Tek Türlü Çarpanlara Ayırma Özelliği: Tam Sayılar ve Ötesi

BÜLENT SARAÇ

Hacettepe Üniversitesi Matematik Bölümü
bsarac@hacettepe.edu.tr

Matematikte bazı sorular vardır ki, sadece yanıtı değil –hatta yanıtı bulunamamış olsa bile– yanıta giden yolun kendisi de tümüyle yepyeni teorilerin doğmasına neden olabilmektedir. **Fermat'nın Son Teoremi** işte bu türden bir sorudur. 17. yüzyılda ünlü Fransız matematikçi Pierre de Fermat tarafından ortaya atılan bu teorem, $n > 2$ için

$$x^n + y^n = z^n$$

denklemini sağlayan bir (x, y, z) pozitif tam sayı üçlüsünün bulunamayacağını iddia eder. Fermat, bu teoremin "harika bir ispatını" bulduğunu ama kitabın kenar boşluğuna sığdıramadığını yazmıştır. Böylesi bir iddia, takip eden yüzyıllar boyunca sadece matematikçileri büyülemekle kalmamış, aynı zamanda çözümü 1994 yılında Andrew Wiles tarafından sağlanana kadar, matematik dünyasında büyük bir merak ve tartışma konusu olmuştur.

Fermat'nın Son Teoremi'nin çözümüne yönelik çabalar, özellikle 19. yüzyılda, matematikte devrim niteliğinde bazı gelişmelere yol açmıştır. Bu dönemde **Gauss**, sayıların cebirsel yapısını anlamak için *karmaşık tam sayılar* ve *modüler aritmetik* gibi kavramları geliştirmiştir. **Dirichlet**, *aritmetik fonksiyonlar* ve *Dirichlet karakterleri* ile asal sayıların dağılımını anlamaya çalışmış, aynı zamanda cebirsel sayı cisimlerinin temelini atmıştır. **Kummer**, Fermat'nın teoremini çözmek için *çevrimsel bölme* (cyclotomy) kuramı üzerinde çalışmış ve bu kurama önemli katkılar sağlamış, ayrıca bazı halkalarda tek türlü çarpanlara ayırma özelliğinin kaybolduğunu fark eden ilk matematikçi olmuştur. Bununla da kalmayarak bu eksikliği telafi etmek için *ideal sayılar* kavramını ortaya koymuştur. 19. yüzyılın sonlarında **Dedekind**, Kummer'in fikirlerini geliştirerek *idealler* kavramını bugünkü anlamıyla tanımlamış ve cebirsel sayı kuramının temellerini atmıştır. Bu matematikçilerin çalışmaları, sadece Fermat'nın teoremini anlamaya yönelik değil; aynı zamanda **tek türlü çarpanlara ayırma** özelliğinin hangi yapılarda geçerli olduğunu sorgulamakla ilgilidir. Bu sorgulama ise, bugünkü anlamıyla modern cebirsel sayı kuramının doğmasına neden olmuştur. Matematiğin altın çağlarından biri olarak kabul edilen bu dönemi bu kadar kısa bir özetle anlatmak elbette ki yeterli değildir. Ancak, bu yazının amaçladığı kapsamın ötesine geçmemek için, bu dönemin önemli matematikçilerini ve onların katkılarını, belli bir motivasyon çerçevesinde kısaca anmakla yetineceğiz. Dileyen okurlarımız daha ayrıntılı bilgi edinmek için [1, 2, 4] kaynaklarını inceleyebilirler. Ayrıca, halkalarda çarpanlara ayırma konusu üzerinde yazılan son derece güzel bir kitap için [5] kaynağından bahsetmemek de haksızlık olur.

Tam sayıların en dikkat çekici özelliklerinden biri de her tam sayının çarpımsal olarak en küçük bileşenlerine (bir nevi atomlarına) ayrıştılabilmesidir. Örneğin, $6 = 2 \times 3$ ve $64\,248\,932\,117 = 1291^2 \times 38557$ gibi. Daha genel konuşmak gerekirse, sıfırdan farklı, 1 ve -1 dışındaki (ileride tanımlanacak olduğu gibi birimsel olmayan) her tam sayı asal sayıların ve birimsel çarpanların (1 veya -1) bir çarpımı olarak yazılabilir ve bu yazım çarpanların sıralanması dikkate alınmadığında tek türlüdür. Antik çağlardan beri bilinen tam sayılardaki bu özellik (bkz., [3]), **Aritmetiğin Temel Teoremi** olarak bilinir. Burada sıralamanın dikkate alınmaması doğaldır. Örneğin 6 sayısı için 2×3 ve 3×2 gibi farklı çarpanlara ayırmalar olsa da, bu yazımların her ikisi de aynı asal çarpanları içerir ve her ikisi de 6 sayısının nasıl parçalandığıyla ilgili bize aynı bilgiyi verir.

Yukarıda bahsedilen bu önemli özellik, tam sayıların cebirsel yapısının temel taşlarından biridir ve literatürde aynı zamanda "tek türlü çarpanlara ayırma" özelliği olarak da bilinir. Ancak, bu özellik sadece tam sayılar için geçerli değildir; rasyonel (gerçel veya karmaşık katsayılı) polinomlar da benzer bir özelliğe

sahiptir. Buna göre sıfırdan farklı sabit olmayan her polinom ileride *indirgenemez* diye tabir edeceğimiz polinomlar ile bir sabit polinomun çarpımı olarak yazılabilir ve bu yazım da sıralama farkıyla tek türlüdür. Örneğin

$$\frac{12}{5}x^7 - \frac{12}{5}x^5 + \frac{6}{5}x^3 - \frac{6}{5}x$$

polinomunu

$$\frac{12}{5} \cdot x \cdot (x-1) \cdot (x+1) \cdot (x^4 + \frac{1}{2})$$

şeklinde yazabiliriz. Üstelik bu yazım daha fazla sayıda çarpanın bulunduğu bir yazıma da dönüştürülemez. Eğer bu özelliği karmaşık katsayılı polinomlar için konuşuyorsak, o zaman sıfırdan farklı sabit olmayan her polinomun, doğrusal polinomların çarpımı olarak tek türlü yazılabildiğini görürüz. Bu özellik **Cebirin Temel Teoremi** olarak bilinir.

Tam sayılar ve polinomlar gibi birbirinden oldukça farklı yapılarda aynı fenomenin — yani tek türlü asal çarpanlara ayırma özelliğinin — gerçekleştiği dikkatlerden kaçmamıştır. Bu gözlem, şu soruları akla getirebilir:

- Tek türlü çarpanlara ayırma özelliği başka yapılarda da görülebilir mi?
- Bu özelliği tartışmanın anlamlı olduğu her yapıda kendiliğinden ortaya çıkması beklenebilir mi?

Bu soruların cevaplarını sırasıyla *evet* ve *hayır* olarak verebiliriz. Bu cevaplara geçmeden önce, çarpanlara ayırma fenomenini tartışabileceğimiz bir zemin oluşturalım: **değişmeli ve birimli halkalar**.

Bir **halka**, üzerinde $+$ simgesi ile gösterilen ve adına toplama denilen bir işlem ve $\cdot$ ile gösterilen ve adına çarpma denilen bir başka işlemin tanımlı olduğu ve bu işlemlerin bazı cebirsel kurallara uyduğu bir kümedir. Daha açık olarak, boştan farklı bir R kümesi için $(R, +, \cdot)$ sistemi aşağıdaki özellikleri taşıyorsa, bu sisteme bir **halka** denir:

(H1) $(R, +)$ bir abelyan gruptur; yani

- Toplama işlemi kapalıdır: her $a, b \in R$ için, $a + b \in R$,
- Toplama işlemi birleşmelidir:
  her $a, b, c \in R$ için $(a + b) + c = a + (b + c)$,
- Toplama işlemi değişmelidir: her $a, b \in R$ için, $a + b = b + a$,
- Toplama işlemi için birim eleman vardır: $0_R \in R$ vardır öyle ki, her $a \in R$ için $a + 0_R = a$,
- Her öğenin bir tersi vardır: her $a \in R$ için bir $-a \in R$ bulunur öyle ki, $a + (-a) = 0_R$.

(H2) Çarpma işlemi kapalıdır ve birleşmelidir; yani her $a, b, c \in R$ için $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(H3) Toplama işleminin çarpma işlemi üzerine dağılma özelliği vardır: her $a, b, c \in R$ için $a \cdot (b + c) = a \cdot b + a \cdot c$ ve $(b + c) \cdot a = b \cdot a + c \cdot a$.

Eğer, ek olarak, çarpma işlemi de değişmeli ise, yani her $a, b \in R$ için $a \cdot b = b \cdot a$ ise, bu halka **değişmeli halka** olarak adlandırılır. Eğer çarpma işlemi için birim eleman varsa, yani her $a \in R$ için $a \cdot 1 = a = 1 \cdot a$ olacak şekilde $1 \in R$ varsa, bu halkaya bir **birimli halka** denir. Dikkat edilirse bir işlemin birim elemanı varsa bu eleman tek olmak zorundadır. Buna göre birimli bir halkanın çarpımsal (ve toplamsal) birimini tek bir sembolle özellikle alışkın olduğumuz şekilde 1 ile (ve 0_R ile) göstermekte bir sakınca yoktur. Zaman zaman çarpımsal birimin 1 tam sayısı ile karışmasını önlemek için çarpımsal birimi 1_R biçiminde de gösterebiliriz. Son olarak sayı sistemleri ile çalışırken öteden beri alıştığımız gibi çarpma işlemini $\cdot$ ile göstermek yerine çarpılan terimler arasına boşluk bırakmayı da tercih edebiliriz.

Pek çok farklı karakterde halkaya rastlamak mümkündür. Örneğin tam sayılar halkası $\mathbb{Z}$, $n > 1$ tam sayı modülüne göre kalan sınıflarının halkası $\mathbb{Z}_n$, rasyonel sayılar halkası $\mathbb{Q}$, reel sayılar halkası $\mathbb{R}$ ve karmaşık sayılar halkası $\mathbb{C}$ birer değişmeli ve birimli halkadır. Ayrıca, değişmeli ve birimli bir R halkası üzerindeki polinomların kümesi $R[x]$ de değişmeli ve birimli bir halkadır. Burada $R[x]$ halkası, R'deki katsayılar ile tanımlı x değişkenine bağlı polinomların kümesidir. Bunların dışında, herhangi bir R halkası üzerindeki $n \times n$ matrislerin halkası $M_n(R)$ bir halka olmakla birlikte, değişmeli değildir. Herhangi boş olmayan bir X kümesi üzerinde tanımlı reel değerli fonksiyonların kümesi de bilinen fonksiyon toplamı ve çarpımına göre

bir halka oluşturur. Bu halka değişmeli ve birimli bir halkadır; fakat böyle olmasına rağmen tam sayılar halkasından epeyce farklıdır.

İki halkanın birbirine benzerliği ya da farklılığı için ölçüt olabilecek pek çok kavram ve özellik vardır. Halkalar bu özellikler üzerinden karşılaştırılabilir ve sınıflara ayrılabilir. Bu yazının konusu olan **tek türlü çarpanlara ayırma** özelliği de bu özelliklerden biridir.

Bir halkayı tanımlamak için seçilen ve yukarıda (H1)–(H3) aksiyomları ile verilen özellikler her halkada sağlanması beklenen temel özelliklerdir ve birbirlerinden bağımsızdır (yani ek koşullar olmadan birbirlerinden mantıksal gerektirmeler ile elde edilemezler) ve bunlardan elde edilebilen bazı özellikler ise sayı sistemleri ile çalışırken kullanmayı sevdiğimiz özelliklerdir. Örneğin, herhangi bir R halkasında her $a \in R$ için $0_R \cdot a = a \cdot 0_R = 0_R$ dir. Bu özellik, aksiyomlar arasında yer almasa da (H1)–(H3) aksiyomlarından kolayca elde edilebilir. Fakat, her $a, b \in R$ için $a \cdot b = 0_R$ olması $a = 0_R$ ya da $b = 0_R$ olmasını gerektirmez. Örneğin $\mathbb{Z}_4$ kalan sınıf halkasında $\bar{2} \cdot \bar{2} = \bar{0}$ dır. Bu özelliğe sahip olan değişmeli ve birimli halkalara **tamlık bölgesi** denir. Yani, R bir tamlık bölgesi ise, $a, b \in R$ ve $a \cdot b = 0_R$ ise, $a = 0_R$ veya $b = 0_R$ olmalıdır. Bu yönüyle bir tamlık bölgesinin tam sayılar halkasına benzer olduğunu söyleyebiliriz. Örneğin bir tamlık bölgesinde sadeleştirme işlemi yapılabilir; yani $a, b, c \in R$ için $a \cdot b = a \cdot c$ ve $a \neq 0_R$ ise $b = c$ olur. Bu denklem çözmede işe yarayabilecek iyi bir özelliktir; ancak, tamlık bölgesi olma özelliği, bir halkada asal çarpanlara ayırma özelliğinin varlığı için yeterli değildir. Bunu ileride daha somut olarak göreceğiz.

Yukarıdaki tartışmaların ışığında, asal sayı ve indirgenemez polinomlar, yaşadıkları evrenin temel yapı taşlarıdır; evrenin önemli bir bölümü bu temel yapı taşlarının çarpımsal birleşimlerinden oluşur. Bu durum bu halkaları mimari olarak cazip bir hesaplama ortamı haline getirir. Ancak, bu yapı taşlarının varlığı ile bu yapı taşlarına tek türlü olarak ayrıştırılabilme özelliği arasında doğrudan bir bağ yoktur. Fakat yine de öncelikle varlıklarını ele almak gerekir. Bunun için bu yapı taşlarının nasıl tanımlandığına bir bakalım:

Tanım 1. (Asal ve İndirgenemez Elemanlar)

R değişmeli ve birimli bir halka olsun.

- Eğer bir $u \in R$ elemanının R içinde çarpımsal tersi varsa, yani $u \cdot u^{-1} = 1_R$ olacak şekilde $u^{-1} \in R$ varsa –ki bu durumda u^{-1} tek türlü belirlidir– u elemanına R'nin bir birimsel (unit) elemanı denir.
- $a, b \in R$ için $a = u \cdot b$ olacak şekilde bir $u \in R$ birimsel elemanı varsa "a, b ile **ilgilidir**" denir ve $a \sim b$ şeklinde yazılır.
- $p \in R$, sıfırdan farklı birimsel olmayan bir eleman olsun. Eğer her $a, b \in R$ için $p \mid ab$ iken $p \mid a$ veya $p \mid b$ oluyorsa p'ye R'nin bir **asal (prime)** elemanı denir.
- $p \in R$, sıfırdan farklı birimsel olmayan bir eleman olsun. Eğer her $a, b \in R$ için $p = ab$ yazılabilmesi ancak a veya b'nin birimsel olması durumunda mümkün ise p'ye R'nin bir **indirgenemez (irreducible)** elemanı denir.

Bilindiği gibi tam sayılarda asal ve indirgenemez elemanlar aynıdır; ancak genel olarak bu iki kavram birbirinden ayrılır. Örneğin $\mathbb{Z}_6$ halkasında $\bar{2}$ bir asal elemandır; ancak indirgenemez değildir, çünkü $\bar{2} = \bar{2} \cdot \bar{4}$ olduğu halde ne $\bar{2}$ ne de $\bar{4}$ birimsel eleman değildir.

Ancak R bir tamlık bölgesi ise iş değişir: bir tamlık bölgesinde her asal eleman indirgenemezdir. R bir tamlık bölgesi ve $p \in R$ asal olsun. $p = ab$ olacak şekilde $a, b \in R$ elemanları varsa, $p \mid ab$ olur. Bu durumda $p \mid a$ veya $p \mid b$ olmalıdır. Genelliği bozmadan $p \mid a$ olduğunu varsayalım. O zaman $a = pc$ olacak şekilde $c \in R$ vardır. Buna göre $p = ab = pcb$ olur. Tamlık bölgelerinde sadeleştirme özelliği olduğundan $1 = cb$ olur; yani b birimseldir. Öte yandan $p \mid b$ olduğunu kabul ettiğimizde a'nın birimsel eleman olması gerekir. Yani, $p = a \cdot b$ yazımı ancak a veya b birimsel eleman ise mümkündür. Bu da p'nin indirgenemez olduğunu gösterir. Bir tamlık bölgesinde her asal eleman indirgenemez olduğu halde her indirgenemez eleman asal olmayabilir. Bunun örneğini ileride vereceğiz.

Bir tamlık bölgesinin elemanlarının ilgili olması özelliği tam sayılarda mutlak değerce eşit olma özelliğine denk gelir. Bunun nedeni tam sayıların birimsel elemanlarının yalnız 1 ve -1 olmasıdır. Genel olarak tamlık bölgelerinde çok sayıda birimsel eleman bulunabilir. Örneğin $\mathbb{C}[x]$ polinom halkasında sıfırdan

farklı tüm karmaşık sayılar birimseldir. R bir tamlık bölgesi olmak üzere eğer bir b elemanı a elemanı ile ilgili ise, o zaman a elemanı da b elemanı ile ilgili olur. Yani, $a \sim b$ ise $b \sim a$ olur. Aslında bir u birimsel elemanı için $a = u \cdot b$ olması $b = u^{-1} \cdot a$ olması ile eşdeğerdir. Dahası, $\sim$ bağıntısı bir denklik bağıntısıdır. Dikkat edilirse $a \sim b$ ise $a \mid b$ ve $b \mid a$ olur. Tamlık bölgelerinde bunun tersi de doğrudur; yani $a \mid b$ ve $b \mid a$ ise $a \sim b$ olur. Ancak yalnızca $a \mid b$ olması $a \sim b$ olmasını gerektirmez. Buradaki istisnai durum b indirgenemez iken a'nın birimsel olmaması durumudur. Buna göre $b = a \cdot c$ olacak şekildeki her c elemanı birimsel olmak zorundadır. Özel olarak iki indirgenemez elemandan birinin diğerini bölmesi ilgili olmaları için yeterlidir. Yani, p ve q indirgenemez elemanlar ve $p \mid q$ ise $p \sim q$ olur.

Her ne kadar *asal* çarpanlara ayırma özelliği olarak dile getirilse de bu özellik aslında bir halkadaki *indirgenemez* elemanlar üzerinden tanımlanır. Fakat bu bir sorun değildir; çünkü sıfırdan farklı birimsel olmayan her elemanın indirgenemez elemanların çarpımı şeklinde tek türlü yazılabildiği halkalarda asal ve indirgenemez elemanlar arasında bir ayrım yoktur. Çarpanlara ayırma konusu ele alındığında akla indirgenemez elemanların gelmesi son derece doğaldır. Örneğin bir tamlık bölgesinde bir a elemanının iki çarpana ayrılması $a = b \cdot c$ eşitliği ile ifade edildiğinde, b ve c elemanlarının birimsel olmayan çarpanlar olması, benzer bir soruyu hem b hem de c için sormamızın önünü açar. Yani, b ve c elemanlarının da çarpanlara ayrılıp ayrılmadığını sorgulayabiliriz. Eğer b ve c elemanları da birimsel olmayan çarpanlara ayrılabiliyorsa, bu işlemi ortaya çıkan tüm yeni çarpanlar için tekrarlayabiliriz. Bu işlemi tekrarladığımızda eğer bir adımdan sonra hiçbir çarpanın daha fazla birimsel olmayan çarpana ayrılamadığını görürsek, elde edilen çarpanlar indirgenemez elemanlar olurlar. Böyle bir durumda elde edilen yazım da a'nın çarpanlara ayrılması olarak maksimal indirgenemez çarpan kümesinin kullanıldığı bir yazım olur. Bu şimdilik indirgenemez elemanların çarpımı olarak yazılabilme konusudur. Eğer bu türden her yazım bir anlamda tek türlü ise o zaman tek türlü çarpanlara ayrıma özelliği adı verilen özellik ortaya çıkar. Peki bu tek türlülüğü nasıl tanımlayacağız? Elbette ki bazı yazımları eşdeğer kabul ederek. Öncelikle çarpmanın değişmeli olması nedeniyle, çarpanların sıralanmasının ayırt edici olmadığını kabul edebiliriz. Yani, $a = b \cdot c$ ve $a = c \cdot b$ yazımları birbirine eşdeğer sayılır. Bunun dışında, eğer b ve c birimsel olmayan çarpanlar ise, b ve c'nin birimsel katları olan $-b$ ve $-c$ ile de aynı yazımı elde edebiliriz. Yani, $a = b \cdot c$ ve $a = (-b) \cdot (-c)$ yazımları da birbirine eşdeğer sayılır. Daha genel olarak, eğer b ve c birimsel olmayan çarpanlar ise, herhangi bir $u \in R$ birimsel elemanı için $b \cdot c = (u \cdot b) \cdot (u^{-1} \cdot c)$ eşitliği sağlanır. Örneğin yine rasyonel katsayılı $x^2 - 1$ polinomunu ele alırsak her $k \geq 0$ tam sayısı için

$$x^2 - 1 = (2^k x - 2^k) \cdot (2^{-k} x + 2^{-k})$$

yazılabilir. Tüm bu yazımları birbirinden ayıran tek şey sadece sabit çarpanlardır. Yani $2^k x - 2^k = 2^k(x-1)$ ve $2^{-k}x + 2^{-k} = 2^{-k}(x+1)$. Başka bir örnek olarak, 6 sayısını ele alalım. $6 = 2 \cdot 3$ ve $6 = (-2) \cdot (-3)$ yazımları birbirine eşdeğerdir. Burada, 2, 3, -2 ve -3 indirgenemez elemanlar; -2, 2'nin, -3 ise 3'ün birimsel katıdır. Bir elemanın birimsel katları o eleman ile çarpımsal olarak aynı özellikleri taşır. Örneğin bir x elemanı bir y elemanını bölerse, x'in ilgili olduğu tüm elemanlar da y'nin ilgili olduğu tüm elemanları böler. Yani, u ve v birer birimsel eleman olmak üzere eğer $x \mid y$ ise $u \cdot x \mid v \cdot y$ olur. Diğer taraftan x'in ürettiği temel ideal $\langle x \rangle$ ile ux'in ürettiği temel ideal $\langle ux \rangle$ eşittir. Bu nedenle, çarpanlara ayırma işlemlerinin ilgililik aracılığıyla çeşitlendirilebiliyor olması, çarpanlara ayırma işleminin tek türlülüğünü etkilemez.

Tanım 2. (Tek Türlü Çarpanlara Ayırma Bölgesi)

R bir tamlık bölgesi olsun. Eğer

(1) sıfırdan farklı birimsel olmayan her $x \in R$ elemanı, herhangi ikisi *ilgili* olmayan $p_1, \ldots, p_n \in R$ indirgenemez elemanlar, u birimsel eleman ve $k_1, \ldots, k_n$ pozitif tam sayılar olmak üzere $x = u p_1^{k_1} \cdots p_n^{k_n}$ biçiminde çarpanlarına ayrılabilir ve

(2) $k_1, \ldots, k_n, l_1, \ldots, l_m$ pozitif tam sayıları, R'nin herhangi ikisi ilgili olmayan indirgenemez elemanla-

rından oluşan $\{p_1, \dots, p_n\}$ ve $\{q_1, \dots, q_m\}$ kümeleri ile u ve v birimsel elemanları için

$$x = up_1^{k_1} \cdots p_n^{k_n} = vq_1^{l_1} \cdots q_m^{l_m}$$

eşitlikleri sağlandığında $n = m$ ve her $1 \leq i \leq n$ için $k_i = l_{j_i}$ ve $p_i \sim q_{j_i}$ olacak şekilde j_i indisleri varsa,

bu halka **tek türlü çarpanlara ayırma bölgesi** (TÇB) olarak adlandırılır.

Yukarıdaki tanım kabaca şunu ifade eder: Eğer R bir tek türlü çarpanlara ayırma bölgesi ise, o zaman

1. R'nin sıfırdan farklı birimsel olmayan her elemanı, indirgenemez çarpanlarına ayrılabilir;
2. R'nin sıfırdan farklı birimsel olmayan bir elemanının herhangi bir indirgenemez çarpanlara ayrılışında aynı sayıda tekrar eden ve birbirleri ile ilgili olmayan sabit sayıda indirgenemez çarpan bulunur ve bunlar herhangi iki çarpanlara ayrılışta ikişer ikişer ilgili olma özelliği ile eşleştirilebilir. Daha açık olmak gerekirse $x = up_1^{k_1} \cdots p_n^{k_n}$ ve $x = vq_1^{l_1} \cdots q_m^{l_m}$, x'in iki indirgenemez çarpanlarına ayrılışı ise $n = m$ ve $\{p_1, \dots, p_n\}$ kümesinden $\{q_1, \dots, q_n\}$ kümesine öyle bir σ birebir eşlemesi tanımlanabilir ki her $1 \leq i \leq n$ için $k_i = l_{\sigma(i)}$ ve $p_i \sim q_{\sigma(i)}$ olur.

Aritmetiğin Temel Teoremi bize tam sayılar halkasının bir TÇB olduğunu söyler. tam sayılar dışında rasyonel katsayılı polinomlar halkası $\mathbb{Q}[x]$'in de bir TÇB olduğunu söyleyebiliriz. Bu iki halka, tek türlü çarpanlara ayırma özelliğini taşıyan en yaygın örneklerdendir. Ancak, bu özellik sadece tam sayılar ve polinomlar için geçerli değildir; başka değişmeli ve birimli halkalarda da bu özelliği görmek mümkündür. Örneğin, $\mathbb{Z}[i]$ **Gauss tam sayıları halkası** da bir tek türlü çarpanlara ayırma bölgesidir.

Gauss tam sayıları, reel ve imajiner kısımları tam sayı olan karmaşık sayılardır. Bunların kümesini $\mathbb{Z}[i]$ ile göstereceğiz. Buna göre $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ olur. Bu kümenin, karmaşık sayıların bilinen toplama ve çarpma işlemleri ile bir tamlık bölgesi olduğunu görmek zor değildir. Bu halka, Carl Friedrich Gauss'un asal sayılarla ilgili yaptığı çalışmalarda ele alınmıştır. Gauss, bu halkada tek türlü çarpanlara ayırma özelliğinin bulunduğunu görmüş, bunun gibi özellikler aracılığıyla tam sayılar hakkında daha fazla bilgi elde edilebileceğini ortaya koymuştur. Böylece tam sayılardan daha geniş bir sistemde aritmetik özellikleri incelemenin yine tam sayılar ile ilgili önemli bilgiler sunabileceği fark edilmiştir. Örneğin, Richard Dedekind, $\mathbb{Z}[i]$ halkasındaki aritmetiği kullanarak Fermat'nın **iki-kare teoremi** olarak bilinen ünlü teoremi için 1877 ve 1894 yıllarında en az iki ispat vermiştir. Bu teorem, bir asal sayının iki kare olarak yazılabilmesi için gerekli ve yeterli koşulları belirler. Bu teoremin ispatı ile ilgili detayları ilerideki yazı dizilerimizde ele alacağız.

$\mathbb{Z}[i]$ Gauss tam sayıları halkasının tek türlü çarpanlara ayırma özelliği, yine tam sayılar halkasında bulunan başka bir aritmetik özellikten faydalanılarak elde edilebilir: **bölme algoritması**. Antik çağlardan beri bilinen tam sayıların bu özelliği şu şekilde ifade edilir: her $a, b \in \mathbb{Z}$ ve $b \neq 0$ için $a = bq+r$ ve $0 \leq r < |b|$ olacak şekilde tek türlü belirli q, r tam sayıları bulunabilir. Burada q bölüm, r ise kalan olarak adlandırılır. Buna göre her tam sayı sıfırdan farklı bir tam sayıya bölünür ve bu bölme işleminden bir bölüm bir de kalan tek türlü olarak elde edilir. Buna benzer bir özellik $\mathbb{Z}[i]$ halkasında da bulunur, ancak bunu matematiksel olarak ifade ederken yukarıda olduğu gibi mutlak değer fonksiyonunu kullanamayacağımız açıktır. Bunun yerine, $\mathbb{Z}[i]$ halkası üzerinde **norm** adı verilen tam sayı değerli bir N fonksiyonu tanımlayacağız. Bu N fonksiyonu, her $z = a + bi \in \mathbb{Z}[i]$ için $N(z) = a^2 + b^2$ şeklinde tanımlanır. Norm fonksiyonun aşağıdaki üç özelliği dikkate değerdir:

- Her $z \in \mathbb{Z}[i]$ için $N(z) \geq 0$ ve $N(z) = 0$ ancak ve ancak $z = 0$.
- Sıfırdan farklı her $z \in \mathbb{Z}[i]$ için $N(z) \geq 1$.
- Norm, çarpma işlemi ile uyumludur: Her $z_1, z_2 \in \mathbb{Z}[i]$ için $N(z_1 z_2) = N(z_1)N(z_2)$.

Buna göre aşağıdaki teoremi verebiliriz:

Teorem 1.

(1) *Sıfırdan farklı her $x, y \in \mathbb{Z}[i]$ için eğer $x \mid y$ ise $N(x) \leq N(y)$ olur.*

(2) *Her $x, y \in \mathbb{Z}[i]$ ve $y \neq 0$ için, $x = yq + r$ ve $N(r) < N(y)$ olacak şekilde $q, r \in \mathbb{Z}[i]$ bulunabilir.*

Kanıt. (1) Eğer $x \mid y$ ise, $y = xc$ olacak şekilde $c \in \mathbb{Z}[i]$ vardır. Dikkat edilirse $y \neq 0$ olduğu için $c \neq 0$ ve böylece $N(c) \geq 1$ olur. Bu durumda, $N(y) = N(xc) = N(x)N(c) \geq N(x)$ elde edilir.

(2) $\mathbb{C}$ karmaşık sayılar kümesinde bilinen bölme işlemi uygulanırsa $\frac{x}{y} = \alpha + \beta i$ olacak şekilde $\alpha, \beta \in \mathbb{Q}$ bulunabilir. Her reel sayı bir tam sayının $1/2$ kapalı komşuluğuna düşeceğinden, $\alpha = n + \alpha'$ ve $\beta = m + \beta'$ olacak şekilde $n, m \in \mathbb{Z}$ ve $\alpha', \beta' \in [-1/2, 1/2]$ rasyonel sayıları bulunabilir. Buna göre $\frac{x}{y} = \alpha + \beta i = (n+\alpha') + (m+\beta')i = (n+mi) + (\alpha' + \beta' i)$ yazılabilir. $q = n + mi$ ve $r = (\alpha' + \beta' i) \cdot y$ denirse $x = yq + r$ olur. Ayrıca $N(r) = N(\alpha' + \beta' i)N(y) \leq (\frac{1}{4} + \frac{1}{4})N(y) = \frac{1}{2}N(y) < N(y)$ elde edilir. Böylece kanıt tamamlanmış olur. □

Örneğin $x = 5+2i$ ve $y = 2-i$ elemanlarını ele alalım. $\mathbb{C}$'de $\frac{x}{y} = \frac{8}{5} + \frac{9}{5}i$ olur. Buna göre $\frac{8}{5} = 2 - \frac{2}{5}, | -\frac{2}{5} | < \frac{1}{2}$ ve $\frac{9}{5} = 2 - \frac{1}{5}, | -\frac{1}{5} | < \frac{1}{2}$ yazılabileceğinden, $\frac{x}{y} = (2+2i) + (-\frac{2}{5} - \frac{1}{5}i)$, buradan da $x = y(2+2i) + y(-\frac{2}{5} - \frac{1}{5}i)$ elde edilir. $q = 2 + 2i$ ve $r = y(-\frac{2}{5} - \frac{1}{5}i)$ denirse $r = -1$ ve $x = yq + r = y(2 + 2i) - 1$ bulunur. Üstelik $N(r) = 1 < N(y) = 5$ olur. Ancak tam sayılar halkasının aksine burada elde edilen bölüm ve kalan tek türlü değildir. Örneğin $x = 5 + 2i$ ve $y = 2 - i$ için $x = yq + r$ ve $N(r) < N(y)$ olacak şekilde iki farklı q, r çifti bulunabilir: $5 + 2i = (2 - i)(2 + 2i) - 1$ ve $5 + 2i = (2 - i)(1 + 2i) + (1 - i)$. Ancak bu durumun $\mathbb{Z}[i]$ halkasının tek türlü çarpanlara ayırma özelliğine olumsuz bir etkisi yoktur.

Aşağıdaki teorem $\mathbb{Z}[i]$ halkasında bölme algoritmasının varlığının önemli bir faydasını ortaya koyar:

Teorem 2.

$\mathbb{Z}[i]$ halkasında asal ve indirgenemez elemanlar aynıdır.

Kanıt. $\mathbb{Z}[i]$ bir tamlık bölgesi olduğundan, yukarıda da gösterildiği gibi, her asal eleman indirgenemezdir. $p \in \mathbb{Z}[i]$ indirgenemez olsun. Kabul edelim ki $a, b \in \mathbb{Z}[i]$ için $p \mid ab$ olsun. Kabul edelim ki $p \nmid a$ olsun. Bölme algoritmasından, $a = p \cdot q_1 + r_1$ ve $N(r_1) < N(q_1)$ olacak şekilde $q_1, r_1 \in \mathbb{Z}[i]$ bulunabilir. $p \nmid a$ olduğundan $r_1 \neq 0$ olur. Bölme algoritmasını bir kere daha p ve r_1 çifti için uygulayalım. Buna göre $p = r_1 \cdot q_2 + r_2$ ve $N(r_2) < N(r_1)$ olacak şekilde $q_2, r_2 \in \mathbb{Z}[i]$ bulunabilir. Bu şekilde devam ederek

$$\begin{aligned} a &= p \cdot q_1 + r_1 \text{ ve } N(r_1) < N(p) \\ p &= r_1 \cdot q_2 + r_2 \text{ ve } N(r_2) < N(r_1) \\ r_1 &= r_2 \cdot q_3 + r_3 \text{ ve } N(r_3) < N(r_2) \\ &\vdots \\ r_{i-1} &= r_i \cdot q_{i+1} + r_{i+1} \text{ ve } N(r_{i+1}) < N(r_i) \end{aligned}$$

şeklinde eşitlikler elde edilebilir. Bu şekilde eşitlikler elde edilmesi işlemine Öklid algoritması denir. $N(p) > N(r_1) > N(r_2) > \ldots > N(r_i) > N(r_{i+1}) \geq 0$ olduğu için sonlu bir adım sonunda bölme algoritmasından sıfır kalanı elde etmemiz gerekir. Dolayısıyla bir n pozitif tam sayısı için $r_n = 0$ olmak zorundadır. Yani $r_{n-2} = r_{n-1} \cdot q_n$ olur. Buna göre $r_{n-1} \mid r_{n-2}$ olur. Öklid algoritmasındaki bir önceki eşitlik $r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}$ olduğundan $r_{n-1} \mid r_{n-3}$ elde edilir. Bu şekilde devam ederek $r_{n-1} \mid r_{n-2}$, $r_{n-1} \mid r_{n-3}, \ldots, r_{n-1} \mid p, r_{n-1} \mid a$ elde edilir. p indirgenemez olduğundan ya r_{n-1} birimseldir ya da p ile ilgilidir. Fakat eğer r_{n-1} p ile ilgili ise $r_{n-1} \mid a$ olduğundan $p \mid a$ olmak zorundadır. Bu da kabulümüz ile çelişir. Dolayısıyla r_{n-1} birimseldir. Şimdi Öklid algoritmamızdaki tüm eşitlikleri b ile çarpalım:

$$\begin{aligned} ab &= pbq_1 + r_1 b \\ pb &= r_1 bq_2 + r_2 b \end{aligned}$$

$$\begin{aligned} r_1 b &= r_2 b q_3 + r_3 b \\ &\vdots \\ r_{n-3} b &= r_{n-2} b \cdot q_{n-1} + r_{n-1} b \\ r_{n-2} b &= r_{n-1} b \cdot q_n \end{aligned}$$

$p \mid ab$ olduğundan ilk eşitlikten $p \mid r_1 b$ olur. İkinci eşitlikten $p \mid r_2 b$ olur. Bu şekilde devam ederek $p \mid r_{n-1} b$ elde edilir. Fakat r_{n-1} birimseldir. Dolayısıyla $p \mid b$ olur. Bu da p'nin asal olduğunu gösterir. □

Teorem 3.
$\mathbb{Z}[i]$ halkası bir TÇB'dir.

Kanıt. Önce sıfırdan farklı birimsel olmayan her $x \in \mathbb{Z}[i]$ elemanının indirgenemez elemanların bir çarpımı ile ilgili olabildiğini gösterelim. Aksini kabul edelim; yani $\mathbb{Z}[i]$'nin sıfırdan farklı birimsel olmayan bir z elemanı, indirgenemez elemanların çarpımı olarak yazılan hiçbir eleman ile ilgili olmasın. Doğal sayıların iyi sıralanma ilkesi gereğince z'yi bu özellikte normu en küçük olan eleman olarak seçebiliriz. Buna göre normu $N(z)$'den küçük olan sıfırdan farklı birimsel olmayan her $x \in \mathbb{Z}[i]$ elemanı indirgenemez elemanların çarpımı olarak yazılabilen bir eleman ile ilgili olur. z indirgenemez elemanların çarpımı olarak yazılamadığından kendisi de indirgenemez olamaz; aksi halde tek başına z'yi indirgenemez elemanların çarpımı olarak düşünebilirdik. Buna göre birimsel olmayan öyle $u, v \in \mathbb{Z}[i]$ elemanları vardır ki $z = u \cdot v$ şeklinde yazılabilir. $N(u) \leq N(z)$'dir. Eğer $N(u) = N(z)$ ise $N(z) = N(u \cdot v) = N(u)N(v)$ ve buradan $N(v) = 1$ olur. Yani $v \in \{\pm 1, \pm i\}$ olur. Bu durumda v birimsel olur ki bu da bir çelişkidir. Dolayısıyla $N(u) < N(z)$ olur. Benzer şekilde $N(v) < N(z)$ olur. $N(u), N(v) < N(z)$ olduğundan u ve v elemanları da normu $N(z)$'den küçük olan sıfırdan farklı birimsel olmayan elemanlar olarak indirgenemez elemanların çarpımı olarak yazılabilen elemanlar ile ilgilidir. Fakat $z = u \cdot v$ olduğundan z de indirgenemez elemanların çarpımı olarak yazılabilen bir eleman ile ilgili olur. Bu da aradığımız çelişkiyi bize verir. Böylece $\mathbb{Z}[i]$'deki sıfırdan farklı birimsel olmayan her eleman indirgenemez elemanların bir çarpımı ile ilgilidir.

Şimdi de $k_1, \ldots, k_n, l_1, \ldots, l_m$ pozitif tam sayıları, herhangi ikisi ilgili olmayan indirgenemez elemanlardan oluşan $\{p_1, \ldots, p_n\}$ ve $\{q_1, \ldots, q_m\}$ kümeleri ile u ve v birimsel elemanları için $z = u p_1^{k_1} \cdots p_n^{k_n}$ ve $z = v q_1^{l_1} \cdots q_m^{l_m}$ biçiminde iki farklı çarpanlara ayırma yazımı bulunsun. Teorem 2'den p_1 indirgenemez elemanı aynı zamanda asal elemandır. $p_1 \mid q_1^{l_1} \cdots q_m^{l_m}$ olduğundan $p_1 \mid q_i$ olacak şekilde bir $1 \leq i \leq m$ vardır. Genelliği bozmadan $i = 1$ olduğunu varsayalım. O zaman q_1 ile p_1 ilgilidir; yani $q_1 = u_1 p_1$ olacak şekilde bir u_1 birimsel elemanı vardır. Buna göre $z = u p_1^{k_1} \cdots p_n^{k_n} = v u_1^{l_1} p_1^{l_1} \cdots q_m^{l_m}$ olur. $\mathbb{Z}[i]$ bir tamlık bölgesi olduğundan, sadeleşme işlemi yapabiliriz. Genelliği bozmadan $k_1 \geq l_1$ olduğunu varsayalım. Bu durumda

$$u p_1^{k_1 - l_1} p_2^{k_2} \cdots p_n^{k_n} = v u_1^{l_1} q_2^{l_2} \cdots q_m^{l_m}$$

elde edilir. Bu yazımda $k_1 - l_1$ bir pozitif tam sayı ise o zaman p_1 asal elemanı $q_2^{l_2} \cdots q_m^{l_m}$ çarpımını böleceği için $q_2, \ldots, q_m$ indirgenemez elemanlarından biri ile ilgili olur. Fakat q_1 de p_1 ile ilgili olduğundan, bu durumda $q_2, \ldots, q_m$ elemanlarından biri q_1 ile ilgili olur –ki bu da kabullerimiz ile çelişir. Dolayısıyla $k_1 - l_1 = 0$ olur. Yani $k_1 = l_1$ elde edilir. Buna göre $v' = v u_1^{l_1}$ denirse v' birimseldir ve $u p_2^{k_2} \cdots p_n^{k_n} = v' q_2^{l_2} \cdots q_m^{l_m}$ eşitliği yazılabilir. Buradan da n (ya da m) üzerine tümevarım ile istenilen sonucu elde edebiliriz. Böylece $\mathbb{Z}[i]$ halkası tek türlü çarpanlara ayırma bölgesi olur.

□

Şimdiye dek $\mathbb{Z}[i]$ Gauss tam sayıları halkasının, sahip olduğu aritmetik özellikler bakımından ne denli ayrıcalıklı bir yapı sergilediğini ortaya koymaya çalıştık. Benzer bir inşa yöntemiyle, karmaşık sayılar kümesi içerisinde başka değişmeli ve birimli halkalar da tanımlanabilmektedir. Ancak, inşa yöntemleri benzeşse de, bu halkaların her biri $\mathbb{Z}[i]$ kadar zengin ve düzenli bir aritmetik yapıya sahip olmayabilir. Bu durumu somutlaştırmak adına, herhangi bir tam sayının karesi olmayan bir d tam sayısı seçelim ve şu kümeyi ele alalım:

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$

Bu küme, karmaşık sayıların toplama ve çarpma işlemleri ile bir tamlık bölgesidir. Dikkat edilirse $d = -1$ seçildiğinde, elde edilen yapı Gauss tam sayıları halkası $\mathbb{Z}[i]$ ile özdeş hâle gelir. Buradaki önemli noktalardan biri de her d değeri için $\mathbb{Z}[\sqrt{d}]$ halkasının $\mathbb{Z}[i]$ kadar zengin bir aritmetik yapıya sahip olmamasıdır. Örneğin, $d = -5$ seçildiğinde elde edilen $\mathbb{Z}[\sqrt{-5}]$ halkası tek türlü çarpanlara ayırma özelliğini taşımaz. Dikkat edilirse $\mathbb{Z}[\sqrt{-5}]$ halkasında $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ ve $6 = 2 \cdot 3$ yazımları bulunur. Ancak bu iki yazımda $1 + \sqrt{-5}$ ve $1 - \sqrt{-5}$ indirgenemez elemanları ne 2 ne de 3 indirgenemez elemanı ile ilgili değildir. Yani, $\mathbb{Z}[\sqrt{-5}]$ halkası tek türlü çarpanlara ayırma özelliğini taşımaz. Buradaki önemli nokta, $\mathbb{Z}[\sqrt{-5}]$ halkasında asal ve indirgenemez elemanların birbirinden ayrılmasıdır. Örneğin, 2 elemanı $\mathbb{Z}[\sqrt{-5}]$ halkasının bir indirgenemez elemanı olmasına rağmen asal elemanı değildir. Halbu ki $\mathbb{Z}[\sqrt{-5}]$ halkasının sıfırdan farklı birimsel olmayan her elemanı indirgenemez elemanların çarpımı olarak yazılabilir. Buradaki eksik, yazımın tek türlü olmak zorunda olmamasıdır ve bunun nedeni olarak da $\mathbb{Z}[\sqrt{-5}]$ halkasında asal elemanların indirgenemez elemanlardan daha dar bir küme olması gösterilebilir. Bu ve benzeri durumlarla ilgili detayları bir sonraki yazımızda ele alacağız. Bir sonraki yazımızda ayrıca $\mathbb{Z}[i]$ halkasının zengin aritmetik yapısı yardımıyla Fermat'nın iki-kare teoreminin nasıl ispatlanabileceğini de göreceğiz.

Kaynaklar

[1] Ian Bruce. *Some Mathematical Works of the 17th & 18th Centuries*. http://www.17centurymaths.com/. Accessed: 2025-07-21.

[2] Davide Crippa, Maria Rosa Massa-Esteve, ed. *The Algebrization of Mathematics during the 17th and 18th Centuries*. College Publications, 2023. ISBN: 978-1-84890-394-4.

[3] Thomas L. Heath. *The Thirteen Books of Euclid's Elements*. C. 9. Translation and commentary of Euclid's original Book IX. New York: Dover Publications, 1956.

[4] Peter L. Ribenboim. *Highlights in the History of Number Theory: 1700 BC–2008*. New York: Springer, 2008. ISBN: 978-0-387-74908-4.

[5] David Sharpe. *Rings and Factorization*. Cambridge: Cambridge University Press, 1987. ISBN: 978-0-521-37524-2.