Kapak Konusu: Halkalar, Asallar ve İndirgenemezler

Polinomlarda Bölme

Polinomlar tamsayılara çok benzerler. Bu yazıda bu benzerliklerin en önemlisini ortaya koyacağız.

Bir tamsayı her zaman bir başka tamsayıya tam olarak bölünmez. Örneğin, 18, 6'ya bölünür ama 17, 6'ya tam bölünmez. Gene de 17'yi 6'ya bölmeye çalışabiliriz. 17'yi 6'ya bölmeye çalıştığımızda bir kalan çıkar: $17 = 6 \times 2 + 5$. Bu, okurun da bildiği genel bir teoremdir:

Olgu. *$a, b \in \mathbb{Z}$ ve $b \neq 0$ olsun. O zaman,*

$$a = bq + r \text{ ve } 0 \leq r < |b|$$

özelliklerini sağlayan bir ve bir tane (q, r) tamsayı çifti vardır.

Polinomların en önemli özelliklerinden biri, bir polinomun bir başka polinoma aşağı yukarı yukardaki anlamda bölünebilmesidir, en azından polinomların katsayıları $\mathbb{R}$ gibi güzel bir halkadaysa. Sadece b tamsayısının mutlak değerinin yerini b polinomunun derecesi alır:

Teorem 1. *$a, b \in \mathbb{R}[X]$ ve $b \neq 0$ olsun. O zaman $a = bq + r$ ve $d°(r) < d°(b)$ özelliklerini sağlayan bir ve bir tane gerçel katsayılı (q, r) polinom çifti vardır.*

Kanıt: Önce, koşulları sağlayan q ve r polinomlarının varlığını a polinomunun derecesi üzerine tümevarımla kanıtlayacağız. q ve r polinomlarının biricikliği konusuna daha sonra saldıracağız.

Eğer $d°(a) < d°(b)$ ise, o zaman, $q = 0$ ve $r = a$ alalım. Hem $a = bq + r$ hem de $d°(r) < d°(b)$ özellikleri sağlanır.

Şimdi $d°(a) \geq d°(b)$ eşitsizliğini varsayalım. $d°(a) = n$ ve $d°(b) = m$ olsun. Demek ki $n \geq m$. Ardından a ve b'yi açalım:

$$a = a(X) = a_0 + a_1X + \ldots + a_nX^n$$
$$b = b(X) = b_0 + b_1X + \ldots + b_mX^m.$$

b_m'nin 0 olmadığına dikkatinizi çekerim. Şimdi

$$c = a - a_nb_m^{-1}bX^{n-m}$$

polinomuna bakalım. (Dikkat: Burada b_m'nin tersini aldık, bu ilerde önemli olacak.) c polinomunun derecesi n'den küçüktür, çünkü c'nin tanımındaki a'nın en son terimi sadeleşir ve c'de belirmez. Tümevarım varsayımını c ve b polinomlarına uygulayalım:

$$c = bq_1 + r \text{ ve } d°(r) < d°(b)$$

özelliklerini sağlayan q_1 ve r polinomları vardır. Demek ki

$$a - a_nb_m^{-1}bX^{n-m} = c = bq_1 + r.$$

Bundan

$$a = b(q_1 + a_nb_m^{-1}X^{n-m}) + r$$

çıkar. Şimdi,

$$q = q_1 + a_nb_m^{-1}X^{n-m}$$

olsun. İstediğimiz $a = bq + r$ eşitliğini buluruz. $d°(r) < d°(b)$ özelliğini zaten biliyorduk.

q ve r polinomlarının varlığını kanıtladık. Şimdi bu çiftin biricikliğini kanıtlayalım.

$$a = bq + r = bq_1 + r_1,$$
$$d°(r) < d°(b)$$

ve

$$d°(r_1) < d°(b)$$

olsun. $q = q_1$ ve $r = r_1$ eşitliklerini kanıtlayacağız. $q \neq q_1$ eşitsizliğini, yani $d°(q - q_1) \geq 0$ eşitsizliğini varsayalım. Bir çelişki elde edeceğiz. $bq + r = bq_1 + r_1$ eşitliğinden,

$$b(q - q_1) = r_1 - r$$

eşitliği çıkar. Dolayısıyla, sayfa 28'deki Önsav 2'den, $d°(r_1 - r) = d°(b(q - q_1)) = d°(b) + d°(q - q_1) \geq d°(b) > \max(d°(r_1), d°(r)) \geq d°(r_1 - r)$ çıkar, bir çelişki. Demek ki $q = q_1$ ve $r = r_1$. □

Yukardaki teoremi $\mathbb{R}[X]$ polinom halkasından bir R halkası için $R[X]$ polinom halkasına genelleştirmeye çalışalım. Aynı kanıtı $\mathbb{R}$ yerine R halkası için yapmaya çalışalım. İki yerde $\mathbb{R}$'ye özel ve her R halkası tarafından paylaşılmayan özellikler kullanmışız: 1) c polinomunu tanımlarken b_m sayısının çarpımsal tersini almışız, yani b_m'nin tersinir olduğunu varsaymışız. 2) Kanıtın sonlarına doğru $d°(b(q - q_1)) = d°(b) + d°(q - q_1)$ eşitliğini kullanmışız. Teorem 1'in kanıtını, bu iki önermenin doğru olduğu R halkalarına uygulayıp $R[X]$ hakkında genel bir teorem elde edebiliriz. Hemen şimdi ikinci önermenin birinci önermenin bir sonucu olduğunu göreceğiz; dolayısıyla Teorem 1'i kanıtlamak için yalnız birinci olguya ihtiyacımız olacak.

Önsav 2. *R bir halka olsun. $b \in R[X]$ olsun. b'nin başkatsayısının tersinir olduğunu varsayalım. Eğer $q \in R[X]$ ise, o zaman*

$$\mathrm{d}°(bq) = \mathrm{d}°(b) + \mathrm{d}°(q).$$

Kanıt: $\mathrm{d}°(b) = n$ ve $\mathrm{d}°(q) = m$ olsun. b'nin başkatsayısı b_n, q'nün en başkatsayısı q_m olsun. b ve q çarpıldığında, b_n tersinir olduğundan, b_nq_m kaybolmaz (yani sıfıra eşit olmaz, bknz. Önsav 4.iii, sayfa 31.) Dolayısıyla bq polinomunun derecesi $n+m$'dir. □

Şimdi Teorem 1'i genelleştirebiliriz:

Teorem 3. *R bir halka olsun. $a, b \in R[X]$ ve $b \neq 0$ olsun. Ayrıca b'nin başkatsayısının R'de tersinir olduğunu varsayalım. O zaman $a = bq + r$ ve $\mathrm{d}°(r) < \mathrm{d}°(b)$ özelliklerini sağlayan bir ve bir tane R katsayılı (q, r) polinom çifti vardır.*

Kanıt: Aynen Teorem 1'in kanıtı gibi. Malum yerde Önsav 2'yi kullanmak gerekiyor. Ayrıntılar okura bile bırakılmamıştır. □

Bölme Yöntemi. Okur, büyük olasılıkla daha önce görmüştür polinomlarla nasıl bölme yapılacağını. Teorem 1'in kanıtı da bölmenin nasıl yapılacağını söylüyor zaten. Bilgisayarda programlama yapabilen ve biraz ilgili bir okur, bir polinomu bilgisayara bir başka polinoma böldürtebilir.

Bir örnekle, uygulamada bir polinomun bir başka polinoma nasıl bölündüğünü gösterelim. Aynen kanıttaki yöntemi uygulayacağımız okurun gözünden kaçmayacaktır.

Diyelim $R = \mathbb{Z}$ ve $a(X) = X^7 - 4X^3 + X + 5$ polinomunu $b(X) = X^3 - 2X + 4$ polinomuna bölmek istiyoruz. Önce $a(X)$'in X^7'si $b(X)$'nin X^3'üne bölünür. Sonuç X^4'tür. Sonra aynı işlem $a(X)$ ve $b(X)$ yerine

$$a(X) - X^4b(X) \text{ ve } b(X)$$

polinomlarına uygulanır ve bu böylece devam eder, ta ki yeni $a(X)$'in derecesi $b(X)$'in derecesinden küçük olana dek.

Uygulamada bir doğal sayıyı bir başka doğal sayıya bölerken yaptığımızı yaparız. Yanda bu bölmeyi adım adım göreceksiniz.

A.

$$\begin{array}{r|l} X^7-4X^3+X+5 & X^3-2X+4 \\ \cline{2-2} & X^4 \end{array}$$

B.

$$\begin{array}{rr|l} & X^7-4X^3+X+5 & X^3-2X+4 \\ \cline{3-3} - & X^7-2X^5+4X^4 & X^4 \\ \cline{2-2} \end{array}$$

C.

$$\begin{array}{rr|l} & X^7-4X^3+X+5 & X^3-2X+4 \\ \cline{3-3} - & X^7-2X^5+4X^4 & X^4 \\ \cline{2-2} & 2X^5-4X^4-4X^3+X+5 & \end{array}$$

D.

$$\begin{array}{rr|l} & X^7-4X^3+X+5 & X^3-2X+4 \\ \cline{3-3} - & X^7-2X^5+4X^4 & X^4+2X^2 \\ \cline{2-2} & 2X^5-4X^4-4X^3+X+5 & \\ - & 2X^5-4X^3+8X^2 & \\ \cline{2-2} & -4X^4-8X^2+X+5 & \end{array}$$

E.

$$\begin{array}{rr|l} & X^7-4X^3+X+5 & X^3-2X+4 \\ \cline{3-3} - & X^7-2X^5+4X^4 & X^4+2X^2-4X \\ \cline{2-2} & 2X^5-4X^4-4X^3+X+5 & \\ - & 2X^5-4X^3+8X^2 & \\ \cline{2-2} & -4X^4-8X^2+X+5 & \\ - & -4X^4+8X^2-16X & \\ \cline{2-2} \end{array}$$

F.

$$\begin{array}{rr|l} & X^7-4X^3+X+5 & X^3-2X+4 \\ \cline{3-3} - & X^7-2X^5+4X^4 & X^4+2X^2-4X \\ \cline{2-2} & 2X^5-4X^4-4X^3+X+5 & \\ - & 2X^5-4X^3+8X^2 & \\ \cline{2-2} & -4X^4-8X^2+X+5 & \\ - & -4X^4+8X^2-16X & \\ \cline{2-2} & -16X^2+17X+5 & \end{array}$$

Sonuç olarak,

$$X^7 - 4X^3 + X + 5 = (X^3 - 2X + 4)(X^4 + 2X^2 - 4X) + (-16X^2 + 17X + 5)$$

bulunur. Burada,

$$a(X) = X^7 - 4X^3 + X + 5$$
$$b(X) = X^3 - 2X + 4$$
$$q(X) = X^4 + 2X^2 - 4X$$
$$r(X) = -16X^2 + 17X + 5$$

dir.

Yukardaki teorem o kadar önemlidir ki, o teorem doğru olmasaydı hiçbirimiz bu dünyada olmazdık. ♠