Kapak Konusu: Halkalar, Asallar ve İndirgenemezler (1)

Halka

Bu yazıda, geçen yazılarda tanımladığımız yapıların ortak özelliklerini ortaya koyup soyut cebirin en önemli birkaç kavramından biri olan olan "halka"yı tanımlayacağız.

Okur, birazdan tanımlayacağımız "halka" kavramını okurken, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ gibi sayı kümelerini, sayfa 25-28'de Polinom Nedir Ne Değildir? yazısında tanımladığımız $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ gibi polinom kümelerini, sayfa 19-20'de Asal Sayının Ne Olduğunu Gerçekten Biliyor musunuz? yazısında tanımladığımız $\mathbb{Z}[\sqrt{d}]$ kümelerini ve sayfa 15'te "Modülo n Sayılar" yazısında tanımladığımız $\mathbb{Z}/n\mathbb{Z}$ kümelerini aklında tutmalıdır. Bu kümelerin herbiri, +, ×, 0, 1 aksesuvarlarıyla birlikte birer halka örneğidir.

Bir halka her şeyden önce bir kümedir, ama bir halka sadece bir küme değildir elbet. Yoksa küme kavramından gayri bir kavram elde etmezdik.

Bir halkada, ayrıca, 0 (**sıfır**) ve 1 (**bir** ya da **birim öğe**) adı verilen iki özel öğe vardır. Dikkat: Halkanın bu 0 ve 1 öğeleri bizim bildiğimiz 0 ve 1 tamsayıları olmayabilirler. Hatta halkanın hiçbir öğesi sayı olmayabilirler. Eğer halkamıza R adını verirsek, bu öğelere belki de 0 ve 1 yerine 0_R ve 1_R adını vermek daha doğru olurdu, çünkü bunlar sayıların değil, R'nin sıfır ve biridir ve R kümesinin sayılarla hiç mi hiç ilgisi olmayabilir.

Bir halkada ayrıca **toplama** ve **çarpma** adı verilen, ama çocukluğumuzdan beri alışık olduğumuz toplama ve çarpmayla ilgisi olmayabilecek iki de işlem vardır. Bu işlemler + ve × olarak yazılırlar. Yani toplama ve çarpma, her ikisi de $R \times R$ kümesinden R kümesine giden birer fonksiyondur. Eğer $(x, y) \in R \times R$ ise, toplama ve çarpma işlemlerinin (fonksiyonlarının) sonucu sırasıyla $x + y$ ve $x \times y$ yazılırlar. Hemen hemen her zaman $x \times y$ yerine xy yazacağız. Ama 1×1 yerine 11 yazmamaya özen göstereceğiz...

Çoğu kez bu hataya düşüldüğünden yinelemekte yarar var: Adına toplama ve çarpma dediğimiz bu işlemler (fonksiyonlar) bizim aşina olduğumuz toplama ve çarpmayla ilgisi olmayabilir. Bu yüzden bu toplama ve çarpma işlemlerine + ve × olarak yazmak yerine belki de $+_R$ ve $\times_R$ olarak yazmayı yeğlemeliydik, ama öyle yapmayacağız, okurun dikkatli olduğunu varsayacağız.

Tekrarlamakta yarar var!!! Bir halkanın öğelerinin sayılarla hiç mi hiç ilgisi olmayabilir. Sözgelimi bir halkada x^y ya da x/y gibi kavramlar olmayabilir.

Demek ki bir halka, bir R kümesinden, bu kümenin 0 ve 1 adı verilen iki öğesinden ve $R \times R$ kümesinden R kümesine giden ve adına toplama (+) ve çarpma (×) denilen iki fonksiyondan (işlemden) oluşan bir beşlidir.

Bu kadarla kalsa iyi. Bu $(R, +, \times, 0, 1)$ beşlisinin halka adına hak kazanması için birtakım özelliklere sahip olması gerekmektedir. Bir halkanın sahip olması gereken bu özellikleri üç ana grupta toplayacağız:

T) Toplama ve 0'la ilgili özellikler: T1-T4.

Ç) Çarpma ve 1'le ilgili özellikler: Ç1-Ç4.

D) Toplama ve çarpmayla ilgili tek bir özellik: D.

Bu özellikleri yavaş yavaş, sindire sindire, tam iki buçuk sayfada vereceğiz.

Şunu da söylemeliyiz ki "halka"nın tanımı konusunda tam bir uzlaşma sağlanmamıştır. Çeşitli kitaplarda çeşitli tanımlar olabilir. Biz, burada "dağılma özelliğini sağlayan, birim elemanı olan değişmeli halka"lardan sözedeceğiz.

T. Toplamanın Özellikleri

T1 [Birleşme Özelliği]. *Her $x, y, z \in R$ için,*
$$x + (y + z) = (x + y) + z.$$

T2 [Etkisiz Öğe]. *Her $x \in R$ için,*
$$0 + x = x + 0 = x.$$

T3 [Ters Öğenin Varlığı]. *Her $x \in R$ için,*
$$x + y = y + x = 0$$
eşitliklerini sağlayan bir $y \in R$ vardır.

T4 [Değişme Özelliği]. *Her x ve $y \in R$ için,*
$$x + y = y + x.$$

Çarpmanın özelliklerine geçmeden önce toplamanın özelliklerini ve bu özelliklerin sonuçlarını irdeleyelim.

T1, bir halkanın öğeleri toplanırken paranteze gerek olmadığını söylüyor. Üç öğe için geçerli olan bu özellik dört öğe için de geçerlidir. Örneğin x, y, z, t öğelerini bu sırayla toplarken işlemlerin hangi sırayla yapıldıkları önemli değildir. Sözgelimi,

$$\begin{aligned}(x + y) + (z + t) &= (x + (y + z)) + t\\ &= ((x + y) + z) + t = (x + y) + (z + t)\\ &= x + ((y + z) + t) = x + (y + (z + t)).\end{aligned}$$

Bu eşitliklerin herbiri T1 özelliği birkaç kez kullanılarak kanıtlanabilir. Dolayısıyla x, y, z, t öğelerin toplamını parantezsiz olarak $x + y + z + t$ biçiminde yazabiliriz, parantezlerin işlevi kalmamıştır. Biz de bundan böyle toplama yaparken parantezleri kullanmayacağız, doğrudan $x + y + z + t$ yazacağız.

T4 özelliğini kullanarak, toplama yaparken x, y, z ve t'nin yerlerinin de önemli olmadığını anlarız. Örneğin, $x + y + z + t = z + x + t + y$.

Önsav 1 [Sadeleştirme]. *Eğer bir halkanın x, z ve t öğeleri $x + z = x + t$ eşitliğini sağlıyorsa o zaman $z = t$'dir.*

Kanıt: y, x için T3 özelliğini sağlayan bir öğe olsun. Demek ki $y + x = 0$. Şimdi hesaplayalım:

$$\begin{aligned}z &= 0 + z = (y + x) + z = y + (x + z) = y + (x + t)\\ &= (y + x) + t = 0 + t = t.\end{aligned}$$ □

Önsav 1'den, T2 özelliğini sağlayan bir tek 0 öğesi olduğu anlaşılır. Nitekim eğer $x + 0' = x$ ise, $x + 0' = x = x + 0$ eşitliğine Önsav 1'i uygularsak, $0' = 0$ buluruz. Bu, daha kolay biçimde, $0 = 0 + 0' = 0'$ eşitliğinden de çıkar. 0'a **sıfır** ya da toplamanın **etkisiz öğesi** denir.

Gene Önsav 1'den, bir halkada, her x için T3 özelliğini sağlayan tek bir y'nin olduğu anlaşılır, nitekim, eğer $x + y = 0 = x + z$ ise, Önsav 1'e göre $y = z$'dir. Madem ki, $x + y = 0$ eşitliğini sağlayan tek bir y var, (x'e bağımlı olan, yani x değiştikçe değişen) bu y öğesine bir ad verebiliriz. Bundan böyle $x + y = 0$ özelliğini sağlayan y'yi $-x$ olarak yazalım. Ayrıca bundan böyle

$x + (-y)$ yerine $x - y$,
$(-x) + y$ yerine $-x + y$
$(-x) + (-y)$ yerine $-x - y$

yazalım.

Demek ki bir halkada (1 diye bir öğe olduğundan) -1 diye de bir öğe vardır.

Eğer x bir halkanın öğesiyse, o halkanın $-x$ öğesine x'nin **toplama için tersi** ya da **toplamsal tersi** denir. Ama biz mahalle arasında "eksi x" deriz.

Önsav 3. i. $-(x + y) = -x - y$
ii. $-(x - y) = -x + y$
iii. $-(-x) = x$.

Kanıt: Örnek olarak ii'yi kanıtlayıp gerisini okura bırakalım. Kanıtlamak istediğimiz $(x - y) + (-x + y) = 0$ eşitliği, yani yukardaki tanımlara göre $(x + (-y)) + ((-x) + y) = 0$ eşitliği ki, bu da kolay. □

Ç. Çarpmanın Özellikleri

Alışageldiği üzere çarpma yaparken $\times$ simgesini kullanmayacağız. $a \times b$ yerine ab yazacağız.

Ç1 [Birleşme Özelliği]. *Her x, y, $z \in R$ için,*
$$x(yz) = (xy)z.$$
Ç2 [Birim Öğe]. *Her $x \in R$ için,*
$$1x = x1 = x.$$
Ç3 [Değişme Özelliği]. *Her x ve $y \in R$ için,*
$$xy = yx.$$
Ç4. $1 \neq 0$.

Halkanın tanımının tam ne olması konusunda bir uzlaşma yoktur. Bu özelliklerin doğru olduğu halkalara bazen **birleşmeli**, **birim öğeli** ve **değişmeli** halkalar denir. Bizim bu sayıda ele alacağımız halkaların herbiri bu üç özelliği sağlayacak.

Ç1 özelliğine göre, bir halkanın birçok öğesi çarpıldığında parantezler gereksizdir. Bundan böyle biz de çok gerekmedikçe parantez kullanmayacağız

Ç2 özelliğini sağlayan tek bir 1 elemanı vardır: Eğer $1'$ bu özelliği sağlayan bir başka eleman olsaydı, $1 = 1 \times 1' = 1'$ olurdu. 1'e halkanın **birim elemanı** ya da **bir**'i denir.

Tanım. *R bir halka olsun. $a \in R$ olsun. Eğer R halkasında $ab = 1$ eşitliğini sağlayan bir b öğesi varsa, a'ya **tersinir öğe** denir. Tersinir öğeler kümesi R^* olarak gösterilir.*

Örneğin $\mathbb{Z}$ halkasının tersinir öğeleri 1 ve -1'dir. Öte yandan 2, $\mathbb{Z}$'de tersinir değildir (çünkü $1/2 \notin \mathbb{Z}$) ama 2, $\mathbb{Q}$'de tersinirdir. $\mathbb{R}[X]$ polinom halkasının tersinir öğeleri, 0 olmayan sabit polinomlardır (okura alıştırma.) 0 öğesi hiçbir halkada tersinir değildir. Öte yandan 1 ve -1 her halkada tersinirdir, -1'in her halkada tersinir olduğunu daha sonra kanıtlayacağız.

Demek ki,

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

Kolayca görüleceği üzere,

$$\mathbb{Z}^* = \{1, -1\}$$
$$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$$
$$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$$

$\mathbb{R}[X]^* = \mathbb{R} \setminus \{0\}$ = sıfır olmayan sabit polinomlar

$\mathbb{Z}[X]^* = \{1, -1\}$.

Eğer $R = \mathbb{Z}/4\mathbb{Z}$ ise, $R[X]$ halkasında

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

olduğundan, $1 - 2X \in R[X]^*$ dir.

Alıştırmalar. 1. $R = \mathbb{Z}/4\mathbb{Z}$ olsun. $R[X]^*$ kümesini bulun.

2. $R = \mathbb{Z}/6\mathbb{Z}$ olsun. $R[X]^*$ kümesini bulun.

3. Eğer R bir **tamlık bölgesi**yse, yani sıfıra eşit olmayan iki öğenin çarpımı hiçbir zaman sıfır olmuyorsa, $R[X]^* = R^*$ eşitliğini kanıtlayın.

4. p herhangi bir asal sayı olsun. $\mathbb{Q}_{<p>}$, paydası p'ye bölünmeyen kesirli sayılar kümesi olsun. Yani,

$$\mathbb{Q}_{<p>} = \{a/b : a, b \in \mathbb{Z} \text{ ve } p, b\text{'yi bölmez}\}$$

olsun. $\mathbb{Q}_{<p>}$ bir halkadır. $\mathbb{Q}_{<p>}^*$ kümesini bulun.

Bir halkada, eğer a verilmişse, $ab = 1$ eşitliğini sağlayan en fazla bir tek b vardır (hiç olmayabilir de). Nitekim $ab = ac = 1$ ise, o zaman $c = c1 = c(ab) = b(ac) = b1 = b$. Dolayısıyla tersinir bir a öğesi için $ab = 1$ eşitliğini sağlayan bir ve bir tane b öğesi vardır. Bu öğe a^{-1} olarak gösterilir ve bu öğeye a'nın (çarpma için) **tersi** ya da **çarpımsal tersi** denir. Demek ki, eğer bir halkada, $ab = 1$ ise a tersinirdir ve $b = a^{-1}$ dir.

Aşağıdaki önsavın kanıtı oldukça kolaydır:

Önsav 4. *R bir halka olsun.*

i. *$x, y \in R^*$ ise $xy \in R^*$ ve $(xy)^{-1} = x^{-1}y^{-1}$.*

ii. *$x \in R^*$ ise $x^{-1} \in R^*$ ve $(x^{-1})^{-1} = x$.*

iii. *$x \in R^*$ ise ve $xy = 0$ ise o zaman $y = 0$.*

iv. *$x \in R^*$ ise ve $xy = xz$ ise o zaman $y = z$.*

Kanıt: i. Hemen hesaplayalım: $(xy)(x^{-1}y^{-1}) = (xx^{-1})(yy^{-1}) = 1 \times 1 = 1$. Demek ki xy tersinir ve $(xy)^{-1} = x^{-1}y^{-1}$.

ii. $x^{-1}x = 1$ olduğundan, x^{-1} elemanı da tersinirdir ve $(x^{-1})^{-1} = x$ dir.

iii. Biraz acele edip (en son eşitlikte) daha kanıtlamadığımız Önsav 5i'yi kullanacağız:

$$y = 1y = (xx^{-1})y = x^{-1}(xy) = x^{-1}0 = 0.$$

iv. $y = 1y = (xx^{-1})y = x^{-1}(xy) = x^{-1}(xz) = (xx^{-1})z = 1z = z$. □

D. Toplamayla Çarpmayı Harmanlayan Özellik

Yukarda sadece toplamayla ve sadece çarpmayla ilgili özellikleri gördük. Şimdi, toplamayla çarpma arasındaki ilişkiyi ortaya koyan özelliği açıklayalım:

D [Dağılma Özelliği]. *Her $x, y, z \in R$ için,*

$$x(y + z) = xy + xz.$$

Halkanın Tanımı. Artık bir halkayı tam olarak tanımlayabiliriz. Bir R kümesinde, yukardaki T1, T2, T3, T4, Ç1, Ç2, Ç3, Ç4 ve D özelliklerini sağlayan 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. Ve ayrıca + ve ×, $R \times R$'den R'ye giden iki fonksiyon olsun. Eğer $(R, +, \times, 0, 1)$ beşlisi yukardaki T1, T2, T3, T4, Ç1, Ç2, Ç3, Ç4 ve D özelliklerini sağlıyorsa, o zaman $(R, +, \times, 0, 1)$ beşlisine kısaca **halka** denir.

Örnekler. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ kümeleri bildiğimiz toplama ve çarpmayla ve 0 ve 1 öğeleriyle birer halkadırlar. Ama $\mathbb{N}$ bir halka değildir, T3 özelliği $\mathbb{N}$'de doğru değildir. Tek tamsayılar kümesine 0 eklersek, bu kümede T1, T2, T3, T4, Ç1, Ç2, Ç3, Ç4 ve D özelliklerinin hepsi geçerli olmasına karşın, bu küme bir halka olmaz, çünkü bu kümede toplama yapılamaz: İki tek sayının toplamı her zaman bir tek sayı ya da 0 değildir. Oysa bir halkada iki öğenin toplamı ve çarpımı gene o halkada olmalıdır.

Örnek. Bir halkanın öğelerinin her zaman sayı olmadıklarını gösteren bir örnek verelim. A, boş olmayan herhangi bir küme olsun. $R = \wp(A)$, A'nın altkümeleri kümesi olsun. Eğer $x, y \in R$ ise, yani x ve y, R'nin birer altkümesiyse,

$$x + y := (x \cup y) \setminus (x \cap y)$$
$$x \times y := x \cap y$$
$$0 := \emptyset$$
$$1 := X$$

olsun. $(R, +, \times, 0, 1)$ bir halkadır (ayrıntıları okura bırakıyoruz.) Bu halkada, her x için, $x^2 = x$ ve $x + x = 0$ eşitlikleri geçerlidir. Görüldüğü gibi, bu halkanın öğeleri sayı değil, A'nın altkümeleri.

Şimdi dağılma özelliğinin sonuçlarını irdeleyelim.

Önsav 5. *R bir halka olsun. $x, y \in R$ olsun.*

i. $x0 = 0$.

ii. $(-x)y = -(xy) = x(-y)$

iii. $(-1)y = -y$.

iv. $(-1)^2 = 1$.

Kanıt: i. $x0 + 0 = x0 = x(0 + 0) = x0 + x0$ eşitliğinden ve Önsav 1'den $x0 = 0$ çıkar.

ii. $xy + (-xy) = 0 = 0y = (x + (-x))y = xy + (-x)y$. Dolayısıyla, Önsav 1'den $(-x)y = -(xy)$ çıkar. İkinci eşitlik birincisinden ve Ç3'ten çıkar.

iii. Yukarda x yerine 1 koyarsak sonuç çıkar.

iv. Yukarda y yerine -1 koyarsak sonuç, Önsav 3.iii'ten çıkar. □

• R bir halka ve $x \in R$ olsun. Her n doğal sayısı için, x'i kendisiyle n kez toplayabiliriz. Bu toplamı nx olarak gösterelim. Daha matematiksel olarak, $n \in \mathbb{N}$ ve $x \in R$ için, R'nin nx öğesini n üzerine tümevarımla şöyle tanımlayalım:

$$0x = 0$$
$$(n + 1)x = nx + x.$$

• Bu paragraflık halkanın birim öğesini 1 yerine 1_R simgesiyle gösterelim, yoksa birler karışabilir. n herhangi bir doğal sayı olsun. Bir üstteki paragrafta x yerine 1_R alacak olursak, R'nin $n1_R$ öğesini buluruz: $n1_R$, halkanın 1_R öğesi n kez kendisiyle toplanarak bulunmuştur. Bu öğeye n_R diyelim.

• Şimdi soru şu: Acaba R halkasının n_Rx öğesi nx'e eşit mi? Evet:

$$nx = x + ... + x = 1_Rx + ... + 1_Rx$$
$$= (1_R + ... + 1_R)x = n_Rx.$$

Demek ki nx ile n_Rx arasında bir ayrım gözetmeye gerek yok. Bundan sonra n_R yerine (sanki bir doğal sayıymış gibi) n yazacağız. Eğer çok çok gerekirse aralarında bir ayrım yaparız.

• Bir halkada nx diye bir öğenin varlığını yukarda gördük: x'in kendisiyle n kez toplanmasıyla elde edilen öğe. Demek ki $-nx$ diye de bir öğe var: nx'in toplama için tersi. Ayrıca $n(-x)$ diye de bir öğe var: $-x$'in kendisiyle n kez toplanmasıyla elde edilen öğe. Acaba bu iki öğe birbirine eşit mi? Evet:

$$nx + n(-x) = n(x + (-x)) = n0 = 0,$$

dolayısıyla $n(-x) = -nx$.

Bundan böyle $(-n)x$ ya da $n(-x)$ sayısını $-nx$ olarak tanımlayacağız.

• Okur alıştırma olarak $(-n_R)x = -nx$ eşitliğini de kanıtlayabilir.

• Demek ki her $n \in \mathbb{Z}$ ve her $x \in R$ için bir $nx \in R$ öğesi tanımladık. Şu özellikleri kanıtlamak oldukça kolaydır: Her $n, m \in \mathbb{Z}$ ve her $x, y \in R$ için,

$$(n + m)x = nx + mx,$$
$$n(mx) = (nm)x,$$
$$(-n)x = -nx = n(-x),$$
$$(nx)(my) = (nm)(xy).$$

Eğer R bir halkaysa ve $R^* = R \setminus \{0\}$ ise, o zaman R'ye **cisim** adı verilir. $\mathbb{Q}$ ve $\mathbb{R}$ birer cisimdir, ama $\mathbb{Z}$ ve polinom halkalarının hiçbiri bir cisim değildir. Önsav 4.iii'e göre her cisim bir tamlık bölgesidir.

Alıştırmalar

1. $\mathbb{Z}/n\mathbb{Z}$ halkasının bir cisim olması için yeterli ve gerekli koşul n'nin bir asal olmasıdır.

2. $d \in \mathbb{N}$ bir tamkare olmasın, örneğin $d = 2$ olabilir. $\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Q}\}$ olsun. Bildiğimiz toplama ve çarpma altında $\mathbb{Q}[\sqrt{d}]$ bir halkadır. Bunun kanıtlanması oldukça kolaydır. $\mathbb{Q}[\sqrt{d}]$ halkasının ayrıca bir cisim olduğunu kanıtlayın.

3. Sonlu bir tamlık bölgesinin (bknz. sayfa 28 ya da 36) bir cisim olduğunu kanıtlayın.

Birkaç Eşitlik. Halkalarda (dolayısıyla polinom halkalarında ve tamsayılarda da) çok bilinen birkaç eşitliği yazarak bitirelim bu yazıyı.

A. Bir halkanın bir x öğesinin pozitif tamsayı güçlerini alabiliriz.

$$x^0 = 1,$$
$$x^1 = x,$$
$$x^2 = x \times x,$$
$$x^3 = x \times x \times x, ...$$

Genel olarak ve daha matematiksel olarak, güç alma, n üzerine tümevarımla

$$x^0 = 1 \text{ ve } x^{n+1} = x^n \times x$$

olarak tanımlanır.

Eğer x ve y bir halkanın birer öğesiyse ve $n > 0$ bir tamsayıysa,

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + ... + xy^{n-2} + y^{n-1})$$

eşitliği herhalde en çok bilinen ve kanıtı oldukça kolay eşitliklerdendir. Eğer n bir tek sayıysa, y yerine $-y$ alıp,

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + ... - xy^{n-2} + y^{n-1})$$

eşitliğini buluruz.

B. Eğer $n! = 1 \times 2 \times ... \times n$, $0! = 1$ ve her $0 \le i \le n$ için $\binom{n}{i}$ sayılarını,

$$\binom{n}{i} = \frac{n!}{i!\,(n-i)!}$$

olarak tanımlarsak, o zaman bir halkanın her x ve y öğesi için ve her $n > 0$ tamsayısı için,

$$(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

eşitliği geçerlidir. Bu eşitliği kanıtlayalım. Ama önce bir önsav:

Önsav 4. *Her n doğal sayısı ve her* $0 \le i < n$ için

$$\binom{n+1}{i+1} = \binom{n}{i} + \binom{n}{i+1}.$$

Kanıt: Doğrudan hesaplayalım:

$$\binom{n}{i} + \binom{n}{i+1} = \frac{n!}{i!\,(n-i)!} + \frac{n!}{(i+1)!\,(n-i-1)!}$$
$$= \frac{n!\,(i+1)}{(i+1)!\,(n-i)!} + \frac{n!\,(n-i)}{(i+1)!\,(n-i)!}$$
$$= \frac{n!\,[(i+1)+(n-i)]}{(i+1)!\,(n-i)!} = \frac{n!\,(n+1)}{(i+1)!\,(n-i)!}$$
$$= \frac{(n+1)!}{(i+1)!\,(n-i)!} = \binom{n+1}{i+1}$$

Teorem 5. *x ve y bir halkanın öğeleriyse ve n bir doğal sayıysa,*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

Kanıt: n üzerine tümevarımla kanıtlayacağız.

Eğer $n = 0$ ya da 1 ise, kanıt oldukça kolay, bu iki şıkkı okura bırakıyoruz. Şimdi eşitliğin n için doğru olduğunu varsayıp eşitliği $n + 1$ için kanıtlayalım. Doğrudan hesaplayalım.

$$(x+y)^{n+1} = (x+y)^n(x+y) = \left(\sum_{i=0}^{n}\binom{n}{i}x^i y^{n-i}\right)(x+y)$$
$$= \left(\sum_{i=0}^{n}\binom{n}{i}x^i y^{n-i}\right)x + \left(\sum_{i=0}^{n}\binom{n}{i}x^i y^{n-i}\right)y$$
$$= \left(\sum_{i=0}^{n}\binom{n}{i}x^{i+1} y^{n-i}\right) + \left(\sum_{i=0}^{n}\binom{n}{i}x^i y^{n+1-i}\right)$$
$$= \left(x^{n+1} + \sum_{i=0}^{n-1}\binom{n}{i}x^{i+1} y^{n-i}\right) + \left(\sum_{i=1}^{n}\binom{n}{i}x^i y^{n+1-i} + y^{n+1}\right)$$
$$= \left(x^{n+1} + \sum_{j=1}^{n}\binom{n}{j-1}x^{j} y^{n-(j-1)}\right) + \left(\sum_{j=1}^{n}\binom{n}{j}x^j y^{n-(j-1)} + y^{n+1}\right)$$
$$= x^{n+1} + \sum_{j=1}^{n}\left(\binom{n}{j-1} + \binom{n}{j}\right)x^j y^{n+1-j} + y^{n+1}$$
$$= x^{n+1} + \sum_{j=1}^{n}\binom{n+1}{j}x^j y^{n+1-j} + y^{n+1} = \sum_{j=0}^{n+1}\binom{n+1}{j}x^j y^{n+1-j}$$
$$= \sum_{i=0}^{n+1}\binom{n+1}{i}x^i y^{n+1-i}.$$

Alıştırmalar. Teorem 5'in aşağıdaki sonuçlarını kanıtlayın:

$$\sum_{i=0}^{n}\binom{n}{i} = 2^n. \qquad \sum_{i=0}^{n}2^i\binom{n}{i} = 3^n.$$

$$\sum_{i=0}^{n}(-1)^i\binom{n}{i} = 0. \qquad \sum_{i=0}^{n}(-2)^i\binom{n}{i} = (-1)^n.$$

Her Yerde Dedekind

Halka kavramı matematiğe Dedekind'le girmiştir. Dedekind terim olarak Almanca "sıralama" demek olan "ordnung"u kullanmıştır. Daha sonra Hilbert "ordnung" yerine "halka" demek olan "ring"i yeğlemiştir. Hilbert'in halka terimini yeğlemesinin nedeni şuydu: $\mathbb{Z}[\sqrt{d}]$ ya da

$$\mathbb{Z}[5^{1/3}] := \{a + b5^{1/3} + c5^{2/3} : a, b, c \in \mathbb{Z}\}$$

gibi birçok sayı halkasında, herhangi bir x elemanının 1, x, x^2, x^3, ... güçlerine bakalım. Belli bir aşamadan sonra her x^n gücü daha önceki 1, x, x^2, x^3, ..., x^{n-1} güçlerinin doğrusal kombinasyonu olarak yazılabilir (yani her x elemanı, $\mathbb{Z}[X] \setminus \{0\}$ kümesinden başkatsayısı 1 olan bir polinomun köküdür.) Bu bir geri dönüşü çağrıştırdığından Hilbert bu yapılara halka adını vermiştir. Bu özellik her halka için doğru değildir elbet, Dedekind ve Hilbert özel halkalardan sözediyorlardı. İlk kez Adolf Abraham Fraenkel (1892-1965) 1914'te genel halka kavramını soyut olarak (yani aksiyomatik yöntemle, bizim yukarda yaptığımız gibi) tanımlamıştır.

Cisim kavramını da ilk kez, $\mathbb{Q}[\sqrt{d}]$ ya da

$$\mathbb{Q}[5^{1/3}] = \{a + b5^{1/3} + c5^{2/3} : a, b, c \in \mathbb{Q}\}$$

gibi cebirsel sayı cisimlerini incelerken, Dedekind bulmuştur.

Genel olarak, modern cebirin Fermat'nın Son Teoremi'ni kanıtlamak için yaratıldığını söylemek pek yanlış olmaz. Bunun için cebirsel sayıları anlamak gerekiyordu. Nitekim,

$$x^p + y^p = \prod_{\alpha^p=-1}(x + \alpha y)$$

eşitliği sayesinde $x^p + y^p$ iki değişkenli polinomunu $\mathbb{Q}$'dan biraz daha büyük bir cisim üzerine birinci dereceden polinomların çarpımı olarak yazılabilir. Cebirsel sayıların indirgenemezlerin çarpımı olarak yazılmalarına karşın, bu yazılımın değişik biçimlerde yapılabilir olması (örneğin $(1 + \sqrt{-5})(1 + \sqrt{-5}) = 2 \times 3$, bknz. sayfa 23-24) Fermat'nın Son Teoremi'nin kanıtında önemli bir engel oluşturmuştur. Bu anormal durumu düzeltmek için Dedekind idealleri keşfetmiş ve modern cebirin gelişmesinde çok önemli bir rol oynamıştır. ♠