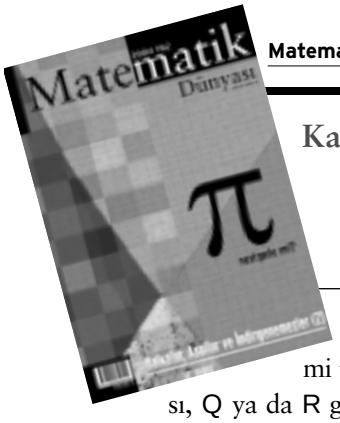


Kapak Konusu: Halkalar, Asallar ve İndirgenemezler (2)

# Polinomlarda İndirgenemezler

Bu yazıda $K$ hep bir cismi temsil edecek. Yani $K$ halkası, $\mathbb{Q}$ ya da $\mathbb{R}$ gibi, sıfır olmayan her elemanının tersinir olduğu bir halka olacak. Dileyen okur, aşağıdaki kanıtlarda hiçbir değişiklik yapmadan $K$ yerine $\mathbb{Q}$ ya da $\mathbb{R}$ alabilir.

Amacımız, $K[X]$ halkasının her indirgenemezinin bir asal olduğunu kanıtlamak. Bu iki kavramı sayfa 25-26'da tanımlamıştık. Bu tanımlara eşdeğer tanımları verelim:

$p$, sabit olmayan bir polinom olsun. Eğer $p$, sadece $K^*$ ve $pK^*$'ın elemanlarına bölünebiliyorsa, o zaman $p$'ye **indirgenemez polinom** deriz.

$p$, gene sabit olmayan bir polinom olsun. Eğer $p$, herhangi iki polinomun çarpımını böldüğünde, o iki polinomdan birini bölüyorsa, o zaman $p$'ye **asal polinom** deriz.

Her asalın her halkada bir indirgenemez olduğunu görmüştük (sayfa 26, Önsav 7). Ama bazı halkalarda bazı indirgenemezler asal değillerdir. Bu oyunbozan halka örneklerini de sayfa 25-26'da görmüştük, örneğin $\mathbb{Z}[\sqrt{5}]$ bu tür halkalardan biridir. Neyse ki bu tür anormalliklere matematikte ve yaşamda en çok kullanılan evcil halkalarda rastlanmaz. Örneğin, $K[X]$ halkasında, bu yazıda kanıtlayacağımız üzere, her indirgenemez bir asaldır.

İleride bu sonucu genelleştirerek, bu sonucun sadece $K[X]$ halkasında değil, $K[X_1, X_2, ..., X_n]$ ve $\mathbb{Z}[X_1, X_2, ..., X_n]$ gibi birçok halkada da geçerli olduğunu göreceğiz.

Bu sonuç sayesinde, $K[X]$ halkasının bir tek çarpanlama bölgesi olduğunu, yani sabit olmayan her polinomun sonlu sayıda asalın çarpımı olarak (aşağı yukarı) tek bir biçimde yazıldığını anlamış olacağız. (Bknz. sf. 27, Teorem 10 ve sf. 25, Teorem 6).

Kanıtlayacağımız sonucu geçen sayımızda $\mathbb{Z}$ için (aslında $\mathbb{N}$ için ama ne fark var ki!) kanıtlamıştık (bknz. MD-2004-I, sayfa 17, Teorem 2). Kanıtımız aynen, ama nerdeyse tıpatıp o kanıt gibi olacak. İki kanıtı sağlı sollu paralel sunacağız ve böylece $\mathbb{Z}$ halkasıyla $K[X]$ halkasının birbirine ne kadar benzer olduğu anlaşılacak.

$\mathbb{Z}$ halkasını diğer halkalardan ayrıcalıklı kılan şey mutlak değer fonksiyonudur. Mutlak değer sayesinde $\mathbb{Z}$ halkasında tümevarımla kanıt yapabiliriz. $K[X]$ halkasında mutlak değer fonksiyonun yerini derece fonksiyonu alır ve aynı işlevi görür: Polinomun derecesi üzerine tümevarım yapabilir ve $\mathbb{Z}$ için kanıtladığımız birçok teoremi $K[X]$ için de kanıtlayabiliriz, hem de kanıtları hemen hemen hiç değiştirmeden, aynen burada yapacağımız gibi.

Bu yazıda polinomlar üzerine kullanacağımız tek olgu, bir polinomu, biraz kalan da olsa bir başka polinoma bölebileceğimiz. Tamsayılarda da buna benzer bir bölme yok mudur?

Eğer $f$ ve $g$ polinomları sadece sabit polinomlara bölünüyorsa, o zaman $f$ ve $g$ polinomlarının **aralarında asal** oldukları söylenir. Bazen, $f$ ve $g$'nin ortak böleni yoktur deriz. (Her ne kadar bu çelişik bir terimse de... Çünkü örneğin 1 ve genel olarak sıfır dışında her sabit polinom, herhangi iki polinomu böler.)

Aşağıda $\mathbb{Z}$ ve $K[X]$ halkalarındaki paralel kanıtları bulacaksınız.

## $K[X]$ HALKASINDA

**Olgu.** [MD-2004-I, sayfa 35, Teorem 3'ün özel bir hali] *$K$ bir halka olsun. $a, b \in K[X]$ ve $b \neq 0$ olsun. O zaman $a = bq + r$ ve $d^\circ(r) < d^\circ(b)$ özelliklerini sağlayan $q$* ve *$r$ polinomları vardır.*

**Önsav (Bézout).** *Eğer $a$ ve $b$ polinomları birbirine asalsa, o zaman $au + bv = 1$ eşitliğini sağlayan $u$ ve $v$ polinomları vardır.*

## $\mathbb{Z}$ HALKASINDA

**Olgu.** [MD-2003-IV, sayfa 48-49] *$a, b \in \mathbb{Z}$ ve $b \neq 0$ olsun. O zaman $a = bq + r$ ve $0 \leq r < |b|$ özelliklerini sağlayan $q$* ve *$r$ tamsayıları vardır.*

**Önsav (Bézout).** *Eğer $a$ ve $b$ tamsayıları birbirine asalsa, o zaman $au + bv = 1$ eşitliğini sağlayan $u$ ve $v$ tamsayıları vardır.*

**Kanıt:** $d^\circ(a) + d^\circ(b)$ üzerinden tümevarımla.

Eğer $a$ ya da $b$ polinomlarından biri $K^*$'daysa, kanıt kolay. Eğer $a$ ya da $b$ polinomlarından biri 0'sa, diğeri $K^*$'da olmak zorunda.

Bundan böyle $a$ ve $b$'nin $K$'da olmadıklarını, yani derecelerinin pozitif olduğunu varsayalım.

$d^\circ(b) \le d^\circ(a)$ olsun. $a$'yı $b$'ye bölelim:

$$a = bq + r \text{ ve } d^\circ(r) < d^\circ(b)$$

özelliklerini sağlayan $(q, r)$ polinom çifti vardır.

Elbette $b$ ve $r$'yi bölen her polinom, $a$ ve $b$'yi de böler. Demek ki $b$ ve $r$ de birbirine asal. Ayrıca,

$$d^\circ(a) + d^\circ(b) \ge d^\circ(b) + d^\circ(b) > d^\circ(r) + d^\circ(b)$$

olduğundan, tümevarım varsayımından dolayı,

$$ru + bv = 1$$

eşitliğini sağlayan $u$ ve $v$ polinomları vardır. Bu formülde $r$ yerine $a - bq$ yazarsak,

$$1 = ru + bv = (a - bq)u + bv = au + b(v - qu)$$

elde ederiz ki bu da önsavımızı kanıtlar. □

**Teorem.** *$K[X]$'in indirgenemez her polinomu asaldır.*

**Kanıt:** $p$, $K[X]$'in indirgenemez bir polinomu olsun. İki $g$ ve $h$ polinomu için $p$'nin $gh$'yi böldüğünü varsayalım. $p$'nin ya $g$'i ya da $h$'yi böldüğünü kanıtlayacağız. Böylece $p$'nin bir asal olduğu anlaşılacak. Bunun için $p$'nin $g$'i bölmediğini varsayıp $h$'yi böldüğünü kanıtlamak yeterli. Biz de bundan böyle $p$'nin $g$'i bölmediğini varsayalım.

$p$ indirgenemez olduğundan, $p$'yi sadece $K^*$ ve $K^*p$'nin elemanları böler. Dolayısıyla $p$ ve $g$ birbirine asaldır. Önsav 3 bize $pu + gv = 1$ eşitliğini sağlayan $u$ ve $v$ polinomları verir. Demek ki

$$hpu + hgv = h.$$

Şimdi, $p$ polinomu sol taraftaki $hpu$ ve $hgv$ polinomlarını böler, demek ki toplamlarını da böler, dolayısıyla sağ taraftaki $h$'yi de böler. □

**Sonuç.** *$K$ bir cisim olsun. $K[X]$'in bir $f$ polinomu sonlu sayıda asalın (ya da indirgenemezin) çarpımı olarak yazılır ve bu yazılım aşağı yukarı tek bir biçimde yapılır: Yani $p_1, ..., p_n$ ve $q_1, ..., q_m$ asal polinomlarsa ve*

$$f = p_1 \cdots p_n = q_1 \cdots q_m$$

*ise, o zaman $n = m$'dir ve öyle bir*

$$\sigma: \{1, ..., n\} \to \{1, 2, ..., n\}$$

*eşlemesi vardır ki, her $i$ için $p_i \sim q_{\sigma(i)}$ denkliği sağlanır.* [Sf. 27, Teorem 10 ve sf. 25, Teorem 6]. ♥

**Kanıt:** $|a| + |b|$ üzerinden tümevarımla.

Eğer $a$ ya da $b$ tamsayılarından biri 0'sa diğeri $\pm 1$ olmak zorunda ve bu durumda kanıt *çok* kolay.

Bundan böyle $a$ ve $b$'nin 0 olmadıklarını, yani mutlak değerlerinin pozitif olduğunu varsayalım.

$|b| \le |a|$ olsun. $a$'yı $b$'ye bölelim:

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

özelliklerini sağlayan $(q, r)$ tamsayı çifti vardır.

Elbette $b$ ve $r$'yi bölen her tamsayı, $a$ ve $b$'yi de böler. Demek ki $b$ ve $r$ de birbirine asal. Ayrıca,

$$|a| + |b| \ge |b| + |b| > |r| + |b|$$

olduğundan, tümevarım varsayımından dolayı,

$$ru + bv = 1$$

eşitliğini sağlayan $u$ ve $v$ tamsayıları vardır. Bu formülde $r$ yerine $a - bq$ yazarsak,

$$1 = ru + bv = (a - bq)u + bv = au + (v - qu)b$$

elde ederiz ki bu da önsavımızı kanıtlar. □

**Teorem.** *İndirgenemez her tamsayı bir asaldır.*

**Kanıt:** $p$ indirgenemez bir sayı olsun. İki $g$ ve $h$ doğal sayısı için $p$'nin $gh$'yi böldüğünü varsayalım. $p$'nin ya $g$'i ya da $h$'yi böldüğünü kanıtlayacağız. Böylece $p$'nin bir asal olduğu anlaşılacak. Bunun için $p$'nin $g$'i bölmediğini varsayıp $h$'yi böldüğünü kanıtlamak yeterli. Biz de bundan böyle $p$'nin $g$'i bölmediğini varsayalım.

$p$ indirgenemez olduğundan, $p$'yi sadece $\pm 1$ ve $\pm p$ böler. Dolayısıyla $p$ ve $g$ birbirine asaldır. Önsav 3′ bize $pu + gv = 1$ eşitliğini sağlayan $u$ ve $v$ tamsayıları verir. Demek ki

$$hpu + hgv = h.$$

Şimdi, $p$ sayısı sol taraftaki $hpu$ ve $hgv$ sayılarını böler, demek ki toplamlarını da böler, dolayısıyla sağ taraftaki $h$'yi de böler. □

**Sonuç.** *Her tamsayı sonlu sayıda asalın (ya da indirgenemezin) çarpımı olarak yazılır ve bu yazılım aşağı yukarı tek bir biçimde yapılır: Yani $p_1, ..., p_n$ ve $q_1, ..., q_m$ asal tamsayılarsa ve*

$$f = p_1 \cdots p_n = q_1 \cdots q_m$$

*ise, o zaman $n = m$'dir ve öyle bir*

$$\sigma: \{1, ..., n\} \to \{1, 2, ..., n\}$$

*eşleşmesi vardır ki, her $i$ için $p_i = \pm q_{\sigma(i)}$ eşitliği sağlanır.* ♥