



Kapak Konusu: Halkalar, Asallar ve İndirgenemezler (1)

## Asal Sayının Ne Olduğunu Gerçekten Biliyor musunuz?

Asal sayı, kendinden ve 1'den başka sayıya bölünmeyen sayı olarak bilinir. Buna bir de sayının 1'den farklı olması koşulu eklenir. Bundan daha yanlış doğru bir önerme olamaz!

Türkçenin kurallarına göre böyle bir sayıya "asal" değil indirgenemez demek daha doğrudur, ve matematikte de öyle denir, çünkü kendinden ve 1'den başka sayıya bölünmeyen bir sayı kendinden daha küçük sayıların çarpımı olarak yazılamaz.

Bu yazıda bu asal sayı tanımının hem neden yanlış hem de neden doğru olduğunu göstereceğiz. Önce doğruluğunu kanıtlayalım, yanlışlığını daha sonra göstereceğiz. İlk olarak tanımları sabitleyelim.

**İndirgenemez Sayı.** Eğer 1'den farklı bir  $p$  doğal sayısı sadece 1 ve  $p$  sayılarına bölünüyorsa<sup>1</sup>, o sayıya indirgenemez sayı diyelim. Bu tanıma göre,  $p > 1$  ise ve her  $x, y \in \mathbb{N}$  için,  $p = xy$  eşitliği doğru olduğunda ya  $x$  ya da  $y$  sayısı 1 olmak zorunda oluyorsa, o zaman  $p$ 'ye indirgenemez denir. Örneğin, 2, 3, 5, 7, 11, 13, 17, 19, 23 indirgenemez doğal sayılardır.

**Asal Sayı.** Asal sayının tanımı başkadır. Eğer 1'den ve 0'dan farklı bir  $p$  doğal sayısı, iki sayının çarpımını böldüğünde çarpanlardan en azından birini bölüyorsa o sayıya asal denir. Yani eğer her  $x, y \in \mathbb{N}$  için,  $p, xy$ 'yi böldüğünde,  $p$  ya  $x$ 'i ya da  $y$ 'yi bölüyorsa  $p$ 'ye asal denir. Örneğin 2, 3, 5, 7, 11, 13, 17, 19, 23 asal sayılardır.

Bugüne ve bu satıra dek asal sayılarla indirgenemez sayılar arasında bir ayrım göremediyseniz "suç" sizde değildir. Çünkü bu iki kavram doğal sayılarda örtüşürler. Yani asal her doğal sayı indirgenemezdir ve indirgenemez her doğal sayı asaldır. Ama bunun kanıtlanması gerekir. Bu yazıda ilk olarak asalla indirgenemez arasında doğal sayılar-

da bir fark olmadığını kanıtlayacağız. Daha sonra, başka sayı kümelerinde, asallarla indirgenemezler arasında bir fark olduğunu göreceğiz.

Matematiğe ilgi duyan okur aşağıdaki kanıtı okumadan önce bu iki kavramın doğal sayılarda aynı kavramlar olduğunu kendi kendine kanıtlamaya çalışmalıdır.

Kolaydan başlayalım; önce her asalın indirgenemez olduğunu kanıtlayalım.

**Teorem 1.** Her asal indirgenemez bir sayıdır.

**Kanıt:**  $p$  bir asal sayı olsun. İki  $x$  ve  $y$  sayısı için,  $p = xy$  eşitliği sağlandığını varsayalım. Ya  $x$ 'in ya da  $y$ 'nin 1 olduğunu kanıtlayacağız, böylece  $p$ 'nin indirgenemezliği kanıtlanmış olacak.  $p$  sayısı  $p$ 'yi böldüğünden,  $p$  sayısı  $xy$ 'yi de böler. Ama  $p$  asal olduğundan, bundan  $p$ 'nin ya  $x$ 'i ya da  $y$ 'yi böldüğü çıkar. Diyelim  $p, x$ 'i bölüyor. Demek ki belli bir  $x_1$  tamsayısı için  $x = px_1$ . Şimdi küçük bir hesap yapalım:  $p = xy = px_1y$ . Bu eşitlikte  $p$ 'leri sadeleştirirsek,  $1 = x_1y$  elde ederiz, ki bundan da  $y = 1$  çıkar. Eğer  $p, y$ 'yi bölseydi, o zaman,  $x = 1$  elde edecektik. □

Yukardaki kanıtın doğal sayıların hemen hemen hiçbir özelliğini kullanmadığına dikkatinizi çekerim. Örneğin tümevarımla kanıt yöntemi kullanmadık. Nitekim, eğer asal ve indirgenemez tanımlarında hafif bir değişiklik yapacak olursak, yukardaki teorem oldukça genel bir teoreme dönüşür. Aynı teorem, sonradan göreceğimiz üzere adına "tamlik bölgesi" denen yapılarda da geçerlidir.

Şimdi her indirgenemez doğal sayının bir asal olduğunu kanıtlayacağız. İki değişik kanıt vereceğiz. Birinci kanıt doğal sayıların dışına çıkıp tamsayıları kullanacak. İkinci kanıt sadece doğal sayıları kullanacak. Ama her iki kanıt da doğal sayılara özgü özellikleri (örneğin tümevarımla kanıt yöntemini) kullanacak.

**Teorem 2.** İndirgenemez her doğal sayı bir asaldır.

<sup>1</sup> Eğer  $y = xz$  eşitliğini sağlayan bir  $z$  sayısı varsa, o zaman " $x, y$ 'yi böler" denir. Demek ki her sayı 0'ı böler, 1 her sayıyı böler, 0 bir tek 0'ı böler ve her sayı kendini böler. Dikkat! "0, 0'ı böler" demek "0/0 diye bir sayı vardır" anlamına gelmez! Yoktur öyle bir sayı.

**Teorem 2'nin Birinci Kanıtı.** Önce bir önsava ihtiyacımız var.

**Önsav 3.** Eğer  $a$  ve  $b$  doğal sayıların doğal sayılarda 1'den başka ortak böleni yoksa, o zaman  $au + bv = 1$  eşitliğini sağlayan  $u$  ve  $v$  tamsayıları vardır.

**Kanıt:**  $a + b$  üzerinden tümevarım yapacağız.  $a$  ya da  $b = 1$  ise, kanıt oldukça kolay. Bundan böyle  $a \neq 1, b \neq 1$  varsayalım. Bu varsayımdan kolayca  $a > 1, b > 1$  çıkar. Elbette  $a \neq b$ . Dolayısıyla ya  $a < b$  ya da  $b < a$ . Birinci varsayımda çalışalım, diğer varsayım bunun simetrik durumu.  $a$  ve  $b - a$ 'nın ortak bölenleri  $a$  ve  $b$ 'nin de ortak bölenleridir elbet. Dolayısıyla  $a$  ve  $b - a$ 'nın 1'den başka ortak böleni yoktur. Tümevarımla  $au + (b-a)v = 1$  eşitliğini sağlayan  $u$  ve  $v$  tamsayıları vardır. Bundan da  $a(u-v) + bv = 1$  çıkar. Önsavımız kanıtlanmıştır.  $\square$

Şimdi Teorem 2'yi kanıtlayabiliriz.

$p$  indirgenemez bir sayı olsun. İki  $x$  ve  $y$  doğal sayısı için  $p$ 'nin  $xy$ 'yi böldüğünü varsayalım.  $p$ 'nin ya  $x$ 'i ya da  $y$ 'yi böldüğünü kanıtlayacağız. Böylece  $p$ 'nin bir asal olduğu anlaşılacak. Bunun için  $p$ 'nin  $x$ 'i bölmediğini varsayıp  $y$ 'yi böldüğünü kanıtlamak yeterli. Biz de bundan böyle  $p$ 'nin  $x$ 'i bölmediğini varsayalım.  $p$  indirgenemez olduğundan,  $p$ 'yi sadece 1 ve  $p$  böler. Dolayısıyla  $p$  ve  $x$ 'i sadece 1 böler. Önsav 3'ten dolayı  $pu + xv = 1$  eşitliğini sağlayan  $u$  ve  $v$  tamsayıları vardır. Demek ki  $ypu + yxv = y$ . Şimdi,  $p$  sayısı sol taraftaki  $ypu$  ve  $yxv$  sayılarını böler, demek ki toplamlarını da böler, dolayısıyla sağ taraftaki  $y$ 'yi de böler.  $\square$

**Teorem 2'nin İkinci Kanıtı:** Aynı kanıtı doğal sayıların dışına çıkmadan (tamsayıları kullanmadan) vermek aşağıda görüldüğü gibi birazcık daha zahmetlidir.

**Önsav 4.** 1'den değişik her doğal sayı indirgenemez bir sayıya bölünür.

**Kanıt:** Doğal sayımıza  $n$  diyelim. Eğer  $n = 0$  ise sorun yok, her sayı 0'ı böler. Bundan böyle  $n \geq 2$  olsun. Önsavı  $n$  üzerine tümevarımla kanıtlayacağız.  $n$ 'den küçük ve 1'den büyük her doğal sayının indirgenemez bir sayıya bölündüğünü varsayalım (buna tümevarım varsayımı diyelim; eğer  $n = 2$  ise tümevarım varsayımımız hiçbir bilgi vermemektedir.) Eğer  $n$  indirgenemezse sorun yok, o zaman  $n$

doğal sayısı  $n$  indirgenemez sayısına bölünür. Eğer  $n$  indirgenebilirse, o zaman 1'den değişik  $a$  ve  $b$  doğal sayıları için  $n = ab$  olarak yazılabilir. Tümevarım varsayımından,  $a$  bir indirgenemeze bölünür ve  $n$ 'de o  $a$ 'yı bölen indirgenemeze bölünür.  $\square$

Şimdi Teorem 2'yi bir defa daha kanıtlayalım.

$p$  indirgenemez bir sayı olsun.  $p$ 'nin asal olduğunu kanıtlayacağız. Kanıtımızı tümevarımla yapacağız. Teoremin  $p$ 'den küçük indirgenemez sayılar için doğru olduğunu, yani  $p$ 'den küçük indirgenemezlerin asal olduklarını varsayalım.

$p, xy$  sayısını bölsün.  $p$ 'nin  $x$ 'i ya da  $y$ 'yi böldüğünü kanıtlayacağız. Diyelim bu doğru değil: diyelim  $p, xy$ 'yi bölüyor ama ne  $x$ 'i ne de  $y$ 'yi bölüyor. Bu tür  $x$  ve  $y$  sayılarının en küçüklerini alalım.  $x$ 'i ve  $y$ 'yi  $p$ 'ye böldüğümüzde kalanlarına  $i$  ve  $j$  diyelim. Demek ki  $p$  sayısı  $ij$ 'yi de bölüyor, ama  $p$  ne  $i$ 'yi ne de  $j$ 'yi bölüyor (Neden?)  $x$  ve  $y$  bu özellikleri sağlayan en küçük sayı olduklarından,  $x = i$  ve  $y = j$  olmak zorunda. Demek ki  $x$  ve  $y$  doğal sayıları  $p$ 'den küçük. Şimdi  $k$  sayısı,  $xy$ 'yi  $p$ 'ye böldüğümüzde elde edilen sonuç olsun, yani  $pk = xy$  eşitliği sağlansın. Eğer  $k = 1$  ise  $p = xy$  olur ve  $p$  indirgenemez olduğundan ya  $x = p$  ya da  $y = p$  elde edilir, varsayımımıza karşı.  $k = 0$  ise de kanıt kolay. Demek ki  $k \geq 2$ . Ayrıca,

$$pk = xy \leq (p-1)^2 = p^2 - 2p + 1 < p^2 - p.$$

Bundan da  $k < p - 1 < p$  çıkar. Önsav 4'e göre  $k$  indirgenemez bir  $q$  sayısına bölünür;  $k = qk'$  olsun. Demek ki  $q \leq k < p$ . Tümevarım varsayımını  $q$ 'ya uygulayalım:  $q$  indirgenemezi bir asaldır. Şimdi  $q, pk$ 'yi böldüğünden  $xy$ 'yi de böler. Asal olduğundan,  $q$  ya  $x$ 'i ya da  $y$ 'yi böler. Diyelim  $x$ 'i böler (diğer varsayım simetrik durumdur);  $x = qx'$  olsun;  $p$  sayısının  $x'$  sayısını bölmediğine dikkatinizi çekerim (yoksa  $x$ 'i bölerdi). Şimdi,  $pkq' = pk = xy = qx'y$ . En sağ ve en soldaki  $q$ 'ları sadeleştirirsek  $pk' = x'y$  çıkar. Ama şimdi  $p$  indirgenemezi  $x'y$  sayısını bölüyor, öte yandan ne  $x'$  sayısını ne de  $y$  sayısını bölüyor. Ama hani  $x$  ve  $y$  bu özelliği sağlayan en küçük sayılardı? Bir çelişki elde ettik.  $\square$

Demek ki doğal sayılarda indirgenemez sayılarla asal sayılar arasında bir fark yok.

Konumuzu genişletmeden önce, sadece Teorem 1'i kullanarak asal sayıların indirgenemez sayılara olan bir üstünlüğünden söz edelim:

**Teorem 5.** Bir doğal sayı sonlu sayıda asalın çarpımı olarak (eğer yazılırsa!) sıralama farkını saymazsak tek bir biçimde yazılır. Daha matematiksel bir deyişle, eğer  $p_1, \dots, p_n, q_1, \dots, q_m$  asalları için  $p_1 \dots p_n = q_1 \dots q_m$  eşitliği sağlanıyorsa, o zaman  $n = m$  eşitliği sağlanır ve her  $p_i$  belli bir  $q_j$ 'ye eşittir.

**Kanıt:** Kanıtımızı  $n$  üzerinden tümevarımla yapalım.

Önce  $n = 1$  şikkını ele alalım.  $p_1, q_1, \dots, q_m$  asalları için  $p_1 = q_1 \dots q_m$  eşitliği sağlansın. Demek ki  $p_1 = (q_1)(q_2 \dots q_m)$ . Dolayısıyla,  $p_1$ , asal olduğundan, ya  $q_1$ 'i ya da  $q_2 \dots q_m$  sayısını böler. İkinci şıkta durmayıp devam edersek, en fazla  $m$  adımda,  $p_1$  asal sayısının  $q_j$ 'lerden birini böldüğünü görürüz. Demek ki belli bir  $x$  için  $q_j = p_1 x$ . Ama  $q_j$  de bir asal, dolayısıyla indirgenemez (Teorem 1). Demek ki  $x = 1$  ve  $q_j = p_1$ . Şimdi,  $p_1 = q_1 \dots q_m$  eşitliğinde  $q_j$  yerine  $p_1$  koyalım:

$$p_1 = q_1 \dots q_{j-1} p_1 q_{j+1} \dots q_m$$

eşitliğini elde ederiz. İki taraftan  $p_1$ 'leri sadeleştirirsek,  $1 = q_1 \dots q_{j-1} q_{j+1} \dots q_m$  eşitliğini elde ederiz. Demek ki sağ taraftaki tüm asal sayılar 1'e eşitler, yani aslında yoklar...

Eğer  $n > 1$  ise, kanıt aynı. Ama biz gene de yapalım kanıtı. Kanıtımızın  $n - 1$  için doğru olduğunu varsayalım.  $p_1, \dots, p_n, q_1, \dots, q_m$  asalları için

$$p_1 \dots p_n = q_1 \dots q_m$$

eşitliği sağlansın. Demek ki  $p_1$ , sol tarafı böldüğünden, sağ tarafı da, yani  $(q_1)(q_2 \dots q_m)$  sayısını da böler. Dolayısıyla,  $p_1$  asal olduğundan,  $p_1$  ya  $q_1$ 'i ya da  $q_2 \dots q_m$  sayısını böler. İkinci şıkta durmayıp devam edersek,  $p_1$  asal sayısının  $q_j$ 'lerden birini böldüğünü görürüz. Demek ki belli bir  $j$  ve bir  $x$  için,  $q_j = p_1 x$ . Yukardaki gibi  $q_j = p_1$  elde ederiz. Şimdi,  $p_1 \dots p_n = q_1 \dots q_m$  eşitliğinde  $q_j$  yerine  $p_1$  koyalım:  $p_1 \dots p_n = q_1 \dots q_{j-1} p_1 q_{j+1} \dots q_m$  eşitliğini elde ederiz. İki taraftan  $p_1$ 'leri sadeleştirirsek,

$$p_2 \dots p_n = q_1 \dots q_{j-1} q_{j+1} \dots q_m$$

eşitliğini elde ederiz ve tümevarım varsayımını kullanarak teoremi kanıtlarız.  $\square$

Dikkat edilirse, yukardaki teoremi kanıtlamak için Teorem 2'yi ve sonrasını kullanmadık.

Bu sefer indirgenemezlerle ilgili bir teorem kanıtlayalım. Gene Teorem 2'yi ve sonrasını kullanmayacağız.

**Teorem 6.** Her  $n \geq 2$  doğal sayısı sonlu sayıda indirgenemez sayının çarpımıdır.

**Kanıt:**  $n \geq 2$  bir doğal sayı olsun. Eğer  $n$  indirgenemezse,  $n$  tek bir indirgenemeyen ( $n$ 'nin) çarpımıdır. Eğer  $n$  indirgenebilirse,  $n = ab$  eşitliğini sağlayan 1'den büyük ama  $n$ 'den küçük  $a$  ve  $b$  sayıları vardır. Tümevarımla  $a$  ve  $b$  sayılarının herbiri sonlu sayıda indirgenemeyen çarpımıdır. Dolayısıyla  $ab$ , yani  $n$  de sonlu sayıda indirgenemeyen çarpımıdır.  $\square$

Yukardaki iki teoremlerden şimdi (bu kez Teorem 2'yi kullanarak) güzel bir sonuç çıkarabiliriz:

**Sonuç 7.** 1'den büyük bir doğal sayı sonlu sayıda asalın (ya da indirgenemeyenin) çarpımı olarak sıralama farkını saymazsak tek bir biçimde yazılır. Daha matematiksel bir deyişle, eğer  $k \geq 2$  ise, o zaman,

a)  $k = p_1 \dots p_n$  eşitliğini sağlayan sonlu sayıda  $p_1, \dots, p_n$  asalı vardır.

b) Eğer  $q_1, \dots, q_m$  asalları için  $k = q_1 \dots q_m$  eşitliği sağlanıyorsa, o zaman  $n = m$  eşitliği sağlanır ve her  $p_i$  belli bir  $q_j$ 'ye eşittir.

**Kanıt:** Teorem 6'ya göre  $k$  sonlu sayıda indirgenemeyen çarpımıdır. Teorem 2'ye göre bu indirgenemezler asaldır. Teorem 5'e göre bu yazılım aşağı yukarı tek bir biçimde yapılır.  $\square$

**Doğal Sayıların Ötesi.** Her ne kadar Teorem 2'de doğal sayılarda asalla indirgenemez arasında bir ayrım olmadığını kanıtlamışsak da, bundan sonraki sonuçları sanki bu kavramlar arasında bir ayrım varmış gibi dikkatlice yazıp kanıtladık. Bunun bir nedeni var: Asallarla indirgenemezler arasında doğal sayılarda ve tamsayılarda bir ayrım yoksa da, başka sayı kümelerinde bu iki kavram arasında bir ayrım vardır. Şimdi bu ayrımdan sözedeceğiz.

Gerçel sayılar kümesi  $\mathbb{R}$ 'nin (ya da karmaşık sayılar kümesi  $\mathbb{C}$ 'nin) çıkarma ve çarpma altında kapalı ve 1'i içeren bir  $A$  altkümesini alalım. Demek ki,  $1 \in A$  ve her  $x, y \in A$  için,  $x - y, xy \in A$ . Örneğin  $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$  olabilir, ya da

$$A = \mathbb{Z}[\sqrt{5}] := \{a + b\sqrt{5} : a, b \in \mathbb{Z}\},$$

$$A = \mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$$

kümeleri olabilir. Okurun, yazının devamını okurken,  $\mathbb{Z}$  ve  $\mathbb{Z}[\sqrt{2}]$  ve  $\mathbb{Z}[\sqrt{5}]$  gibi  $\mathbb{Z}[\sqrt{d}]$  türünden örnekleri aklında tutmasında yarar vardır. Eğer karmaşık sayıları biliyorsa  $\mathbb{Z}[\sqrt{-3}]$  türünden örnekler de yararlıdır (burada  $\sqrt{-3}$ , karesi  $-3$  olan yepyeni bir "sayı"dır.)

Yukardaki özellikleri sağlayan  $A$  kümelerine **sayı halkası** ya da daha kısa olarak **halka** adı verilir.

lir. Bundan böyle  $A$  bir sayı halkasını simgelesin.

$0 = 1 - 1 \in A$  olduğundan,  $0$  sayısı da  $A$ 'dadır. Dolayısıyla, her  $a, b \in A$  için,  $a + b = a - (0 - b) \in A$ . Demek ki bir sayı halkası sadece çıkarma ve çarpma altında değil, toplama altında da kapalıdır. Bütün bunlardan  $Z \subseteq A$  çıkar.

Bir sayı halkasının asallarının ve indirgenemelerinin tanımlarını vereceğiz ve bu iki kavramın her zaman aynı olmadığını göreceğiz. Zaten sayılar kuramını ilginç kılan da bu "anormallik"tir.

Tanımlara başlıyoruz.

**Bölmek.**  $x, y \in A$  olsun. Eğer  $xa = y$  eşitliğini sağlayan bir  $a \in A$  varsa, o zaman " $x, y$ 'yi  $A$ 'da böler" denir. Bu bazen  $x|y$  olarak yazılır. Elbette, eğer  $x \neq 0$  ise,  $x|y$  ancak ve ancak  $y/x \in A$  ise,

**Alıştırmalar.**  $A$  bir sayı halkası olsun.

A1.  $0$  sadece  $0$ 'ı böler.

A2. Her sayı  $0$ 'ı böler.

A3.  $1$  ve  $-1$  her sayıyı bölerler.

A4. Her sayı kendini böler.

A5.  $x|y$  ve  $y|z$  ise  $x|z$ .

A6.  $x|y$  ise, her  $z \in A$  için  $x|yz$ .

A7.  $x|y$  ise ve  $x \neq 0$  ise o zaman  $xa = y$  eşitliğini sağlayan tek bir  $a \in A$  vardır ve bu  $a$  elbette  $y/x$ 'tir.

A8.  $x|y$  ve  $x|z$  ise her  $a, b \in A$  için,  $x|(ay + bz)$ .

**Tersinir Elemanlar.**  $x \in A$  olsun. Eğer  $1/x \in A$  ise, o zaman  $x$ 'e **tersinir eleman** denir. Bu durumda  $1/x$ 'e  $x$ 'in **tersi** adı verilir.

Daha dikkatli olmak isteseydik, "tersinir"den öte " $A$ 'da tersinir" derdik. Çünkü tersinir olmak  $A$  halkasına göre değişir:  $A$ 'da tersinir olmayan bir eleman, daha geniş bir halkada tersinir olabilir.

$1 \times 1 = 1$  olduğundan,  $1$  elemanı her halkada tersinirdir.  $-1$  de her halkada tersinirdir. Ama  $0$  hiçbir halkada tersinmez. Bir halkanın iki tersinir elemanının çarpımı da tersinirdir. Dolayısıyla tersinir bir  $x$  elemanının  $x^n$  güçleri de tersinirdir.

Nasıl  $1$  her sayıyı bölüyorsa, tersinir elemanlar da  $A$ 'daki her sayıyı bölerler. Nitekim eğer  $x$  tersinirse ve  $y \in A$  ise,  $y$ 'yi  $x$ 'e bölünce  $A$ 'nın  $(1/x)y$ , yani  $y/x$  elemanını buluruz. Burada önemli olan bölme işleminin sonucunun gene  $A$ 'da olmasıdır, çünkü "bölme" kavramı halkaya göre değişir; örneğin  $2, 3$ 'ü  $Z$ 'de bölmez ama  $Q$ 'da böler.

$A$  halkasının tersinir öğelerinin kümesi  $A^*$  ola-

rak simgelenir. Örneğin

$$Z^* = \{1, -1\},$$

$$Q^* = Q \setminus \{0\}$$

Bunlar kolay. Ama  $Z[\sqrt{d}]^*$  türünden kümeleri belirlemek çok daha zordur. Okur, görece kolay bir alıştırmaya olarak, daha şimdiden, daha sonra kanıtlayacağımız, eğer  $d \in Z \setminus \{0, 1\}$ ,  $1$  dışında bir tamkareye bölünmüyorsa,

$Z[\sqrt{d}]^* = \{a + b\sqrt{d} : a, b \in Z, a^2 - db^2 = \pm 1\}$  eşitliğini kanıtlayabilir. Örneğin  $1 + \sqrt{2}$  ve bu elemanın tüm güçleri  $Z[\sqrt{2}]^*$  kümesindedir.

Ama yukardaki eşitliği bulmak  $Z[\sqrt{2}]^*$  kümesini belirlemek için yeterli değildir.  $Z[\sqrt{2}]^*$  kümesini belirlemek için  $a^2 - 2b^2 = \pm 1$  denklemlerinin  $Z$ 'deki tüm çözümlerini bulmak lazım. Okur, belli bir  $d$  için,  $a^2 - db^2 = \pm 1$  denklemlerinin tüm çözümlerini bulmayı deneyebilir, ama bu pek kolay değildir, hatta hiç kolay değildir.

**Alıştırmalar.**

B1.  $u \in A^*$  ancak ve ancak  $u|1$  ise.

B2.  $Q[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in Q\}$  olsun.  $Q[\sqrt{d}]^* = Q[\sqrt{d}] \setminus \{0\}$  eşitliğini kanıtlayın.

B3. Tersinir elemanlar ancak tersinir elemanlara bölünebilirler.

B4. Her  $x, y \in A$  ve  $x \neq 0$  için, eğer  $x|y$  ise  $y \in A^*$ .

B5. Her  $x, y \in A$  için,  $xy \in A^*$  ise  $x, y \in A^*$ .

B6. Her  $x, y \in A$  için,  $x|y$  ve  $y|x$  ancak ve ancak  $x = uy$  eşitliğini sağlayan bir  $u \in A^*$  varsa.

B7.  $B6$ 'daki koşullardan herhangi biri sağlanıyorsa  $x \sim y$  yazalım. O zaman, her  $x, y, z \in A$  için,

- i.  $x \sim x$ .
- ii.  $x \sim y$  ise  $y \sim x$ .
- iii.  $x \sim y$  ve  $y \sim z$  ise  $x \sim z$ .

B8.  $x, y \in A$  olsun. Eğer  $ux + vy = 1$  eşitliğini sağlayan  $u, v \in A$  varsa, o zaman  $x$  ve  $y$ 'nin ortak bölünenleri sadece  $A$ 'nın tersinir elemanlarıdır.

B9.  $A = Z[\sqrt{d}]$  olsun.  $A^* \cap Z = \{1, -1\}$  eşitliğini kanıtlayın.

Şimdi  $A$  halkasının asallarını ve indirgenemelerini tanımlayacağız. Tanımımızı  $Z$ 'ye uyguladığımızda  $Z$ 'nin asal ve indirgenemez kavramlarını bulacağız.

**İndirgenemezler.**  $0 \neq x \in A \setminus A^*$  olsun. Eğer  $y, z \in A$  için,  $x = yz$  eşitliği doğru olduğunda  $y$  ya da  $z$  elemanlarından biri  $A$ 'da tersinirse o zaman  $x$ 'e ( $A$ 'da) **indirgenemez** denir.

Örneğin, 2, 3, 5, 7, 11, 13, 17 sayıları  $Z$ 'nin indirgenemez sayılarıdır. Ama bu sayıların yanısıra  $-2, -3, -5, -7, -11, -13, -17$  sayıları da  $Z$ 'nin indirgenemezleridir.

Öte yandan 2,  $Z$ 'nin indirgenemezi olmasına karşın  $Z[\sqrt{2}]$ 'nin indirgenemezi değildir; 2,  $Z[\sqrt{2}]$  halkasında  $\sqrt{2} \times \sqrt{2}$  olarak indirgenebilir. Ayrıca,

$$7 = (3 + \sqrt{2})(3 - \sqrt{2})$$

eşitliğinden dolayı 7 de  $Z[\sqrt{2}]$  halkasında indirgenen bir sayıdır. Görüldüğü gibi  $Z$ 'de indirgenemez olan bir sayı,  $Z[\sqrt{2}]$  halkasında indirgenabiliyor. Demek ki  $A \subseteq B$  sayı halkalarıysa,  $A$ 'nın bir indirgenemezi  $B$ 'de indirgenir bir sayıya dönüşebiliyor.

#### Alıştırmalar.

**C1.** Eğer  $x \in A$  indirgenemezse ve  $u \in A^*$  ise  $xu$  da indirgenemezdir. Yani  $x \in A$  indirgenemezse ve  $x \sim y$  ise  $y$  de indirgenemezdir.

**C2.**  $x^2$  hiçbir zaman indirgenemez olamaz.

**C3.**  $x \in A$  olsun. " $x$  indirgenemez ancak ve ancak  $y|x$  koşulunu sağlayan her  $y \in A$  için, ya  $y \in A^*$  ya da  $x \sim y$ " önermesini kanıtlayın.

**Asallar.**  $0 \neq x \in A \setminus A^*$  olsun. Eğer her  $y, z \in A$  için,  $x, yz$  çarpımını böldüğünde ya  $y$ 'yi ya da  $z$ 'yi bölüyorsa, o zaman  $x$ 'e **asal** denir.

Örneğin 2, 3, 5, 7, 11, 13, 17, 19, 23 sayıları  $Z$  halkasının asal sayılarıdır. Bunların negatifleri de asaldır.  $Z$ 'de asallarla indirgenemezlerin aynı şey olduğunu yukarıda gördük.

#### Alıştırmalar.

**D1.** Eğer  $x \in A$  asalsa ve  $u \in A^*$  ise  $xu$  da asaldır. Yani  $x \in A$  asalsa ve  $x \sim y$  ise  $y$  de asaldır.

**D2.**  $x^2$  hiçbir zaman asal olamaz.

**D3.**  $\mathbb{Q}$  ve  $\mathbb{R}$  halkalarında hiç indirgenemez ve asal sayı yoktur.

Her asal bir indirgenemezdir. Bunun kanıtı da hemen hemen aynen Teorem 1'in kanıtı gibidir.

**Teorem 8.** Bir sayı halkasının her asalı bir indirgenemezdir.

**Kanıt:**  $p$  bir asal olsun. İki  $x$  ve  $y$  sayısı için,  $p = xy$  eşitliği sağlandığını varsayalım. Ya  $x$ 'in ya da  $y$ 'nin tersinir olduğunu kanıtlayacağız, böylece  $p$ 'nin indirgenemezliği kanıtlanmış olacak.  $p$  sayısı  $p$ 'yi böldüğünden,  $p, xy$ 'yi de böler. Ama  $p$  asal ol-

duğundan, bundan  $p$ 'nin ya  $x$ 'i ya da  $y$ 'yi böldüğü çıkar. Diyelim  $p, x$ 'i bölüyor. Demek ki belli bir  $x_1$  için  $x = px_1$ . Şimdi küçük bir hesap yapalım:  $p = xy = px_1y$ . Bu eşitlikte  $p$ 'leri sadeleştirirsek,  $1 = x_1y$  elde ederiz, ki bu da  $y \in A^*$  demektir. Eğer  $p, y$ 'yi bölseydi, o zaman,  $x \in A^*$  elde edecektik.  $\square$

Her asal her halkada indirgenemezdir ama her indirgenemez her halkada bir asal değildir. Birazdan örnekler vereceğiz. Ama önce asallar ve indirgenemezlerle ilgili bir teorem sunalım.

Yukarıda nasıl Teorem 1'i genelleştirdiysek, Teorem 5'i de genelleştirebiliriz. Önce bir tanım:

$x, y \in A$  olsun. Eğer belli bir  $u \in A^*$  için  $x = uy$  ise, o zaman  $x$  ve  $y$ 'ye **denk elemanlar** diyelim. Alıştırma B7'de bunu  $x \sim y$  olarak yazmıştık. Okur bu aşamada, eğer yapmadıysa o alıştırma yapabilir. Örneğin  $Z$ 'de  $n$  ile  $-n$  birbirine denktir.

**Teorem 9.** Bir sayı halkasında eğer bir eleman sonlu sayıda asalin çarpımı olarak yazılıyorsa, o zaman bu yazılım aşağı yukarı tek bir biçimde yapılır. Daha matematiksel bir deyişle, eğer  $p_1, \dots, p_n, q_1, \dots, q_m$  asalları için ve  $u$  tersinir elemanı için,

$$p_1 \dots p_n = uq_1 \dots q_m$$

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

**Kanıt:** Kanıtımızı  $n$  üzerinden tümevarımla yapalım.

Önce  $n = 1$  şikkını ele alalım.  $p_1, q_1, \dots, q_m$  asalları ve  $u \in A^*$  için  $p_1 = uq_1 \dots q_m$  eşitliği sağlansın. Demek ki  $p_1 = (q_1)(uq_2 \dots q_m)$ . Dolayısıyla,  $p_1$  asal olduğundan,  $p_1$  ya  $q_1$ 'i ya da  $uq_2 \dots q_m$  sayısını böler. İkinci şıkta durmayıp devam edersek, en fazla  $m$  adımda,  $p_1$  asalının  $q_j$ 'lerden birini böldüğünü görürüz (çünkü  $p_1$  asalı tersinir bir eleman olan  $u$ 'yu bölemez, Alıştırma B3.) Demek ki belli bir  $v$  için  $q_j = p_1v$ . Ama  $q_j$  de bir asal, dolayısıyla indirgenemez (Teorem 8). Demek ki  $v \in A^*$  ve  $q_j \sim p_1$ . Şimdi,  $p_1 = uq_1 \dots q_m$  eşitliğinde  $q_j$  yerine  $vp_1$  koyalım:

$$p_1 = uvq_1 \dots q_{j-1}p_1q_{j+1} \dots q_m$$

eşitliğini elde ederiz. İki taraftan  $p_1$ 'leri sadeleştirirsek,  $1 = uvq_1 \dots q_{j-1}q_{j+1} \dots q_m$  eşitliğini elde ederiz. Demek ki sağ taraftaki tüm asal sayılar tersinirler, yani aslında yoklar...

Eğer  $n > 1$  ise, kanıt aynı. Ama biz gene de yapalım kanıtı. Kanıtımızın  $n - 1$  için doğru olduğu-

nu varsayalım.  $p_1, \dots, p_n, q_1, \dots, q_m$  asalları ve  $u \in A^*$  için,

$$p_1 \dots p_n = uq_1 \dots q_m$$

eşitliği sağlansın.  $p_1$ , sol tarafı böldüğünden, sağ tarafı da, yani  $(q_1)(uq_2 \dots q_m)$  sayısını da böler. Dolayısıyla,  $p_1$  asal olduğundan,  $p_1$  ya  $q_1$ 'i ya da  $uq_2 \dots q_m$  sayısını böler. İkinci şıkta durmayıp devam edersek,  $p_1$  asal sayısının  $q_j$ 'lerden birini böldüğünü görürüz (çünkü  $p_1$  asalı tersinir bir eleman olan  $u$ 'yu bölemez, Alıştırma B3.) Demek ki belli bir  $j$  ve bir  $v$  için  $q_j = vp_1$ . Ama  $q_j$  de bir asal, dolayısıyla indirgenemez (Teorem 8). Demek ki  $v \in A^*$  ve  $q_j \sim p_1$ . Şimdi,  $p_1 = uq_1 \dots q_m$  eşitliğinde  $q_j$  yerine  $vp_1$  koyalım:

$$p_1 \dots p_n = uvq_1 \dots q_{j-1}p_1q_{j+1} \dots q_m$$

eşitliğini elde ederiz. İki taraftan  $p_1$ 'leri sadeleştirsek,  $p_2 \dots p_n = uvq_1 \dots q_{j-1}q_{j+1} \dots q_m$  eşitliğini elde ederiz ve  $uv \in A^*$  olduğundan tümevarım varsayımını kullanarak teoremi kanıtlarız.  $\square$

Acaba Teorem 1 ve 5'i genelleştirdiğimiz gibi Teorem 6'yı da genelleştirebilir miyiz, yani bir halkada bir sayıyı indirgenemezlerin çarpımı olarak yazabilir miyiz? Bu soru biraz daha zor.

Teorem 1 ve 5'i genelleştirmede bir sorun yaşamamıştık, hemen hemen aynı kanıtı tekrarlamıştık, ama Teorem 6'nın kanıtı biraz değişik: Teorem 6'nın kanıtında, indirgenemezlerin çarpımı olarak yazacağımız sayı üzerine tümevarım yapmıştık, oysa herhangi bir sayı halkasında tümevarım yapmak kolay değildir, hatta imkânsız bile olabilir.

Aşağıda en azından  $Z[\sqrt{d}]$  halkalarında tümevarım yapmamızı ve böylece Teorem 6'yı bu halkalara genelleştirmemizi sağlayacak bir yöntem geliştireceğiz.

$Z[\sqrt{d}]$  halkasının bir ögesi  $x, y \in Z$  için  $x + y\sqrt{d}$  olarak yazıldığını unutmayalım. Bir de anlaşma yapalım:  $Z[\sqrt{d}]$  halkasının bir ögesini  $x + y\sqrt{d}$  olarak yazdığımız zaman  $x$  ve  $y$ 'nin  $Z$ 'de olduklarını söylemeden varsayacağız.

**Eşlenik Eleman.**  $d \in Z \setminus \{0, 1\}$  sayısı,  $Z$ 'de 1'den başka bir tamkareye bölünmeyen bir sayı olsun. (Karmaşık sayıları bilmeyenler  $d \in \mathbb{N}$  alabilirler.) Bu paragrafta  $Z[\sqrt{d}]$  sayı halkasıyla ilgileneceğiz.  $A$ 'nın bir  $x + y\sqrt{d}$  ögesi için,

$$\overline{x + y\sqrt{d}} = x - y\sqrt{d}$$

olsun.  $x + y\sqrt{d} = z + t\sqrt{d}$  eşitliği  $x = z$  ve  $y = t$  eşitliğini verdiğinden (neden?), yukardaki tanımı yapmaya hakkımız vardır. (Örneğin  $d = 4$  olsaydı, bu tanımdan bir çelişki elde ederdik. Niye?)  $x + y\sqrt{d}$  ve  $x - y\sqrt{d}$  sayılarına **eşlenik sayılar** denir.

**Önsav 10.** Her  $\alpha, \beta \in Z[\sqrt{d}]$  için,

$$\begin{aligned} \overline{\overline{\alpha}} &= \alpha, \\ \overline{\alpha + \beta} &= \overline{\alpha} + \overline{\beta}, \\ \overline{\alpha\beta} &= \overline{\alpha}\overline{\beta}. \end{aligned}$$

**Kanıt:** Sadece hesaptan ibaret olan kanıtı okura bırakıyoruz.  $\square$

**Alıştırmalar.**

**E1.**  $Z[\sqrt{d}]$ 'de bir tamsayının eşleniği kendisidir ve sadece tamsayılar bu özelliği sağlarlar.

**E2.**  $A$  ve  $B$  birer sayı halkası olsun ve  $f : A \rightarrow B$  fonksiyonu her  $\alpha, \beta \in A$  için,

$$f(\alpha + \beta) = f(\alpha) + f(\beta)$$

$$f(\alpha\beta) = f(\alpha)f(\beta)$$

eşitliklerini sağlasın. Ayrıca  $f \neq 0$  olsun. Aşağıdakileri kanıtlayın.

- i.  $f(0) = 0$ ,
- ii.  $f(1) = 1$ ,
- iii. Her  $n \in \mathbb{N}$  için  $f(n) = n$ ,
- iv. Her  $\alpha \in A$  için,  $f(-\alpha) = -f(\alpha)$ ,
- v. Her  $n \in Z$  için  $f(n) = n$ ,
- vi. Eğer  $\alpha \in A^*$  ise  $f(\alpha) \in B^*$  ve  $f(\alpha^{-1}) = f(\alpha)^{-1}$ .
- vii. Her  $q \in \mathbb{Q} \cap A$  için,  $f(q) = q$ .
- viii. Eğer  $\alpha \in A$  tamkatsayılı bir polinomun köküyse,  $f(\alpha)$  da aynı polinomun köküdür.

**E3.**  $A = Z[\sqrt{d}]$  olsun ve  $f : A \rightarrow A$  yukardaki alıştırmadaki gibi olsun. Ya her  $\alpha \in A$  için  $f(\alpha) = \alpha$  ya da her  $\alpha \in A$  için

$$f(\alpha) = \overline{\alpha}$$

eşitliğini gösterin.

**Norm.**  $d$  ve  $A = Z[\sqrt{d}]$  bir önceki paragrafta olduğu gibi olsun. Şimdi  $N : A \rightarrow A$  fonksiyonunu, her  $\alpha \in A$  için,

$$N(\alpha) = \alpha\overline{\alpha}$$

olarak tanımlayalım.  $N(\alpha)$ 'ya  $\alpha$ 'nın **normu** denir.  $N(1) = N(-1) = 1$  ve  $N(0) = 0$  eşitliklerine dikkatini zi çekirim. Genel olarak, her  $a \in Z$  için,  $N(a) = a^2$ .

**Önsav 11. i.** Eğer  $\alpha = x + y\sqrt{d} \in Z[\sqrt{d}]$  ise  
 $N(\alpha) = x^2 - y^2d \in Z$ .

ii. Eğer  $\alpha, \beta \in Z[\sqrt{d}]$  ise,  $N(\alpha\beta) = N(\alpha)N(\beta)$ .

iii.  $N(\alpha) = 0$  ancak ve ancak  $\alpha = 0$  ise.

**Kanıt:** (i) çok kolay. (ii), Önsav 10'ün üçüncü eşitliğinden ve  $N$ 'nin tanımından hemen çıkar. (iii),  $d$ 'nin bir tamkare olmamasından çıkar.  $\square$

**Önsav 12.**  $\alpha \in Z[\sqrt{d}]$  olsun.  $\alpha \in Z[\sqrt{d}]^*$  ancak ve ancak  $N(\alpha) = \pm 1$  ise. Bu durumda

$$\alpha^{-1} = N(\alpha)\bar{\alpha}.$$

**Kanıt:**  $\alpha \in Z[\sqrt{d}]^*$  olsun. Demek ki  $\alpha\beta = 1$  eşitliğini sağlayan bir  $\beta \in Z[\sqrt{d}]$  var. Eşitliğin her iki tarafının da normlarını alalım. Önsav 11.ii'ye göre,  $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$ . Öte yandan, Önsav 11.i'ye göre,  $N(\alpha)$  ve  $N(\beta)$  birer tamsayı. Çarpımları 1 olduğundan,  $N(\alpha) = \pm 1$ .

$$\alpha(N(\alpha)\bar{\alpha}) = N(\alpha)\bar{\alpha}\alpha = N(\alpha)^2 = (\pm 1)^2 = 1.$$

Şimdi  $N(\alpha) = \pm 1$  eşitliğini varsayalım ve hesaplayalım:

Demek ki  $\alpha$ 'nın tersi  $A$ 'daymış ve önsavda söylenildiği gibiymiş.  $\square$

**Örnek:**  $3 - 2\sqrt{2} \in Z[\sqrt{2}]^*$ ,  $2 + \sqrt{5} \in Z[\sqrt{5}]^*$ .

**Sonuç 13.** Eğer  $d < -1$  ise  $Z[\sqrt{d}]^* = \{1, -1\}$ .

**Kanıt:** Yukarıdaki gibi.  $\square$

**Sonuç 14.**  $Z[\sqrt{-1}]^* = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$ .

**Kanıt:**  $d = -1$  ve  $\alpha = x + y\sqrt{d} \in Z[\sqrt{d}]^*$  olsun. Aynen yukardaki gibi düşünerek,  $x^2 + y^2 = \pm 1$  denklemini çözmemiz gerektiği anlaşılır. Bundan da istediğimiz sonuç çıkar.  $\square$

$Z[\sqrt{-1}]$  sayı halkasının öğelerine **Gauss tamsayıları** denir. Her ne kadar  $\sqrt{-1}$  ile  $-\sqrt{-1}$  arasında bir fark gözetmek imkânsızsa da, bunlardan biri yerine  $i$  yazmak bir gelenek haline gelmiştir.

**Sonuç 15.**  $\alpha \in Z[\sqrt{d}]$  olsun. Eğer  $N(\alpha)$ ,  $Z$ 'nin bir asalıysa, o zaman  $\alpha$ ,  $Z[\sqrt{d}]$  halkasında bir indirgenemezdir.

**Kanıt:**  $\alpha$ 'nın indirgenir olduğunu varsayalım. Demek ki  $Z[\sqrt{d}]$ 'nin tersinir olmayan  $\beta$  ve  $\gamma$  elemanları için,  $\alpha = \beta\gamma$ . Eşitliğin her iki tarafının da normunu alalım.  $N(\alpha) = N(\beta)N(\gamma)$ .  $\beta$  ve  $\gamma$  elemanları tersinir olmadıklarından,  $N(\beta)$  ve  $N(\gamma)$  sayıları  $\pm 1$ 'den değişik. Demek ki  $N(\alpha)$  asal bir tamsayı olamaz.  $\square$

**İndirgenemelere Ayrılış.** Şimdi  $Z[\sqrt{d}]$  halkasının her öğesinin indirgenemezlerin bir çarpımı olarak yazılabileceğini kanıtlayabiliriz. Böylece Teorem 6'nın  $Z[\sqrt{d}]$  halkası için de doğru olduğunu kanıtlamış olacağız.

Okur bu aşamada Teorem 6'nın kanıtına bakarsa, o kanıtta indirgenemezlerin çarpımı olarak yazılacak eleman üzerine tümevarım yaptığımızı farkedecektir. Bu yöntemi  $Z[\sqrt{d}]$  sayı halkası için kullanacağız, ancak tümevarımı, indirgenemezlerin çarpımı olarak yazılacak eleman üzerine yapamayız, çünkü  $Z$  ya da  $N$ 'de değil,  $Z[\sqrt{d}]$  sayı halkasındayız. Tümevarımı  $Z[\sqrt{d}]$ 'nin elemanlarının normunun mutlak değeri üzerine yapacağız.

Eğer  $\alpha \in Z[\sqrt{d}]$  ise  $M(\alpha) = |N(\alpha)| \in \mathbb{N}$  olarak tanımlayalım. Her  $\alpha, \beta \in Z[\sqrt{d}]$  için, Önsav 11.ii'den dolayı  $M(\alpha\beta) = M(\alpha)M(\beta)$  eşitliği de geçerlidir elbet.

**Teorem 16.** Her  $0 \neq \alpha \in Z[\sqrt{d}] \setminus Z[\sqrt{d}]^*$ ,  $Z[\sqrt{d}]$  halkasının indirgenemizin çarpımı olarak yazılır.

**Kanıt:**  $0 \neq \alpha \in Z[\sqrt{d}] \setminus Z[\sqrt{d}]^*$  olsun. Teoremi aynen Teorem 6'yı kanıtladığımız gibi kanıtlayacağız, ancak bu sefer  $M(\alpha)$  üzerine tümevarım yapacağız. Eğer  $\alpha$  indirgenemezse, o zaman  $\alpha$  tek bir indirgenemizin ( $\alpha$ 'nın) çarpımıdır. Eğer  $\alpha$  indirgenebilirse o zaman  $\alpha = \beta\gamma$  eşitliğini sağlayan  $0 \neq \beta, \gamma \in Z[\sqrt{d}] \setminus Z[\sqrt{d}]^*$  vardır. Her iki tarafın da  $M$ 'sini alalım:  $M(\alpha) = M(\beta)M(\gamma)$ .  $\beta$  ve  $\gamma$  tersinir olmadıklarından,  $M(\beta)$  ve  $M(\gamma)$  doğal sayıları 1'den büyükler. Demek ki her ikisi de  $M(\alpha)$ 'dan küçükler. Tümevarımla  $\beta$  ve  $\gamma$  elemanları  $Z[\sqrt{d}]$  halkasının sonlu sayıda indirgenemizin çarpımıdır. Dolayısıyla  $\beta\gamma$ , yani  $\alpha$  da sonlu sayıda indirgenemizin çarpımıdır.  $\square$

Ne yazık ki  $Z[\sqrt{d}]$  sayı halkasının her indirgenemezi bir asal değildir ve Sonuç 7 bu sayı halkalarında doğru değildir.

**Örnek.**  $Z[\sqrt{5}]$  sayı halkasına bakalım. Bu halkada  $4 = 2 \times 2 = (\sqrt{5} + 1)(\sqrt{5} - 1)$  eşitliği geçerlidir. Ayrıca ne  $\sqrt{5} + 1$  ne de  $\sqrt{5} - 1$  sayıları  $Z[\sqrt{5}]$  sayı halkasında 2'nin bir çarpımıdır (kanıtı çok kolay, yazınca çıkıyor), dolayısıyla ne  $\sqrt{5} + 1$  ne de  $\sqrt{5} - 1$  sayısı 2'ye denk. Dolayısıyla Teorem 9'a göre 2,  $\sqrt{5} - 1$  ve  $\sqrt{5} + 1$  sayılarının hepsi birden asal olamazlar. Öte yandan bu sayılar bu halkada indirgenemezdirler. Birazdan kanıtlayacağız bunu. Ama bu sonucu kabul edersek, en azından bu halkada her

indirgenemez bir asal olmadığı anlaşılır. Demek ki her sayı halkasında her sayı asalların çarpımı olarak yazılamıyor ve indirgenemezlerin çarpımı olarak yazılsa da, indirgenemezlerin çarpımı olarak tek bir biçimde yazılamıyor.

Şimdi  $2$ ,  $\sqrt{5} - 1$  ve  $\sqrt{5} + 1$  sayılarının indirgenemez olduklarını kanıtlayalım. Bu sayıların herbirinin normu  $4$ . Demek ki, indirgenemez olmasalardı, normu  $2$  ya da  $-2$  olan iki sayının çarpımı olarak yazılacaktı. Oysa  $Z[\sqrt{5}]$  sayı halkasında normu  $\pm 2$  olan bir eleman yoktur! Bunun kanıtı çok kolay.  $x + y\sqrt{5}$  normu  $\pm 2$  olan bir sayı olsun. O zaman,  $x^2 - 5y^2 = \pm 2$ . Modülo  $5$  düşünürsek,  $x^2 \equiv \pm 2 \pmod{5}$  olur. Ama bu denklemlerin modülo  $5$  sayılarda çözümü yoktur.

Görüldüğü üzere asallarla indirgenemezler arasında çok çok ince ama bir o kadar da önemli bir ayrım vardır. Tarihte bu iki kavramın karıştırıldığı zamanlar olmuştur ve bu kavram kargaşası önemli matematiksel hatalara neden olmuştur.

Çok ilginç bir konu olan  $Z[\sqrt{d}]$  sayı halkaları-na gerek matematiksel olarak gerek tarihsel gelişimi açısından ilerde daha çok değinmek isteriz.

#### Alıştırmalar.

**F1.**  $Z[1/2] = \{a/2^n : n \in \mathbb{N} \text{ ve } a \in \mathbb{Z}\}$  olsun. Bu sayı halkasının tersinir elemanlarını, asallarını ve indirgenemezlerini bulun.

**F2.**  $Z[\sqrt{-1}]$  sayı halkasının indirgenemezlerinin asal olduğunu gösterin. ♣

## Öklid Bölgeleri

$A$  bir sayı halkası (ya da bir tamlık bölgesi, bkz. sayfa 28) olsun.  $M : A \setminus \{0\} \rightarrow \mathbb{N}$  şu özellikleri sağlayan bir fonksiyon olsun: Her  $a \in A$  ve  $0 \neq b \in A$  için,

- i)  $M(a) \leq M(ab)$
- ii) öyle  $r, q \in A$  vardır ki,  $a = bq + r$  ve  $ya r = 0$ 'dır ya da  $M(r) < M(b)$ .

Birinci koşul,  $M$ 'yi bir tür derece ya da mutlak değer olarak algılamamızı sağlar. İkinci koşulu " $a, b$ 'ye bölündüğünde sonuç  $q$  çıkar, kalan da  $r$ 'dir" diye yorumlayabiliriz.

Böyle bir  $M$  fonksiyonunun olduğu halkalara **Öklid bölgesi** adı verilir. Tamsayılar kümesi ve (gerçek katsayılı) polinomlar halkası (Teorem 1, sayfa 34) Öklid bölgeleridir.

Bir  $A$  Öklid bölgesinde,

- $a \in A^*$  ise her  $b \neq 0$  için  $M(a) \leq M(b)$ .
- $a, b \in A^*$  ise  $M(a) = M(b) = M(1)$ .
- Gerekirse  $M$  yerine  $M - M(1)$  alarak her  $a \in A^*$  için  $M(a) = 0$  eşitliğini varsayabiliriz.
- $0 \neq b \in A^*$  ve  $a \neq 0$  ise  $M(a) < M(ab)$ .

(Neden?) Bu son özellik sayesinde bir Öklid bölgesinde her elemanın sonlu sayıda indirgenemez çarpımı olduğu kanıtlanabilir (Nasıl?) İkinci koşul, her indirgenemez bir asal olduğunu kanıtlamakta kullanılır (Nasıl? Bunu kanıtlamak biraz daha zor olabilir.) Demek ki bir Öklid bölgesinin sıfır ve tersinir olmayan her elemanı asallarına tek bir biçimde ayrılır (yani bir tek çarpanların bölgesidir, bkz. sayfa 38).

Bundan böyle  $d \in \mathbb{Z} \setminus \{0, 1\}$ ,  $1$ 'den başka bir tamkareye bölünmeyen bir sayı olsun.

$$\mathbb{Q}[\sqrt{d}] = \{r + s\sqrt{d} : r, s \in \mathbb{Q}\}$$

ve

$A_d = \{\alpha \in \mathbb{Q}[\sqrt{d}] : a, b \in \mathbb{Z} \text{ için } \alpha^2 + a\alpha + b = 0\}$  olsun. O zaman  $Z[\sqrt{d}] \subseteq A_d$  (Neden?) Hatta,

$$A_d = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{eğer } d \equiv 2 \text{ ya da } 3 \pmod{4} \text{ ise} \\ \mathbb{Z}\left[\frac{-1 + \sqrt{d}}{2}\right] & \text{eğer } d \equiv 1 \pmod{4} \text{ ise} \end{cases}$$

(Neden?) Hangi  $d$ 'ler için  $A_d$ 'nin bir Öklid bölgesi olduğu bilinmiyor.  $Z[\sqrt{14}]$ 'ün Öklid bölgesi olduğu sanılıyor ama bildiğimiz kadarıyla henüz kanıtlanamadı.

$M(a) = |N(a)|$  olarak tanımlanan fonksiyonun  $A_d$ 'yi Öklid bölgesi yaptığı  $d$ 'lerin hepsi biliniyor:  $d = -1, -2, -3, -7, -11, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$ . Bunlar dışında, David A. Clark 1994'te  $A_{69}$ 'un da (çarpımsal bir  $M$  için) Öklid bölgesi olduğunu kanıtladı.

Hangi  $d$ 'ler için  $A_d$ 'nin tek çarpanlama bölgesi olduğu da bilinmiyor. Bir sanıya göre sonsuz sayıda  $d > 0$  için  $A_d$  tek çarpanlama bölgesidir.

Bu arada,  $A_{-3}$ ,  $A_{-7}$  ve  $A_{-11}$  birer Öklid bölgesi olmasına karşın,  $Z[\sqrt{-3}]$ ,  $Z[\sqrt{-7}]$  ve  $Z[\sqrt{-11}]$  Öklid bölgesi değildir, örneğin  $Z[\sqrt{-3}]$ 'te  $4 = 2 \times 2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$ . ♣