$ bir pozitif tamsayıdır. Bu durum m 'nin en küçük olması ile çelişir. O halde O_K 'da asal olan her ideal maksimal idealdir.

Tanım 2.26. K bir cebirsel sayı cismi olsun. O_K 'nın bir tabanına K için bir integral tabanı veya tamsayı tabanı denir [1].

Teorem 2.48. K bir kuadratik cisim olsun. $K = \mathbb{Q}(\sqrt{m})$ olacak biçimdeki tek türlü belirli karesiz tamsayı m olsun. $m \equiv 2, 3 \pmod{4}$ ise $\{1, \sqrt{m}\}$ K 'nın bir tamsayı tabanıdır. $m \equiv 1 \pmod{4}$ ise $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$ K 'nın bir tamsayı tabanıdır [1].

Tanım 2.27. K derecesi n olan bir cebirsel sayı cismi olsun. $\{\mu_1, \mu_2, \dots, \mu_n\}$ K için bir tamsayı tabanı olsun. Bu takdirde $D(\mu_1, \mu_2, \dots, \mu_n)$ 'ye K 'nın diskriminantı denir ve $d(K)$ ile gösterilir [1].

Teorem 2.49. K bir kuadratik cisim olsun. $K = \mathbb{Q}(\sqrt{m})$ olacak biçimdeki tek türlü belirli karesiz tamsayı m olsun. Bu takdirde K 'nın diskriminantı $d(K)$,

$$d(K) = \begin{cases} 4m & , m \equiv 2, 3 \pmod{4} \text{ ise} \\ m & , m \equiv 1 \pmod{4} \text{ ise} \end{cases}$$

ile verilir [1].

Tanım 2.28. K derecesi n olan bir cebirsel sayı cismi olsun. O_K 'nin sıfırdan farklı bir ideali I olsun. Bu takdirde I idealinin normu $N(I)$ diye yazılır ve

$$N(I) = \sqrt{\frac{D(I)}{d(K)}}$$

olarak tanımlanır [1].

Teorem 2.50. K derecesi n olan bir cebirsel sayı cismi olsun. O_K 'nin sıfırdan farklı bir ideali I olsun. Bu takdirde I idealinin normu olan $N(I)$ bir pozitif tamsayıdır [1].

Örnek 2.25. $K = \mathbb{Q}(\sqrt{-5})$ olsun. O_K 'nin 2 ve $1 + \sqrt{-5}$ elemanları ile üretilen ideali I olsun. Yani $I = \langle 2, 1 + \sqrt{-5} \rangle$ olsun. I idealinin normu olan $N(I)$ 'yi bulalım. Öncelikle I 'nin bir tabanını bulalım. $O_K = \{x + y\sqrt{-5} \mid x, y \in \mathbb{Z}\}$ olduğundan

$$\begin{aligned}
I &= \left\{ 2(a+b\sqrt{-5}) + (1+\sqrt{-5})(c+d\sqrt{-5}) \mid a,b,c,d \in \mathbb{Z} \right\} \\
&= \left\{ (2a+c-5d) + (2b+c+d)\sqrt{-5} \mid a,b,c,d \in \mathbb{Z} \right\} \\
&= \left\{ (2a+(y-2b-d)-5d) + y\sqrt{-5} \mid a,b,d,y \in \mathbb{Z} \right\} \\
&= \left\{ 2(a-b-3d) + y + y\sqrt{-5} \mid a,b,d,y \in \mathbb{Z} \right\} \\
&= \left\{ 2x + y + y\sqrt{-5} \mid x,y \in \mathbb{Z} \right\} \\
&= \left\{ 2x + (1+\sqrt{-5})y \mid x,y \in \mathbb{Z} \right\}
\end{aligned}$$

elde edilir. Yani $\{2, 1+\sqrt{-5}\}$, I 'nin bir tabanıdır. O zaman

$$D(I) = D(2, 1+\sqrt{-5}) = \begin{vmatrix} 2 & 1+\sqrt{-5} \\ 2 & 1-\sqrt{-5} \end{vmatrix}^2 = (-4\sqrt{-5})^2 = -80$$

olur. Teorem 2.49'dan dolayı

$$d(K) = 4(-5) = -20$$

olur. Böylece

$$N(I) = \sqrt{\frac{D(I)}{d(K)}} = \sqrt{\frac{-80}{-20}} = \sqrt{4} = 2$$

elde edilir.

Örnek 2.26. m karesiz bir tamsayı ve $m \equiv 2, 3 \pmod{4}$ olmak üzere $K = \mathbb{Q}(\sqrt{m})$

olsun. Böylece $O_K = \{x + y\sqrt{m} \mid x, y \in \mathbb{Z}\}$ olur. $\alpha = a + b\sqrt{m} \in O_K$ olsun. $\langle \alpha \rangle$ esas

idealinin normunu bulalım.

$$\begin{aligned}
\langle \alpha \rangle &= \langle a + b\sqrt{m} \rangle = \left\{ (x + y\sqrt{m})(a + b\sqrt{m}) \mid x, y \in \mathbb{Z} \right\} \\
&= \left\{ x(a + b\sqrt{m}) + y(bm + a\sqrt{m}) \mid x, y \in \mathbb{Z} \right\}
\end{aligned}$$

elde edilir. Yani $\{a + b\sqrt{m}, bm + a\sqrt{m}\}$ elemanları $\langle \alpha \rangle$ 'nın bir tabanıdır. O zaman

$$D(\langle \alpha \rangle) = \begin{vmatrix} a + b\sqrt{m} & bm + a\sqrt{m} \\ a - b\sqrt{m} & bm - a\sqrt{m} \end{vmatrix}^2 = \left((a + b\sqrt{m})(bm - a\sqrt{m}) - (a - b\sqrt{m})(bm + a\sqrt{m}) \right)^2$$

olur.

$$(A + B)(C - D) - (A - B)(C + D) = 2(BC - AD)$$

özdeşliği kullanılırsa

$$D(\langle \alpha \rangle) = 2^2 m (a^2 - mb^2)^2$$

olduğu görülür. Ayrıca Teorem 2.49'a göre $d(K) = 4m$ idi. Böylece

$$N(\langle \alpha \rangle) = \sqrt{\frac{2^2 m (a^2 - mb^2)^2}{4m}} = |a^2 - mb^2|$$

elde edilir.

Teorem 2.51. K bir kuadratik cisim olsun. $K = \mathbb{Q}(\sqrt{m})$ olacak biçimdeki tek türlü belirli karesiz tamsayı m olsun.

a. $m \equiv 2, 3 \pmod{4}$ olsun. $a, b, c \in \mathbb{Z}$ için $a \neq 0$, $c \neq 0$, $c \mid a$, $c \mid b$, $ac \mid b^2 - mc^2$

olsun. Bu takdirde $N\left(\left\langle a, b + c\sqrt{m} \right\rangle\right) = |ac|$ dir.

b. $m \equiv 1 \pmod{4}$ olsun. $a, b, c \in \mathbb{Z}$ için $a \neq 0$, $c \neq 0$, $b \equiv c \pmod{2}$, $c \mid a$, $c \mid b$,

$4ac \mid b^2 - mc^2$ olsun. Bu takdirde $N\left(\left\langle a, \frac{b + c\sqrt{m}}{2} \right\rangle\right) = |ac|$ dir [1].

Teorem 2.52. K derecesi n olan bir cebirsel sayı cismi olsun. c sıfırdan farklı bir rasyonel tamsayı olsun. Bu takdirde O_K ’nin c tarafından üretilen esas ideali olan $\langle c \rangle$ ’nin normu

$$N(\langle c \rangle) = |c|^n$$

dir [1].



BÖLÜM 3. DEDEKİND BÖLGELERİ

Tanım 3.1. Bir D tamlık bölgesi

- a. D bir Noetherian bölgesidir
- b. D tam kapalıdır
- c. D 'nin her asal ideali bir maksimal idealdir

ile verilen üç özelliği sağlıyorsa, D 'ye bir Dedekind bölgesi denir [1].

Teorem 3.1. K bir cebirsel sayı cismi olsun. K 'nın tamsayılar halkası O_K olsun. Bu takdirde O_K bir Dedekind bölgesidir [1].

İspat. Teorem 2.44, Teorem 2.28 ve Teorem 2.47' den hemen görülür.

Teorem 3.2. D bir esas ideal bölgesi olsun. Bu takdirde D bir Dedekind bölgesidir [1].

İspat. D bir esas ideal bölgesi olsun. Teorem 1.22' ye göre D bir Noetherian bölgesidir. Teorem 1.25' ya göre D bir tek türlü çarpanlarına ayrılabilir bölgedir. Dolayısıyla Teorem 2.9' a göre D tam kapalıdır. Ayrıca Teorem 1.12' ye göre D 'nin her asal ideali bir maksimal idealdir. O halde D bir Dedekind bölgesidir.

Tanım 3.2. D bir tamlık bölgesi ve D 'nin kesir cismi K olsun. $I \neq \{0\}$, D 'nin bir ideali olsun. $\beta \in K, \beta \neq 0$ olmak üzere $\beta I = \{\beta x \mid x \in I\}$ kümesine D 'nin bir

kesir ideali denir. Bundan böyle D 'nin ideallerine integral ideal veya tam ideali denilecektir. Bu tanıma göre $\beta = 1$ alınırsa D 'nin her tam ideali de bir kesir ideali olur [2].

Tanım 3.3. D bir tamlık bölgesi olsun. A ve B , D 'nin iki kesir ideali olsun. Bu durumda $A = \beta_1 I$, $B = \beta_2 J$ olacak biçimde D 'nin I, J idealleri ve $\beta_1 \neq 0$, $\beta_2 \neq 0$, $\beta_1 \in K$, $\beta_2 \in K$ vardır. Bu durumda

$$AB = \left\{ \sum_{j=1}^n \beta_1 x_j \beta_2 y_j \mid x_j \in I, y_j \in J \right\} = \left\{ \beta_1 \beta_2 \sum_{j=1}^n x_j y_j \mid x_j \in I, y_j \in J \right\} = \beta_1 \beta_2 IJ$$

olur. IJ bir ideal olduğundan AB 'de D 'nin bir kesir ideali olur [2].

Teorem 3.3. D bir Dedekind bölgesi olsun. I , D 'nin sıfırdan farklı bir ideali olsun. Bu takdirde D 'nin bir J ideali ve sıfırdan farklı bir $\alpha \in D$ elemanı $IJ = \langle \alpha \rangle$ olacak biçimde vardır [2].

Teorem 3.4. D bir Dedekind bölgesi olsun. A , D 'nin bir kesir ideali olsun. Bu durumda bir B kesir ideali $AB = D$ olacak biçimde vardır [2].

İspat. D 'nin kesir cismi K olsun. A bir kesir ideali olduğundan $A = \beta I$ olacak biçimde D 'nin bir $I \neq \{0\}$ ideali ve $\beta \in K, \beta \neq 0$ vardır. Teorem 3.3'e göre $IJ = \langle \alpha \rangle$ olacak biçimde D 'nin bir J ideali ve $\alpha \in D, \alpha \neq 0$ vardır. $B = \frac{1}{\alpha\beta} J$

olarak alınırsa B bir kesir ideali olur. Buradan

$$AB = (\beta I) \left(\frac{1}{\alpha\beta} J \right) = \frac{1}{\alpha} IJ = \frac{1}{\alpha} \langle \alpha \rangle = \langle 1 \rangle = D$$

elde edilir.

Tanım 3.4. D bir Dedekind bölgesi ve A 'da D 'nin bir kesir ideali olsun. Teorem 3.3'deki B idealine A 'nın tersi denir [2].

Teorem 3.5. D bir Dedekind bölgesi olsun. D 'deki her tam ideal $(\neq \langle 0 \rangle, D)$ asal ideallerin bir çarpımı biçimindedir ve bu gösterim tek türdür. Buradaki tek türlü gösterim şu şekildedir: P_i ve Q_i 'ler asal idealler olmak üzere

$$P_1 P_2 \dots P_n = Q_1 Q_2 \dots Q_m$$

ise o zaman $n = m$ 'dir ve (eğer gerekiyorsa) yeniden numaralandırarak

$$P_i = Q_i, (i = 1, 2, \dots, n)$$

olduğu kabul edilebilir [1].

Tanım 3.5. D bir Dedekind bölgesi olsun. A ve B 'ler D 'nin sıfırdan farklı tam idealleri olsun. $B = AC$ olacak biçimde D 'nin bir C ideali varsa o zaman A böler B denir ve bu $A|B$ ile gösterilir [2].

Teorem 3.6. D bir Dedekind bölgesi olsun. Bu takdirde D 'nin sıfırdan farklı bütün kesir idealleri çarpma işlemine göre değişmeli bir gruptur [2].

Tanım 3.6. K bir cebirsel sayı cismi olsun. K 'nın tamsayılar halkası O_K olsun. Teorem 3.6'ya göre O_K 'nin sıfırdan farklı bütün kesir ideallerinin kümesi çarpma işlemine göre bir değişmeli gruptur ve bu grup $I(K)$ ile gösterilir [2].

Teorem 3.7. D bir Dedekind bölgesi olsun. A ve B , D 'nin iki ideali ve $A \neq \{0\}$ olsun. Bu takdirde $A|B$ olmasının gerek ve yeter koşulu $B \subseteq A$ olmasıdır [1].

İspat. $\Rightarrow$: $A|B$ olsun. O zaman $B=AC$ olacak biçimde bir C ideali vardır. Böylece $B=AC \subseteq A$ elde edilir.

$\Leftarrow$: $B \subseteq A$ olsun. $B = \{0\}$ ise $A|B$ olduğu açıktır. $B \neq \{0\}$ olsun. Ayrıca $A \neq \{0\}$ olduğundan $AJ = \langle \alpha \rangle$ olacak biçimde bir J ideali ve bir $\alpha \in D, \alpha \neq 0$ elemanı vardır. $C = \frac{1}{\alpha}JB$ olsun. C, D 'nin bir idealidir. Böylece $AC = \frac{1}{\alpha}AJB = \frac{1}{\alpha}\langle \alpha \rangle B = B$ olur. $AC = B$ olduğundan $A|B$ 'dir.

Teorem 3.8. D bir Dedekind bölgesi olsun. A, D 'nin bir kesir veya tam ideali olsun. Bu takdirde A ideali en fazla iki eleman tarafından üretilmiştir [1].

Teorem 3.9. D bir Dedekind bölgesi olsun. A, B ve J idealleri için $JA = JB$ olsun. Bu takdirde $J \neq \{0\}$ ise $A = B$ dir [2],[1].

İspat. $J \neq \{0\}$ olduğundan $IJ = \langle \alpha \rangle$ olacak biçimde D 'nin bir J ideali ve bir $\alpha \neq 0$ vardır. $JA = JB$ olduğundan $I(JA) = I(JB)$ ve $IJ(A) = IJ(B)$ olur. Buradan $\langle \alpha \rangle A = \langle \alpha \rangle B$ elde edilir. $x \in A$ olsun. $\alpha x \in \langle \alpha \rangle A$ 'dır. $\langle \alpha \rangle A = \langle \alpha \rangle B$ olduğundan $\alpha x \in \langle \alpha \rangle B$ olur. O halde $\alpha x = \alpha y$ olan $y \in B$ vardır. Buradan $x = y \in B$ elde edilir. O halde $A \subseteq B$ dir. Benzer biçimde $B \subseteq A$ olduğu gösterilebileceğinden $A = B$ elde edilir.

Tanım 3.7. D bir Dedekind bölgesi, A ve B, D 'nin idealleri olsun.

- a. A ile B 'nin en az biri sıfırdan farklı olsun. A ile B 'nin en büyük ortak bölüneni bir E idealidir öyle ki $E|A, E|B$ 'dir ve bir E' ideali için $E'|A,$

$E' \mid B$ ise $E' \mid E$ 'dir. A ile B 'nin en büyük ortak böleni $\text{ebob}(A, B)$ veya kısaca (A, B) ile gösterilir.

- b.** A ile B 'nin ikisi de sıfırdan farklı olsun. A ile B 'nin en küçük ortak katı bir F idealidir öyle ki $A \mid F$, $B \mid F$ 'dir ve bir F' ideali için $A \mid F'$, $B \mid F'$ ise $F \mid F'$ 'dir. A ile B 'nin en küçük ortak katı $\text{ekok}(A, B)$ veya kısaca $[A, B]$ ile gösterilir [2],[1].

Teorem 3.10. D bir Dedekind bölgesi olsun. A ve B idealler olsun. Bu takdirde

- a.** $(A, B) = A + B$ 'dir.
b. $[A, B] = A \cap B$ 'dir.

İspat. a. $A \subset A + B$ ve $B \subset A + B$ olduğundan $A + B \mid A$ ve $A + B \mid B$ 'dir. Şimdi bir J ideali için $J \mid A$ ve $J \mid B$ olsun. O zaman $A = JA_1$, $B = JB_1$ olan A_1, B_1 idealleri vardır. $A + B = JA_1 + JB_1 = J(A_1 + B_1)$ olduğundan $J \mid A + B$ olur. O halde $(A, B) = A + B$ 'dir.

b. $A \cap B \subset A$ ve $A \cap B \subset B$ olduğundan $A \cap B \mid A$ ve $A \cap B \mid B$ 'dir. Şimdi bir J ideali için $A \mid J$ ve $B \mid J$ olsun. O zaman $J \subset A$ ve $J \subset B$ 'dir. Dolayısıyla $J \subset A \cap B$ olur. Buradan $A \cap B \mid J$ elde edilir. O halde $[A, B] = A \cap B$ 'dir.

Tanım 3.8. D bir Dedekind bölgesi, A ve B idealler olsun. $(A, B) = D$ ise A ile B 'ye aralarında asal denir.

Teorem 3.11. D bir Dedekind bölgesi, A ve B idealler olsun. $A+B=D$ ise $A \cap B = AB$ dir.

Teorem 3.12. D bir Dedekind bölgesi ve P_1, P_2, A idealler olsun. $P_1 | A$, $P_2 | A$ ve $(P_1, P_2) = D$ ise $P_1 P_2 | A$ 'dır.

İspat. $(P_1, P_2) = D$ olduğundan Teorem 3.11'e göre $P_1 \cap P_2 = P_1 P_2$ 'dir. Ayrıca $P_1 | A$ ve $P_2 | A$ olduğundan $A \subset P_1$ ve $A \subset P_2$ 'dir. O halde $A \subset P_1 \cap P_2 = P_1 P_2$ olur. Buradan $P_1 P_2 | A$ elde edilir.

Teorem 3.13. D bir Dedekind bölgesi olsun. P, P_1, P_2 idealler ve P asal ve $P | P_1 P_2$ olsun. $(P, P_1) = D$ ise $P | P_2$ 'dir.

İspat. $(P, P_1) = D$ ise Teorem 3.10'a göre $P + P_1 = D$ 'dir. Buradan $P_2(P + P_1) = P_2 D = P_2$ elde edilir. Ayrıca $P_2(P + P_1) = P_2 P + P_2 P_1$ olduğundan $P_2 P + P_2 P_1 = P_2$ 'dir. Hipotezden $P | P_1 P_2$ idi. O halde $P_1 P_2 = PJ$ olan bir J ideali vardır. Bu takdirde $P_2 = P_2 P + P_2 P_1 = P_2 P + PJ = P(P_2 + J)$ olur. O halde $P | P_2$ elde edilir.

Teorem 3.14. D bir Dedekind bölgesi ve P, P_1, P_2 idealler olsun. $(P, P_1) = D$ ve $(P, P_2) = D$ ise $(P, P_1 P_2) = D$ 'dir.

İspat. $(P, P_1) = D$ ve $(P, P_2) = D$ ise $P + P_1 = D$ ve $P + P_2 = D$ 'dir. O halde $1 = p + p_1, 1 = p' + p_2$ olan $p, p' \in P, p_1 \in P_1, p_2 \in P_2$ vardır. O halde

$$1 = 1 \cdot 1 = (p + p_1)(p' + p_2) = pp' + pp_2 + p_1p + p_1p_2 \in P + P_1P_2$$

elde edilir. $1 \in P + P_1P_2$ olduğundan $P + P_1P_2 = D$ 'dir. O halde $(P, P_1P_2) = D$ elde edilir.

Aşağıdaki teoremin ispatı tümevarımla yapılır.

Teorem 3.15. D bir Dedekind bölgesi, A, B idealler ve $(A, B) = D$ olsun. Bu takdirde her n doğal sayısı için $(A, B^n) = D$ ve $(A^n, B^n) = D$ 'dir.

Teorem 3.16. D bir Dedekind bölgesi ve A, B, J idealler olsun. Bu takdirde $(JA, JB) = J(A, B)$ 'dir.

İspat. En büyük ortak bölen tanımından $(JA, JB) = JA + JB = J(A + B) = J(A, B)$ elde edilir.

Teorem 3.17. D bir Dedekind bölgesi ve A, B, J, A_1, B_1 idealler olsun. $(A, B) = J$ ve $A = JA_1, B = JB_1$ olsun. Bu takdirde $(A_1, B_1) = D$ 'dir.

İspat. $JD = J = A + B = JA_1 + JB_1 = J(A_1 + B_1)$ 'dir. O halde Teorem 3.9'a göre kısaltma yapılırsa $A_1 + B_1 = D$ elde edilir.

Teorem 3.18. D bir Dedekind bölgesi ve A, B idealler olsun. Her n pozitif tamsayısı için $(A^n, B^n) = (A, B)^n$ dir.

İspat. $J = (A, B)$ olsun. O zaman $A = JA_1$, $B = JB_1$, $(A_1, B_1) = D$ olan A_1, B_1 idealleri vardır. Dolayısıyla

$$(A^n, B^n) = ((JA_1)^n, (JB_1)^n) = (J^n A_1^n, J^n B_1^n) = J^n (A_1^n, B_1^n) = J^n D = J^n = (A, B)^n$$

elde edilir.

Teorem 3.19. D bir Dedekind bölgesi, A, B idealler olsun ve $(A, B) = D$ olsun. $AB = C^n$ ($n \geq 2$) olacak biçimde bir C ideali varsa $A = A_1^n$, $B = B_1^n$, $A_1 B_1 = C$ olan A_1, B_1 idealleri vardır.

İspat. $A_1 = (A, C)$, $B_1 = (B, C)$ seçilirse

$$A_1^n = (A, C)^n = (A^n, C^n) = (A^n, AB) = (AA^{n-1}, AB) = A(A^{n-1}, B) = AD = A$$

ve

$$B_1^n = (B, C)^n = (B^n, C^n) = (B^n, AB) = (BB^{n-1}, AB) = B(B^{n-1}, A) = BD = B$$

elde edilir.

Teorem 3.20. D bir Dedekind bölgesi ve A, B, J idealler, $J \neq \{0\}$ olsun. Bu takdirde $[JA, JB] = J[A, B]$ dir.

İspat. $E = [A, B]$, $F = [JA, JB]$ olsun. $JE = F$ olduğu gösterilecek. $E = [A, B]$

olduğundan $A|E$ ve $B|E$ 'dir. Buradan $JA|JE$ ve $JB|JE$ olur. Dolayısıyla $[JA, JB]|JE$ 'dir. Yani $F|JE$ elde edilir.

$F=[JA, JB]$ olduğundan $JA|F$ ve $JB|F$ 'dir. Ayrıca $J|JA$ olduğundan $J|F$ olur. Dolayısıyla $F=JX$ olan bir X ideali vardır. $JA|F$ ve $JB|F$ olduğundan $JA|JX$ ve $JB|JX$ olur. Buradan $A|X$ ve $B|X$ elde edilir. O halde $[A, B]|X$ 'dır. Yani $E|X$ elde edilir. Buradan $JE|JX$ dolayısıyla $JE|F$ olur.

O halde $F|JE$ ve $JE|F$ olduğundan $JE=F$ elde edilir.

Teorem 3.21. D bir Dedekind bölgesi ve A, B idealler olsun. Bu takdirde $A, B = AB$ 'dir.

İspat. $J=(A, B)$ olsun. O zaman $A=JA_1$, $B=JB_1$, $(A_1, B_1)=D$ olan A_1, B_1 idealleri vardır. Dolayısıyla Teorem 3.20, Teorem 3.11 ve Teorem 3.12 kullanılırsa

$$A, B = [JA_1, JB_1]J = JJ[A_1, B_1] = JJ(A_1 \cap B_1) = JJA_1B_1 = JA_1JB_1 = AB$$

elde edilir.

Teorem 3.22. D bir Dedekind bölgesi, A, B, C idealler olsun. Bu takdirde $(A, BC) = (A, B(A, C))$ 'dir.

İspat. $E=(A, BC)$, $J=(A, C)$ ve $F=(A, BJ)$ olsun. $E=F$ olduğu gösterilecek. $J=(A, C)$ olduğundan $J|A$ ve $J|C$ olur. İkinci ifadeden $BJ|BC$ elde edilir. $F=(A, BJ)$ olduğundan $F|A$ ve $F|BJ$ olur. $F|BJ$ ve $BJ|BC$ olduğundan $F|BC$ 'dir. $F|A$ ve $F|BC$ olduğundan $F|(A, BC)$ 'dir. Yani $F|E$ elde edilir.

Şimdi $E = (A, BC)$ olduğundan $E | A$ ve $E | BC$ 'dir. O zaman $E | AB + BC$ olur. Ayrıca $J = (A, C)$ olduğundan $J = A + C$ 'dir. Buradan $JB = AB + BC$ elde edilir. $E | AB + BC$ ve $JB = AB + BC$ idi. O zaman $E | JB$ olur. Böylece $E | A$ ve $E | JB$ olduğundan $E | (A, BJ)$ elde edilir. Yani $E | F$ 'dir. Dolayısıyla $F | E$ ve $E | F$ olduğundan $E = F$ 'dir.

Teorem 3.23. D bir Dedekind bölgesi, A, B, C idealler ve $(B, C) = D$ olsun. Bu takdirde $(A, BC) = (A, B)(A, C)$ 'dir.

İspat. $(A, BC) = (A, (A, B)C) = (A, C(A, B)) = (A, (A, C)(A, B))$ 'dir. $(A, B) | A$, $(A, C) | A$ ve $((A, C), (A, B)) = D$ olduğundan $(A, C)(A, B) | A$ elde edilir. O zaman $(A, (A, C)(A, B)) = (A, C)(A, B)$ elde edilir.

Teorem 3.24. D bir Dedekind bölgesi, A, B, C, T idealler, $(A, B) = D$ ve $AB = CT^n$ ($n \geq 2$) olsun. Bu takdirde $A = A_1T_1^n$, $B = B_1T_2^n$, $A_1B_1 = C$, $T_1T_2 = T$ olacak biçimde A_1, B_1, T_1, T_2 idealleri vardır.

İspat. $A_1 = (A, C)$, $B_1 = (B, C)$ olsun. O halde

$$A_1B_1 = (A, C)(B, C) = (AB, C) = (CT^n, C) = C$$

bulunur. Ayrıca $A_1 = (A, C)$, $B_1 = (B, C)$ olduğundan $A = A_1X$, $B = B_1Y$, $(X, Y) = D$ olacak biçimde X, Y idealleri vardır. $AB = CT^n$ olduğundan

$$CT^n = AB = A_1XB_1Y = A_1B_1XY = CXY$$

elde edilir. Buradan $XY = T^n$ olur. X ve Y aralarında asal olduğundan Teorem 3.19'a göre $X = T_1^n$, $Y = T_2^n$, $T_1 T_2 = T$ olacak biçimde T_1, T_2 idealleri vardır. O halde $A = A_1 X = A_1 T_1^n$, $B = B_1 Y = B_1 T_2^n$ elde edilir.

Teorem 3.25. D bir Dedekind bölgesi olsun. D 'nin tek türlü çarpanlarına ayrılabilir bölge olmasının gerek ve yeter koşulu D 'nin esas ideal bölgesi olmasıdır [1].

Teorem 3.26. K derecesi n olan bir cebirsel sayı cismi olsun. K 'nın tamsayılar halkası O_K olsun. O_K 'nin sıfırdan farklı bir ideali A olsun. Bu takdirde

$$N(A) = \text{kard} \left(\frac{O_K}{A} \right)$$

dir [1].

Tanım 3.9. K derecesi n olan bir cebirsel sayı cismi olsun. $\alpha \in K$ olsun. $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ 'ler α 'nın K eşlenikleri olsun. Bu takdirde α 'nın normu $N(\alpha)$ ile gösterilir ve

$$N(\alpha) = \alpha_1 \alpha_2 \dots \alpha_n$$

olarak tanımlanır [1].

Teorem 3.27. K derecesi n olan bir cebirsel sayı cismi olsun. $\alpha, \beta \in K$ olsun. Bu takdirde

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

dir [1].

Teorem 3.28. K derecesi n olan bir cebirsel sayı cismi olsun.

- a. Eğer α sayısı O_K 'nin bir birimi ise $N(\alpha) = \pm 1$ 'dir.
- b. Eğer $\alpha \in O_K$ ve $N(\alpha) = \pm 1$ ise α sayısı O_K 'nin bir birimidir [1].

Teorem 3.29. K derecesi n olan bir cebirsel sayı cismi olsun. $\alpha \in O_K$ için, p bir asal sayı olmak üzere

$$N(\alpha) = \pm p$$

ise α sayısı O_K 'da indirgenemezdir [1].

Teorem 3.30. K derecesi n olan bir cebirsel sayı cismi ve $\alpha \in O_K$ olsun. Bu takdirde

$$N(\langle \alpha \rangle) = |N(\alpha)|$$

dir [1].

Teorem 3.31. K derecesi n olan bir cebirsel sayı cismi ve $\alpha \in K$ olsun.

$$\text{ind}_{\mathbb{Q}}(\alpha) = x^m + b_{m-1}x^{m-1} + \dots + b_0 \in \mathbb{Q}[x]$$

olsun. Bu takdirde

$$N(\langle \alpha \rangle) = |b_0|^{n/m}$$

dir [1].

Örnek 3.1. $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ olsun. $N(\langle \sqrt{2} \rangle)$ 'yi bulalım. $\sqrt{2}$ sayısının $\mathbb{Q}$ 'daki minimal polinomu $x^2 - 2$ 'dir. O halde Teorem 3.31'deki gösterimler ile $n=4$, $m=2$, $b_1=0$, $b_0=-2$ elde edilir. Dolayısıyla Teorem 3.31'e göre

$$N(\langle \sqrt{2} \rangle) = |-2|^{4/2} = 2^2 = 4$$

elde edilir.

Teorem 3.33. K bir cebirsel sayı cismi olsun. A ve B 'ler $D = O_K$ 'nin sıfırdan farklı tam idealleri olsun. Bu takdirde

$$N(AB) = N(A)N(B)$$

dir [1].

Tanım 3.10. K bir cebirsel sayı cismi olsun. K 'nin tamsayılar halkası O_K olsun. A , O_K 'nin sıfırdan farklı bir kesir ideali olsun. Bu takdirde

$$A = \frac{1}{\alpha} I$$

olacak biçimde O_K 'nin sıfırdan farklı bir I tam ideal ve O_K 'nin sıfırdan farklı bir α elemanı vardır. $N(I)$ ve $N(\langle \alpha \rangle)$ 'lar sırasıyla I ve $\langle \alpha \rangle$ ideallerinin normu olmak üzere A kesir idealinin normu $N(A)$,

$$N(A) = \frac{N(I)}{N(\langle \alpha \rangle)}$$

ile tanımlanır [1].

Teorem 3.34. K bir cebirsel sayı cismi olsun. K 'nin tamsayılar halkası O_K olsun.

A ve B 'ler O_K 'nin sıfırdan farklı kesir idealleri olsun. Bu takdirde

$$N(AB) = N(A)N(B)$$

dir [1].

Örnek 3.2. $K = \mathbb{Q}(\sqrt{6})$ olsun. O zaman $O_K = \{a + b\sqrt{6} \mid a, b \in \mathbb{Z}\}$ olur. A , O_K nin

$$A = \left\langle 1, \frac{1}{2}\sqrt{6} \right\rangle$$

ile verilen kesir ideali olsun. Bu takdirde $I = \langle 2, \sqrt{6} \rangle$ tam ideal olmak üzere

$$A = \frac{1}{2}I$$

dır. O halde

$$I^2 = \langle 2, \sqrt{6} \rangle^2 = \langle 4, 2\sqrt{6}, 6 \rangle = \langle 2 \rangle \langle 2, \sqrt{6}, 3 \rangle = \langle 2 \rangle$$

dır. Böylece

$$N(I)^2 = N(I^2) = N(\langle 2 \rangle) = 2^2$$

elde edilir. Dolayısıyla

$$N(I) = 2$$

olur. O halde

$$N(A) = N\left(\frac{1}{2}I\right) = \frac{N(I)}{N(\langle 2 \rangle)} = \frac{2}{2^2} = \frac{1}{2}$$

bulunur.

Teorem 3.35. K bir cebirsel sayı cismi olsun. O_K 'nin bir asal ideali P olsun. Bu takdirde

$$P \mid \langle p \rangle$$

olacak biçimde tek türlü belirli bir p asal sayısı vardır [1].

İspat. P , O_K 'nin bir asal ideali olduğundan, Teorem 1.17'ye göre $P \cap \mathbb{Z}$ kümesi $\mathbb{Z}$ de bir asal idealdir. O halde, Teorem 1.19 ve Teorem 1.6'ya göre bir p asal sayısı

$$P \cap \mathbb{Z} = \langle p \rangle$$

olacak biçimde vardır. Dolayısıyla

$$P \supseteq \langle p \rangle$$

olur. Böylece Teorem 3.7'ye göre

$$P \mid \langle p \rangle$$

elde edilir. Şimdi kabul edelim ki q sayısı

$$P \mid \langle q \rangle$$

olacak biçimde başka bir asal sayı olsun. Bu takdirde $P \supseteq \langle p \rangle$ ve $P \supseteq \langle q \rangle$ olacağından

$$P \supseteq \langle p, q \rangle$$

olur. p ve q 'lar farklı asal sayılar olduklarından $\text{ebob}(p, q) = 1$ olur. Dolayısıyla $ap + bq = 1$ olacak biçimde a, b tamsayıları vardır. O zaman $1 \in \langle p, q \rangle \subseteq P$ olur. Dolayısıyla $O_K \subseteq P$ elde edilir ki bu mümkün değildir. O halde $P \mid \langle p \rangle$ olacak biçimdeki p asal sayısı tek türlü belirlidir.

Tanım 3.11. K bir cebirsel sayı cismi olsun. O_K 'nin bir asal ideali P olsun.

$$P \mid \langle p \rangle$$

olacak biçimde tek türlü belirli bir asal sayı p olsun. Bu p asal sayısına P 'nin altında bulunan asal, P idealine ise p 'nin üzerinde bulunan ideal denir [1].

Teorem 3.36. K derecesi n olan bir cebirsel sayı cismi olsun. P , O_K 'nin bir asal ideali olsun. p , P 'nin altında bulunan asal olsun. Bu takdirde

$$N(P) = p^f$$

olacak biçimde $f \in \{1, 2, \dots, n\}$ tamsayısı vardır [1].

İspat. p , P 'nin altında bulunan asal olduğundan $P \mid \langle p \rangle$ 'dir. O halde O_K 'nin bir Q tam ideali $\langle p \rangle = PQ$ olacak biçimde vardır. Teorem 3.33 kullanılırsa

$$N(\langle p \rangle) = N(PQ) = N(P)N(Q)$$

elde edilir. Teorem 2.36'ya göre p 'nin K eşlenikleri n kere tekrarlanan p 'lerden oluştuğundan

$$N(p) = p^n$$

olur. Böylece Teorem 3.30 kullanılırsa

$$N(\langle p \rangle) = |N(p)| = p^n$$

bulunur. O halde

$$p^n = N(P)N(Q)$$

olur ki bu da bir $f \in \{1, 2, \dots, n\}$ için

$$N(P) = p^f$$

demektir.

Tanım 3.12. K derecesi n olan bir cebirsel sayı cismi olsun. P , O_K 'nin bir asal ideali olsun. p , P 'nin altında bulunan asal olsun. Bu takdirde $N(P) = p^f$ olacak biçimdeki pozitif f tamsayısına P 'nin O_K 'daki inertial derecesi veya eylemsizlik derecesi denir ve bu $f_K(P)$ ile gösterilir [1].

Teorem 3.26 ve Teorem 3.36'dan dolayı $\text{kard}(O_K/P) = p^f$ olduğu görülür. Yani O_K/P bir sonlu cisimdir ve p^f elemanı vardır. O_K/P 'nin bir $a+P$ ($a \in \mathbb{Z}$) elemanını ele alalım. $a, a' \in \mathbb{Z}$ için $a \equiv a' \pmod{p}$ ise $p \mid a - a'$ olur. Böylece $\langle p \rangle \mid \langle a - a' \rangle$ elde edilir. Fakat $P \mid \langle p \rangle$ idi. O zaman $P \mid \langle a - a' \rangle$ olur. Dolayısıyla $a \equiv a' \pmod{P}$ olur. Yani $a+P = a'+P$ olur. Tersine $a+P = a'+P$ ($a, a' \in \mathbb{Z}$) olduğunu kabul edelim. Bu takdirde $a - a' \in P$ ve $\langle a - a' \rangle \subseteq P$ elde edilir. Buradan $P \mid \langle a - a' \rangle$ olur. O zaman

$$\langle a - a' \rangle = PQ$$

olacak biçimde O_K 'nin bir Q tam ideali vardır. İki tarafında normu alınırsa

$$|a - a'|^n = N(\langle a - a' \rangle) = N(PQ) = N(P)N(Q) = p^f N(Q)$$

olur. Buradan $p \mid (a - a')^n$ elde edilir. p bir asal sayı olduğundan, $p \mid a - a'$ olur.

Buradan $a \equiv a' \pmod{p}$ olduğu görülür. Dolayısıyla $a, a' \in \mathbb{Z}$ için $a+P = a'+P \Leftrightarrow a \equiv a' \pmod{p}$

elde edilir. Dolayısıyla $a + P$ ($a \in \{0, 1, 2, \dots, p-1\}$) sınıfları birbirinden farklıdır ve O_K/P 'nin asal cismi

$$F = \{a + P \mid a = 0, 1, 2, \dots, p-1\}$$

dir.

Eğer $f_K(P) = 1$ ise $[O_K/P : F] = 1$ olur. Böylece $O_K/P = F$ olur. Yani

$$O_K/P = \{a + P \mid a = 0, 1, 2, \dots, p-1\}$$

olur. $\alpha \in O_K$ olsun. Bu takdirde $\alpha + P \in O_K$ 'dir. Böylece bir $a \in \{0, 1, 2, \dots, p-1\}$ için $\alpha + P = a + P$ olur. O halde $f_K(P) = 1$ ise bir $a \in \mathbb{Z}$ için $\alpha \equiv a \pmod{p}$ 'dir.

Teorem 3.37. K derecesi n olan bir cebirsel sayı cismi olsun. p bir asal sayı olsun. $\langle p \rangle$ esas ideali O_K 'da

$$\langle p \rangle = P_1^{e_1} P_2^{e_2} \dots P_g^{e_g}$$

biçiminde çarpanlarına ayrılsın. Burada $P_1, P_2, \dots, P_g$ 'ler O_K 'da birbirlerinden farklı asal idealler ve $e_1, e_2, \dots, e_g$ 'ler pozitif tamsayılardır. f_i 'ler P_i 'lerin ($i = 1, 2, \dots, g$) K 'daki eylemsizlik dereceleri olsun. Yani $f_i = f_K(P_i)$ olsun. Bu takdirde

$$e_1 f_1 + e_2 f_2 + \dots + e_g f_g = n$$

dir [1].

İspat. f_i 'ler P_i 'lerin K 'daki eylemsizlik dereceleri olduklarından $N(P_i) = p^{f_i}$ ($i = 1, 2, \dots, g$) elde edilir. Böylece

$$\begin{aligned}
 p^n &= N(\langle p \rangle) = N(P_1^{e_1} P_2^{e_2} \dots P_g^{e_g}) = N(P_1)^{e_1} N(P_2)^{e_2} \dots N(P_g)^{e_g} \\
 &= (p^{f_1})^{e_1} (p^{f_2})^{e_2} \dots (p^{f_g})^{e_g} = p^{f_1 e_1 + f_2 e_2 + \dots + f_g e_g}
 \end{aligned}$$

olur. O halde

$$f_1 e_1 + f_2 e_2 + \dots + f_g e_g = n$$

dir.

Teorem 3.37'ye göre $i = 1, 2, \dots, g$ olmak üzere $e_i \in \{1, 2, \dots, n\}$, $f_i \in \{1, 2, \dots, n\}$ olduğunu belirtelim. Ayrıca yine aynı teoreme göre P asal ideali için $P^n | \langle p \rangle$ ise $\langle p \rangle = P^n$ olduğu görülür.

Tanım 3.13. K derecesi n olan bir cebirsel sayı cismi ve p bir asal sayı olsun. $\langle p \rangle$ esas ideali O_K 'da

$$\langle p \rangle = P_1^{e_1} P_2^{e_2} \dots P_g^{e_g}$$

biçiminde çarpanlarına ayrılsın. Burada $P_1, P_2, \dots, P_g$ 'ler O_K 'da birbirlerinden farklı asal idealler ve $e_1, e_2, \dots, e_g$ 'ler pozitif tamsayılardır. Buradaki g pozitif tamsayısına p 'nin K 'daki parçalanma sayısı denir ve bu $g_K(p)$ ile gösterilir [1].

Teorem 3.38. K derecesi n olan bir cebirsel sayı cismi olsun. p bir asal sayı olsun. Bu takdirde $g_K(p) \leq n$ dir [1].

İspat. Teorem 3.37'deki gösterimler ile; $e_1, e_2, \dots, e_g, f_1, f_2, \dots, f_g$ 'ler pozitif tamsayılar olduklarından

$$n = e_1 f_1 + e_2 f_2 + \dots + e_g f_g \geq 1 + 1 + \dots + 1 = g$$

elde edilir.

Bu teoreme göre, derecesi n olan bir cebirsel sayı cismindeki p asal sayısı için $\langle p \rangle$ esas ideali en fazla n tane farklı asal idealin kuvveti biçimde çarpanlarına ayrılabilir.

Tanım 3.14. K derecesi n olan bir cebirsel sayı cismi olsun. P , O_K 'nin bir asal ideali olsun. p , P 'nin altında bulunan asal sayı olsun. Bu takdirde

$$P^e \mid \langle p \rangle, P^{e+1} \nmid \langle p \rangle$$

olacak biçimdeki tek türlü belirli e pozitif tamsayısına P 'nin K 'daki dallanma indeksi denir ve bu $e_K(P)$ ile gösterilir [1].

Teorem 3.37'ye göre $e_K(P) \leq n$ olduğu görülür. Ayrıca Teorem 3.37'deki gösterimler ile

$$e_K(P_i) = e_i, f_K(P_i) = f_i, g_K(p) = g$$

elde edilir.

Tanım 3.15. K derecesi n olan bir cebirsel sayı cismi ve p bir asal sayı olsun. $P_1, P_2, \dots, P_g$ 'ler O_K 'da p 'nin üzerinde bulunan asal idealler olsun. Bu takdirde

$$e_i = e_K(P_i), i = 1, 2, \dots, g$$

olmak üzere

$$\langle p \rangle = P_1^{e_1} P_2^{e_2} \dots P_g^{e_g}$$

dir. $e_i > 1$ olan $i \in \{1, 2, \dots, g\}$ varsa p 'ye K 'da dallanır denir. Her $i = 1, 2, \dots, g$ için $e_i = 1$ ise p 'ye K 'da dallanmaz denir [1].

Teorem 3.39. K bir cebirsel sayı cismi olsun. Bu takdirde p asal sayısının K 'da dallanmasının gerek ve yeter koşulu $p \mid d(K)$ olmasıdır [1].

Teorem 3.40. K bir cebirsel sayı cismi olsun. $I(\neq \langle 0 \rangle)$ O_K 'nın bir ideali olsun.

- a. p bir asal olmak üzere $N(I) = p$ ise I bir asal idealdir.
- b. $N(I) \in I$ 'dir [1].

Teorem 3.40'a göre bir cebirsel sayı cisminin tamsayılar halkasındaki her I ideali için $N(I) \in I$ olduğundan, $\langle N(I) \rangle \subseteq I$ 'dir. Dolayısıyla $I \mid \langle N(I) \rangle$ elde edilir.

Teorem 3.41. K bir kuadratik cisim olsun. O halde $K = \mathbb{Q}(\sqrt{m})$ olacak biçimde bir karesiz m tamsayısı vardır. p bir asal sayı olsun.

- a. Eğer $p > 2$, $\left(\frac{m}{p}\right) = 1$ veya $p = 2$, $m \equiv 1 \pmod{8}$ ise P_1 ve P_2 'ler birbirlerinden farklı asal idealler ve $N(P_1) = N(P_2) = p$ olmak üzere $\langle p \rangle = P_1 P_2$ 'dir.
- b. Eğer $p > 2$, $p \mid m$ veya $p = 2$, $m \equiv 2, 3 \pmod{4}$ ise P bir asal ideal ve $N(P) = p$ olmak üzere $\langle p \rangle = P^2$ 'dir.
- c. Eğer $p > 2$, $\left(\frac{m}{p}\right) = -1$ veya $p = 2$, $m \equiv 5 \pmod{8}$ ise $\langle p \rangle$, O_K 'nın bir asal idealidir [1].

İspat. m karesiz olduğundan $m \equiv 1, 2, 3 \pmod{4}$ elde edilir. Yedi durum ele alınacaktır.

1. $p > 2$, $\left(\frac{m}{p}\right) = 1$ olsun. $\left(\frac{m}{p}\right) = 1$ olduğundan $a^2 \equiv m \pmod{p}$ olacak

biçimde $a \in \mathbb{Z}$ vardır. $p \nmid m$ olduğundan $p \nmid a$ elde edilir. $P_1 = \langle p, a + \sqrt{m} \rangle$

ve $P_2 = \langle p, a - \sqrt{m} \rangle$ olsun. Öncelikle $P_1 \neq P_2$ olduğunu gösterelim. Aksine

$P_1 = P_2$ olsun. Bu takdirde $2a = (a + \sqrt{m}) + (a - \sqrt{m}) \in P_1$ olur. Fakat

$2a \in \mathbb{Z}$ 'dir. O zaman $2a \in P_1 \cap \mathbb{Z} = \langle p \rangle$ olur. O halde $p \mid 2a$ 'dır. Bu ise

çelişkidir. Çünkü p tek ve $p \nmid a$ idi. Şimdi $\langle p \rangle = P_1 P_2$ olduğunu gösterelim.

$$\begin{aligned} P_1 P_2 &= \langle p, a + \sqrt{m} \rangle \langle p, a - \sqrt{m} \rangle = \langle p^2, p(a + \sqrt{m}), p(a - \sqrt{m}), a^2 - m \rangle \\ &= \langle p \rangle \left\langle p, a + \sqrt{m}, a - \sqrt{m}, \frac{(a^2 - m)}{p} \right\rangle = \langle p \rangle I \end{aligned}$$

olur. Buradaki I ideali

$$I = \left\langle p, a + \sqrt{m}, a - \sqrt{m}, \frac{(a^2 - m)}{p} \right\rangle$$

dir. $\text{ebob}(2a, p) = 1$ olduğundan

$$xp + y(2a) = 1$$

olacak biçimde x ve y tamsayıları vardır. Dolayısıyla

$$1 = xp + y(a + \sqrt{m}) + y(a - \sqrt{m}) \in I$$

olacağından $I = \langle 1 \rangle$ olur. Bu da $\langle p \rangle = P_1 P_2$ olduğunu gösterir. O halde bu durum (a) şikkına tekabül eder.

2. $p > 2$, $\left(\frac{m}{p}\right) = -1$ olsun. $\langle p \rangle = P_1 P_2$, $(P_1 \neq P_2)$ veya $\langle p \rangle = P_1^2$ olduğunu

kabul edelim. İki durumda da $N(P_1) = p$ olur. Böylece $f_K(P_1) = 1$ elde

edilir. O halde $\sqrt{m} \in O_K$ olduğundan

$$\sqrt{m} \equiv a \pmod{P_1}$$

olacak biçimde $a \in \mathbb{Z}$ vardır. Böylece

$$m \equiv a^2 \pmod{P_1}$$

olur. Fakat $m \in \mathbb{Z}$, $a^2 \in \mathbb{Z}$ ve $P_1 \mid \langle p \rangle$ olduğundan

$$m \equiv a^2 \pmod{p}$$

olmalıdır ki bu $\left(\frac{m}{p}\right) = -1$ olması ile çelişir. O halde $\langle p \rangle$, O_K 'da bir asal

idealdir. Bu durum (c) şıkkına tekabül eder.

3. $p > 2$, $p \mid m$ olsun. $P = \langle p, \sqrt{m} \rangle$ alınsın. Bu takdirde

$$P^2 = \langle p, \sqrt{m} \rangle \langle p, \sqrt{m} \rangle = \langle p^2, p\sqrt{m}, m \rangle = \langle p \rangle \left\langle p, \sqrt{m}, \frac{m}{p} \right\rangle = \langle p \rangle I$$

olur. Buradaki I ideali,

$$I = \left\langle p, \sqrt{m}, \frac{m}{p} \right\rangle$$

dir. m karesiz olduğunda, $\text{ebob}\left(p, \frac{m}{p}\right) = 1$ elde edilir. Böylece

$$xp + y\left(\frac{m}{p}\right) = 1$$

olacak biçimde x ve y tamsayıları vardır. O halde

$$1 = xp + y\left(\frac{m}{p}\right) \in I$$

olur. Böylece $I = \langle 1 \rangle$ olur. Yani $\langle p \rangle = P^2$ 'dir. Bu durum (b) şıkkına tekabül eder.

4. $p = 2$, $m \equiv 2 \pmod{4}$ olsun. $P = \langle 2, \sqrt{m} \rangle$ alınsın. Bu takdirde

$$P^2 = \langle 2, \sqrt{m} \rangle \langle 2, \sqrt{m} \rangle = \langle 4, 2\sqrt{m}, m \rangle = \langle 2 \rangle I$$

olur. Buradaki I ideali

$$I = \left\langle 2, \sqrt{m}, \frac{m}{2} \right\rangle$$

dir. $\frac{m}{2}$ tek olduğundan $\frac{m}{2} = 2k+1$, $k \in \mathbb{Z}$ olsun. O zaman

$$1 = (-k)2 + (1)\frac{m}{2} \in I$$

elde edilir. Böylece $I = \langle 1 \rangle$ olur. Yani $\langle p \rangle = P^2$ olur. Bu durum (b) şıkkına tekabül eder.

5. $p = 2$, $m \equiv 3 \pmod{4}$ olsun. $P = \langle 2, 1 + \sqrt{m} \rangle$ alınsın. $1 - \sqrt{m} = 2 - (1 + \sqrt{m})$

olduğundan $P = \langle 2, 1 - \sqrt{m} \rangle$ olduğu görülür. Bu takdirde

$$P^2 = \langle 2, 1 + \sqrt{m} \rangle \langle 2, 1 - \sqrt{m} \rangle = \langle 4, 2(1 + \sqrt{m}), 2(1 - \sqrt{m}), 1 - m \rangle = \langle 2 \rangle I$$

olur. Buradaki I ideali

$$I = \left\langle 2, 1 + \sqrt{m}, 1 - \sqrt{m}, \frac{1-m}{2} \right\rangle$$

dir. $m \equiv 3 \pmod{4}$ olduğundan, $\frac{1-m}{2}$ bir tek tamsayıdır ve $I = \langle 1 \rangle$ olur. O

halde $\langle 2 \rangle = P^2$ 'dir. Bu durum (b) şıkkına tekabül eder.

6. $p = 2$, $m \equiv 1 \pmod{8}$ olsun. $P_1 = \left\langle 2, \frac{1+\sqrt{m}}{2} \right\rangle$ ve $P_2 = \left\langle 2, \frac{1-\sqrt{m}}{2} \right\rangle$ olsun.

Dolayısıyla

$$P_1 P_2 = \left\langle 2, \frac{1+\sqrt{m}}{2} \right\rangle \left\langle 2, \frac{1-\sqrt{m}}{2} \right\rangle = \left\langle 4, 2\left(\frac{1+\sqrt{m}}{2}\right), 2\left(\frac{1-\sqrt{m}}{2}\right), \frac{1-m}{4} \right\rangle = \langle 2 \rangle I$$

olur. Buradaki I ideali,

$$I = \left\langle 2, \frac{1+\sqrt{m}}{2}, \frac{1-\sqrt{m}}{2}, \frac{1-m}{8} \right\rangle$$

dir. Ayrıca

$$1 = \frac{1+\sqrt{m}}{2} + \frac{1-\sqrt{m}}{2} \in I$$

dır. Böylece $I = \langle 1 \rangle$ olur. Dolayısıyla $\langle 2 \rangle = P_1 P_2$ elde edilir. $P_1 = P_2$ ise

$$1 = \frac{1+\sqrt{m}}{2} + \frac{1-\sqrt{m}}{2} \in P_1$$

olur ki bu mümkün değildir. Bu durum (a) şıkkına tekabül eder.

7. $p = 2$, $m \equiv 5 \pmod{8}$ olsun. $\langle 2 \rangle = P_1 P_2$, $(P_1 \neq P_2)$ veya $\langle 2 \rangle = P_1^2$ olsun. Bu takdirde, iki durumda da $N(P_1) = 2$ elde edilir. Buradan $f_K(P_1) = 1$ olduğu

görülr. O halde $\frac{1+\sqrt{m}}{2} \in O_K$ olduğundan,

$$\frac{1+\sqrt{m}}{2} \equiv a \pmod{P_1}$$

olacak biçimde bir a rasyonel tamsayısı vardır. Dolayısıyla

$$\frac{1-\sqrt{m}}{2} = 1 - \left(\frac{1+\sqrt{m}}{2} \right) \equiv 1-a \pmod{P_1}$$

dir. Buradan

$$\frac{1-m}{4} = \left(\frac{1+\sqrt{m}}{2} \right) \left(\frac{1-\sqrt{m}}{2} \right) \equiv a(1-a) \pmod{P_1}$$

olduğu görölür. $\frac{1-m}{4} \in \mathbb{Z}$, $a(1-a) \in \mathbb{Z}$ ve $P_1 | \langle 2 \rangle$ olduğundan

$$\frac{1-m}{4} \equiv a(1-a) \pmod{2}$$

elde edilir. Dolayısıyla

$$\frac{1-m}{4} \equiv 0 \pmod{2}$$

dır. Böylece $m \equiv 1 \pmod{8}$ olur ki bu $m \equiv 5 \pmod{8}$ olmasıyla çelişir. O

halde $\langle 2 \rangle$, O_K 'da eylemsiz kalır ve bu durum (c) şıkkına tekabül eder.

Teorem 3.41'nin ispatından şu sonuçlar elde edilir. m karesiz bir tamsayı olmak üzere $K = \mathbb{Q}(\sqrt{m})$ kuadratik cismi verildiğinde, p bir asal sayı olmak üzere $\langle p \rangle$ esas idealinin O_K 'nın asal ideallerinin çarpımı biçiminde ifade edilişleri aşağıdaki gibidir:

$$\langle 2 \rangle = \begin{cases} \langle 2 \rangle & , \quad m \equiv 5 \pmod{8} \text{ ise} \\ \left\langle 2, \frac{1}{2}(1+\sqrt{m}) \right\rangle \left\langle 2, \frac{1}{2}(1-\sqrt{m}) \right\rangle & , \quad m \equiv 1 \pmod{8} \text{ ise} \\ \langle 2, 1+\sqrt{m} \rangle^2 & , \quad m \equiv 3 \pmod{8} \text{ ise} \\ \langle 2, \sqrt{m} \rangle^2 & , \quad m \equiv 2 \pmod{8} \text{ ise} \end{cases}$$

ve $p > 2$ için

$$\langle p \rangle = \begin{cases} \langle p \rangle & , \quad p \nmid m \text{ ve } x^2 \equiv (\text{mod } p) \text{ nin çözümü yok ise} \\ \langle p, x+\sqrt{m} \rangle \langle p, x-\sqrt{m} \rangle & , \quad p \nmid m \text{ ve } x^2 \equiv (\text{mod } p) \text{ nin çözümü var ise} \\ \langle p, \sqrt{m} \rangle^2 & , \quad p \mid m \text{ ise} \end{cases}$$

Tanım 3.16. d bir karesiz tamsayı ve $d \equiv 0,1 \pmod{4}$ olsun. $\left(\frac{d}{2}\right)$ Kronecker sembolü

$$\left(\frac{d}{2}\right) = \begin{cases} 0 & , \quad d \equiv 0 \pmod{4} \text{ ise} \\ 1 & , \quad d \equiv 1 \pmod{4} \text{ ise} \\ -1 & , \quad d \equiv 5 \pmod{4} \text{ ise} \end{cases}$$

olarak tanımlanır.

Kronecker sembolü ile Teorem 3.41 aşağıdaki gibi yeniden ifade edilebilir.

Teorem 3.42. K bir kuadratik cisim olsun. $d = d(K)$ olsun. p bir asal sayı olsun.

Bu takdirde $\left(\frac{d}{p}\right)$, $p > 2$ için Legendre sembolünü, $p = 2$ için Kronecker sembolünü göstermek üzere

- a. $\langle p \rangle$ parçalanır (denir) $\Leftrightarrow \left(\frac{d}{p}\right) = 1$
- b. $\langle p \rangle$ dallanır (denir) $\Leftrightarrow \left(\frac{d}{p}\right) = 0$
- c. $\langle p \rangle$ eylemsiz kalır (denir) $\Leftrightarrow \left(\frac{d}{p}\right) = -1$

Diğer bir deyişle,

- a. P_1, P_2 asal idealler olmak üzere $\langle p \rangle = P_1 P_2$ biçimindedir $\Leftrightarrow \left(\frac{d}{p}\right) = 1$
- b. P asal ideal olmak üzere $\langle p \rangle = P^2$ biçimindedir $\Leftrightarrow \left(\frac{d}{p}\right) = 0$
- c. $\langle p \rangle$ bir asal idealdir $\Leftrightarrow \left(\frac{d}{p}\right) = -1$

dir [1].

Örnek 3.3. Teorem 3.42'ye göre

1. $\left(\frac{-163}{11}\right) = \left(\frac{2}{11}\right) = -1$ olduğundan $\langle 11 \rangle$ ideali $\mathbb{Q}(\sqrt{-163})$ 'de eylemsiz kalır.
2. $\left(\frac{37}{23}\right) = \left(\frac{14}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) = (+1)(-1) = -1$ olduğundan $\langle 23 \rangle$ ideali $\mathbb{Q}(\sqrt{37})$ 'de eylemsiz kalır.
3. $\left(\frac{28}{2}\right) = 0$ olduğundan $\langle 2 \rangle$ ideali $\mathbb{Q}(\sqrt{7})$ 'de dallanır. Gerçekten $\langle 2 \rangle = \langle 2, 1 + \sqrt{7} \rangle^2$ 'dir.
4. $\left(\frac{28}{3}\right) = \left(\frac{1}{3}\right) = 1$ olduğundan $\langle 3 \rangle$ ideali $\mathbb{Q}(\sqrt{7})$ 'de parçalanır. Gerçekten $x^2 \equiv 7 \pmod{3}$ için $x=1$ bir çözüm olduğundan $\langle 3 \rangle = \langle 3, 1 + \sqrt{7} \rangle \langle 3, 1 - \sqrt{7} \rangle$ 'dir.

5. $\left(\frac{28}{7}\right) = 0$ olduğundan $\langle 7 \rangle$ ideali $\mathbb{Q}(\sqrt{7})$ 'de dallanır. Gerçekten $\langle 7 \rangle = \langle \sqrt{7} \rangle^2$ 'dir.

Teorem 3.43. $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ 'nin bütün birimleri $n \in \mathbb{Z}$ olmak üzere $\pm(1 + \sqrt{2})^n$ biçimindedir [1].

Teorem 3.44. m tamkare olmayan bir pozitif tamsayı olsun. Bu takdirde

$$x^2 - my^2 = 1$$

olacak biçimde $(x, y) \neq (1, 0)$ olan x ve y tamsayıları vardır [1].

Teorem 3.45. m bir pozitif karesiz tamsayı olsun. x ve y 'nin ikisi de tamsayı veya ikisi de tek tamsayıların yarısı olsun. $x^2 - my^2 = 1$ olsun. Bu takdirde

$$x > 0, y > 0 \Leftrightarrow x + y\sqrt{m} > 1,$$

$$x > 0, y < 0 \Leftrightarrow 0 < x + y\sqrt{m} < 1,$$

$$x < 0, y > 0 \Leftrightarrow -1 < x + y\sqrt{m} < 0,$$

$$x < 0, y < 0 \Leftrightarrow x + y\sqrt{m} < -1$$

özellikleri geçerlidir [1].

Tanım 3.17. m bir pozitif karesiz tamsayı olsun. $m = 2, 3 \pmod{4}$ ise

$$S_m = \left\{ (x, y) \mid x, y \in \mathbb{N} \right\}, \quad m = 1 \pmod{4} \text{ ise } S_m = \left\{ \left(\frac{x}{2}, \frac{y}{2} \right) \mid x, y \in \mathbb{N}, x \equiv y \pmod{2} \right\}$$

olsun. Teorem 3.44'e göre $a^2 - mb^2 = 1$ denkleminin (a, b) çözümü olduğunun garantisi vardır. $a^2 - mb^2 = 1$ denkleminin a 'sı en küçük olan çözümü $(a, b) \in S_m$

ve $\varepsilon = a + b\sqrt{m}$ olsun. Böylece ε sayısı $O_{\mathbb{Q}(\sqrt{m})}$ 'nin normu 1 olan bir birimidir. ε birimine $O_{\mathbb{Q}(\sqrt{m})}$ 'nin normu 1 olan temel birimi denir [1].

Bu tanıma göre, $m = 2, 3 \pmod{4}$ ise $\varepsilon \geq 1 + \sqrt{m} \geq 1 + \sqrt{2} > 1$ ve $m = 1 \pmod{4}$ ise

$$\varepsilon \geq \frac{1 + \sqrt{m}}{2} \geq \frac{1 + \sqrt{5}}{2} > 1$$

olduğu görülür. Dolayısıyla $\varepsilon > 1$ elde edilir.

Teorem 3.46. m bir pozitif karesiz tamsayı ve ε sayısı $O_{\mathbb{Q}(\sqrt{m})}$ 'nin normu 1 olan temel birimi olsun. Bu takdirde

- a. ε birimi $O_{\mathbb{Q}(\sqrt{m})}$ 'nin normu 1 olup da 1'den büyük olan en küçük birimidir.
- b. $O_{\mathbb{Q}(\sqrt{m})}$ 'nin normu 1 olan her birimi bir n tamsayısı için $\pm \varepsilon^n$ biçimindedir.
- c. Eğer τ sayısı $O_{\mathbb{Q}(\sqrt{m})}$ 'nin normu 1 olan bir birimi ve $\tau > 1$ ve $O_{\mathbb{Q}(\sqrt{m})}$ 'de normu 1 olan her birim bir k tamsayısı için $\pm \tau^k$ biçiminde ise o zaman $\tau = \varepsilon$ 'dir [1].

Teorem 3.47. m bir pozitif karesiz tamsayı olsun. $O_{\mathbb{Q}(\sqrt{m})}$ 'de normu -1 olan birimlerin bulunduğunu kabul edelim. Bu takdirde $O_{\mathbb{Q}(\sqrt{m})}$ 'de normu -1 olan tek türlü belirli bir $\sigma > 1$ birimi vardır ve $O_{\mathbb{Q}(\sqrt{m})}$ 'nin her birimi bir n tamsayısı için $\pm \sigma^n$ biçimindedir [1].

Tanım 3.18. m bir pozitif karesiz tamsayı olsun ve bu m için $O_{\mathbb{Q}(\sqrt{m})}$ 'de normu -1 olan birimler bulunsun. Normu -1 olup tek türlü belirli olan birim $\sigma > 1$ için

$O_{\mathbb{Q}(\sqrt{m})}$ 'nin her birimi $\pm\sigma^n$ ($n \in \mathbb{Z}$) biçimindedir. Bu σ birimine $O_{\mathbb{Q}(\sqrt{m})}$ 'nin normu -1 olan temel birimi denir [1].

Teorem 3.48. m bir pozitif karesiz tamsayı ve bu m için $O_{\mathbb{Q}(\sqrt{m})}$ 'de normu -1 olan birimler mevcut olsun. Bu takdirde normu 1 olan ε temel birimi ile normu -1 olan σ temel birimi için

$$\varepsilon = \sigma^2$$

bağıntısı geçerlidir [1].

Tanım 3.19. m bir pozitif karesiz tamsayı olsun. $O_{\mathbb{Q}(\sqrt{m})}$ 'nin temel birimi şöyle tanımlanır: $O_{\mathbb{Q}(\sqrt{m})}$ 'de normu -1 olan birimler varsa $\eta = \sigma$ 'dır. Burada σ , Tanım 3.18'de tanımlandığı gibi normu -1 olan temel birimdir. Normu -1 olan birimler yoksa $\eta = \varepsilon$ 'dur. Burada ε , Tanım 3.17'de tanımlandığı gibi normu 1 olan temel birimdir. Ayrıca $\mu > 1$ 'dir [1].

Teorem 3.49. m bir pozitif karesiz tamsayı olsun. Bu takdirde η , $O_{\mathbb{Q}(\sqrt{m})}$ 'nin temel birimi olmak üzere, $O_{\mathbb{Q}(\sqrt{m})}$ 'nin bütün birimleri $\pm\eta^n$ ($n \in \mathbb{Z}$) biçimindedir. $O_{\mathbb{Q}(\sqrt{m})}$ de normu -1 olan birimler var ise o zaman normu -1 olan birimler n tek olmak üzere $\pm\eta^n$ ve normu 1 olan birimler de n çift olmak üzere $\pm\eta^n$ biçimindedir [1].

Teorem 3.50. K bir reel kuadratik cisim olsun. Bu takdirde $U(O_K) \simeq \mathbb{Z}_2 \times \mathbb{Z}$ dir[1].

Teorem 3.51. K bir reel kuadratik cisim olsun. O_K 'nın temel birimi, O_K 'nın 1 'den büyük olan en küçük birimidir [1].

m karesiz pozitif bir tamsayı ve $2 \leq m \leq 40$ olmak üzere $O_{\mathbb{Q}(\sqrt{m})}$ 'nin ε , σ ve η değerleri Tablo 3.1 'de gösterilmiştir.

Tablo 3.1. $2 \leq m \leq 40$, m karesiz, $O_{\mathbb{Q}(\sqrt{m})}$ 'nin temel birimi [1].

m	Normu 1 olan temel birim ε	Normu -1 olan temel birim σ	Temel birim μ	Temel birimin normu $N(\mu)$
2	$3+2\sqrt{2}$	$1+\sqrt{2}$	$1+\sqrt{2}$	-1
3	$2+\sqrt{3}$		$2+\sqrt{3}$	1
5	$(3+\sqrt{5})/2$	$(1+\sqrt{5})/2$	$(1+\sqrt{5})/2$	-1
6	$5+2\sqrt{6}$		$5+2\sqrt{6}$	1
7	$8+3\sqrt{7}$		$8+3\sqrt{7}$	1
10	$19+6\sqrt{10}$	$3+\sqrt{10}$	$3+\sqrt{10}$	-1
11	$10+3\sqrt{11}$		$10+3\sqrt{11}$	1
13	$(11+3\sqrt{13})/2$	$(3+\sqrt{13})/2$	$(3+\sqrt{13})/2$	-1
14	$15+4\sqrt{14}$		$15+4\sqrt{14}$	1
15	$4+\sqrt{15}$		$4+\sqrt{15}$	1
17	$33+8\sqrt{17}$	$4+\sqrt{17}$	$4+\sqrt{17}$	-1
19	$170+39\sqrt{19}$		$170+39\sqrt{19}$	1
21	$(5+\sqrt{21})/2$		$(5+\sqrt{21})/2$	1

Tablo 3.1. (Devamı)

m	Normu 1 olan temel birim ε	Normu -1 olan temel birim σ	Temel birim μ	Temel birimin normu $N(\mu)$
22	$197+42\sqrt{22}$		$197+42\sqrt{22}$	1
23	$24+5\sqrt{23}$		$24+5\sqrt{23}$	1
26	$51+10\sqrt{26}$	$5+\sqrt{26}$	$5+\sqrt{26}$	-1
29	$(27+5\sqrt{29})/2$	$(5+\sqrt{29})/2$	$(5+\sqrt{29})/2$	-1
30	$11+2\sqrt{30}$		$11+2\sqrt{30}$	1
31	$1520+273\sqrt{31}$		$1520+273\sqrt{31}$	1
33	$23+4\sqrt{33}$		$23+4\sqrt{33}$	1
34	$35+6\sqrt{34}$		$35+6\sqrt{34}$	1
35	$6+\sqrt{35}$		$6+\sqrt{35}$	1
37	$73+12\sqrt{37}$	$6+\sqrt{37}$	$6+\sqrt{37}$	-1
38	$37+6\sqrt{38}$		$37+6\sqrt{38}$	1
39	$25+4\sqrt{39}$		$25+4\sqrt{39}$	1

Teorem 3.52. p bir asal ve $p \equiv 1 \pmod{4}$ olsun. Bu takdirde $O_{\mathbb{Q}(\sqrt{p})}$ 'nin temel biriminin normu -1 'dir [1].

Teorem 3.53. m bir pozitif karesiz tamsayı olsun. m sayısını bölen bir $q \equiv 3 \pmod{4}$ asal sayısı varsa $O_{\mathbb{Q}(\sqrt{m})}$ 'nin temel biriminin normu 1 'dir [1].

Teorem 3.54. p bir asal ve $p \equiv 5 \pmod{8}$ olsun. Bu takdirde $O_{\mathbb{Q}(\sqrt{2p})}$ 'nin temel biriminin normu -1 'dir [1].

Teorem 3.55. p ve q farklı asal sayılar ve $p \equiv q \equiv 1 \pmod{4}$, $\left(\frac{p}{q}\right) = -1$ olsun. Bu takdirde $O_{\mathbb{Q}(\sqrt{pq})}$ 'nin temel biriminin normu -1 'dir [1].

Tanım 3.20. K bir cebirsel sayı cismi olsun. O_K 'nin sıfırdan farklı tamsayı ve kesir ideallerinin grubu $I(K)$ ile gösterilsin. $I(K)$ 'nin esas idealleri $\alpha \in K - \{0\}$ olmak üzere $\langle \alpha \rangle = \{r\alpha \mid r \in O_K\}$ biçimindedir ve bunlar $I(K)$ 'nin $P(K)$ alt grubunu oluşturur. Çünkü $\langle \alpha \rangle, \langle \beta \rangle \in P(K)$ için $\langle \alpha \rangle \langle \beta \rangle^{-1} = \langle \alpha\beta^{-1} \rangle \in P(K)$ olur. $I(K)$ değişmeli grup olduğundan $P(K)$ bir normal altgruptur. Bu takdirde $I(K)/P(K)$ bölüm grubuna K 'nin ideal sınıf grubu denir ve $H(K)$ ile gösterilir [1].

Tanım 3.21. K bir cebirsel sayı cismi olsun. $H(K)$ ideal sınıf grubunun mertebesine K 'nin sınıf sayısı denir ve $h(K)$ ile gösterilir [1].

Tanım 3.22. K bir cebirsel sayı cismi olsun. O_K 'nin sıfırdan farklı A ve B iki ideali, $H(K) = I(K)/P(K)$ 'nin aynı sınıfında ise A ile B denktir denir ve $A \sim B$ yazılır. Bu durumda

$$\begin{aligned}
 A \sim B &\Leftrightarrow AP(K) = BP(K) \\
 &\Leftrightarrow A^{-1}B \in P(K) \\
 &\Leftrightarrow A^{-1}B = \langle \alpha \rangle \text{ olacak biçimde } \alpha \in K - \{0\} \text{ vardır.} \\
 &\Leftrightarrow B = A\langle \alpha \rangle \text{ olacak biçimde } \alpha \in K - \{0\} \text{ vardır.} \\
 &\Leftrightarrow \langle a \rangle A = \langle b \rangle B \text{ olacak biçimde } a, b \in O_K - \{0\} \text{ vardır.}
 \end{aligned}$$

Burada $\alpha \in K - \{0\}$ ise $a, b \in O_K - \{0\}$ olmak üzere $\alpha = \frac{a}{b}$ biçiminde yazıldığına dikkat edelim [1].

Örnek 3.4. $\mathbb{Q}(\sqrt{-5})$ 'de $\langle 2, 1 - \sqrt{-5} \rangle \sim \langle 3, 1 + \sqrt{-5} \rangle$ 'dir. Çünkü

$$\langle 3 \rangle \langle 2, 1 - \sqrt{-5} \rangle = \langle 6, 3(1 - \sqrt{-5}) \rangle = \langle (1 + \sqrt{-5})(1 - \sqrt{-5}), 3(1 - \sqrt{-5}) \rangle = \langle 1 - \sqrt{-5} \rangle \langle 1 + \sqrt{-5}, 3 \rangle$$

dir. $3, 1 - \sqrt{-5} \in O_{\mathbb{Q}(\sqrt{-5})}$ olduğundan $\langle 2, 1 - \sqrt{-5} \rangle \sim \langle 3, 1 + \sqrt{-5} \rangle$ elde edilir.

Teorem 3.56. K bir cebirsel sayı cismi olsun. Bu takdirde

$h(K) = 1 \Leftrightarrow O_K$ bir esas ideal bölgesidir. $\Leftrightarrow O_K$ bir tek türlü çarpanlarına ayrılabilir bölgedir [1].

Teorem 3.57. $K = \mathbb{Q}(\theta)$ derecesi n olan bir cebirsel sayı cismi olsun. θ 'nın reel eşleniklerinin sayısı r ve kompleks eşlenik çiftlerinin sayısı s olsun. O zaman K nin derecesi $n = r + 2s$ olur. $C \in H(K)$ olsun. Bu takdirde C 'de

$$N(B) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d(K)|}$$

olacak biçimde bir $B \neq \langle 0 \rangle$ tam ideali vardır [1].

Teorem 3.58. K bir cebirsel sayı cismi ve k bir pozitif tamsayı olsun. Bu takdirde O_K 'da normu k olan sadece sonlu sayıda A tam ideali vardır [1].

Teorem 3.59. K bir cebirsel sayı cismi olsun. Bu takdirde K 'nin ideal sınıf grubu $H(K)$ bir sonlu gruptur, dolayısıyla $h(K) = \text{kard}(H(K))$ sınıf sayısı sonludur[1].

Tanım 3.23. $K = \mathbb{Q}(\theta)$ derecesi n olan bir cebirsel sayı cismi olsun. θ 'nın reel eşleniklerinin sayısı r ve kompleks eşlenik çiftlerinin sayısı s olsun. O zaman $n = r + 2s$ olur. K için Minkowski sınırı M_K ile gösterilir ve

$$M_K = \left(\frac{2}{\pi}\right)^s \sqrt{|d(K)|}$$

ile verilir [1].

Teorem 3.58'e göre O_K 'da normu $N(B) \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d(K)|}$ olacak biçimde sonlu sayıda B tam ideali vardır. Böylece Teorem 3.57'ye göre her ideal sınıfı, sonlu bir kümeden seçilen O_K 'nın bir tam ideali ile temsil edilir. İdeal sınıflarının bu temsilcilerini belirlemek için, O_K 'nın normu M_K 'dan küçük veya eşit olan tam ideallerine bakmak yeterlidir. O_K 'nın A tam idealinin normu M_K 'dan küçük veya eşit ise $P|A$ olan her P asal ideali için $N(P) \leq M_K$ 'dir. Ayrıca P asal idealinin normu, p bir asal sayı ve f bir pozitif tamsayı olmak üzere $N(P) = p^f$ biçimindedir. O halde herhangi bir A tam idealinin asal çarpanlarına ayrılışında karşılaştığımız bütün asal idealler, $p \leq M_K$ olan asal sayıların çarpımlarından oluşur. Dolayısıyla $p \leq M_K$ olan her p asal sayısı alınıp, $\langle p \rangle$ 'nin O_K 'daki asal ideallerin çarpımı biçiminde yazılışları belirlenir ve bu belirlenen asal ideallerin normu M_K 'dan küçük veya eşit olan tüm olası çarpımları yazılırsa her ideal sınıfının en azından bir temsilcisi bulunmuş olur. Özellikle $p \leq M_K$ olan her p asal sayısı için $\langle p \rangle$ idealinin O_K 'daki asal ideallerin çarpımı biçiminde yazılışları hep bir esas ideal ise o

zaman K 'nın sınıf sayısı $h(K)=1$ dir. Bu durumda O_K 'da tanımlanan her ideal bir esas ideal olacağından O_K bir esas ideal bölgesi olur.

Örnek 3.5'den Örnek 3.8'e kadar kullanılan metodla bazı negatif k değerleri için Tablo 3.2 oluşturulabilir.

Tablo 3.2. $-30 < k < 0$, k karesiz, $H(\mathbb{Q}(\sqrt{k}))$ 'nın ideal sınıf grubları [1].

k	$H(\mathbb{Q}(\sqrt{k}))$
-5	$\{1, A\} \simeq \mathbb{Z}_2$, $A = \left[\left\langle 2, 1 + \sqrt{-5} \right\rangle \right]$, $A^2 = 1$
-6	$\{1, A\} \simeq \mathbb{Z}_2$, $A = \left[\left\langle 2, \sqrt{-6} \right\rangle \right]$, $A^2 = 1$
-10	$\{1, A\} \simeq \mathbb{Z}_2$, $A = \left[\left\langle 2, \sqrt{-10} \right\rangle \right]$, $A^2 = 1$
-13	$\{1, A\} \simeq \mathbb{Z}_2$, $A = \left[\left\langle 2, 1 + \sqrt{-13} \right\rangle \right]$, $A^2 = 1$
-14	$\{1, A, A^2, A^3\} \simeq \mathbb{Z}_4$, $A = \left[\left\langle 3, 1 + \sqrt{-14} \right\rangle \right]$, $A^2 = \left[\left\langle 2, \sqrt{-14} \right\rangle \right]$, $A^3 = \left[\left\langle 3, 1 - \sqrt{-14} \right\rangle \right]$, $A^4 = 1$
-15	$\{1, A\} \simeq \mathbb{Z}_2$, $A = \left[\left\langle 2, \frac{1}{2}(3 + \sqrt{-15}) \right\rangle \right]$, $A^2 = 1$
-17	$\{1, A, A^2, A^3\} \simeq \mathbb{Z}_4$, $A = \left[\left\langle 3, 1 + \sqrt{-17} \right\rangle \right]$, $A^2 = \left[\left\langle 2, 1 + \sqrt{-17} \right\rangle \right]$, $A^4 = 1$
-21	$\{1, A, B, AB\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, $A = \left[\left\langle 2, 1 + \sqrt{-21} \right\rangle \right]$, $B = \left[\left\langle 3, \sqrt{-21} \right\rangle \right]$, $AB = \left[\left\langle 5, 3 + \sqrt{-21} \right\rangle \right]$, $A^2 = B^2 = (AB)^2 = 1$
-22	$\{1, A\} \simeq \mathbb{Z}_2$, $A = \left[\left\langle 2, \sqrt{-22} \right\rangle \right]$, $A^2 = 1$

Tablo 3.2. (Devamı)

k	$H\left(\mathbb{Q}\left(\sqrt{k}\right)\right)$
-23	$\{1, A, A^2\} \simeq \mathbb{Z}_3, A = \left[\left\langle 2, \frac{1}{2}(1 + \sqrt{-23}) \right\rangle \right], A^2 = \left[\left\langle 2, \frac{1}{2}(1 - \sqrt{-23}) \right\rangle \right],$ $A^3 = 1$
-26	$\{1, A, A^2, A^3, A^4, A^5\} \simeq \mathbb{Z}_6, A = \left[\left\langle 5, 2 + \sqrt{-26} \right\rangle \right], A^2 = \left[\left\langle 3, 1 - \sqrt{-26} \right\rangle \right],$ $A^3 = \left[\left\langle 2, \sqrt{-26} \right\rangle \right], A^4 = \left[\left\langle 3, 1 + \sqrt{-26} \right\rangle \right], A^5 = \left[\left\langle 5, 2 - \sqrt{-26} \right\rangle \right],$ $A^6 = 1$
-29	$\{1, A, A^2, A^3, A^4, A^5\} \simeq \mathbb{Z}_6, A = \left[\left\langle 3, 1 + \sqrt{-29} \right\rangle \right], A^2 = \left[\left\langle 5, 1 + \sqrt{-26} \right\rangle \right],$ $A^3 = \left[\left\langle 2, 1 + \sqrt{-26} \right\rangle \right], A^4 = \left[\left\langle 5, 1 - \sqrt{-26} \right\rangle \right], A^5 = \left[\left\langle 3, 1 - \sqrt{-26} \right\rangle \right],$ $A^6 = 1$
-30	$\{1, A, B, AB\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2, A = \left[\left\langle 2, \sqrt{-30} \right\rangle \right], B = \left[\left\langle 3, \sqrt{-30} \right\rangle \right],$ $AB = \left[\left\langle 5, \sqrt{-30} \right\rangle \right], A^2 = B^2 = (AB)^2 = 1$

Tabloda yer almayan k değerleri için sınıf sayısı 1 dir.

Örnek 3.5’den Örnek 3.8’e kadar kullanılan metodla bazı pozitif k değerleri için Tablo 3.3 oluşturulabilir.

Tablo 3.3. $2 \leq k < 100$, k karesiz, $H\left(\mathbb{Q}\left(\sqrt{k}\right)\right)$ ’nın ideal sınıf grubları [1].

k	$H\left(\mathbb{Q}\left(\sqrt{k}\right)\right)$
10	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, \sqrt{10} \right\rangle \right], A^2 = 1$
15	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, 1 + \sqrt{15} \right\rangle \right], A^2 = 1$
26	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, \sqrt{26} \right\rangle \right], A^2 = 1$

Tablo 3.3. (Devamı)

k	$H(\mathbb{Q}(\sqrt{k}))$
30	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, \sqrt{30} \right\rangle \right], A^2 = 1$
34	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, 1 + \sqrt{34} \right\rangle \right], A^2 = 1$
35	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, 1 + \sqrt{35} \right\rangle \right], A^2 = 1$
39	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, 1 + \sqrt{39} \right\rangle \right], A^2 = 1$
42	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, \sqrt{42} \right\rangle \right], A^2 = 1$
51	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 3, \sqrt{51} \right\rangle \right], A^2 = 1$
55	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, 1 + \sqrt{55} \right\rangle \right], A^2 = 1$
58	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, \sqrt{58} \right\rangle \right], A^2 = 1$
65	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 5, \sqrt{65} \right\rangle \right], A^2 = 1$
66	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 3, \sqrt{66} \right\rangle \right], A^2 = 1$
70	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, \sqrt{70} \right\rangle \right], A^2 = 1$
74	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, \sqrt{74} \right\rangle \right], A^2 = 1$
78	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, \sqrt{78} \right\rangle \right], A^2 = 1$
79	$\{1, A, A^2\} \simeq \mathbb{Z}_3, A = \left[\left\langle 3, 1 + \sqrt{79} \right\rangle \right], A^2 = \left[\left\langle 3, 1 - \sqrt{79} \right\rangle \right], A^3 = 1$
82	$\{1, A, A^2, A^3\} \simeq \mathbb{Z}_4, A = \left[\left\langle 3, 2 + \sqrt{82} \right\rangle \right], A^2 = \left[\left\langle 2, \sqrt{82} \right\rangle \right],$ $A^3 = \left[\left\langle 3, 2 - \sqrt{82} \right\rangle \right], A^4 = 1$
85	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 5, \sqrt{85} \right\rangle \right], A^2 = 1$

Tablo 3.3. (Devamı)

k	$H\left(\mathbb{Q}(\sqrt{k})\right)$
87	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, 1 + \sqrt{87} \right\rangle \right], A^2 = 1$
91	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, 1 + \sqrt{91} \right\rangle \right], A^2 = 1$
95	$\{1, A\} \simeq \mathbb{Z}_2, A = \left[\left\langle 2, 1 + \sqrt{95} \right\rangle \right], A^2 = 1$

Tabloda yer almayan k değerleri için sınıf sayısı 1 dir.

BÖLÜM 4. BACHET DENKLEMİNİN ÇÖZÜMÜ

Teorem 4.1. M ve N tamsayılar, $M \equiv 3 \pmod{4}$, $N \equiv 2 \pmod{4}$ olsun. p asal ve $p \mid \frac{N}{2}$ ise $p \equiv 1 \pmod{4}$ olsun. $k = M^3 - N^2$ olsun. Bu takdirde $y^2 = x^3 + k$ denkleminin tamsayılarda çözümü yoktur [1].

İspat. $y^2 = x^3 + k$ 'nin tamsayılarda bir çözümü $(x, y) \in \mathbb{Z}^2$ olsun. $k \equiv -1 \pmod{4}$ olduğundan $y^2 \equiv x^3 - 1 \pmod{4}$ elde edilir. Ayrıca her y tamsayısı için $y^2 \equiv 0, 1 \pmod{4}$ 'dür. O halde x tek'tir. Çünkü x çift olursa $y^2 \equiv x^3 - 1 \equiv 0 - 1 \equiv -1 \pmod{4}$ olur. Bu ise mümkün değildir. $x \equiv 1 \pmod{4}$ 'tür. Çünkü $x \equiv 3 \pmod{4}$ olursa $y^2 \equiv x^3 - 1 \equiv 27 - 1 \equiv 2 \pmod{4}$ olur. Bu ise mümkün değildir. O zaman $k = M^3 - N^2$ olduğundan

$$y^2 + N^2 = x^3 + M^3 = (x + M)(x^2 - Mx + M^2)$$

olduğu görülür. $x \equiv 1 \pmod{4}$ ve $M \equiv 3 \pmod{4}$ olduğundan $x^2 - Mx + M^2 \equiv 3 \pmod{4}$ elde edilir. O halde $x^2 - Mx + M^2$ tektir ve $p \equiv 3 \pmod{4}$ olan bir p asal sayısı $p \mid x^2 - Mx + M^2$ olacak biçimde vardır. Dolayısıyla $y^2 \equiv -N^2 \pmod{p}$ olur. Hipotezden dolayı $p \nmid N$ 'dir. O halde

$$\left(\frac{-1}{p} \right) = \left(\frac{-N^2}{p} \right) = \left(\frac{y^2}{p} \right) = 1$$

olur ki bu $p \equiv 3 \pmod{4}$ olması ile çelişir. O halde $y^2 = x^3 + k$ denkleminin tamsayılarda çözümü yoktur.

Örnek 4.1. Teorem 4.1.'deki şartların geçerli olduğu bazı M, N, k değerleri şunlardır. $M = -1, N = 2, k = M^3 - N^2 = -5$ ve $M = 15, N = 58, k = M^3 - N^2 = 11$ ve $M = 3, N = 2, k = M^3 - N^2 = 23$ ve $M = 3, N = 10, k = M^3 - N^2 = -73$ için Teorem 4.1'in şartları sağlanır. Dolayısıyla $y^2 = x^3 - 5, y^2 = x^3 + 11, y^2 = x^3 + 23$ ve $y^2 = x^3 - 73$ denklemlerinin tamsayılarda çözümü yoktur.

Teorem 4.2. M ve N tamsayılar, $M \equiv 2 \pmod{4}, N \equiv 1 \pmod{4}$ olsun. p asal ve $p \mid N$ ise $p \equiv 1 \pmod{4}$ olsun. $k = M^3 - N^2$ olsun. Bu takdirde $y^2 = x^3 + k$ denkleminin tamsayılarda çözümü yoktur [1].

İspat. $y^2 = x^3 + k$ 'nin tamsayılarda bir çözümü $(x, y) \in \mathbb{Z}^2$ olsun. $k = M^3 - N^2 \equiv -1 \pmod{4}$ olduğundan $y^2 \equiv x^3 - 1 \pmod{4}$ elde edilir. O halde aynı Teorem 4.1'in ispatındaki gibi x tek ve $x \equiv 1 \pmod{4}$ olduğu gösterilebilir. O zaman $k = M^3 - N^2$ olduğundan

$$y^2 + N^2 = x^3 + M^3 = (x + M)(x^2 - Mx + M^2)$$

olarak yazılabilir. $x \equiv 1 \pmod{4}$ ve $M \equiv 2 \pmod{4}$ olduğundan $x^2 - Mx + M^2 \equiv 3 \pmod{4}$ elde edilir. O halde $x^2 - Mx + M^2$ tektir ve $p \equiv 3 \pmod{4}$ olan bir p asal sayısı $p \mid x^2 - Mx + M^2$ olacak biçimde vardır. Dolayısıyla $y^2 \equiv -N^2 \pmod{p}$ olur. Hipotezden dolayı $p \nmid N$ 'dir. O halde

$$\left(\frac{-1}{p}\right) = \left(\frac{-N^2}{p}\right) = \left(\frac{y^2}{p}\right) = 1$$

olur ki bu $p \equiv 3 \pmod{4}$ olması ile çelişir. O halde $y^2 = x^3 + k$ denkleminin tamsayılarda çözümü yoktur.

Örnek 4.2. Teorem 4.2.'deki şartların geçerli olduğu bazı M, N, k değerleri şunlardır: $M = 2, N = 1, k = M^3 - N^2 = 7$ ve $M = -2, N = 1, k = M^3 - N^2 = -9$ ve $M = 2, N = 5, k = M^3 - N^2 = -17$ ve $M = -2, N = 5, k = M^3 - N^2 = -33$ ve $M = 6, N = 13, k = M^3 - N^2 = 47$ ve $M = 14, N = 53, k = M^3 - N^2 = -65$ ve $M = 6, N = 17, k = M^3 - N^2 = -73$ değerleri için $y^2 = x^3 + 7, y^2 = x^3 - 9, y^2 = x^3 - 17, y^2 = x^3 - 33, y^2 = x^3 + 47, y^2 = x^3 - 65$ ve $y^2 = x^3 - 73$ denklemlerinin Teorem 4.2'e göre tamsayılarda çözümü yoktur.

Teorem 4.3. M ve N tamsayılar, $M \equiv 4, 6 \pmod{8}, N \equiv 1 \pmod{2}$ olsun. p asal ve $p \mid N$ ise $p \equiv \pm 1 \pmod{8}$ olsun. $k = M^3 + 2N^2$ olsun. Bu takdirde $y^2 = x^3 + k$ denkleminin tamsayılarda çözümü yoktur [1].

İspat. $y^2 = x^3 + k$ 'nin tamsayılarda bir çözümü $(x, y) \in \mathbb{Z}^2$ olsun. $k = M^3 + 2N^2 \equiv 2 \pmod{4}$ olduğundan $y^2 = x^3 + k \equiv x^3 + 2 \pmod{4}$ elde edilir. Dolayısıyla x çift olamaz. Çünkü x çift olursa $y^2 = x^3 + 2 \equiv 2 \pmod{4}$ olur. Bu ise mümkün değildir. O zaman x tektir. $x \equiv 3 \pmod{4}$ 'tür. Çünkü $x \equiv 1 \pmod{4}$ olursa $y^2 = x^3 + 2 \equiv 3 \pmod{4}$ olur. Bu ise mümkün değildir. Ayrıca

$$y^2 - 2N^2 = x^3 + M^3 = (x + M)(x^2 - Mx + M^2)$$

elde edilir. Eğer $x \equiv 3 \pmod{8}$ ise

$$x^2 - Mx + M^2 \equiv 1 - 3M + M^2 \equiv \pm 3 \pmod{8}$$

olur. Dolayısıyla $x^2 - Mx + M^2$ tektir. Bu $p \equiv 3, 5 \pmod{8}$ olan bir p asal sayısının mevcut olduğunu gösterir. Çünkü $x^2 - Mx + M^2$ 'yi bölen tüm asal sayılar

$p \equiv \pm 1 \pmod{8}$ ise $x^2 - Mx + M^2 \equiv \pm 1 \pmod{8}$ olur. O halde $p \equiv 3, 5 \pmod{8}$ dir.

O zaman $p \nmid N$ ve $y^2 \equiv 2N^2 \pmod{p}$ 'dir. Böylece

$$\left(\frac{2}{p}\right) = \left(\frac{2N^2}{p}\right) = \left(\frac{y^2}{p}\right) = 1$$

olur. Yani $p \equiv \pm 1 \pmod{8}$ olur ki bu $p \equiv 3, 5 \pmod{8}$ olması ile çelişir.

Eğer $x \equiv 7 \pmod{8}$ ise

$$x + M \equiv 7 + M \equiv \pm 3 \pmod{8}$$

olur. Dolayısıyla $x + M$ tektir. Bu $p \equiv 3, 5 \pmod{8}$ olan bir p asal sayısının mevcut olduğunu gösterir. O zaman $p \nmid N$ ve $y^2 \equiv 2N^2 \pmod{p}$ 'dir. Böylece

$$\left(\frac{2}{p}\right) = \left(\frac{2N^2}{p}\right) = \left(\frac{y^2}{p}\right) = 1$$

dir. Yani $p \equiv \pm 1 \pmod{8}$ olur ki bu $p \equiv 3, 5 \pmod{8}$ olması ile çelişir.

O halde $y^2 = x^3 + k$ denkleminin tam sayılarda çözümü yoktur.

Örnek 4.3. Teorem 4.3.'deki şartların geçerli olduğu bazı M, N, k değerleri şunlardır: $M = -2$, $N = 1$, $k = M^3 + 2N^2 = -6$ ve $M = -4$, $N = 7$, $k = M^3 + 2N^2 = 34$ ve $M = -10$, $N = 23$, $k = M^3 + 2N^2 = 58$ ve $M = -4$, $N = 1$, $k = M^3 + 2N^2 = -62$ ve $M = 4$, $N = 1$, $k = M^3 + 2N^2 = 66$ ve $M = -2$, $N = 7$, $k = M^3 + 2N^2 = 90$ değerleri için $y^2 = x^3 - 6$, $y^2 = x^3 + 34$, $y^2 = x^3 + 58$, $y^2 = x^3 - 62$, $y^2 = x^3 + 66$ ve $y^2 = x^3 + 90$ denklemlerinin Teorem 4.3'e göre tamsayılarda çözümü yoktur.

Teorem 4.4. M ve N tamsayılar, $M \equiv 4 \pmod{8}$, $N \equiv 1 \pmod{2}$ olsun. p asal ve $p \mid N$ ise $p \equiv 1, 3 \pmod{8}$ olsun. $k = M^3 - 2N^2$ olsun. Bu takdirde $y^2 = x^3 + k$ denkleminin tamsayılarda çözümü yoktur [1].

İspat. $y^2 = x^3 + k$ 'nin tamsayılarda bir çözümü $(x, y) \in \mathbb{Z}^2$ olsun. $k = M^3 - 2N^2 \equiv 2 \pmod{4}$ olduğundan $y^2 \equiv x^3 + 2 \pmod{4}$ elde edilir. O halde x tek. Çünkü x çift olursa $y^2 \equiv x^3 + 2 \equiv 0 + 2 \equiv 2 \pmod{4}$ olur. Bu ise mümkün değildir. Bu durumda $x \equiv 3 \pmod{4}$ 'tür. Çünkü $x \equiv 1 \pmod{4}$ olursa $y^2 \equiv x^3 + 2 \equiv 1 + 2 \equiv 3 \pmod{4}$ olur. Bu ise mümkün değildir. Ayrıca $k \equiv -2 \pmod{8}$ olduğundan $y^2 \equiv x^3 - 2 \pmod{8}$ dir. O halde $x \equiv 3 \pmod{8}$ olur. Ayrıca

$$y^2 + 2N^2 = x^3 + M^3 = (x + M)(x^2 - Mx + M^2)$$

olduğu görülür. $x \equiv 3 \pmod{8}$ ve $M \equiv 4 \pmod{8}$ olduğundan $x + M \equiv 7 \pmod{8}$ elde edilir. Dolayısıyla $x + M$ tek ve $p \equiv 5, 7 \pmod{8}$ olan bir p asal sayısı $p \mid x + M$ olacak biçimde vardır. Bu ise $p \nmid N$ ve $y^2 \equiv -2N^2 \pmod{p}$ olduğunu gösterir. O halde

$$\left(\frac{-2}{p} \right) = \left(\frac{-2N^2}{p} \right) = \left(\frac{y^2}{p} \right) = 1$$

olur ki bu $p \equiv 5, 7 \pmod{8}$ olması ile çelişir. O halde $y^2 = x^3 + k$ denkleminin tamsayılarda çözümü yoktur.

Örnek 4.4. Teorem 4.4.'deki şartların geçerli olduğu bazı M, N, k değerleri şunlardır: $M = 4$, $N = 3$, $k = M^3 - 2N^2 = 46$ ve $M = 4$, $N = 1$, $k = M^3 - 2N^2 = 62$ ve $M = -4$, $N = 1$, $k = M^3 - 2N^2 = -66$ ve $M = -4$, $N = 3$, $k = M^3 - 2N^2 = -82$ ve $M = 4$, $N = 9$, $k = M^3 - 2N^2 = -98$ değerleri için $y^2 = x^3 + 46$, $y^2 = x^3 + 62$,

$y^2 = x^3 - 66$, $y^2 = x^3 - 82$ ve $y^2 = x^3 - 98$ denklemlerinin Teorem 4.4'e göre tamsayılarda çözümü yoktur.

Teorem 4.5. K bir cebirsel sayı cismi olsun. K 'nın sınıf sayısı h ile gösterilsin. A , O_K 'nin bir tam ideali olsun. h ile aralarında asal olan bir k pozitif tamsayısı için A^k bir esas ideal olsun. Bu takdirde A 'da bir esas idealdir [1].

İspat. A 'nın sınıfı $[A]$ ile gösterilsin. $H(K)$ 'nin mertebesi h olduğundan, $[A]^h = 1$ dir. Böylece A^h bir esas idealdir. $\text{ebob}(h, k) = 1$ olduğundan, $rh + sk = 1$ olacak biçimde r ve s tamsayıları vardır. Bu takdirde, A^h bir esas ideal olduğundan

$$A = A^1 = A^{rh+sk} = (A^h)^r (A^k)^s$$

da bir esas idealdir.

Teorem 3.19 ve Teorem 4.5 kullanılarak $y^2 = x^3 + k$ Diophantine denkleminin eğer varsa çözümleri bulunabilir. $y^2 = x^3 + k$ 'nin tamsayılarda bir çözümü x ve y olsun. Böylece $y + \sqrt{k}$ ve $y - \sqrt{k}$ 'lar $K = \mathbb{Q}(\sqrt{k})$ kuadratik cisminin tamsayıları olmak üzere

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

olur. k 'nın karesiz ve $k \equiv 2, 3 \pmod{4}$ olduğu kabul edilsin. O zaman $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{k}$ olur. İdeallere geçilirse,

$$\langle x \rangle^3 = \langle y + \sqrt{k} \rangle \langle y - \sqrt{k} \rangle$$

elde edilir. k sayıları $\langle y + \sqrt{k} \rangle$ ve $\langle y - \sqrt{k} \rangle$ esas idealleri aralarında asal olacak biçimde seçilirse, Teorem 3.19'a göre, O_K 'da

$$\langle y + \sqrt{k} \rangle = A^3$$

olacak biçimde bir A idealinin mevcut olduğu görülür. Ayrıca K 'nın sınıf sayısı 3 ile bölünebilir değil ise Teorem 4.5'e göre A 'da bir esas idealdir. $a, b \in \mathbb{Z}$ için

$$A = \langle a + b\sqrt{k} \rangle$$

olsun. Dolayısıyla

$$\langle y + \sqrt{k} \rangle = \langle a + b\sqrt{k} \rangle^3 = \langle (a + b\sqrt{k})^3 \rangle$$

olur. Böylece Teorem 1.3'e göre

$$y + \sqrt{k} = \varepsilon (a + b\sqrt{k})^3$$

olacak biçimde O_K 'nın bir ε birimi vardır. Burada k 'nın pozitif veya negatif olmasına göre iki durumla karşılaşılır. k negatif ise ε için sadece sonlu sayıda olasılık mevcuttur. Aslında Teorem 2.17'ye göre $k \neq -1$ ise $\varepsilon = \pm 1$ ve $k = -1$ ise $\varepsilon = \pm 1, \pm i$ 'dir. Tek kuvvetler $(a + b\sqrt{k})^3$ ifadesinin içine alınabileceği için ve $-1 = (-1)^3$, $-i = (-i)^3$ olduğundan, denklem

$$y + \sqrt{k} = (a + b\sqrt{k})^3$$

halini alır. $\sqrt{k}$ 'nin katsayıları eşitlenirse,

$$1 = 3a^2b + kb^3 = b(3a^2 + kb^2)$$

elde edilir. O halde $b = \pm 1$ olmalıdır. Burdan sonra a için olasılıkları hesaplamak yeterlidir. Böylece $y^2 = x^3 + k$ denkleminin x, y tamsayı çözümleri bulunur. Teorem 4.6'da bu gösterilecektir. k pozitif ise o zaman ε için sonsuz çoklukta olasılık

mevcuttur. Aslında, Teorem 3.49'a göre, $\mu = T + U\sqrt{k}$ ($\mu > 1$), O_K 'nin temel birimi ve $l \in \mathbb{Z}$ olmak üzere $\varepsilon = \pm \mu^l$ biçimindedir. $-1 = (-1)^3$, $-\zeta^m = (-\zeta^m)^3$ ifadeleri $(a + b\sqrt{k})^3$ 'nin içine alınabileceği için, sadece

$$y + \sqrt{k} = (a + b\sqrt{k})^3$$

$$y + \sqrt{k} = \mu(a + b\sqrt{k})^3$$

$$y + \sqrt{k} = \mu^2(a + b\sqrt{k})^3$$

denklemlerini incelemek yeterlidir. Bu üç denklemden ilki $k < 0$ durumundaki gibi incelenebilir. Diğer iki denklemde k 'nin durumuna bağlı olarak çözüm olmayabilir. Bu Teorem 4.7'de ele alınacaktır. $y^2 = x^3 + k$ 'nin tüm çözümleri bulunurken $(a + b\sqrt{k})^3$ 'nin içine atılan küpler dikkate alınmalıdır.

Teorem 4.6. k bir tamsayı ve $k < -1$, k karesiz, $k \equiv 2, 3 \pmod{4}$, $3 \nmid h(\mathbb{Q}(\sqrt{k}))$ olsun.

- a. Eğer $k = 1 - 3a^2$ olacak biçimde bir a tamsayısı var ise o zaman $y^2 = x^3 + k$ denkleminin çözümleri sadece $x = 4a^2 - 1$, $y = \pm(3a - 8a^3)$ dir.
- b. Eğer $k = -1 - 3a^2$ olacak biçimde bir a tamsayısı varsa o zaman $y^2 = x^3 + k$ denkleminin çözümleri sadece $x = 4a^2 + 1$, $y = \pm(3a + 8a^3)$ dir.
- c. Eğer her a tamsayısı için $k \neq \pm 1 - 3a^2$ ise o zaman $y^2 = x^3 + k$ denkleminin tamsayılarda çözümü yoktur [1].

İspat. $y^2 = x^3 + k$ 'nin tamsayılarda x ve y çözümünün olduğu kabul edilsin. O zaman ya (a) şıkkının yada (b) şıkkının sağlanması gerekir. İkisi birden sağlanamaz çünkü (a) şıkkında $k \equiv 1 \pmod{3}$ ve (b) şıkkında ise $k \equiv 2 \pmod{3}$ 'dür.

Öncelikle $x \equiv 1 \pmod{2}$ olduğunu gösterelim. $y^2 \equiv 0, 1 \pmod{4}$ ve $k \equiv 2, 3 \pmod{4}$ olduğundan $x^3 = y^2 - k \equiv 1, 2, 3 \pmod{4}$ olur. Fakat tamsayılarda $x^3 \equiv 2 \pmod{4}$ olamaz. O halde $x^3 \equiv 1, 3 \pmod{4}$ 'dir. Yani $x \equiv 1 \pmod{2}$ elde edilir.

Şimdi $\text{ebob}(x, k) = 1$ olduğunu gösterelim. Aksine x ve k aralarında asal olmasın. O zaman $p \mid x$ ve $p \mid k$ olacak biçimde bir p asal sayısı vardır. Bu durumda $p \mid x^3 + k$ yani $p \mid y^2$ bulunur. O halde $p \mid y$ 'dir. Buradan $p^2 \mid y^2 - x^3$ elde edilir. Bu ise $p^2 \mid k$ olmasını gerektirir. k karesiz olduğundan bu olamaz. Dolayısıyla $\text{ebob}(x, k) = 1$ 'dir.

$x \equiv 1 \pmod{2}$ ve $\text{ebob}(x, k) = 1$ olduğundan $\text{ebob}(x, 2k) = 1$ dir. O halde $lx + m(2k) = 1$ olacak biçimde $l, m \in \mathbb{Z}$ vardır.

$K = \mathbb{Q}(\sqrt{k})$ olsun. $k < -1$ olduğundan K bir kompleks kuadratik cisimdir. $k \equiv 2, 3 \pmod{4}$ olduğundan K 'nın tamsayılar halkası $O_K = \{u + v\sqrt{k} \mid u, v \in \mathbb{Z}\}$ olur.

Şimdi $\langle y + \sqrt{k} \rangle$ ve $\langle y - \sqrt{k} \rangle$ esas ideallerinin O_K 'da aralarında asal olduğunu gösterelim. Aksine bu iki ideal aralarında asal olmasın. O zaman

$$P \mid \langle y + \sqrt{k} \rangle, P \mid \langle y - \sqrt{k} \rangle$$

olacak biçimde bir P asal ideali vardır. Bu ise $\langle y + \sqrt{k} \rangle \subset P$ ve $\langle y - \sqrt{k} \rangle \subset P$ olmasını gerektirir. O halde $y + \sqrt{k} \in P$, $y - \sqrt{k} \in P$ olur. Dolayısıyla $2\sqrt{k} = (y + \sqrt{k}) - (y - \sqrt{k}) \in P$ 'dir. O halde $2k = \sqrt{k}(2\sqrt{k}) \in P$ olur. Ayrıca

$$\langle y + \sqrt{k} \rangle \langle y - \sqrt{k} \rangle = \langle y^2 - k \rangle = \langle x^3 \rangle = \langle x \rangle^3$$

olduğundan $P \mid \langle x \rangle^3$ elde edilir. P bir asal ideal olduğundan $P \mid \langle x \rangle$ olur. O halde $x \in P$ 'dir. $lx + m(2k) = 1$, $2k = \sqrt{k}(2\sqrt{k}) \in P$, $x \in P$ olduğundan, $1 \in P$ olduğu

görülür. Bu ise P 'nin asal olması ile çelişir O halde $\langle y + \sqrt{k} \rangle$ ve $\langle y - \sqrt{k} \rangle$ idealleri O_K 'da aralarında asaldır ve $\langle y + \sqrt{k} \rangle \langle y - \sqrt{k} \rangle = \langle x \rangle^3$ 'dir.

K bir cebirsel sayı cismi olduğundan, Teorem 3.1'e göre O_K bir Dedekind bölgesidir. Dolayısıyla Teorem 3.19'dan dolayı O_K 'da

$$\langle y + \sqrt{k} \rangle = A^3$$

olacak biçimde bir A ideali vardır. O halde A^3 bir esas idealdir. $3 \nmid h(\mathbb{Q}(\sqrt{k}))$ olduğundan, Teorem 4.5'ye göre A 'da bir esas idealdir, $a, b \in \mathbb{Z}$ olmak üzere

$$A = \langle a + b\sqrt{k} \rangle \text{ olsun. O halde } \langle y + \sqrt{k} \rangle = \langle a + b\sqrt{k} \rangle^3 = \langle (a + b\sqrt{k})^3 \rangle \text{ olur.}$$

Teorem 1.2'den dolayı $y + \sqrt{k} = \varepsilon (a + b\sqrt{k})^3$ biçimde bir $\varepsilon \in O_K$ birimi vardır.

$k < -1$ ve $k \equiv 2, 3 \pmod{4}$ olduğundan, Teorem 2.17'ye göre $\varepsilon = \pm 1$ 'dir.

$y + \sqrt{k} = \varepsilon (a + b\sqrt{k})^3$ 'den eşleniklere geçilirse $y - \sqrt{k} = \varepsilon (a - b\sqrt{k})^3$ olur.

Dolayısıyla

$$\begin{aligned} x^3 = y^2 - k &= (y + \sqrt{k})(y - \sqrt{k}) = (a + b\sqrt{k})^3 (a - b\sqrt{k})^3 \\ &= ((a + b\sqrt{k})(a - b\sqrt{k}))^3 = (a^2 - kb^2)^3 \end{aligned}$$

dır. Böylece $x = a^2 - kb^2$ elde edilir. $y + \sqrt{k} = \varepsilon (a + b\sqrt{k})^3$ ve

$y - \sqrt{k} = \varepsilon (a - b\sqrt{k})^3$ 'yi sırasıyla toplayarak ve çıkartarak

$$2y = \varepsilon \left((a + b\sqrt{k})^3 + (a - b\sqrt{k})^3 \right)$$

ve

$$2\sqrt{k} = \varepsilon \left((a + b\sqrt{k})^3 - (a - b\sqrt{k})^3 \right)$$

elde edilir. Böylece $y = \varepsilon(a^3 + 3kab^2)$, $1 = \varepsilon b(3a^2b + kb^3)$ olur.

$1 = \varepsilon b(3a^2b + kb^3)$ denkleminde $b = \pm 1$ elde edilir. Böylece $b = \pm \varepsilon$ olur. $b = \varepsilon$ ise $x = a^2 - k$, $y = \varepsilon(a^3 + 3ka)$, $1 = 3a^2 + k$ olur. Yani $k = 1 - 3a^2$ ve $x = 4a^2 - 1$, $y = \pm(3a - 8a^3)$ dir. Bu durumda

$$x^3 + k = (4a^2 - 1)^3 + (1 - 3a^2) = 64a^6 - 48a^4 + 9a^2 = (8a^3 - 3a)^2 = y^2$$

elde edilir. Eğer $b = -\varepsilon$ ise $x = a^2 - k$, $y = \varepsilon(a^3 + 3ka)$, $1 = -3a^2 - k$ olur.

Dolayısıyla $k = -1 - 3a^2$ ve $x = 4a^2 + 1$, $y = \pm(3a + 8a^3)$ dir. Bu durumda da

$$x^3 + k = (4a^2 + 1)^3 + (-1 - 3a^2) = 64a^6 + 48a^4 + 9a^2 = (8a^3 + 3a)^2 = y^2$$

elde edilir.

Örnek 4.5 $k = -2$ sayısı Teorem 4.6'nın (a) şikkını sağlar. Çünkü $k = -2 = 1 - 3 \cdot 1^2$ ve $h(\mathbb{Q}(\sqrt{-2})) = 1$ 'dir. O halde $y^2 = x^3 - 2$ denkleminin tamsayılardaki çözümleri sadece $(x, y) = (3, \pm 5)$ dir.

Örnek 4.6. $-200 < k < -2$ aralığında; k 'nın sadece -74 ve -146 değerleri Teorem 4.6'nın (a) şikkını sağlar. Çünkü $k = -74 = 1 - 3 \cdot 5^2$ ($h(\mathbb{Q}(\sqrt{-74})) = 10$) ve $k = -146 = 1 - 3 \cdot 7^2$ ($h(\mathbb{Q}(\sqrt{-146})) = 16$) dir. O halde $y^2 = x^3 - 74$ 'ün tamsayılardaki çözümleri sadece $(x, y) = (99, \pm 985)$ ve $y^2 = x^3 - 146$ 'nın tamsayılardaki çözümleri sadece $(x, y) = (195, \pm 2723)$ 'dür.

Örnek 4.7. Teorem 4.6'nın (b) şikkını sağlayan mutlak değer olarak en küçük k değeri $k = -13 = -1 - 3 \cdot 2^2 \left(h\left(\mathbb{Q}\left(\sqrt{-13}\right)\right) = 2 \right)$ 'dür. O halde $y^2 = x^3 - 13$ 'ün tamsayılardaki çözümleri sadece $(x, y) = (17, \pm 70)$ dir.

Örnek 4.8. $-200 < k < -1$ aralığında, Teorem 4.6'nın (b) şikkını sağlayan -13 den farklı tek değer -193 'dür. Çünkü $k = -193 = -1 - 3 \cdot 8^2 \left(h\left(\mathbb{Q}\left(\sqrt{-193}\right)\right) = 4 \right)$ dir. O halde $y^2 = x^3 - 193$ 'ün tamsayılardaki çözümleri sadece $(x, y) = (257, \pm 4120)$ 'dir.

Örnek 4.9. $k = -5$ sayısı Teorem 4.6'nın (c) şikkını sağlar. k 'nın bu değeri için $h\left(\mathbb{Q}\left(\sqrt{-5}\right)\right) = 2$ dir. O halde $y^2 = x^3 - 5$ denkleminin tamsayılarda çözümü yoktur. Benzer biçimde $k = -6, -10, -14, -17, -21, -22$ değerleri için de $y^2 = x^3 + k$ denkleminin tamsayılarda çözümünün olmadığı görülür.

Teorem 4.7. k karesiz pozitif bir tamsayı, $k \equiv 2, 3 \pmod{4}$, $3 \nmid h\left(\mathbb{Q}\left(\sqrt{k}\right)\right)$ olsun. $K = \mathbb{Q}\left(\sqrt{k}\right)$ 'nin normu 1 olan temel birimi $T + U\sqrt{k}$ olsun.

$$k \equiv 4 \pmod{9}, U \equiv 0 \pmod{9}$$

veya

$$k \equiv 7 \pmod{9}, U \equiv \pm 3 \pmod{9}$$

veya

$$k \equiv 4 \pmod{7}, U \equiv 0 \pmod{7}$$

ise o zaman $y^2 = x^3 + k$ 'nin tamsayılarda çözümü yoktur [1].

İspat. Teorem 4.6'nın ispatındaki gibi bir $\varepsilon \in O_K$ biriminin

$$y + \sqrt{k} = \varepsilon (a + b\sqrt{k})^3$$

olacak biçimde mevcut olduğu gösterilebilir. η , O_K 'nin temel birimi olsun. O zaman Teorem 3.49'a göre

$$\varepsilon = \pm \eta^l$$

olacak biçimde bir $l \in \mathbb{Z}$ vardır. $-1 = (-1)^3$ ve $\eta^{3m} = (\eta^m)^3$ ifadeleri $(a + b\sqrt{k})^3$

ifadesinin içine atılabildiğinden, $\varepsilon = 1, \eta, \eta^2$ olmak üzere $y + \sqrt{k} = \varepsilon (a + b\sqrt{k})^3$ elde

edilir. Ayrıca $\eta = \eta^3 / \eta^2$ ve $\eta^2 = \eta^3 / \eta$ olduğundan, $\varepsilon \in \left\{1, \eta, \frac{1}{\eta}\right\}$ veya

$\varepsilon \in \left\{1, \frac{1}{\eta^2}, \eta^2\right\}$ olmak üzere $y + \sqrt{k} = \varepsilon (a + b\sqrt{k})^3$ olarak yazılabilir. η 'nin normu

1 ise $\varepsilon \in \left\{1, \eta, \frac{1}{\eta}\right\}$, η 'nin normu -1 ise $\varepsilon \in \left\{1, \frac{1}{\eta^2}, \eta^2\right\}$ seçelim. İki durumda da,

$T + U\sqrt{k}$ O_K 'nin normu 1 olan temel birimi olmak üzere

$$\varepsilon \in \{1, T + U\sqrt{k}, T - U\sqrt{k}\}$$

olur. $\varepsilon = 1$ ise, $\sqrt{k}$ 'nin katsayıları eşitlenerek $1 = 3a^2b + kb^3$ elde edilir. Buradan $b \mid 1$

olduğu görülür. Dolayısıyla $b = \pm 1$ olur. O halde

$\pm 1 = b = 3a^2b^2 + kb^4 = 3a^2 + k \geq k > 1$ elde edilir ki bu bir çelişkidir. O halde

$\varepsilon = T \pm U\sqrt{k}$ 'dir. O zaman

$$\begin{aligned} y + \sqrt{k} &= (T \pm U\sqrt{k})(a + b\sqrt{k})^3 \\ &= (T \pm U\sqrt{k})((a^3 + 3kab^2) + (3a^2b + kb^3)\sqrt{k}) \\ &= (T(a^3 + 3kab^2) \pm Uk(3a^2b + kb^3)) + (T(3a^2b + kb^3) \pm U(a^3 + 3kab^2)\sqrt{k}) \end{aligned}$$

olur. Böylece

$$1 = T(3a^2b + kb^3) \pm U(a^3 + 3kab^2)$$

elde edilir.

1. $k \equiv 4 \pmod{9}$, $U \equiv 0 \pmod{9}$ olsun. $U \equiv 0 \pmod{9}$ ve $T^2 - kU^2 = 1$ olduğundan $T \equiv \pm 1 \pmod{81}$ elde edilir. $T \equiv \varepsilon \pmod{81}$, $\varepsilon = \pm 1$ olsun. Bu takdirde $1 = T(3a^2b + kb^3) \pm U(a^3 + 3kab^2)$ ifadesini mod 9 da incelersek $1 \equiv \varepsilon(3a^2b + 4b^3) \pmod{9}$ elde edilir. Burada $3 \nmid b$ olmalıdır. O zaman $b \equiv \pm 1 \pmod{3}$ olur. $b \equiv \lambda \pmod{3}$, $\lambda = \pm 1$ olsun. Dolayısıyla $b^3 \equiv \lambda \pmod{9}$ olur. O zaman $1 \equiv \varepsilon(3a^2b + 4b^3) \pmod{9}$ ifadesinden $1 \equiv \varepsilon\lambda(3a^2 + 4) \pmod{9}$ yazılabilir. Böylece $3a^2 + 4 \equiv \varepsilon\lambda \equiv \pm 1 \pmod{9}$ elde edilir. Bu da $3a^2 \equiv 4, 6 \pmod{9}$ demektir ki bu mümkün değildir.
2. $k \equiv 7 \pmod{9}$, $U \equiv \pm 3 \pmod{9}$ olsun. $U^2 \equiv 0 \pmod{9}$ 'dur. O zaman $T^2 - kU^2 = 1$ olduğundan $T^2 \equiv 1 \pmod{9}$ elde edilir. Böylece $T \equiv \pm 1 \pmod{9}$ olur. $1 = T(3a^2b + kb^3) \pm U(a^3 + 3kab^2)$ ifadesini mod 3 de incelersek $1 \equiv Tkb^3 \pmod{3}$ olur. Buradan $1 \equiv 7Tb^3 \pmod{3}$ yani $1 \equiv Tb^3 \pmod{3}$ bulunur. Her iki taraf T ile çarpılırsa $T \equiv T^2b^3 \pmod{3}$ olur. Buradan $T \equiv b^3 \pmod{3}$ yani $\pm 1 \equiv b^3 \pmod{3}$ dolayısıyla $\pm 1 \equiv b \pmod{3}$ bulunur. Şu halde $b^3 \equiv \pm 1 \pmod{9}$ ve $b^6 \equiv 1 \pmod{9}$ 'dir. Ayrıca $1 = T(3a^2b + kb^3) \pm U(a^3 + 3kab^2)$ ifadesini mod 9 da incelersek $1 \equiv T(3a^2b + kb^3) \pm 3a^3 \pmod{9}$ elde edilir. Her iki tarafı T ile çarparsak $\pm 1 \equiv 3a^2b + kb^3 \pm 3a^3 \pmod{9}$ olur. Her iki tarafı b^3 ile çarparsak $\pm 1 \equiv 3a^2b^4 + kb^6 \pm 3a^3 \pmod{9}$ elde edilir. Buradan $\pm 1 \equiv 3a^2b^4 + k \pm 3a^3 \pmod{9}$ yani $3a^2b^4 + 7 \pm 3a^3 \equiv \pm 1 \pmod{9}$ bulunur. Bu durumda $3 \nmid a$ olmalıdır. O zaman $a^3 \equiv \pm 1 \pmod{9}$ olur. Bu durumda

$3a^2b^4 + 7 \pm 3a \equiv \pm 1 \pmod{9}$ kongrüansından $3a^2b^4 + 7 \pm 3 \equiv \pm 1 \pmod{9}$ elde edilir. Dolayısıyla $3a^2b^4 + 10 \equiv \pm 1 \pmod{9}$ veya $3a^2b^4 + 4 \equiv \pm 1 \pmod{9}$ 'dir. O halde $3a^2b^4 \equiv -9 \pmod{9}$ veya $3a^2b^4 \equiv -3 \pmod{9}$ bulunur. $3a^2b^4 \equiv -9 \pmod{9}$ kongrüansından $3 \mid a^2b^4$ elde edilir. Bu olamaz. Çünkü $3 \nmid a$ ve $3 \nmid b$ 'dir. $3a^2b^4 \equiv -3 \pmod{9}$ kongrüansından $(ab^2)^2 \equiv -1 \pmod{3}$ olur ki bu da mümkün değildir.

3. $k \equiv 4 \pmod{7}$, $U \equiv 0 \pmod{7}$ olsun. $y + \sqrt{k} = (T \pm U\sqrt{k})(a + b\sqrt{k})^3$ ifadesinden $y - \sqrt{k} = (T \mp U\sqrt{k})(a - b\sqrt{k})^3$ elde edilir. Böylece

$$\begin{aligned} x^3 = y^2 - k &= (y + \sqrt{k})(y - \sqrt{k}) \\ &= (T \pm U\sqrt{k})(a + b\sqrt{k})^3 (T \mp U\sqrt{k})(a - b\sqrt{k})^3 \\ &= (T^2 - kU^2)(a^2 - kb^2)^3 \\ &= (a^2 - kb^2)^3 \end{aligned}$$

olur. O halde $x = a^2 - kb^2$ dir. Ayrıca $x^3 \equiv 0, 1, 6 \pmod{7}$ ve $y^2 \equiv 0, 1, 2, 4 \pmod{7}$ dir. $y^2 - x^3 = k \equiv 4 \pmod{7}$ olması gerektiğinden $x^3 \equiv 0 \pmod{7}$ ve $y^2 \equiv 4 \pmod{7}$ olmalıdır. Dolayısıyla $x \equiv 0 \pmod{7}$ dır. Böylece $a^2 - kb^2 = x \equiv 0 \pmod{7}$ olur. O halde $a^2 - 4b^2 \equiv 0 \pmod{7}$ bulunur. Yani $a \equiv \pm 2b \pmod{7}$ 'dir. $U \equiv 0 \pmod{7}$ ve $T^2 - kU^2 = 1$ olduğundan $T^2 \equiv 1 \pmod{49}$ elde edilir. Böylece $T \equiv \pm 1 \pmod{49}$ olur. O zaman $1 = T(3a^2b + kb^3) \pm U(a^3 + 3kab^2)$ ifadesinden $1 \equiv \pm 2b^3 \pmod{7}$ elde edilir ki bu mümkün değildir.

Örnek 4.10. $k=58$ seçilirse $k \equiv 2 \pmod{4}$ ve $k \equiv 4 \pmod{9}$ olur. Burada $h\left(\mathbb{Q}(\sqrt{58})\right)=2$ dir ve $\mathbb{Q}(\sqrt{58})$ 'in temel birimi normu -1 olan $99+13\sqrt{58}$ dir. O zaman normu 1 olan temel birim $(99+13\sqrt{58})^2=19603+2574\sqrt{58}$ olur. Böylece $U=2574 \equiv 0 \pmod{9}$ dur. Dolayısıyla Teorem 4.7'ye göre, $y^2=x^3+58$ denkleminin tamsayılarda çözümü yoktur.

Örnek 4.11. $k=7$ olsun. O zaman $k \equiv 3 \pmod{4}$ ve $k \equiv 3 \pmod{4}$ olur. Burada $h\left(\mathbb{Q}(\sqrt{7})\right)=1$ dir ve $\mathbb{Q}(\sqrt{7})$ 'nin temel birimi normu 1 olan $8+3\sqrt{7}$ dir. Böylece $U=3 \equiv 3 \pmod{9}$ dur. O halde, Teorem 4.7'ye göre $y^2=x^3+7$ denkleminin tamsayılarda çözümü yoktur.

Örnek 4.12. $k=158$ olsun. O zaman $k \equiv 2 \pmod{4}$ ve $k \equiv 7 \pmod{9}$ olur. Burada $h\left(\mathbb{Q}(\sqrt{158})\right)=1$ dir ve $\mathbb{Q}(\sqrt{158})$ 'in temel birimi normu 1 olan $7743+616\sqrt{158}$ dir. Böylece $U=616 \equiv 0 \pmod{9}$ olur. O halde, Teorem 4.7'ye göre $y^2=x^3+158$ denkleminin tamsayılarda çözümü yoktur.

Teorem 4.8. $y^2=x^3-31$ denkleminin tamsayılarda çözümü yoktur [1].

İspat. $y^2=x^3-31$ denkleminin tamsayılarda bir çözümü (x,y) olsun.

Önce $(x,y)=1$ olduğunu gösterelim. Tersine $p|x$ ve $p|y$ olan bir p asal sayısı mevcut olsun. Bu durumda $p|31$ olur. p asal olduğundan $p=31$ dir. O halde $31|x$, $31|y$ olacağından $x=31a$, $y=31b$ olacak biçimde a,b tamsayıları vardır. Bu takdirde $y^2=x^3-31$ 'den $(31b)^2=(31a)^3-31$ olur. Buradan

$31(31b^2) = 31(31^2a^3) - 31$ yazılabilir. Yani $31b^2 = 31^2a^3 - 1$ olur. Böylece $31|1$ elde edilir ki bu mümkün değildir. O halde $(x, y) = 1$ 'dir.

Şimdi x 'in çift tamsayı olduğunu gösterelim. Aksine x tek olsun. $x \equiv 1 \pmod{4}$ ise $x^3 - 31 \equiv 1 - 31 - 30 \equiv 2 \pmod{4}$ olacağından $y^2 \equiv 2 \pmod{4}$ elde edilir ki bu mümkün değildir. O halde $x \equiv 3 \pmod{4}$ 'dür. Ayrıca

$$y^2 + 4 = x^3 - 31 + 4 = x^3 - 27 = (x-3)(x^2 + 3x + 9)$$

dir. $x^2 + 3x + 9 > 1$ 'dir ve $x^2 + 3x + 9 \equiv 1 + 9 + 9 \equiv 3 \pmod{4}$ 'dür. O halde $p|x^2 + 3x + 9$ ve $p \equiv 3 \pmod{4}$ olan bir p asal sayısı vardır. Buradan $p|y^2 + 4$ elde edilir. $p|y^2 + 4$ ve $p \equiv 3 \pmod{4}$ olduğundan $p|y$ ve $p|2$ elde edilir. Bu ise mümkün değildir. Dolayısıyla x çift tamsayıdır. O halde y tek tir.

$y^2 + 31 = x^3$ olduğundan $\frac{y^2 + 31}{4} = 2\left(\frac{x}{2}\right)^3$ yazılabilir. Dolayısıyla

$$\left(\frac{y + \sqrt{-31}}{2}\right)\left(\frac{y - \sqrt{-31}}{2}\right) = 2\left(\frac{x}{2}\right)^3 \text{ elde edilir. İdeallere geçilirse}$$

$$\left\langle \frac{y + \sqrt{-31}}{2} \right\rangle \left\langle \frac{y - \sqrt{-31}}{2} \right\rangle = \langle 2 \rangle \left\langle \frac{x}{2} \right\rangle^3$$

olur. Buradaki $\left\langle \frac{y + \sqrt{-31}}{2} \right\rangle$ ve $\left\langle \frac{y - \sqrt{-31}}{2} \right\rangle$ idealleri aralarında asaldır. Bunu

göstermek için, bir asal J ideali $J|\left\langle \frac{y + \sqrt{-31}}{2} \right\rangle$ ve $J|\left\langle \frac{y - \sqrt{-31}}{2} \right\rangle$ olacak biçimde

mevcut olsun. O zaman Teorem 3.7'e göre $\left\langle \frac{y + \sqrt{-31}}{2} \right\rangle \subset J$ ve $\left\langle \frac{y - \sqrt{-31}}{2} \right\rangle \subset J$

olur. Dolayısıyla $\frac{y + \sqrt{-31}}{2} \in J$ ve $\frac{y - \sqrt{-31}}{2} \in J$ dir. Buradan

$$\left(\frac{y+\sqrt{-31}}{2}\right) - \left(\frac{y-\sqrt{-31}}{2}\right) = \frac{2y}{2} = y \in J,$$

$$\left(\frac{y+\sqrt{-31}}{2}\right) \left(\frac{y-\sqrt{-31}}{2}\right) = \frac{y^2+31}{4} = 2\left(\frac{x}{2}\right)^3 \in J$$

elde edilir. $2 \in J$ ise y tek ve $y \in J$ olduğundan $1 \in J$ elde edilir. Çünkü y tek ise

$y = 2k+1$, $k \in \mathbb{Z}$ vardır. Böylece $1 = y - 2k \in J$ olur. Eğer $\left(\frac{x}{2}\right)^3 \in J$ ise o zaman

$\frac{x}{2} \in J$ olur. $\left(\frac{x}{2}, y\right) = 1$ olduğundan $1 \in J$ elde edilir. Sonuç olarak $1 \in J$

olduğundan $J = D$ olur. Dolayısıyla $\left(\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle, \left\langle \frac{y-\sqrt{-31}}{2} \right\rangle\right) = D$ 'dir. Yani

$\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle$ ve $\left\langle \frac{y-\sqrt{-31}}{2} \right\rangle$ idealleri aralarında asaldır.

$K = \mathbb{Q}(\sqrt{-31})$ 'in bir tamsayı tabanı $\left\{1, \frac{1+\sqrt{-31}}{2}\right\}$ 'dir. 2'nin O_K 'da asal ideallerin

çarpımı biçiminde yazılışı, Teorem 3.41'den dolayı

$$\langle 2 \rangle = \left\langle 2, \frac{1+\sqrt{-31}}{2} \right\rangle \left\langle 2, \frac{1-\sqrt{-31}}{2} \right\rangle$$

biçimindedir. O halde

$$\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle \left\langle \frac{y-\sqrt{-31}}{2} \right\rangle = \left\langle 2, \frac{1+\sqrt{-31}}{2} \right\rangle \left\langle 2, \frac{1-\sqrt{-31}}{2} \right\rangle \left\langle \frac{x}{2} \right\rangle^3$$

olarak yazılabilir.

Şimdi $\left\langle 2, \frac{1+\sqrt{-31}}{2} \right\rangle$ bir esas ideal olmadığını gösterelim. Tersine

$\left\langle 2, \frac{1+\sqrt{-31}}{2} \right\rangle = \langle \alpha \rangle$ olacak biçimde bir $\alpha \in O_K$ mevcut olsun. O zaman $2 \in \langle \alpha \rangle$,

$\frac{1+\sqrt{-31}}{2} \in \langle \alpha \rangle$ olur. Böylece $2 - \left(\frac{1+\sqrt{-31}}{2} \right) = \frac{3-\sqrt{-31}}{2} \in \langle \alpha \rangle$ 'dir. $2 \in \langle \alpha \rangle$ ve

$\frac{3-\sqrt{-31}}{2} \in \langle \alpha \rangle$ ifadelerinde normlara geçerse $N(\alpha) | 4$ ve $N(\alpha) | \frac{40}{4}$ olur. Yani

$N(\alpha) | 4$ ve $N(\alpha) | 10$ 'dur. Dolayısıyla $N(\alpha) | (4, 10)$ olur. O halde $N(\alpha) | 2$ elde

edilir. Ayrıca $N(\alpha) > 1$ 'dir. Buradan $N(\alpha) = 2$ elde edilir. Fakat $\alpha \in \mathcal{O}_K$ ise

$\alpha = \frac{a+b\sqrt{-31}}{2}$ olacak biçimde $a, b \in \mathbb{Z}$ vardır.

$N(\alpha) = N\left(\frac{a+b\sqrt{-31}}{2}\right) = \frac{a^2+31b^2}{4}$ ve $N(\alpha) = 2$ olduğundan $a^2+31b^2 = 8$ elde

edilir ki bu mümkün değildir. O halde $\left\langle 2, \frac{1+\sqrt{-31}}{2} \right\rangle$ ideali esas ideal değildir.

Benzer biçimde $\left\langle 2, \frac{1-\sqrt{-31}}{2} \right\rangle$ idealinin de esas ideal olmadığı gösterilebilir. Şimdi

$$\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle \left\langle \frac{y-\sqrt{-31}}{2} \right\rangle = \langle 2 \rangle \left\langle \frac{x}{2} \right\rangle^3 \text{ ve } \langle 2 \rangle = \left\langle 2, \frac{1+\sqrt{-31}}{2} \right\rangle \left\langle 2, \frac{1-\sqrt{-31}}{2} \right\rangle$$

olduğu biliniyor. O halde Teorem 3.24'e göre

$$\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle = A_1 T_1^3, \left\langle \frac{y-\sqrt{-31}}{2} \right\rangle = A_2 T_2^3$$

olacak biçimde A_1, A_2, T_1, T_2 idealleri vardır. A_1, A_2 aralarında asal ve

$\left\langle 2, \frac{1+\sqrt{-31}}{2} \right\rangle$ ile $\left\langle 2, \frac{1-\sqrt{-31}}{2} \right\rangle$ aralarında asal olduğundan $A_1 A_2 = \langle 2 \rangle$ olur. O

halde dört durum vardır.

$$1. \text{ Durum. } A_1 = \left\langle 2, \frac{1+\sqrt{-31}}{2} \right\rangle, A_2 = \left\langle 2, \frac{1-\sqrt{-31}}{2} \right\rangle$$

$$2. \text{ Durum. } A_1 = \left\langle 2, \frac{1-\sqrt{-31}}{2} \right\rangle, A_2 = \left\langle 2, \frac{1+\sqrt{-31}}{2} \right\rangle$$

$$3. \text{ Durum. } A_1 = D, A_2 = \left\langle 2, \frac{1+\sqrt{-31}}{2} \right\rangle \left\langle 2, \frac{1-\sqrt{-31}}{2} \right\rangle$$

$$4. \text{ Durum. } A_1 = \left\langle 2, \frac{1+\sqrt{-31}}{2} \right\rangle \left\langle 2, \frac{1-\sqrt{-31}}{2} \right\rangle, A_2 = D$$

Ayrıca sınıf sayısı 3 olduğundan T_1^3 ve T_2^3 esas ideallerdir.

1. durumda T_1^3 ve $\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle$ esas idealler ve $\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle = A_1 T_1^3$ olduğundan

$\left\langle 2, \frac{1+\sqrt{-31}}{2} \right\rangle$ esas ideal olur ki bu mümkün değildir.

2. durumda T_1^3 ve $\left\langle \frac{y-\sqrt{-31}}{2} \right\rangle$ esas idealler ve $\left\langle \frac{y-\sqrt{-31}}{2} \right\rangle = A_1 T_1^3$ olduğundan

$\left\langle 2, \frac{1-\sqrt{-31}}{2} \right\rangle$ esas ideal olur ki bu mümkün değildir.

3. durumda $\left\langle \frac{y-\sqrt{-31}}{2} \right\rangle = \langle 2 \rangle T_2^3$ olur. O zaman $\langle 2 \rangle \mid \left\langle \frac{y-\sqrt{-31}}{2} \right\rangle$ elde edilir.

Buradan $\left\langle \frac{y-\sqrt{-31}}{2} \right\rangle \subset \langle 2 \rangle$ olur. O halde $\frac{y-\sqrt{-31}}{2} = 2 \left(\frac{c+d\sqrt{-31}}{2} \right)$ olacak

biçimde $c, d \in \mathbb{Z}$ vardır. Buradan $y - \sqrt{-31} = 2c + 2d\sqrt{-31}$ olur. Yani $y = 2c$ elde edilir. Fakat y tek olduğundan bu mümkün değildir.

4. durumda $\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle = \langle 2 \rangle T_1^3$ olur. Benzer biçimde $y = 2c$ elde edilir. Fakat y

tek olduğundan bu da mümkün değildir.

Sonuç olarak $y^2 = x^3 - 31$ denkleminin tamsayılarda çözümü yoktur.

Bazı negatif k değerleri için $y^2 = x^3 + k$ denkleminin çözümleri Tablo 4.1 de verilmiştir.

Tablo 4.1. $-20 \leq k < 0$ olmak üzere $y^2 = x^3 + k$ 'nın $(x, y) \in \mathbb{Z}^2$ çözümleri [1].

k	$y^2 = x^3 + k$ 'nın (x, y) çözümleri
-1	$(1, 0)$
-2	$(3, \pm 5)$
-3	çözümü yok
-4	$(2, \pm 2), (5, \pm 11)$
-5	çözümü yok
-6	çözümü yok
-7	$(2, \pm 1), (32, \pm 181)$
-8	$(2, 0)$
-9	çözümü yok
-10	çözümü yok
-11	$(3, \pm 4), (15, \pm 58)$
-12	çözümü yok
-13	$(17, \pm 70)$
-14	çözümü yok
-15	$(4, \pm 7)$
-16	çözümü yok
-17	çözümü yok
-18	$(3, \pm 3)$
-19	$(7, \pm 18)$
-20	$(6, \pm 14)$

Bazı pozitif k değerleri için $y^2 = x^3 + k$ denkleminin çözümleri Tablo 4.2 de verilmiştir.

Tablo 4.2. $0 < k \leq 20$ olmak üzere $y^2 = x^3 + k$ 'nın $(x, y) \in \mathbb{Z}^2$ çözümleri [1].

k	$y^2 = x^3 + k$ 'nın (x, y) çözümleri
1	$(-1, 0), (0, \pm 1), (2, \pm 3)$
2	$(-1, \pm 1)$
3	$(1, \pm 2)$
4	$(0, \pm 2)$
5	$(-1, \pm 2)$
6	çözümü yok
7	çözümü yok
8	$(-2, 0), (1, \pm 3), (2, \pm 4), (46, \pm 312)$
9	$(-2, \pm 1), (0, \pm 3), (3, \pm 6), (6, \pm 15), (40, \pm 253)$
10	$(-1, \pm 3)$
11	çözümü yok
12	$(-2, \pm 2), (13, \pm 47)$
13	çözümü yok
14	çözümü yok
15	$(1, \pm 4), (109, \pm 1138)$
16	$(0, \pm 4)$
17	$(-2, \pm 3), (-1, \pm 4), (2, \pm 5), (4, \pm 9), (8, \pm 23), (43, \pm 282),$ $(52, \pm 375), (5234, \pm 378661)$
18	$(7, \pm 19)$
19	$(5, \pm 12)$
20	çözümü yok

BÖLÜM 5. SONUÇ VE ÖNERİLER

Bu çalışmada cebirsel sayılar kullanılarak Dedekind bölgelerinde ideallerin asal ideallerin çarpımı biçiminde yazılışları incelenmiştir. Ayrıca verilen bir k tamsayısı için $y^2 = x^3 + k$ Bachet denkleminin tamsayılarda çözümlerinin hangi durumlarda olmadığı incelenmiştir. Çözümü varsa, cebirsel sayılar kullanılarak bu çözümlerin nasıl elde edildiği gösterilmiştir. Özellikle $k = -31$ için denklemin çözümünün olmadığı ispatıyla verilmiştir. Benzer metodla $k = 13$ ve $k = 51$ için de Bachet denkleminin çözümünün olmadığı gösterilebilir. İdeallerin asal ideallerin çarpımı biçiminde yazılışları Bachet denklemi gibi Diyofant denklemlerinin çözümünde kolaylık sağlamaktadır. Bu nedenle Diyofant denklemlerinin çözümüyle ilgilenmek isteyen için cebirsel sayılar önem taşımaktadır. Konuyla ilgilenmek isteyenlere [1] ve [2] numaralı kaynaklar tavsiye edilebilir.

KAYNAKLAR

- [1] Alaca, Ş., Williams, K.S., Introductory Algebraic Number Theory, Cambridge University Press, New York, 2004.
- [2] Marcus, D.A., Number fields, Springer-Verlag, New York, 1977
- [3] Vold, E.H., Unique Factorization of Ideals, Norwegian University of Science and Technology, Department of Mathematical Sciences, Master thesis, 2013
- [4] Yang, M., Ideals and class group of number fields, Kent State University, Master thesis, 2018.
- [5] Fraleigh, J.B., A First Course in Abstract Algebra, Seventh Edition, Pearson Education, Harlow, 2014.

ÖZGEÇMİŞ

Ahmet Şamil ÖZMEN, 13.02.1990'da Alanya'da doğdu. İlk, orta ve lise eğitimini Sakarya'da tamamladı. 2007 yılında Figen Sakallıoğlu Anadolu Lisesi'nden mezun oldu. 2008 yılında başladığı Sakarya Üniversitesi Matematik Bölümü'nü 2012 yılında bitirdi. 2012 yılında Sakarya Üniversitesi'nde yüksek lisans eğitimine başladı.

