



Polinomların Kökleri

Polinomları geçen sayımızda oldukça ayrıntılı bir biçimde tanımlamıştık. Özetle, eğer R bir halkaysa¹, R katsayılı bir polinom, $p_0, p_1, \dots, p_n \in R$ için,
$$p(X) = p_0 + p_1X + \dots + p_nX^n \in R[X]$$
 biçiminde yazılan bir terimdir.

Eğer $x \in R$ ise, p polinomunu x 'te değerlendirip, R 'nin

$$p(x) = p_0 + p_1x + \dots + p_nx^n$$

elemanını bulabiliriz. Sadece uygulamalı cebirin değil, cebirin kendisinin en önemli sorunlarından biri, $p(x) = 0$ eşitliğini sağlayan $x \in R$ elemanlarını bulmaktır. Bu tür $x \in R$ elemanlarına $p(X)$ polinomunun **kökü** denir.

Örneğin $X^2 - 2$ polinomunun \mathbb{Q} halkasında kökü yoktur ama \mathbb{R} halkasında iki kökü vardır: $\sqrt{2}$ ve $-\sqrt{2}$. Bir başka örnek: $2X - 1$ polinomunun \mathbb{Z} 'de kökü yoktur ama \mathbb{Q} 'da vardır: $1/2$. Son bir örnek: $X^2 - X$ polinomunun $\mathbb{Z}/6\mathbb{Z}$ 'de tam dört kökü vardır: $0, 1, 3, 4$.

Yukardaki örneklerde de görüldüğü gibi, bir polinomun kökleri polinoma göre olduğu kadar kökleri hangi halkada aradığımıza göre de değişir.

Bu bölümün amacı polinomların kökleriyle ilgili birkaç sonuç bulmak.

Eğer $p_n \neq 0$ ise p_n 'ye p polinomunun **başkatsayısı** adı verilir. Ayrıca, bu durumda, p 'nin derecesine n denir ve $d^\circ(p) = n$ yazılır. Eğer $p = 0$ ise, 0 olmayan bir katsayı yoktur ve o zaman da $d^\circ(p) = -\infty$ olarak tanımlanır.

Aynen tamsayılarda olduğu gibi (ama gerçekten aynen tamsayılarda olduğu gibi), çoğu zaman bir kalan da olsa, bir polinomu bir başka polinoma bölebiliriz. Bunu geçen sayımızda görmüştük:

Olgu. [MD-2004-I, sayfa 35, Teorem 3]. R bir halka olsun. $a, b \in R[X]$ olsun. Ayrıca b 'nin başkatsayısının R 'de tersinir olduğunu varsayalım. O za-

man $a = bq + r$ ve $d^\circ(r) < d^\circ(b)$ özelliklerini sağlayan bir ve bir tane R katsayılı (q, r) polinom çifti vardır.

\mathbb{Z} 'ye uygulaması çok pratik olan bir sonuçla başlayalım:

Önsav 1. R bir halka, $x \in R$ ve

$$p(X) = p_0 + p_1X + \dots + p_nX^n \in R[X]$$

olsun. $x \in R$, $p(X)$ 'in bir köküyse, x, p_0 'ı R 'de böler.

Kanıt: $0 = p(x)$ olduğundan, doğrudan $p(X)$ 'in tanımından,

$$p_0 = -x(p_1 + \dots + p_nx^{n-1})$$

buluruz. \square

Örnek. $p(X) = X^4 - 4X^3 - 19X^2 - 8X - 42$ polinomunun \mathbb{Z} 'deki tüm köklerini bulalım. Eğer x tamsayısı bu polinomun bir köküyse, Önsav 1'e göre, $x, 42$ 'yi \mathbb{Z} 'de bölmeli. Demek ki x ancak $\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42$ sayılarından biri olabilir. Teker teker deneyerek $x = -3, 7$ buluruz.

Kanıtlayacağımız ikinci sonuç konunun abecesidir diyebiliriz.

Teorem 2. R bir halka, $a \in R$ ve $p(X) \in R[X]$ olsun. a 'nın p 'nin kökü olması için gerek ve yeter koşul $X - a$ polinomunun $p(X)$ polinomunu $R[X]$ halkasında bölmesidir.

Kanıt: Önce $X - a$ polinomunun $p(X)$ polinomunu $R[X]$ 'te böldüğünü varsayalım. Bu varsayıma göre, bir $q(X) \in R[X]$ için

$$p(X) = (X - a)q(X).$$

Her iki tarafı da a 'da değerlendirelim:

$$p(a) = (a - a)q(a) = 0 \times q(a) = 0$$

elde ederiz. Demek ki $p(a) = 0$.

Şimdi, $p(a) = 0$ eşitliğini varsayalım. Yukardaki olguyu uygulayarak $p(X)$ polinomunu $X - a$ polinomuna bölelim:

$$p(X) = (X - a)q(X) + r(X)$$

eşitliğini ve

$$d^\circ(r(X)) < d^\circ(X - a) = 1$$

¹ Halka kavramıyla haşır neşir olmak istemeyen okur, bu ve bundan sonraki yazılarda R yerine $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ gibi bilinen sayı halkalarından herhangi birini alabilir. Halka kavramının tanımını sayfa 21'de bulabilirsiniz.

eşitsizliğini sağlayan $q(X)$ ve $r(X)$ polinomları bulunur. İkinci eşitsizlikten $r(X)$ 'in sabit bir polinom olduğu, yani bir $r \in R$ için $r(X) = r$ eşitliği çıkar. Demek ki

$$p(X) = (X - a)q(X) + r.$$

Şimdi bu eşitliğin sağını ve solunu a 'da değerlendirilim: $0 = p(a) = (a - a)q(a) + r = 0 \times q(a) + r = 0 + r = r$ buluruz. $r = 0$ bulduk. Sonuç:

$$p(X) = (X - a)q(X) + r = (X - a)q(X). \quad \square$$

Örnek. $p(X) = X^4 - 4X^3 - 19X^2 - 8X - 42$ polinomunun Z 'deki köklerini yukarıda bulmuştuk: -3 ve 7 . Teorem 2'ye göre $X + 3$ ve $X - 7$ polinomları $p(X)$ 'i $Z[X]$ 'te bölmeli. Nitekim, kolayca sağlaması yapılacağı üzere,

$$p(X) = (X + 3)(X^3 - 7X^2 + 2X - 14)$$

ve

$$p(X) = (X - 7)(X^3 + 3X^2 + 2X + 6).$$

Aslında, $(X + 3)(X - 7)$ polinomu da $p(X)$ 'i $Z[X]$ 'te böler:

$$p(X) = (X - 7)(X + 3)(X^2 + 2).$$

Okur bu örneğe aldanarak yanlış çıkarımlarda bulunmasın, aşağıda da göreceğimiz üzere, eğer bir R halkasının a ve b elemanları $p(X) \in R[X]$ polinomunun iki değişik köküyse, $(X - a)(X - b)$ polinomu her zaman $p(X)$ 'i bölmeyiz.

Örnek. $X^2 - X$ polinomunun $Z/6Z$ 'deki köklerini $Z/6Z$ 'nin altı elemanını da teker teker deneyerek bulabiliriz: $0, 1, 3$ ve 4 bulunur. Yukarıdaki teoreme göre $X, X-1, X-3$ ve $X-4$ polinomları $Z/6Z[X]$ halkasında $X^2 - X$ 'i böler. Nitekim:

$$X^2 - X = X(X - 1) = (X - 3)(X - 4).$$

Ancak, yukarıdaki örneğin tersine, $Z/6Z[X]$ halkasında $(X - 1)(X - 3)$ polinomu $X^2 - X$ polinomunu bölmeyiz.

Bir sonraki teoremdede, eğer R bir **tamlık bölgesi**yse (yani $ab = 0$ olduğunda ya a 'nın ya da b 'nin 0 olmak zorunda olduğu bir halkaysa), o zaman $R[X]$ halkasında her şeyin yolunda gittiğini göreceğiz. Zaten yukarıdaki ikinci örnekteki sorun $Z/6Z$ halkasının bir tamlık bölgesi olmamasından kaynaklanıyordu. (Bknz. sayfa 50.)

Teorem 3. R bir tamlık bölgesi, $p(X) \in R[X]$ ve $a_1, \dots, a_n \in R$ elemanları $p(X)$ 'in birbirinden değişik kökleri olsun. O zaman, $(X - a_1) \dots (X - a_n)$ polinomu $p(X)$ polinomunu $R[X]$ 'te böler.

Kanıt: Kanıtı n üzerine tümevarımla yapacağız. Eğer $n = 1$ ise, bu, aynen Teorem 2'dir. Şimdi $a_1, \dots, a_n, a_{n+1} \in R$ elemanları $p(X)$ 'in birbirinden değişik kökleri olsun. $(X - a_1) \dots (X - a_n)$ polinomunun $p(X)$ 'i $R[X]$ 'te böldüğünü varsayalım (tümevarım varsayımı). Diyelim,

$$p(X) = (X - a_1) \dots (X - a_n)q(X).$$

(Burada $q(X) \in R[X]$.) Bu eşitliğin iki tarafını da a_{n+1} 'de değerlendirelim:

$$0 = p(a_{n+1}) = (a_{n+1} - a_1) \dots (a_{n+1} - a_n)q(a_{n+1}).$$

a_i 'ler birbirinden değişik olduğundan, sağdaki terimin $a_{n+1} - a_i$ çarpanlarının hiçbirisi 0 olamaz. R bir bölge olduğundan, bundan $q(a_{n+1}) = 0$ çıkar. Şimdi Teorem 2'yi $q(X)$ ve a_{n+1} 'e uygulayabiliriz: $X - a_{n+1}$ polinomu $q(X)$ polinomunu böler, yani, belli bir $s(X) \in R[X]$ için,

$$q(X) = (X - a_{n+1})s(X).$$

Dolayısıyla,

$$\begin{aligned} p(X) &= (X - a_1) \dots (X - a_n)q(X) \\ &= (X - a_1) \dots (X - a_n)(X - a_{n+1})s(X). \end{aligned}$$

Teorem kanıtlanmıştır. \square

Sonuç 4. Eğer R bir tamlık bölgesiye, $R[X]$ halkasında sıfır olmayan her polinomun en fazla derecesi kadar kökü vardır.

Kanıt: $p(X) \in R[X]$, derecesi n olan bir polinom olsun. $a_1, \dots, a_k \in R$ elemanları $p(X)$ 'in birbirinden değişik kökleri olsun. O zaman, Teorem 3'e göre k dereceli ve 1 başkatsayılı $(X - a_1) \dots (X - a_k)$ polinomu, n -inci dereceden bir polinom olan $p(X)$ polinomunu $R[X]$ 'te böler. Demek ki $k \leq n$. ♥

Z/nZ Halkasında

İkinci Dereceden Denklemler

$X^2 - X = 0$ denkleminin $Z/6Z$ halkasında tam dört çözümü vardır: $0, 1, 3$ ve 4 . $Z/30Z$ halkasında ise sekiz kökü vardır. Arayan bulur!

Genel olarak, $X^2 - X = 0$ denkleminin Z/nZ halkasında kaç çözümü vardır?

Okur mutlaka gerçel sayılarda ikinci dereceden denklemleri çözmeyi biliyordur. Viète formülünden ikinci dereceden bir denklemin gerçel sayılarda en fazla iki kökü olduğu anlaşılır. Bu, daha genel olarak özneliği 2 olmayan herhangi bir cisim için de geçerlidir.

Peki, Z/nZ halkasında $aX^2 + bX + c = 0$ denkleminin kaç kökü vardır?