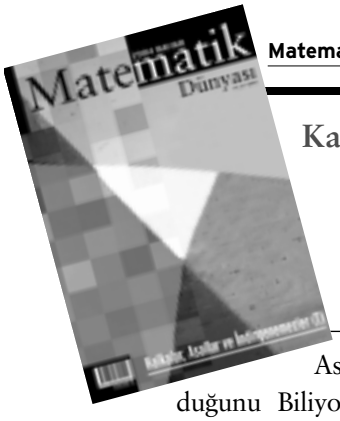


Kapak Konusu: Halkalar, Asallar ve İndirgenemezler (1)

# Asallar ve İndirgenemezler Üzerine Biraz Daha

Asal Sayının Gerçekten Ne Olduğunu Biliyor musunuz? yazısında sayı halkaları adını verdiğimiz birtakım özel halkalarda, indirgenemez ve asalların tanımını verip bunlar hakkında bazı sonuçlar kanıtlamıştık. Aslında o yazının tamamı bu iki kavram üzerine kuruluydu. Bu yazıda aynı kavramlar üzerine düşüneceğiz.

İndirgenemez ve asal eleman tanımlarını bazı halkalara genelleştirebiliriz. Hatta yukarda sözünü ettiğimiz yazıda kanıtladığımız bazı teoremleri bile kimileyin kanıtlayabiliriz. Bizim ilgi alanımız, her elemanın indirgenemezlerin ya da asalların çarpımı olarak yazılıp yazılmaması, yazıldığında da tek bir biçimde yazılıp yazılmadığı konusu. Önce tanımları yazalım.

## TANIMLAR

**Tanım 1.** Bir **tamlık bölgesi**, $xy = 0$ eşitliğinin ancak $x = 0$ ya da $y = 0$ için mümkün olduğu bir halkadır. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ve $\mathbb{Z}/p\mathbb{Z}$ ($p$ asalsa), ve genel olarak her cisim (sayfa 16, Alıştıma 3 ve sayfa 32) bir tamlık bölgesidir. Ayrıca $R$ bir tamlık bölgesiyse, $R[X]$ polinom halkası da bir tamlık bölgesidir (Sonuç 3, sayfa 28). Dolayısıyla $R$ bir tamlık bölgesiyse, örneğin bir cisimse, $R[X]$ polinom halkaları da birer tamlık bölgesidir (Sonuç 3, sayfa 28).

Bundan böyle bu yazıda $R$ hep bir tamlık bölgesini simgeleyecek.

**Tanım 2.** $R$ bir halka olsun.

$R^* = \{x \in R$ : belli bir $y \in R$ için $xy = 1\}$

kümesini anımsayın (sayfa 30). Bu kümenin elemanları $R$'nin adına **tersinir** dediğimiz elemanlarıydı.

**Tanım 3.** Bir $R$ halkasında $a = bx$ denklemi sağlayan bir $x \in R$ varsa o zaman $b$, $a$'yı **böler** denir. Bir cisimde, 0 olmayan her eleman her elemanı böler.

**Tanım 4.** Eğer bir $R$ halkasında $a = bx$ denklemi belli bir $x \in R^*$ için sağlanıyorsa o zaman $a$ ve $b$ **denktir** denir. Bir cisimde 0 olmayan tüm elemanlar birbirine denktir.

**Tanım 5.** $0 \neq x \in R \setminus R^*$ olsun. Eğer $y, z \in R$ için, $x = yz$ eşitliği doğru olduğunda ya $y$ ya da $z$ elemanlarından en azından biri tersinir olmak zorundaysa o zaman $x$'e **indirgenemez** denir. Bir cisimde hiç indirgenemez yoktur.

**Tanım 6.** $0 \neq x \in R \setminus R^*$ olsun. Eğer her $y, z \in R$ için, $x$, $yz$ çarpımını böldüğünde ya $y$'yi ya da $z$'yi bölmek zorundaysa, o zaman $x$'e **asal** denir. Bir cisimde hiç asal yoktur.

## ASALLAR

**Teorem 1.** *Bir tamlık bölgesinin her asalı bir indirgenemezdir.*

**Kanıt:** Aynen sayfa 21, Teorem 8'deki gibi. □

**Örnek.** $\mathbb{Z}/6\mathbb{Z}$'de 2, 3, 4 asaldır, ama 2 ve 4 indirgenemez değildir.

**Teorem 2.** *Bir tamlık bölgesinin bir elemanı sonlu sayıda asalın çarpımı olarak yazılıyorsa, o zaman bu yazılım aşağı yukarı tek bir biçimde yapılabilir. Daha matematiksel bir deyişle, eğer $p_1, \ldots, p_n, q_1, \ldots, q_m$ asalları için ve $u$ tersinir elemanı için,*

$$p_1 \ldots p_n = uq_1 \ldots q_m$$

*eşitliği sağlanıyorsa, o zaman $n = m$ eşitliği sağlanır ve her $p_i$ belli bir $q_j$'ye denktir.*

**Kanıt:** Aynen sayfa 21, Teorem 9'daki gibi. □

## İNDİRGENEMEZLER

Sayfa 19, Teorem 6'da aşağıdaki olguyu doğal sayı üzerine tümevarımla kanıtlamıştık:

**Olgu.** *Her $n \geq 2$ doğal sayısı sonlu sayıda indirgenemez sayının çarpımıdır.*

Daha sonra doğal sayılarda indirgenemezlerle asalların aynı kavram olduğunu kanıtlamıştık, ama $\mathbb{Z}[\sqrt{d}]$ halkasında bunun her zaman doğru olmadığını görmüştük.

Aynı yazıda, sayfa 23, Teorem 16'da yukardaki olguyu $\mathbb{Z}[\sqrt{d}]$ halkalarına genelleştirmiştik:

**Olgu.** $d \in \mathbb{Z} \setminus \{0, 1\}$ sayısı, $\mathbb{Z}$'*de* 1'*den başka bir tamkareye bölünmeyen bir sayı olsun. Her* $0 \neq \alpha \in \mathbb{Z}[\sqrt{d}] \setminus \mathbb{Z}[\sqrt{d}]^*$, $\mathbb{Z}[\sqrt{d}]$ *halkasının indirgenemezlerinin sonlu çarpımı olarak yazılır.*

Bu olguları genel olarak bir tamlık bölgesine genelleştiremeyiz. Yukardaki olguların kanıtını okuyan ve anlayan bu olguları neden genelleştiremeyeceğimizi de anlar. Çünkü yukardaki olguların kanıtları tümevarımla yapılmıştı: Birinci olgunun kanıtını $\alpha$ tamsayısının mutlak değeri $|\alpha|$ üzerine, ikinci olgunun kanıtını $M(\alpha) = |N(\alpha)|$ üzerine tümevarımla yapmıştık. Oysa genel olarak bir tamlık halkasında tümevarım yapacak doğal sayı bulamayız.

Öte yandan yukardaki olguların kanıtlarını bazı polinom halkalarına genelleştirebiliriz.

Önce birkaç tanım anımsatalım: $K$ bir cisim olsun. Yani $K$, her $a \in K \setminus \{0\}$ için $ax = 1$ denkleminin çözülebildiği bir halka olsun. Tanım gereği, $K[X]$ halkasının indirgenemez polinomları sabit polinom değildirler ve sabit olmayan iki polinomun çarpımı olarak yazılamazlar. Örneğin derecesi 1 olan her polinom indirgenemezdir. Ama $(X - 1)(X + 2)$, $X^2$ gibi polinomlar indirgenir polinomlardır. $X^2 - 2$ polinomu $\mathbb{Q}[X]$'te indirgenmez ama $\mathbb{R}[X]$'te indirgenir:$X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$.

Şimdi sayfa 19'daki Teorem 6'yı ve sayfa 23'teki Teorem 16'yı $K[X]$ polinom halkası için kanıtlayabiliriz.

**Teorem 3.** *Eğer K bir cisimse,* $K[X]$*'in sabit olmayan her polinomu sonlu sayıda indirgenemezin çarpımıdır.*

**Kanıt:** Aynen sayfa 19'daki Teorem 6 ve sayfa 23'teki Teorem 16 gibi... Tek farkla ki bu kez tümevarımı polinomun derecesi üzerine yapacağız. $f(X) \in K[X]$ sabit olmayan herhangi bir polinom olsun. Eğer $f(X)$ indirgenemezse sorun yok. Eğer $f(X)$ indirgenirse, o zaman $f(X)$, sabit olmayan iki polinomun, diyelim $g(X)$ ve $h(X)$ polinomlarının çarpımına eşittir: $f = gh$. Şimdi her iki tarafın da derecelerine bakalım. Katsayılar bir cisimde olduğundan, sayfa 28, Önsav 2.iv'e göre,

$$\mathrm{d}^\circ(f) = \mathrm{d}^\circ(gh) = \mathrm{d}^\circ(g) + \mathrm{d}^\circ(h).$$

Ama $g$ ve $h$ sabit polinom olmadıklarından dereceleri 1'den büyük, demek ki her ikisinin de derecesi $f$'nin derecesinden küçük. Dolayısıyla tümevarım varsayımına göre hem $g$ hem $h$ sonlu sayıda indirgenemezin çarpımıdır. Dolayısıyla $f$ de sonlu sayıda indirgenemezin çarpımıdır. □

Galiba burada genel bir yöntem bulduk:

**Teorem 4.** *R bir tamlık bölgesi olsun. R'den doğal sayılar kümesi* $\mathbb{N}$*'ye giden* ve

**i.** *her* $x \neq 0$ *ve* $0 \neq y$ *için,* $d(xy) \geq d(x)$,

**ii.** *her* $x \neq 0$ *ve* $0 \neq y \notin R^*$ *için,* $d(xy) > d(x)$

*özelliklerini sağlayan bir* $d : R \to \mathbb{N}$ *fonksiyonu varsa* $R \setminus R^*$ *kümesinin* 0 *olmayan her elemanı sonlu sayıda indirgenemezin çarpımıdır*[1].

**Kanıt:** Aynen sayfa 19 Teorem 6'nın, sayfa 23 Teorem 16'nın ve biraz önceki Teorem 3'ün kanıtı gibi. Dördüncü kez kanıtlamayacağız. □

Teorem 4'ü uygulayalım. Teorem 4'teki gibi bir $d$ fonksiyonu olan tamlık bölgelerine **dereceli tamlık bölgesi** diyelim. Literatürde bunun örneğine rastlamadığımız için bu terimi uydurmak zorunda kaldık. $d$ fonksiyonuna da o tamlık bölgesinin **derece fonksiyonu** diyelim, $d(x)$'e de $x$'in **derecesi**...

Teorem 4'e göre her dereceli tamlık bölgesinde, tersinir ya da 0 olmayan elemanlar indirgenemezlerin çarpımı olarak yazılabilirler.

**Teorem 5.** *Eğer R dereceli bir tamlık bölgesiyse,* $R[X]$ *de dereceli bir tamlık bölgesidir.*

**Kanıt:** $R$ bir tamlık bölgesi olduğunda, $R[X]$'in de bir tamlık bölgesi olduğunu biliyoruz.

Şimdi $d : R \to \mathbb{N}$ fonksiyonu $R$'nin bir derece fonksiyonu olsun. $R[X]$ halkası için bir $d_1 : R[X] \to \mathbb{N}$ derece fonksiyonu tanımlayacağız.

$0 \neq f = f(X) = f_0 + f_1X + f_2X^2 + ... + f_nX^n \in R[X]$ olsun. Ayrıca $f_n$'nin 0 olmadığını, yani $f$'nin derecesinin $n$ olduğunu varsayalım. $d_1$ fonksiyonunun $f$'deki değerini,

$$d_1(f) = d(f_n) + n$$

olarak tanımlayalım. Ayrıca $d_1(0) = 0$ (ya da başka bir sayı) olsun. Bakalım $d_1$ fonksiyonu $R[X]$ halkası üzerine bir derece mi? $f \neq 0$ ve $g \neq 0$ birer polinom olsunlar. $d_1(fg) \geq d_1(f)$ eşitsizliğini ve eğer $g \notin R[X]^*$ ise $d_1(fg) > d_1(f)$ eşitsizliğini kanıtlamak istiyoruz.

$$f = f_0 + f_1X + ... + f_nX^n$$

ve

$$g = g_0 + g_1X + ... + g_mX^m$$

1 Bunun tersi de hemen hemen doğru. Tersinir ve sıfır olmayan her elemanın indirgenemezlerin çarpımı olduğu bir $R$ halkası ele alalım. Her $0 \neq x \in R$ için,

$$d(x) := \max\{n : x = p_1 \ldots p_n \text{ ve } p_i \text{ indirgenemez}\}$$

sonlu bir sayı olsun. O zaman $d$ fonksiyonu yukardaki koşulları sağlar.

olsun ($f_n, g_m \in R \setminus \{0\}$). Bir yandan, $R$ bir tamlık bölgesi olduğundan

$$d_1(fg) = d(f_n g_m) + n + m.$$

Öte yandan,

$$d_1(f) = d(f_n) + n.$$

Şimdi hesap yapalım:

$$d_1(fg) = d(f_n g_m) + n + m \geq d(f_n g_m) + n \geq d(f_n) + n = d_1(f).$$

Böylece $d_1(fg) \geq d_1(f)$ eşitsizliği kanıtlandı. Eğer $m > 0$ ise, $d_1(fg) > d_1(f)$ eşitsizliği de bu hesaptan dolayı bariz. Sadece, $m = 0$ ve $g = g_m \notin R^*$ olduğunda, $d_1(fg) > d_1(f)$ eşitsizliğini kanıtlamak kaldı. Ama bu doğrudan $d(f_n g_m) > d(f_n)$ eşitsizliğinden çıkar. □

### Çok Değişkenli Polinom Halkaları

$R$ bir halka olsun. $R[X]$ polinom halkasını biliyoruz. Bu polinom halkasının elemanlarını katsayı olarak kullanarak iki değişkenli $(R[X])[Y]$ polinom halkasını elde edebiliriz. Bu son polinom halkası $R[X, Y]$ olarak yazılır. Elbette $R[X, Y]$ ile $R[Y, X]$ arasında dişe dokunur bir fark yoktur. Daha genel olarak, tümevarımla

$$R[X_1, ..., X_n, X_{n+1}]$$

halkaları $(R[X_1, ..., X_n])[X_{n+1}]$ olarak tanımlanır.

**Sonuç 6.** *Aşağıdaki halkaların herbirinde tersinir ve sıfır olmayan her eleman sonlu sayıda indirgenemezin çarpımıdır*:

$K[X_1, ..., X_n]$ (Burada $K$ bir cisim)
$\mathbb{Z}[X_1, ..., X_n]$
$(\mathbb{Z}[\sqrt{d}])[X_1, ..., X_n]$

## ASALLARIN ÇARPIMI

Her elemanın sonlu sayıda indirgenemezin çarpımı olması iyi güzel de, Teorem 2'den dolayı, her elemanın sonlu sayıda asalın çarpımı olarak yazılması daha çok işimize gelir.

Eğer bir tamlık bölgesinin sıfır ya da tersinir olmayan elemanları sonlu sayıda indirgenemezin çarpımı olarak (Teorem 2'de açıklandığı gibi) aşağı yukarı tek bir biçimde yazılabiliyorsa, o zaman o tamlık bölgesine **tek çarpanlama bölgesi** diyelim. Demek ki bir çarpım bölgesinde bir eleman sonlu sayıda indirgenemezin çarpımı olarak yazılır ve bu yazılım aşağı yukarı tek bir biçimde yapılabilir, yani eğer $p_1, ..., p_n, q_1, ..., q_m$ indirgenemezleri için ve bir $u$ tersinir elemanı için,

$$p_1 ... p_n = uq_1 ... q_m$$

eşitliği sağlanıyorsa, o zaman $n = m$ eşitliği sağlanır ve her $p_i$ belli bir $q_j$'ye denktir.

**Teorem 7.** *Bir tek çarpanlama bölgesinde her indirgenemez bir asaldır.*

**Kanıt:** $R$ bir tek çarpanlama bölgesi olsun. $a$ bir indirgenemez olsun ve $a$, $bc$ çarpımını bölsün. Diyelim $ax = bc$. Şimdi $x$'i, $b$'yi ve $c$'yi indirgenemezlerine ayıralım:

$$x = p_1 ... p_n$$
$$b = q_1 ... q_m$$
$$c = r_1 ... r_t$$

O zaman,

$$ap_1 ... p_n = q_1 ... q_m r_1 ... r_t.$$

Demek ki $a$, ya $q_i$'lerden birine ya da $r_j$'lerden birine denk olmalı. Birinci olasılıkta $a$, $b$'yi böler; ikinci olasılıkta $c$'yi. Dolayısıyla $a$ bir asal. □

Demek ki bir tek çarpanlama bölgesinde asallarla indirgenemezler arasında bir ayrım yok. Sonuç olarak, bir tek çarpanlama bölgesinde sıfır ya da tersinir olmayan her eleman sonlu sayıda asalın çarpımıdır ve bu çarpım hemen hemen tek bir biçimde gerçekleşir.

Tek çarpanlama bölgesi kavramını şöyle de tanımlayabilirdik: Eğer bir tamlık bölgesinin sıfır ya da tersinir olmayan elemanları sonlu sayıda asalın (dolayısıyla indirgenemezin de) çarpımı olarak (Teorem 2'de açıklandığı gibi) aşağı yukarı tek bir biçimde yazılabiliyorsa, o zaman o tamlık bölgesine **tek çarpanlama bölgesi** denir. İki tanım arasında bir fark yoktur. Kanıtı kolaydır. Bunu okura alıştırma olarak bırakıyoruz.

**Olgu 8.** *Eğer $R$ bir tek çarpanlama bölgesiyse, $R[X]$ de bir çarpım bölgesidir.*

Ne yazık ki bu olguyu burada kanıtlayacak yerimiz yok. Gelecek sayıda halkalar konusuna devam edeceğiz ve bu olguyu kanıtlayacağız.

**Sonuç 9.** *Aşağıdaki halkaların herbirinde tersinir ve sıfır olmayan her eleman sonlu sayıda asaln çarpımıdır*:

$K[X_1, ..., X_n]$ (Burada $K$ bir cisim)
$\mathbb{Z}[X_1, ..., X_n]$

**Alıştırma [Gauss].** *Eğer $p \in R$ elemanı $R$'de asalsa $R[X]$'te de asaldır.* ♠