Bölüm 11

Tamlık Bölgelerinde Çarpanlara Ayırma

Bu bölümde polinomların sıfırları ve indirgenmez polinom kavramları tanımlanacaktır. Ayrıca tek türlü çarpanlara ayırma bölgeleri ile Euclid bölgeleri ele alınacak bu bölgeler arasındaki ilişkiler incelenecektir. Bu bölümde F bir cisim olarak alınacaktır.

11.1 Polinomlar Halkasında Çarpanlara Ayırma

Tanım 11.1.1 *$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$ olsun. $c \in F$ için*

$$g : F \to F,\ g(c) = a_0 + a_1c + \cdots + a_nc^n$$

şeklinde tanımlı fonksiyona bir **polinom fonksiyonu** *denir.*

Tanım 11.1.2 *$c \in F$ olmak üzere $\sigma_c(f(x)) = f(c)$ ile tanımlı $\sigma_c : F[x] \to F$ fonksiyonu bir epimorfizmadır ve bu epimorfizmaya* **değer epimorfizması** *adı verilir.*

Tanım 11.1.3 *$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$ olsun. Eğer bir $c \in F$ için $f(c) = 0$ oluyorsa c ye $f(x)$ polinomunun bir* **sıfırı** *denir.*

Örnek 11.1.4 $f(x) = x^2 + \overline{1} \in \mathbb{Z}_5[x]$ polinomu için $f(\overline{2}) = \overline{2}^2 + \overline{1} = 0$ olduğundan $f(x)$ polinomunun bir sıfırı $\overline{2}$ dir. ▲

Teorem 11.1.5 (Kalan Teoremi) *$f(x) \in F[x]$ ve $c \in F$ olsun. Bu durumda $f(x)$ polinomunun $x - c$ ye bölümünden kalan $f(c)$ dir.*

Teorem 11.1.6 (Çarpan Teoremi) *$f(x) \in F[x]$ ve $c \in F$ olsun. $x - c \mid f(x)$ olması için gerek ve yeter şart $f(c) = 0$ olmasıdır.*

Örnek 11.1.7 $f(x) = x^3 + \overline{a}x^2 + \overline{4}x + \overline{6} \in \mathbb{Z}_7[x]$ polinomunun bir çarpanının $x + \overline{3}$ olması için $\overline{a}$ nin ne olması gerektiğini bulalım. Eğer $x + \overline{3}$, $f(x)$ in bir çarpanı ise $f(\overline{4}) = \overline{64} + \overline{16}\overline{a} + \overline{16} + \overline{6} = \overline{0}$ ve buradan $2\overline{a} + \overline{2} = \overline{0}$ olup $2\overline{a} = -\overline{2} = \overline{5}$ tir. Dolayısıyla $\overline{a} = \overline{6}$ dır. ▲

Teorem 11.1.8 *$f(x) \in F[x]$ derecesi n, başkatsayısı a olan bir polinom olsun. Eğer $f(x)$ polinomunun F cismi içerisinde n tane farklı sıfırı $c_1,\ c_2, \cdots,\ c_n$ ise*

$$f(x) = a(x - c_1)(x - c_2)\cdots(x - c_n)$$

şeklinde yazılabilir.

Sonuç 11.1.9 *$n \in \mathbb{Z}^+$ olmak üzere F cismi üzerinde derecesi n olan bir polinomun F cismi içerisinde en fazla n tane farklı sıfırı vardır.*

İndirgenmez Eleman ve İndirgenmez Polinom

Tanım 11.1.10 *R birimli ve değişmeli bir halka, $a,\ b,\ c \in R$ olmak üzere eğer*

(1) *$c \neq 0$ ve c tersinir değil,*

(2) *$c = ab$ iken a ya da b tersinir*

ise c ye R de bir **indirgenmez eleman** *denir.*

Örnek 11.1.11 $\mathbb{Z}_{10}$ halkasında $\bar{2}$ elemanı asal olmasına rağmen indirgenmez değildir. ▲

Teorem 11.1.12 *R bir tamlık bölgesi olsun. Bu durumda R nin her asal elemanı indirgenmezdir.*

Teorem 11.1.13 *R bir esas ideal bölgesi ve $p \in R$ olsun. p nin asal olması için gerek ve yeter şart p nin indirgenmez olmasıdır.*

Tanım 11.1.14 *R birimli bir halka, x bir belirsiz, n pozitif bir tamsayı olmak üzere $f(x) \in R[x]$ sabit olmayan bir polinom olsun. Eğer $f(x) = g(x) \cdot h(x)$ şartını sağlayan her $g(x), h(x) \in R[x]$ için $g(x)$ ya da $h(x)$ tersinir ise $f(x)$ polinomuna R üzerinde (ya da $R[x]$ içinde) bir* **indirgenmez polinom** *denir.*

Örnek 11.1.15 $p(x) = 2+4x \in \mathbb{Z}[x]$ polinomunu göz önüne alalım. $p(x) = 2+4x = 2(x+2)$ yazılışında çarpanların her ikisi de $\mathbb{Z}[x]$ içinde tersinir olmadığından verilen polinom $\mathbb{Z}$ de indirgenmez değildir. Fakat $p(x) = 2 + 4x = 2(x + 2)$ yazılışında 2 tersinir olduğundan $p(x)$ polinomu $\mathbb{Q}[x]$ içinde indirgenmezdir. ▲

Uyarı 11.1.16 Katsayıları bir F cisminden alınan sıfırdan farklı birinci dereceden her polinom F üzerinde indirgenmezdir. ♦

Örnek 11.1.17 $f(x) = x^4 + 1 \in \mathbb{Q}[x]$ polinomunu göz önüne alalım.

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

olduğundan $f(x)$ polinomu $\mathbb{Q}$ da indirgenmez olmasına rağmen $\mathbb{R}$ de indirgenebilirdir. ▲

Örnek 11.1.18 $f(x) = x^2 + 1$ polinomunu göz önüne alalım.

$$x^2 + 1 = (x - i)(x + i)$$

olduğundan $f(x)$ polinomu $\mathbb{C}$ de indirgenebilir olmasına rağmen $\mathbb{R}$ de ve $\mathbb{Q}$ da indirgenmezdir. ▲

Teorem 11.1.19 *$f(x) \in F[x]$ polinomunun derecesi 2 ya da 3 olsun. Bu durumda $f(x)$ in F üzerinde indirgenmez olması için gerek ve yeter şart $f(x)$ in F cismi içinde bir sıfıra sahip olmamasıdır.*

Örnek 11.1.20 $f(x) = x^4 + 2x^2 + 1 \in \mathbb{Q}[x]$ polinomunu göz önüne alalım. $f(x)$ polinomu

$$x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$$

şeklinde yazılabilir. Dolayısıyla $f(x)$ polinomu $\mathbb{Q}$ içinde bir sıfıra sahip olmamasına rağmen $\mathbb{Q}[x]$ içinde indirgenebilirdir. ▲

Örnek 11.1.21 $\mathbb{Z}_3$ üzerinde indirgenmez ve derecesi 2 olan bütün monik polinomları belirleyelim. Aradığımız polinomların derecesi 2 olduğundan Teorem 11.1.19 gereğince bu polinomların $\mathbb{Z}_3$ üzerinde indirgenmez olmaları için gerek ve yeter şart bu polinomların $\mathbb{Z}_3$ içerisinde bir sıfıra sahip olmamasıdır. Bu sebeple aradığımız polinomlar $x^2 + \overline{1}$, $x^2 + x + \overline{2}$, $x^2 + \overline{2}x + \overline{2}$ şeklindedir. ▲

Teorem 11.1.22 *$p(x) \in F[x]$ indirgenmez bir polinom olmak üzere eğer $p(x) \mid f(x)g(x)$ ise $p(x) \mid f(x)$ veya $p(x) \mid g(x)$ dir.*

Sonuç 11.1.23 *$p(x) \in F[x]$ indirgenmez bir polinom olmak üzere eğer $p(x) \mid f_1(x)f_2(x)\cdots f_n(x)$ ise en az bir $1 \leq i \leq n$ için $p(x) \mid f_i(x)$ dir.*

Teorem 11.1.24 (Tek Türlü Çarpanlara Ayırma Teoremi) *F cismi üzerinde pozitif dereceli her polinom, bu polinomun başkatsayısı ile F cismi üzerinde sonlu sayıda monik indirgenmez polinomun çarpımı olarak yazılabilir. Bu çarpım çarpanların sırası farkıyla bir tektir.*

Örnek 11.1.25 $f(x) = \overline{2}x^4 + x^3 + \overline{3}x^2 + \overline{2}x + \overline{4} \in \mathbb{Z}_5[x]$ veriliyor. $f(\overline{0}) = \overline{4}$, $f(\overline{1}) = \overline{2}$, $f(\overline{2}) = \overline{0}$, $f(\overline{3}) = \overline{1}$, $f(\overline{4}) = \overline{1}$ olduğundan $\overline{2}$, $f(x)$ in bir sıfırıdır. Çarpan Teoremi gereğince, $f(x)$ in bir böleni $x-\overline{2}$ dir. Bu nedenle $f(x) = (x-\overline{2})g(x)$ olacak biçimde $g(x) = \overline{2}x^3+\overline{3}x+\overline{3}$ polinomu elde edilir. $g(\overline{0}) = \overline{3}$, $g(\overline{1}) = \overline{3}$, $g(\overline{2}) = \overline{0}$ olduğundan $\overline{2}$, $g(x)$ in bir sıfırıdır. Bu nedenle $g(x) = (x - \overline{2})h(x)$ olacak biçimde $h(x) = \overline{2}x^2 + \overline{4}x + \overline{1}$ polinomu vardır. Fakat bu polinomun $\mathbb{Z}_5$ içerisinde sıfırı yoktur. $h(x)$ in derecesi 2 olduğundan $h(x)$ indirgenmezdir. Ayrıca,

$$\begin{aligned} f(x) &= (x - \overline{2})(x - \overline{2})(\overline{2}x^2 + \overline{4}x + \overline{1}) \\ &= (x - \overline{2})^2(\overline{2}x^2 + \overline{4}x + \overline{1}) \\ &= \overline{2}(x - \overline{2})^2(x^2 + \overline{2}x + \overline{3}) \\ &= \overline{2}(x + \overline{3})^2(x^2 + \overline{2}x + \overline{3}) \end{aligned}$$

dir. Böylece $f(x)$ polinomu başkatsayısı $\overline{2}$ ile sonlu sayıda monik indirgenmez polinomun çarpımı biçiminde ifade edilmiş olur. ▲

11.2 Tek Türlü Çarpanlara Ayırma Bölgesi (TÇAB)

Tanım 11.2.1 *D bir tamlık bölgesi ve a, $b \in D$ olsun. Eğer $a = bu$ olacak şekilde $u \in U(D)$ varsa a ve b ye* **bağdaşıktır** *denir.*

Tanım 11.2.2 *D bir tamlık bölgesi olsun. Eğer*

(1) *D nin sıfırdan farklı tersinir olmayan her a elemanı D nin indirgenmez elemanlarının bir çarpımı ise yani $a = p_1^{n_1} \cdots p_r^{n_r}$ olacak şekilde $p_i \in D$ $(1 \leq i \leq r)$ indirgenmez elemanları ve $n_i \in \mathbb{Z}^+$ var ve*

(2) *$a = p_1^{n_1} \cdots p_r^{n_r} = q_1^{m_1} \cdots q_s^{m_s}$, herhangi iki p_i ve herhangi iki q_j bağdaşık olmayacak şekilde p_i, q_j $(1 \leq i \leq r,\ 1 \leq j \leq s)$ indirgenmez elemanları ve n_i, $m_j \in \mathbb{Z}^+$ varsa, o zaman $r = s$, $n_i = m_j$ ve p_i, yalnız bir q_j ile bağdaşık*

ise D ye bir **tek türlü çarpanlara ayırma bölgesi (TÇAB)** *denir.*

Örnek 11.2.3 $\mathbb{Z}$ ve $\mathbb{Z}[x]$ halkaları TÇAB dir. ▲

Teorem 11.2.4 *Her esas ideal bölgesi bir TÇAB dir.*

Sonuç 11.2.5 *Bir F cismi için $F[x]$ bir TÇAB dir.*

Euclid Fonksiyonu ve Euclid Bölgesi

Tanım 11.2.6 *D bir tamlık bölgesi ve $d : D \setminus \{0\} \to (\mathbb{Z}^+ \cup \{0\})$ bir fonksiyon olsun. Eğer*

(1) *her $a,\ b \in D \setminus \{0\}$ için $d(a) \leq d(ab)$,*

(2) *eğer $a,\ b \in D$, $b \neq 0$ ise $a = bq + r$; $r = 0$ veya $d(r) < d(b)$ olacak şekilde $q,\ r \in D$ vardır*

şartları sağlanıyorsa D ye bir **Euclid bölgesi** *ve d ye de bir* **Euclid fonksiyonu** *denir.*

Örnek 11.2.7 $\mathbb{Z}$ halkası $d(a) = |a|$ ile tanımlı d fonksiyonu ile bir Euclid bölgesidir. ▲

Örnek 11.2.8 F bir cisim olmak üzere $F[x]$ polinomlar halkası $d(f(x)) = \text{der} f(x)$ ile tanımlı d fonksiyonu ile bir Euclid bölgesidir. ▲

Örnek 11.2.9 $\mathbb{Z}[i] = \{a + bi |\ a,\ b \in \mathbb{Z}\}$ Gauss tamsayılar halkası $d(a + bi) = a^2 + b^2$ ile tanımlı d fonksiyonu ile bir Euclid bölgesidir. ▲

Teorem 11.2.10 *Her Euclid bölgesi bir esas ideal bölgesidir.*

Sonuç 11.2.11 *Her Euclid bölgesi bir TÇAB dir.*