ONDOKUZ MAYIS ÜNİVERSİTESİ
UZAKTAN EĞİTİM MERKEZİ

Ondokuz Mayıs Üniversitesi
Fen Edebiyat Fakültesi
Matematik Bölümü
Dijital Ders Platformu

Cebir 2

Polinom Halkalarında Asal Çarpanlara Ayrılış

Prof. Dr. Şenol EREN

Ders 12

BÖLÜM 6

POLİNOMLARDA ASAL ÇARPANLARA AYRILIŞ

Bu bölümde aksi söylenmediği müddetçe R halkası TAG bölge alınacaktır.

Tanım 6.1 $f(x) = a_n x^n + \dots + a_1 x + a_0 \in R[x]$ polinomu için $ebob(a_0, \dots, a_n)$'ne f polinomunun kapsamı denir. $c(f)$ ile gösterilir. $c(f) = 1$ ise f'ye ilkel polinom denir.

Teorem 6.2 $f(x) \in R[x]$ ve $f(x) \neq 0$ ise $f(x) = c(f) \cdot f^*(x)$ olacak şekilde $\exists f^*(x) \in R[x]$ vardır. Üstelik bu yazılış tek türlüdür.

İspat: $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $c = c(f)$ olsun. $i = 0, 1, \dots, n$ için $a_i = c k_i$, $ebob(k_0, \dots, k_n) = 1$ dir.

$f^*(x) = k_n x^n + \dots + k_1 x + k_0$ istenilen özelliktedir.

$f(x) \in R[x]$ için $f(x) = c \cdot f^*(x) = d\, g^*(x)$ şeklinde iki yazılışı olsun. $c(f^*) = c(g^*) = 1$ olduğundan $c(f) = c$ ve $c(f) = d$ olur. Dolayısıyla kapsam ilgililik farkıyla tek olduğundan istenen görülür.

Teorem 6.3 İlkel iki polinomun çarpımı da ilkeldir.

İspat: $f(x) = a_n x^n + \dots + a_1 x + a_0$, $g(x) = b_m x^m + \dots + b_1 x + b_0$ ve $\forall i \geq 0$ için $c_i = a_i b_0 + \dots + a_0 b_i$ olmak üzere $f \cdot g = c_{m+n} x^{m+n} + \dots + c_1 x + c_0$ dır. p, R'nin asal elemanı olmak üzere f ilkel olduğu için a_i'lerin, g ilkel olduğu için b_j'lerin bazıları p ile bölünmez. $p \nmid a_i$ ve $p \nmid b_j$ ilk katsayılar olsun. $p \nmid a_i b_j$ dir.

$c_{i+j} = a_0 b_{i+j} + \dots + a_i b_j + \dots + a_{i+j} b_0$ ve

$0 \le k < i$ için $p \mid a_k$, $0 \le t < j$ için $p \mid b_t$ olup $p \mid c_{i+j}$ olması $p \mid a_i b_j$ gerektirir. p asal olduğundan bu $p \mid a_i \vee p \mid b_j$ demektir. Bu bir çelişkidir. O halde c_k $(k=0,1,\ldots,m+n)$ lerin hepsini bölen bir asal yoktur. Dolayısıyla $c(f \cdot g) = 1$ dir.

Teorem 6.4 F, R halkasının kesir cismi, $f(x) \in F[x]$, $f(x) \neq 0$ olsun. $f(x) = a^* \cdot f^*(x)$, $\exists a^* \in F$, $\exists f^*(x) \in R[x]$ ilkel polinomu vardır.

İspat: F, R nin kesir cismi olduğundan F nin her elemanı $a, b \in R$, $b \neq 0$ için $\frac{a}{b}$ şeklindedir. $f(x) \in F[x]$ F nin uygun bir elemanı ile çarpılarak $R[x]$ elemanı yapılabilir. Teorem 6.2 kullanılarak istenen bulunur.

Örnek 6.5 $f(x) = \frac{2}{3}x^3 + \frac{1}{4}x^2 + \frac{1}{5}x + 2 \in Q[x]$, $[3,4,5] = 60$

$60 f(x) = 40x^3 + 15x^2 + 12x + 120 \in Z[x]$, $f(x) = \frac{1}{60}[40x^3 + 15x^2 + 12x + 120]$

Teorem 6.5 $f(x) \in R[x]$ ilkel polinom olsun. $f(x)$'in $R[x]$ de asal olması için gerek ve yeter şart, F, R'nin kesir cismi olmak üzere $f(x)$'in $F[x]$'de asal olmasıdır.

İspat: (Örneklerle Soyut Cebir Önerme 4.7.4)

Teorem 6.6 R bir TAG bölge ve f, $R[x]$ de ilkel polinom olsun. $f(x)$, $R[x]$ de asal elemanların çarpımı biçiminde yazılabilir ve bu yazılış tek türlüdür.

İspat: (Örneklerle Soyut Cebir Önerme 4.7.5)

Teorem 6.7 R bir TAG bölge ise $R[x]$'de TAG bölgedir.

İspat: (Örneklerle Soyut Cebir Teorem 4.7.1)

Teorem 6.8 $f(x) \in F[x]$, $d^0 f = 2 \vee 3$ olsun. Bu taktirde $f(x)$, $F[x]$ indirgenemezdir $\Longleftrightarrow$ $f(x)$, F'de köke sahip değildir.

İspat: $(\Longrightarrow)$ $f(x)$, $F[x]$ indirgenemez ve $d^0 f = 3$ olsun. köke sahip ve bu kök a ise $x-a \mid f(x)$, $f(x)$, $F[x]$'de indirgenirdir.

$(\Longleftarrow)$ $f(x)$, F'de köke sahip olmasın. $f(x)$ indirgenebilir olsun. $f(x) = g(x) \cdot h(x)$, $d^0 g, d^0 h \geq 1$, $g(x), h(x) \in F[x]$ vardır. $d^0(g \cdot h) = d^0 g + d^0 h = 3$ olduğundan ya $d^0 g = 2 \wedge d^0 h = 1$ yada $d^0 g = 1 \wedge d^0 h = 2$ dir. $d^0 g = 1$, $d^0 h = 2$ olsun. $g(x) = ax + b$, $a \neq 0$, $-a^{-1}b \in F$ ve $g(-a^{-1}b) = 0$ olur. Bu ise kabulle çelişir. O halde indirgenemezdir. $d^0 f = 2$ içinde ispat benzer şekilde yapılır.

Örnek 6.9 $f(x) = x^3 + \bar{2}x + \bar{1} \in \mathbb{Z}_3[x]$ olsun.

$f(\bar{0}) = \bar{1} \neq \bar{0}$ $f(\bar{1}) = \bar{1} \neq \bar{0}$, $f(\bar{2}) = \bar{1} \neq \bar{0}$ olup

$f(x)$, $\mathbb{Z}_3[x]$ indirgenemez (Asal) polinomdur.

Teorem 6.10 $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$, $d^0 f = n > 1$ olsun. $\bar{f}(x) = \bar{a_0} + \bar{a_1}x + \dots + \bar{a_n}x^n \in \mathbb{Z}_p[x]$'de indirgenemez ve $d^0 f = d^0 \bar{f}$ olacak şekilde bir p asalı varsa $f(x)$, $\mathbb{Q}[x]$'de indirgenemezdir (Asaldır).

İspat: $f(x)$ polinomu p asalı için teoremin şartlarını sağlasın. $f(x)$, $\mathbb{Q}[x]$ de indirgenebilir olsun. O zaman $f(x) = g(x)h(x)$, $g(x) = b_0 + b_1x + \dots + b_mx^m$, $h(x) = c_0 + c_1x + \dots + c_kx^k$ $(m+k=n)$ olacak şekilde $g(x), h(x) \in \mathbb{Z}[x]$ vardır.

$\bar{a_0} + \bar{a_1}x + \dots + \bar{a_n}x^n = (\bar{b_0} + \bar{b_1}x + \dots + \bar{b_m}x^m)(\bar{c_0} + \bar{c_1}x + \dots + \bar{c_k}x^k)$

$\bar{b_m} \cdot \bar{c_k} \neq \bar{0}$, $\bar{b_m} \cdot \bar{c_k} \in \mathbb{Z}_p$ dir. $\Rightarrow$ $\bar{b_m} \neq \bar{0}$, $\bar{c_k} \neq \bar{0}$ dır. Burada $\bar{g}(x)$, $\bar{h}(x)$ birim değildir, $\bar{f}(x)$, $\mathbb{Z}_p[x]$ indirgenemez olmaz.

bu bir çelişkidir. O halde $f(x)$, $\mathbb{Q}[x]$ de indirgenemezdir.

Örnek 6.11 $f(x)=\frac{5}{7}x^3-\frac{1}{2}x+1 \in \mathbb{Q}[x]$ polinomu için

$[7,2]=14$ $\quad 14f(x)=10x^3-7x+14 \in \mathbb{Z}[x]$

$p=3$ alınırsa $\bar{f}_1(x)=\overline{10}x^3-\bar{7}x+\overline{14}=x^3-x+\bar{2}$ olur.

$\bar{f}_1(\bar{0})=\bar{2}\neq\bar{0}$, $f(\bar{1})=\bar{2}\neq\bar{0}$, $f(\bar{2})=\bar{2}\neq\bar{0}$ olup

$\bar{f}_1(x)$, $\mathbb{Z}_3[x]$ köke sahip değil $14f(x)\in\mathbb{Q}[x]$'de indirgenemezdir. 14, $\mathbb{Q}[x]$'de birimsel olduğundan $f(x)$, $\mathbb{Q}[x]$ indirgenemezdir.

Teorem 6.12 $f(x)=a_0+a_1x+\dots+a_nx^n \in \mathbb{Z}[x]$, $d^\circ f=n$ $a_0\neq 0$ olsun. u, v aralarında asal olmak üzere $\frac{u}{v}\in\mathbb{Q}$ $f(x)$'in bir kökü ise $u|a_0$, $v|a_n$ dir.

İspat: $\frac{u}{v}$, $f(x)$ kökü olsun.

$$0 = f\left(\frac{u}{v}\right) = a_0 + a_1\left(\frac{u}{v}\right) + \cdots + a_n\left(\frac{u}{v}\right)^n$$

$$0 = a_0 v^n + a_1 u.v^{n-1} + \cdots + a_n u^n$$

$$v\left(a_0 v^{n-1} + \cdots + a_{n-1} u^{n-1}\right) = -a_n u^n$$

$\Rightarrow v \mid -a_n u^n \Rightarrow v \mid a_n$ bulunun. Benzer sekilde $u \mid a_0$ olduğuda gösterilebilir.

Örnek 6.13 $f(x) = 2x^3 - 7x + 1$, $(u, v) = 1$ $f\left(\frac{u}{v}\right) = 0$ olsun.

$u \mid 1$, $v \mid 2$ $\Rightarrow u = \mp 1$, $v = \mp, \mp 2$ $\frac{u}{v} = \mp 1, \mp \frac{1}{2}$ olmalı

$f(1) \neq 0$, $f(-1) \neq 0$, $f\left(\frac{1}{2}\right) \neq 0$ $f\left(-\frac{1}{2}\right) \neq 0$ dır.

$f(x)$, $\mathbb{Q}$'da köke sahip degil

Teorem 6.13 (Eisenstein Asallık Kriteri) R bir TAG bölge ve $f = a_0 + a_1x + \dots + a_nx^n \in R[x]$ ilkel polinom olsun. R'de aşağıdaki özellikleri sağlayan π asal elemanı varsa f, $R[x]$'de asaldır.

i) $\pi \mid a_0, a_1, \dots, a_{n-1}$

ii) $\pi \nmid a_n$

iii) $\pi^2 \nmid a_0$

İspat: Kabul edelim ki $f(x) \in R[x]$ asal olmasın.
$a_0 + a_1x + \dots + a_nx^n = (b_0 + b_1x + \dots + b_rx^r)(c_0 + c_1x + \dots + c_sx^s)$
$(r+s=n,\ r \geq 1,\ s \geq 1)$ yazılsın. $a_0 = b_0c_0$ ve $\pi^2 \nmid a_0$ ise π, b_0 ve c_0 ın ikisini birden bölmez. Fakat $\pi \mid a_0 = b_0c_0$ olduğundan $\pi \mid b_0 \vee \pi \mid c_0$ dır. Kabul edelim ki $\pi \nmid b_0 \wedge \pi \mid c_0$ olsun f ilkel olduğundan $b_0 + b_1x + \dots + b_rx^r$ ve $c_0 + c_1x + \dots + c_sx^s$ de ilkel dolayısıyla c_i lerin hepsi

birden π ile bölünmez. Bu katsayıların ilki c_v olsun. $0 \leq i < v$, $\pi | c_i$, $\pi | a_v$ $(v<n)$ dir

$$a_v = b_0 c_v + \cdots + b_v c_0 \Rightarrow \pi | b_0 c_v = a_v - (b_1 c_{v-1} + \cdots + b_v c_0)$$

bulunur. Bu bir çelişkidir. $f(x)$, $R[x]$ asaldır.

Sonuç 6.14 Teoremin şartları altında F, R'nin kesir cismi ise f, $F[x]$'de asaldır.

Örnek 6.15 $f(x) = x^4 + 3x^3 - 3x + 6 \in \mathbb{Z}(x)$

$\pi = 3$ alınırsa $\mathbb{Z}[x]$ ve $\mathbb{Q}(x)$ de asaldır.

Ondokuz Mayıs Üniversitesi
Fen Edebiyat Fakültesi
Matematik Bölümü
Dijital Ders Platformu

Teşekkürler

Prof. Dr. Şenol EREN

Cebir II

Ders 12