ONDOKUZ MAYIS ÜNİVERSİTESİ UZAKTAN EĞİTİM MERKEZİ

Ondokuz Mayıs Üniversitesi
Fen Edebiyat Fakültesi
Matematik Bölümü
Dijital Ders Platformu

Cebir 2

Polinom Halkaları

Prof. Dr. Şenol EREN

Ders 9

BÖLÜM 4

POLİNOM HALKALARI

Tanım 4.1 R bir halka, x bilinmeyen ve $a_0, a_1, \dots, a_n$ler R'nin elemanları olmak üzere $a_0 + a_1x + \dots + a_nx^n$ ifadesine R'den katsayılı polinom denir. Tüm bu polinomlar kümesi $R[x]$ ile gösterilir.

Tanım 4.2 $f(x) = a_0 + a_1x + \dots + a_nx^n$ ve $g(x) = b_0 + \dots b_mx^m$ $R[x]$'te iki polinom olsun.

$f(x) = g(x) \iff \forall i \geq 0,\ a_i = b_i$ ise $f(x)$ ve $g(x)$ polinomlarına eşittirler denir.

Tanım 4.3 R bir halka olsun. Bütün katsayıları sıfır olan polinoma sıfır polinomu denir. R halkasının her bir elemanını bir polinom olarak düşünebiliriz. Bu polinomlara sabit polinomlar denir.

Örnek 4.4 Bir polinomda sıfır katsayılı terimler yazılmayabilir.

$$f(x) = \frac{2}{3} + 3x - \frac{5}{7}x^2 \in \mathbb{Q}[x]$$

Tanım 4.5 $f(x) = a_0 + a_1 x + \dots + a_n x^n \in R[x]$ ve $a_n \neq 0$ olsun. a_n'e polinomun başkatsayısı, n'ye polinomun derecesi, a_0'a polinomun sabiti denir. Sıfır polinomunun derecesi $-\infty$ olarak tanımlanır. $f(x)$ polinomunun derecesi $d^0 f(x)$ ile gösterilir. Ayrıca sıfırdan farklı sabit polinomun derecesi 0'dır.

Tanım 4.6 $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $g(x) = b_0 + b_1 x + \dots + b_m x^m$ olsun. $\forall i \geqslant 0$ için $c_i = a_i + b_i$ olmak üzere, f ve g polinomlarının toplamı $f(x) + g(x) = c_0 + c_1 x + \dots + c_k x^k$ ile tanımlanır.

Tanım 4.7 Yukarıda verilen $f(x)$ ve $g(x)$ polinomlarının çarpımı $\forall i \geq 0$ için $c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$ olmak üzere $f(x) \cdot g(x) = c_0 + c_1 x + \cdots + c_t x^t$ ile tanımlanır.

Örnek 4.8 $f(x) = 3 + x - 2x^2$ $g(x) = x^2 - 3x^3 \in \mathbb{Z}[x]$ için $f(x) + g(x)$ ve $f(x) \cdot g(x)$ polinomlarını bulunuz.

Teorem 4.9 R bir halka ise $R[x]$ de bir halkadır.

İspat: Öğrenciye bırakılmıştır. Toplama ve çarpma işlemleri yukarıda tanımlandı.

Teorem 4.10 R Tamlık bölgesi ise $R[x]$'de tamlık bölgesidir.

İspat: R birimli ve birimi 1_R ise $\forall f(x) \in R[x]$ için $f \cdot 1_R = 1_R f = f$ olup $R[x]$'de birimlidir.

$\forall a, b \in R$ için $a.b = ba$ ise $\forall f(x), g(x) \in R[x]$ için $f(x)g(x) = g(x)f(x)$ olur, o halde $R[x]$ değişmelidir.

R sıfır bölensiz olsun. $f, g \in R[x]$ için $f \neq 0, g \neq 0$ olsun. $f(x) = a_0 + a_1 x + \dots + a_m x^m$, $(a_m \neq 0)$ ve $g(x) = b_0 + b_1 x + \dots + b_n x^n$, $(b_n \neq 0)$ diyelim.

$C_{n+m} = a_{m+n} b_0 + \dots + a_m b_n + \dots + b_{m+n}$ dir. $i > m$ için $a_i = 0$ ve $j > n$ için $b_j = 0$ olduğundan $C_{m+n} = a_m b_n$ bulunur. $a_m \neq 0$, $b_n \neq 0$ aldığımızdan $C_{m+n} = a_m b_n \neq 0$ olur $(R, T.B)$ O halde $R[x]$ de $f \cdot g \neq 0$ bulunur.

Dolayısıyla $R[x]$ sıfır bölensizdir.

Sonuç 4.11. F cisim ise $F[x]$ tamlık bölgesidir.

Sonuç 4.12 R bir tamlık bölgesi ise $\forall f, g \in R[x]$ için $d^\circ(f g) = d^\circ f + d^\circ g$ dir.

Eğer R tamlık bölgesi değilse $d^\circ(f \cdot g) \leq d^\circ f + d^\circ g$ dir.

Örnek 4.13 $\mathbb{Z}_{10}$ da $f(x) = \bar{2} + x + 5x^3$ $g(x) = 1 + 2x^2$ olsun. $f(x) \cdot g(x) = \bar{2} + x + \bar{4}x^2 + \bar{7}x^3$ bulunur.

$d^\circ f = 3$ $\quad d^\circ g = 2$ $\quad d^\circ(f \cdot g) = 3$ olup

$3 \leq 5$ dir.

Tanım 4.14 $f(x) = a_0 + a_1x + \dots + a_m x^m \in R[x]$ ve $a \in R$ olsun. $f(a) = a_0 + a_1 a + \dots + a_m a^m \in R$'ye f polinomunun a'daki değeri denir. Eğer $f(a) = 0$ ise a, ya f polinomunun kökü adı verilir.

Teorem 4.15 R değişmeli ve birimli bir halka $f, g \in R[x]$ olsun. $g(x) \neq 0$ ve $g(x)$'in baş katsayısı terslenebilsin. Bu durumda $f(x) = q(x)g(x) + r(x)$ ve $d^0 r < d^0 g$ olacak şekilde teklikle belirli $\exists q, r \in R[x]$ vardır.

İspat: $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $d^0 f = n$, $b_m^{-1} \in R$ olmak üzere $g(x) = b_0 + \dots + b_m x^m$, $d^0 g = m$ olsun.
Önce varlığını gösterelim. n üzerinde tümevarım uygulayalım. $n = 0 \Longrightarrow 0 = d^0 f < d^0 g \Rightarrow q = 0,\ r = f$ alınır.
$0 = d^0 f = d^0 g \Longrightarrow r = 0,\ q = a_0 b_0^{-1}$ alınabilir.

iddia derecesi n'den küçük olan polinomlar için doğru olsun. Genelliği bozmadan $d^0 g \leq d^0 f$ alabiliriz. Aksi halde $q=0$, $r=f$ alınır. $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$ diyelim $d^0 f_1 < n$ olduğundan $\exists q_1, r \in \mathbb{R}[x]$ ve $d^0 r < d^0 g$ polinomları vardır ki $f_1(x) = q_1(x) g(x) + r(x)$ olur.

$$f(x) = a_n b_m^{-1} x^{n-m} g(x) + q_1(x) g(x) + r(x)$$

$$= [a_n b_m^{-1} x^{n-m} + q_1(x)] g(x) + r(x), \quad d^0 r < d^0 g$$

$q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$ ve $r(x) \in \mathbb{R}[x]$ bulunmuş olur.

Tekliğini gösterelim $f(x) = q_1(x) g(x) + r_1(x) = q_2(x) g(x) + r(x)$ $d^0 r_1 < d^0 g$ ve $d^0 r_2 < d^0 g$ olsun. $(q_1(x) - q_2(x)) g(x) = r_2(x) - r_1(x)$ eşitliğinden dereceler karşılaştırılırsa

$d^0(r_2(x) - r_1(x)) = d^0(q_1(x) - q_2(x)) + d^0 g$ bulunur.

$d^0(r_2(x) - r_1(x)) < d^0 g$ olduğundan bu ancak $q_1(x) = q_2(x)$ olmasıyla sağlanır. Dolayısıyla $r_1(x) = r_2(x)$ bulunur.

Sonuç 4.16 F bir cisim ise bölme algoritması geçerlidir.

Sonuç 4.17 $f \in R[x]$ olsun. $f(x) = (x-a)q(x) + r(x)$ olacak şekilde bir tek $q(x) \in R[x]$ vardır.

İspat: $f(x)$ ve $x-a$ polinomlarına bölme algoritması uygularsak $f(x) = (x-a)q(x) + r(x)$, $\exists q, r \in R[x]$ bulunabilir. Ayrıca $d^0 r < d^0(x-a) = 1$ yani $r(x) = r \in R$ sabittir. $x = a$ için $f(a) = r(a) = r$ olur ve $q(x)$ teklikle belirlidir.

Tanım 4.18 $f(x), g(x) \in F[x]$, $f \neq 0$, $g \neq 0$ olsun.
$f(x) = h(x).g(x)$ olacak şekilde $h(x) \in F[x]$ varsa $g(x)$, $f(x)$'i bölüyor denir ve $g(x) \mid f(x)$ ile gösterilir.

Tanım 4.19 ikisi birden sıfır olmayan $f(x), g(x) \in F[x]$ için,

1- $d(x) \mid f(x) \wedge d(x) \mid g(x)$

2- $h(x) \mid f(x) \wedge h(x) \mid g(x) \Rightarrow h(x) \mid d(x)$

şartlarını sağlayan $d(x)$ monik polinomuna $f(x)$ ve $g(x)$ polinomlarının en büyük ortak böleni denir. $d(x) = ebob(f(x), g(x))$ ile gösterilir.

Tanım 4.20 $f(x), g(x) \in F[x]$ polinomları için $ebob(f, g) = 1$ ise bu polinomlara aralarında asaldırlar denir.

Teorem 4.21 F cisim ve $f \in F[x]$, $d^\circ f \geq 1$ olsun. $(f) = f(x)F[x]$ temel ideali için $F[x]/(f)$ bölüm halkasının tam temsilciler sistemi olarak $d^\circ r < d^\circ f$ olan $r(x) \in F[x]$ polinomları alınabilir.

İspat: $\forall g \in F[x]$-i f ile kalanlı bölersek

$g(x) = f(x)q(x) + r(x)$, $d^\circ r < d^\circ f$. $\exists q, r \in F[x]$ bulunabilir.

$g \equiv r \pmod f$ dir. O halde her mod f denklik sınıfında $d^\circ r < d^\circ f$ olacak şekilde $\exists r \in F[x]$ var. Ayrıca $r_1 \neq r_2$, $d^\circ r_1 < d^\circ f$, $d^\circ r_2 < d^\circ f$ ise r_1 ve r_2 aynı sınıfta olamaz. $r_1 \equiv r_2 \pmod f \Longleftrightarrow r_1 - r_2 \in (f) \Longleftrightarrow r_1 - r_2 = f.g$ demektir. $d^\circ(r_1 - r_2) \leq \max(d^\circ r_1, d^\circ r_2) < d^\circ f$ olduğundan denklik ancak $r_1 = r_2$ için sağlanır.

$F[x]/(f)$ bölüm halkası için $\{ r \in F[x] \mid d^\circ r < d^\circ f \}$

tam temsilciler sistemidir.

Örnek 4.22 $f = 1 + x + x^2 \in \mathbb{Z}_2[x]$ için $\mathbb{Z}_2[x]/(f)$ bölüm halkasının tam temsilciler sistemi

$\{\bar{a} + \bar{b}x \mid a, b \in \mathbb{Z}_2\} = \{\bar{0}, \bar{1}, x, \bar{1} + x\}$ bulunur.

$\mathbb{Z}_2[x]/(f) = \{(f), \bar{1} + (f), x + (f), \bar{1} + x + (f)\}$ dir.

Üstelik $\mathbb{Z}_2[x]/(f)$ cisimdir.

$\cdot$	$\bar{1}+(f)$	$x+(f)$	$\bar{1}+x+(f)$
$1+(f)$	$\bar{1}+(f)$	$x+(f)$	$\bar{1}+x+(f)$
$x+(f)$	$x+(f)$	$\bar{1}+x+(f)$	$1+(f)$
$\bar{1}+x+(f)$	$\bar{1}+x+(f)$	$1+(f)$	$x+(f)$

$+$	(f)	$\bar{1}+(f)$	$x+(f)$	$\bar{1}+x+(f)$
(f)	(f)	$1+(f)$	$x+(f)$	$\bar{1}+x+(f)$
$1+(f)$	$1+(f)$	(f)	$1+x+(f)$	$x+(f)$
$x+f$	$x+f$	$1+x+(f)$	(f)	$1+(f)$
$1+x+f$	$1+x+(f)$	$x+(f)$	$1+(f)$	(f)

ONDOKUZ MAYIS ÜNİVERSİTESİ
UZAKTAN EĞİTİM MERKEZİ

Ondokuz Mayıs Üniversitesi
Fen Edebiyat Fakültesi
Matematik Bölümü
Dijital Ders Platformu

Teşekkürler

Prof. Dr. Şenol EREN

Cebir II

Ders 9