



Kapak Konusu: Halkalar, Asallar ve İndirgenemezler (1)

Polinom Nedir Ne Değildir?

Bir **değişkenli bir polinom** ya da kısaca **polinom**,

$$a_0 + a_1X + a_2X^2 + \dots + a_nX^n$$

biçiminde yazılan bir terimdir.

Burada n bir doğal sayıdır. Bu giriş yazısında, en azından başlangıçta, a_i 'leri gerçel sayı olarak alalım, a_i 'leri daha sonra başka yerlerden alalım.

Eğer $n = 0$ ise, gerçel sayıları buluruz. Demek ki her gerçel sayı bir polinomdur. Bunlara **sabit polinomlar** denir.

X 'in ne olduğunu hiç sormayın... X bir ŞEY'dir, anlamı olmayan bir ŞEY. X ŞEY'ine **değişken** denir. Sadece X değil X^i 'lerin herbiri **monom** adı verilen bir ŞEY'lerdir. X yerine Y, Z, T gibi bir başka harf de kullanabiliriz. X 'e ve X^i 'lere hiçbir anlam yüklemeyin. Bir anlamları yoktur. Onları yabancı bir nesne olarak kabul edin.

X 'leri ŞEY'likten kurtarıp polinomları çok daha matematiksel olarak tanımlayabiliriz, ama bir giriş yazısında o kadar soyut olmak gerekmez.

Polinomlarda a_iX^i terimlerinin hangi sırayla yazıldıkları önemli değildir; öte yandan X 'in **gücü** olan i 'ye göre soldan sağa küçükten büyüğe doğru (kimileyin de büyükten küçüğe doğru) sıralayarak yazmak yerleşmiş bir gelenektir.

a_i 'lere polinomun **katsayıları** denir.

$3 + 7X + 0X^2 + (-5)X^3 + 1X^4$ bir (gerçel katsayılı) polinom örneğidir. Bu polinom daha kısa bir şekilde $3 + 7X - 5X^3 + X^4$ olarak yazılabilir ve öyle de yazılmalıdır. $X + \pi X^3 - 3\sqrt{\pi}X^{2004}$ bir başka polinom örneğidir.

Eğer $a_n \neq 0$ ise, tanım gereği,

$$a_0 + a_1X + a_2X^2 + \dots + a_nX^n$$

polinomunun **derecesi** n 'dir. O zaman a_n katsayısına polinomun **başkatsayısı** adını verelim. Örneğin, $8 + 7X - 5X^3$ polinomunun derecesi 3, başkatsayısı -5 'tir.

Dikkat: Bir polinom

$$a_0 + a_1X + a_2X^2 + \dots + a_nX^n$$

olarak yazıldı diye derecesi illa n olmak zorunda değildir; eğer $a_n = 0$ ise, bu polinomun derecesi n 'den küçüktür.

Eğer polinomda a_n 'nin sıfır olmadığı bir n yoksa, yani her a_n için $a_n = 0$ ise, yani polinom **sıfır polinomu**ysa, o zaman, tanım gereği, polinomun derecesi $-\infty$ 'dur. Sıfır polinomu sanki bir sayıymış gibi 0 olarak yazılır. Demek ki 0 polinomunun derecesi $-\infty$.

Derecesi 0 olan polinomlar sıfır olmayan gerçel sayılardır. Bunlar belli $a_0 \in \mathbb{R} \setminus \{0\}$ için a_0 biçiminde yazılırlar. Derecesi 1 olan polinomlar belli $a_0 \in \mathbb{R}$ ve $a_1 \in \mathbb{R} \setminus \{0\}$ sayıları için $a_0 + a_1X$ biçiminde yazılırlar. Derecesi 2 olan polinomlar belli $a_0, a_1 \in \mathbb{R}$ ve $a_2 \in \mathbb{R} \setminus \{0\}$ sayıları için $a_0 + a_1X + a_2X^2$ biçiminde yazılırlar. Ve bu böyle devam eder.

Her ne kadar X 'e “bilinmeyen” diyenler varsa da, X 'in bilinmeyenle alakası yoktur. Ancak bilinebilecek bir şeye “bilinmeyen” denilebilir, oysa bir polinomun bilinecek bir şeyi yoktur, bir polinom sadece ve sadece bir terimdir ve anlamsız bir terimdir. Polinomda beliren X de sadece bir X 'tir ve başka bir şey değildir.

Bir polinomu p gibi bir harfle ya da, kullanılan X 'i illa belirtmek istiyorsak, $p(X)$ olarak simgeleyebiliriz. Kimileyin p polinomunun katsayıları p_i olarak yazılır, yani p polinomunu

$$p = p(X) = p_0 + p_1X + p_2X^2 + \dots + p_nX^n$$

olarak yazarız. Bunun gibi, bir a polinomunu

$$a = a(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$$

olarak yazarız. Böylece polinom ve polinomun katsayıları arasında biçimsel bir ilişki kurulur ve kanıtlar daha kolay anlaşılır.

Bir p polinomunun derecesi $d^\circ(p)$ olarak gösterilir. O zaman, p polinomunu

$$p = p(X) = p_0 + p_1X + p_2X^2 + \dots + p_{d^\circ(p)}X^{d^\circ(p)}$$

olarak yazabiliriz. Ama bu tür ukâlalıklar yapmaya çağız.

X 'e pek bilinmeyen denmez ama çoğu kez **değişken** denir. Bu terim de yanıltıcıdır, çünkü bir polinom fonksiyon değildir, bir polinomda değişen bir şey yoktur. Değişken denen şey polinomlarda değil fonksiyonlarda bulunur. Her polinom \mathbb{R} 'den \mathbb{R} 'ye giden bir fonksiyon verir, doğru, ama polinomun kendisi bir fonksiyon değildir. Nitekim katsayıları gerçel sayı olan

$$a_0 + a_1X + a_2X^2 + \dots + a_nX^n$$

polinomunda X değişkeni yerine bir x gerçel sayısı koyarsak, $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ gerçel sayısını elde ederiz, dolayısıyla,

$$x \ni a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

kuralı \mathbb{R} 'den \mathbb{R} 'ye giden bir fonksiyon tanımlar. Eğer polinoma $a(X)$ dersek, yani

$$a(X) = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$$

ise, X yerine x gerçel sayısını koyarak elde ettiğimiz sayı $a(x)$ olarak gösterilir:

$$a(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n.$$

$a(x)$, $a(X)$ polinomunun x gerçel sayısında **değerlendirilmesi** ya da **değeridir**. Demek ki her $a(X)$ polinomu $x \ni a(x)$ kuralıyla tanımlanmış \mathbb{R} 'den \mathbb{R} 'ye giden bir fonksiyon belirler.

Her polinom bir fonksiyon tanımlamasına karşın – tekrar ediyoruz – bir polinom bir fonksiyon değildir. Bir polinom sadece bir terimdir, anlamı olmayan bir terim.

X^0 terimini (tanım gereği) 1 olarak kabul edersek, o zaman bir polinom

$$a_0X^0 + a_1X + a_2X^2 + \dots + a_nX^n$$

ya da (“nokta nokta nokta”yı sevmeyenler tarafından)

$$\sum_{k=0}^n a_k X^k$$

olarak yazılır. Örneğin, $X + 2X^2 + 3X^3 + 4X^4$ polinomu,

$$\sum_{k=0}^4 kX^k$$

olarak yazılabilir. Bunun gibi, okur aşağıdaki yazımlara da alışmalıdır:

$$1 - X^2 + X^4 - X^6 = \sum_{k=0}^3 (-1)^k X^{2k}$$

$$2X - 4X^2 + 8X^3 - 16X^4 = \sum_{k=1}^4 (-1)^{k-1} 2^k X^k$$

Eğer a_k 'lerin büyük k 'ler için 0 olduklarını varsayarsak (ki öyleler, yoksa polinom olmazlardı), yani belli bir n için, $a_{n+1} = a_{n+2} = a_{n+3} = \dots = 0$ ise, bir polinomu,

$$\sum_{k=0}^{\infty} a_k X^k$$

ya da daha da basit bir yazılımla,

$$\sum_k a_k X^k$$

olarak da yazabiliriz. Bu son iki yazılımın tek kusuru polinomun derecesinin belli olmamasıdır. Bu kusuruna karşın, önemli avantajlar içerdiğinden ve tanımlarda hatırı sayılır kolaylık sağladığından biz de

ne de bu son yazılımı tercih edeceğiz.

Her polinomun belli bir derecesi olmalıdır. Örneğin $1 + X + X^2 + X^3 + \dots$ diye sonsuza kadar giden terim, yani

$$\sum_{k=0}^{\infty} X^k$$

terimi bir polinom değildir.

$$\sum_k a_k X^k$$

teriminin bir polinom olabilmesi için, belli bir aşamadan sonra a_k katsayılarının hepsi 0 olmalıdır.

Bir polinomda X^{-1} , X^{-2} gibi terimler beliremez, X 'in sadece negatif olmayan güçleri alınır. Ayrıca, $X^{1/2}$ ya da \sqrt{X} gibi terimler de beliremez polinomlarda. Bir polinomda X 'in güçleri mutlaka 0, 1, 2, 3 gibi doğal sayılar olmalıdır. Sonra...

$$\frac{X^2 + 1}{X - 1}$$

gibi yazılan terimler de genellikle polinom değildir, bir polinomun paydasında şimdilik X 'li bir terim kabul etmiyoruz.

Katsayıları gerçel sayılar olan polinomlar kümesi $\mathbb{R}[X]$ olarak yazılır. Katsayıları tamsayı olarak alsaydık, o zaman polinomlar kümesi $\mathbb{Z}[X]$ olarak yazılırdı. Genel olarak, katsayıları R adı verilen bir kümede olan polinomlar kümesi $R[X]$ olarak gösterilir. Elbette $\mathbb{Z}[X] \subset \mathbb{Q}[X] \subset \mathbb{R}[X]$.

II. Polinomlarda Toplama ve Çarpma.

Polinomları (aynen olmasa da benzer bir biçimde) sayılar gibi toplayıp çarpabiliriz. Her iki işlem de olabilecek en doğal biçimde yapılır. Yani size silah zoruyla iki polinomu toplayıp çarpmamız istendiğinde, o iki polinomu mecburen nasıl toplayıp çarparsanız, polinomlarda toplama ve çarpma işte aynen öyle tanımlanır. Bu açıklamanın matematiksel kesinliğe alışmış okur tarafından yeterli bulunmayacağını göz önüne alarak matematiksel tanımları vereceğiz. Örneklerle başlayalım. $5 - X + 3X^2$ ve $-5 + 3X + X^2 + 7X^4$ polinomlarını toplayalım:

$$(5 - X + 3X^2) + (-5 + 3X + X^2 + 7X^4) = 2X + 4X^2 + 7X^4.$$

Görüldüğü gibi polinomları toplamak için monomların birbirine tekabül eden katsayıları teker teker toplanıyor.

Çarpmanın tanımı da doğaldır ama biraz daha az kolaydır. Çarpma, $(a_i X^i)(b_j X^j) = a_i b_j X^{i+j}$ ve $a_i X^i + b_j X^j = b_j X^j + a_i X^i$ eşitlikleri ve toplamaya göre dağılım özelliği (bknz. aşağıdaki D özelliği) doğru ola-

cak biçimde tanımlanır. Örneğin, $5 - X + 3X^2$ ve $5 + 2X + X^2 + 7X^4$ polinomlarını çarpalım:

$$\begin{aligned} & (5 - X + 3X^2)(5 + 2X + X^2 + 7X^4) \\ &= 5(-5 + 2X + X^2 + 7X^4) \\ &\quad - X(-5 + 2X + X^2 + 7X^4) \\ &\quad + 3X^2(-5 + 2X + X^2 + 7X^4) \\ &= (-25 + 10X + 5X^2 + 35X^4) \\ &\quad - (-5X + 2X^2 + X^3 + 7X^5) \\ &\quad + (-15X^2 + 6X^3 + 3X^4 + 21X^6) \\ &= -25 + 10X + 5X^2 + 35X^4 + 5X - 2X^2 - X^3 \\ &\quad - 7X^5 - 15X^2 + 6X^3 + 3X^4 + 21X^6 \\ &= -25 + 15X - 12X^2 + 5X^3 + 38X^4 - 7X^5 + 21X^6. \end{aligned}$$

Yukarda yaptığımız gibi sağdaki $-5 + 2X + X^2 + 7X^4$ polinomunu soldaki $5 - X + 3X^2$ polinomuna dağıtmak yerine, soldakini sağdakine dağıtıp çarpımı öyle hesaplayabilirdik, sonuç değişmezdi elbette.

Şimdi toplama ve çarpmanın biçimsel (matematiksel) tanımlarını verelim. Önce oldukça kolay olan toplamadan başlayalım:

$$\sum_k a_k X^k + \sum_k b_k X^k = \sum_k (a_k + b_k) X^k.$$

Çarpma için, çarpımı yapılacak polinomların, çarpıldığında aynı gücü verecek monomların katsayıları çarpılıp toplanır:

$$\begin{aligned} & (a_0 + a_1X + \dots + a_nX^n)(b_0 + b_1X + \dots + b_mX^m) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 \\ &\quad + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)X^3 + \dots + a_nb_mX^{n+m}. \end{aligned}$$

Daha biçimsel olarak, çarpma,

$$\left(\sum_k a_k X^k \right) \left(\sum_k b_k X^k \right) = \sum_k \left(\sum_{i+j=k} a_i b_j \right) X^k$$

olarak tanımlanır.

III. Halka Özellikleri. Polinomların şu özellikleri vardır:

T1 [Birleşme Özelliği]. Her $p, q, r \in R[X]$ için,
 $p + (q + r) = (p + q) + r.$

T2 [Etkisiz Öğenin Varlığı]. Her $p \in R[X]$ için,
 $0 + p = p + 0 = p.$

T3 [Ters Öğenin Varlığı]. Her $p \in R[X]$ için,
 $p + q = q + p = 0$

eşitliklerini sağlayan bir $q \in R[X]$ vardır. (Eğer

$p = \sum_k a_k X^k$ ise $q = \sum_k (-a_k) X^k$ dir ve bu $q, -p$ olarak yazılır.)

T4 [Değişme Özelliği]. Her p ve $q \in R[X]$ için,
 $p + q = q + p.$

Bunlar toplamının özellikleriydi. Şimdi çarpmanın özelliklerine geçelim.

Ç1 [Birleşme Özelliği]. Her $p, q, r \in R[X]$ için,
 $p(qr) = (pq)r.$

Ç2 [Birim Öge]. Her $p \in R[X]$ için,
 $1p = p1 = p.$

Ç3 [Değişme Özelliği]. Her p ve $q \in R[X]$ için,
 $pq = qp.$

Son olarak, toplamayla çarpma arasındaki ilişkiyi ortaya koyan özellik:

D [Dağılma Özelliği]. Her $p, q, r \in R[X]$ için,
 $p(q + r) = pq + pr.$

Bu özellikleri kanıtlamayacağız. Okur tanımlara geri dönerek bu özelliklerin doğru olduklarını kolaylıkla kanıtlayabilir. Bazı kanıtlar, örneğin Ç1 uzun ve yorucu olabilir, ama kolaydır.

Yukardaki özellikler salt $R[X]$ için değil, $Z[X]$, $Q[X]$ gibi polinom kümeleri için de geçerlidir. Bu özelliklerin doğru olduğu daha binlerce, ne binlercesi! sonsuz sayıda matematiksel yapı vardır. Örneğin Z/nZ kümesinin “modülo n ” toplama ve çarpma altında bir halka olduğunu gördük. Matematikte bu özelliklerle öylesine sık karşılaşılır ki, bu özellikleri sağlayan bir yapıya özel bir ad verilmiştir: **Halka**. Bu önemli kavramı biraz daha açalım, gerekecek.

Bir R kümesinde, yukardaki T1, T2, T3, T4, Ç1, Ç2, Ç3 ve D özelliklerini sağlayan, toplama ve çarpma adı verilen iki işlem ve 0 ve 1 adı verilen öğeler tanımlanmışsa, o zaman R kümesine **halka** adı verilir. Daha matematiksel bir deyişle: R bir küme olsun. Ayrıca R 'de adına 0 ve 1 diyeceğimiz iki öğe olsun. Ayrıca $+$ ve \times , $R \times R$ 'den R 'ye giden iki fonksiyon olsun. Eğer $(R, +, \times, 0, 1)$ beşlisi yukardaki T1, T2, T3, T4, Ç1, Ç2, Ç3 ve D özelliklerini sağlıyorsa¹, o zaman $(R, +, \times, 0, 1)$ beşlisine kısaca **halka**² denir.

Örneğin, $Z, Q, R, Z/nZ, Z[X], Q[X], R[X]$ kümeleri bildiğimiz toplama ve çarpma ve 0 ve 1 öğeleriyle birer halkadırlar. Ama N bir halka değildir, T4 özelliği N 'de doğru değildir.

Bir sonraki yazımızda bu önemli kavramı daha fazla açacağız.

Eğer R bir halkaysa, katsayıları R halkasında olan polinomlardan söz edebiliriz. Bu polinomlar

1 Özelliklerin herbirinde $R[X]$ yerine R yazılacak.

2 Bazen (sırasıyla) Ç1, Ç2 ve Ç3 özelliklerinden dolayı, **birleşmeli, değişmeli ve birimli halka** dendiği de olur. Bizim halkalarımızda bu özelliklerin herbiri olacak.

kümesi, daha önce de söylendiği gibi, $R[X]$ olarak yazılır. $R[X]$ kümesinde toplama ve çarpma ve 0 ve 1 polinomları aynen yukarıda $R[X]$ kümesi için tanımladığımız gibi tanımlanır.

Teorem 1. *Eğer R bir halkaysa $R[X]$ de bir halkadır.*

Kanıt: Uzun ve sıkıcı ancak kolay kanıtları okura alıştırmaya bırakarak bırakmak MD'nin yayın ilkele-rindedir. \square

Dolayısıyla $(\mathbb{Z}/n\mathbb{Z})[X]$ de bir halkadır. Ayrıca eğer R bir halkaysa, $(R[X])(Y)$ de bir halkadır. Bu son halka $R[X, Y]$ olarak gösterilir. Böylece polinomlar-da değişken sayısını birden ikiye çıkarmış oluruz.

$R[X]$ halkasının önemli bir özelliği daha vardır:

TB. *Her $p, q \in R[X]$ için, eğer $pq = 0$ ise, o zaman ya $p = 0$ ya da $q = 0$.*

Yukardaki TB özelliğini sağlayan bir halkaya **tamlık bölgesi** ya da kısaca **bölge** denir. Her halka bir bölge değildir. Örneğin "modülo 4" sayılar, yani $4 = 0$ eşitliğinin kabul edildiği $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ kümesi, "doğal" toplama ve çarpma işlemleri için bölge olmayan bir halkadır, çünkü bu halkada $2 \times 2 = 0$ 'dır.

Önsav 2. *R bir halka olsun. $p, q \in R[X]$ olsun.*

i. $d^\circ(p + q) \leq \max(d^\circ(p), d^\circ(q))$.

ii. *Eğer $d^\circ(p) \neq d^\circ(q)$ ise,*

$$d^\circ(p + q) = \max(d^\circ(p), d^\circ(q)).$$

iii. $d^\circ(pq) \leq d^\circ(p) + d^\circ(q)$.

iv. *Eğer R bir bölgeyse,*

$$d^\circ(pq) = d^\circ(p) + d^\circ(q).$$

Kanıt: Bu önsav, tanımların bir sonucudur. Kanıtı okura bırakılmıştır. \square

Sonuç 3. *Eğer R bir tamlık bölgesiyse, $R[X]$ de bir tamlık bölgesidir.*

Kanıt: Bu teorem, yukardaki önsavın son kısmının doğrudan bir sonucudur. Kanıtın ayrıntıları (eğer kalmışsa) okura bırakılmıştır. \spadesuit

$\mathbb{Q}[X]$ 'ten herhangi bir $p(X)$ polinomu alalım. Bu polinomu

$$p(X) = \frac{a_0}{b_0} + \frac{a_1}{b_1}X + \dots + \frac{a_n}{b_n}X^n$$

($a_i, b_i \in \mathbb{Z}$) olarak gösterelim. a_i/b_i katsayılarını ortak paydaya getirerek c_i/d olarak yazalım. O zaman, eğer,

$$q(X) = c_0 + c_1X + c_2X^2 + \dots + c_nX^n \in \mathbb{Z}[X]$$

ise, $p(X) = q(X)/d$ eşitliği geçerlidir. Yani $\mathbb{Q}[X]$ ile $\mathbb{Z}[X]$ arasında küçük bir ayrım vardır.

$\mathbb{Z}/n\mathbb{Z}$ Halkalarında Tuhafliklar

Okur, belki ikinci dereceden bir denklemin sadece iki çözümü olmasına alışmış olabilir. Ama $6 = 0$ eşitliğinin sağlandığı $\mathbb{Z}/6\mathbb{Z}$ halkasında, $x^2 + x = 0$ denkleminin, ne bir fazla ne bir eksik, tam dört çözümü vardır: $x = 0, 2, 3, 5$. Bunun gibi, $\mathbb{Z}/8\mathbb{Z}$ halkasında da, $x^2 + 2x = 0$ denkleminin tam dört çözümü vardır: $x = 0, 2, 4, 6$.

Ama bu tür tuhafliklara bir tamlık bölgesinde rastlanamaz. Ne $\mathbb{Z}/6\mathbb{Z}$ halkası ne de $\mathbb{Z}/8\mathbb{Z}$ halkası birer tamlık bölgesidir, nitekim birincisinde $2 \times 3 = 0$, ikincisinde $2 \times 4 = 0$ eşitlikleri geçerlidir. Eğer bir tamlık bölgesinde $x^2 + x = 0$ ise, $x(x + 1) = 0$, dolayısıyla ya $x = 0$ ya da $x + 1 = 0$, yani ya $x = 0$ ya da $x = -1$.

$\mathbb{Z}/n\mathbb{Z}$ halkasının tamlık bölgesi olması için gerek ve yeter koşul n 'nin asal olmasıdır.

İleride, bir R tamlık bölgesinde, katsayıları R 'de olan n -inci dereceden bir polinomun en fazla n kökünün olduğunu göreceğiz; yani $p \in R[X]$ ise, $p(x) = 0$ denklemini sağlayan R 'nin en fazla $d^\circ(p)$

tane x ögesi olduğunu göreceğiz.

Bir başka tuhaflik: Eğer $R = \mathbb{Z}/6\mathbb{Z}$ ise, $R[X]$ halkasında,

$$X(X + 1) = (X - 2)(X - 3)$$

eşitliği sağlanır. Ya da eğer $R = \mathbb{Z}/4\mathbb{Z}$ ise, $R[X]$ halkasında da, pek alışık olmadığımız

$$X^2 = (X - 2)^2$$

eşitliği geçerlidir.

Bu tür tuhafliklara da tamlık bölgelerinde rastlanmaz:

Alıştırma. Eğer bir R halkasında her a in R için, $a = 2c$ eşitliğini sağlayan bir ve bir tek c varsa ve $a = y^2$ eşitliğini sağlayan en fazla iki y varsa o zaman R halkasında $x^2 + ax + b = 0$ denkleminin en fazla iki çözümü olduğunu kanıtlayın. Ayrıca, böyle bir halkada

$$(X - a)(X - b) = (X - c)(X - d)$$

polinom eşitliğinin ancak $\{a, b\} = \{c, d\}$ eşitliğiyle mümkün olacağını gösterin.