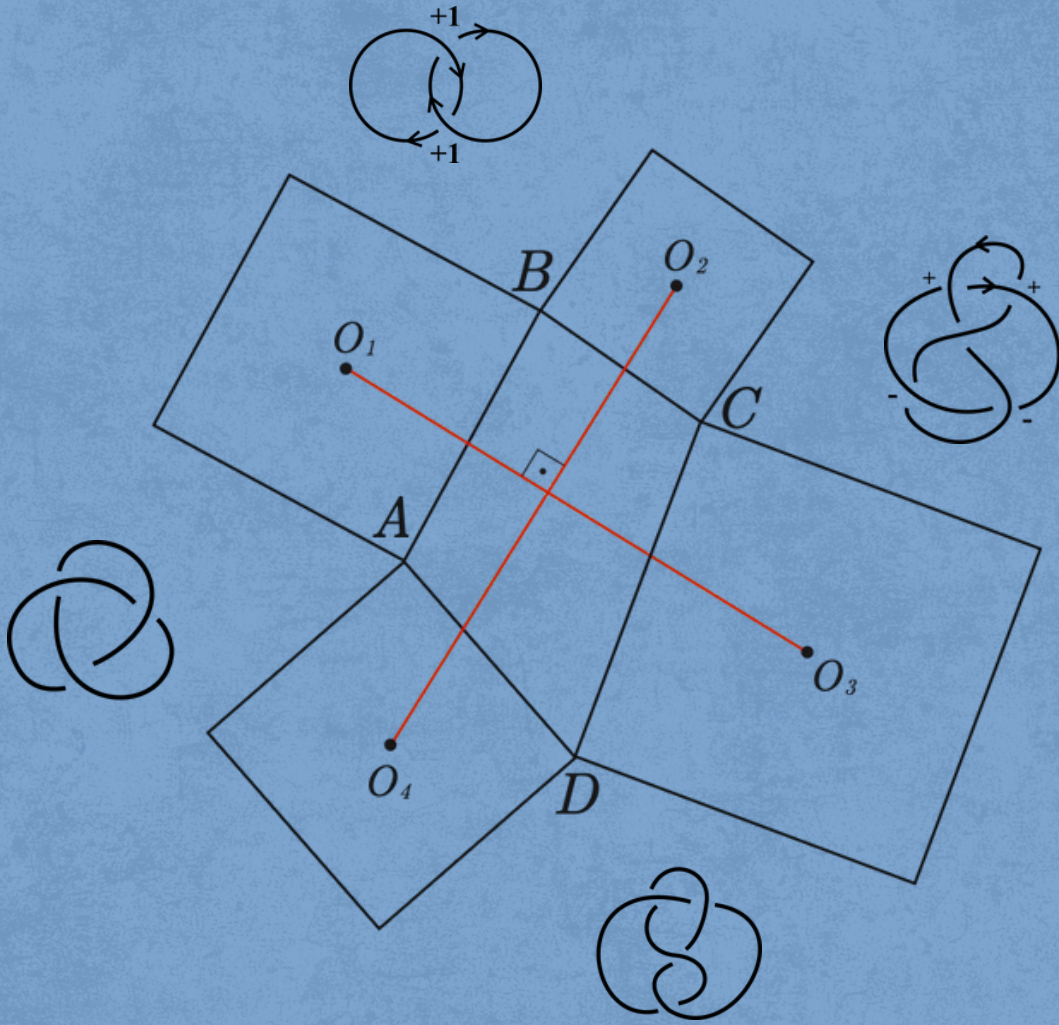


HACETTEPE LİSANS

MATEMATİK

DERGİSİ



Akademik Yazılar / Öğrenci Yazıları / Matematik Söyleşileri / Matematğin İzinde
Kitaplar / Erasmus Günlükleri / Mezun Hikâyeleri / Meraklısına Problemler

İçindekiler

- 2 Bölüm Başkanının Mesajı
İsmet Yurduşen
- 3 Editörden Mektup
Orhan Oğulcan Tuncer
- 4 Bir Mantıkçının Gözünden Sıkça Sorulan Sorulara Yanıtlar
Ahmet Çevik
- 9 Belki De Bu Yüzden Yalnızca Cesurların İşidir Kanıt
Orhan Oğulcan Tuncer
- 21 İyi Temellendirilmemiş Kümeler
Sebahattin Emre Şahin
- 27 Matematik Söyleşileri
Selcan Şenyurt & Talha Tin
- 34 Karmaşık Sayılar ve Düzlem Geometrisi
Uğur Gül
- 46 Matematiksel Düşünmeyi Anlamak: Kavramsal Temellerden Öğrenme Ortamlarına
Şenol Dost
- 51 Paranoyak Bir Matematikçi: Kurt Gödel
Ali Berk Koyuncu
- 56 Matematiğin İzinde Kitaplar
Pınar Aydoğdu
- 60 Tek Türlü Çarpanlara Ayırma Özelliği: Tam Sayılar ve Ötesi
Bülent Saraç
- 68 Bilgisayarlar Nasıl Çalışabilir?
Murat Erşen Ünal
- 72 Nizami İki Karma Metodunun Matematiksel İzahı
Talha Tin
- 77 Esnek Çokgenler (Fleksagonlar) ve Biraz Sihir
Cansu Betin Onur & Elif Medetoğulları
- 82 Kategori Teorisi: Temel Kavramlar, Tarihsel Gelişim ve Matematiksel Düşünceye Katkısı
Sultan Eylem Toksoy
- 87 Düğüm Teorisine Giriş: Temel bir değişmez "Bağlanma Sayısı" üzerine
Sinem Onaran
- 92 Diffie-Hellman Anahtar Değişimi
Sümeyye Soylu
- 96 Erasmus Günlükleri
- 98 Mezun Hikâyeleri
- 107 Meraklısına Problemler
Refail Alizade

Bölüm Başkanının Mesajı



Hacettepe Üniversitesi Matematik Bölümü olarak, yıllardır derslerde, sınavlarda ve araştırmalarda paylaştığımız akademik ortamı şimdi farklı bir boyuta taşımanın heyecanını yaşıyoruz. Elinizdeki bu dergi, yalnızca bir yayın değil, bölümümüzün ortak kültürüne, hafızasına ve değerlerine dayanan kolektif bir yolculuğun ilk adımıdır.

Bu dergide öğrencilerimizin, öğretim üyelerimizin ve mezunlarımızın; matematikle kesişen düşünceleri, deneme yazıları, akademik katkıları ve kişisel deneyimleri yer alıyor. Amacımız yalnızca bilgi sunmak değil; farklı kuşaklardan matematikçileri ve matematikseverleri bir araya getiren aktif ve üretken bir paylaşım alanı oluşturmaktır.

Dergimiz aynı zamanda, bölümümüze duyulan aidiyetin taşıyıcısı olmayı hedefliyor. Öğrencilerimizin eğitimleri sırasında bu sayfalarda kendi seslerini bulmaları, mezunlarımızın ise deneyimlerini aktararak yeni kuşaklara ilham vermeleri, zamanla bu yayını kuşakları birbirine

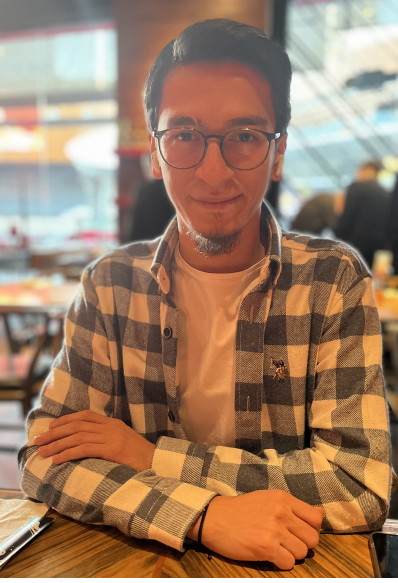
bağlayan kalıcı bir köprüye dönüştürecektir.

Bu dergi fikrini ilk ortaya atan ve hayata geçmesi için büyük bir özveriyle çalışan Bölüm Başkan Yardımcımız Dr. Orhan Oğulcan Tuncer'e ayrıca içten teşekkürlerimi sunmak isterim. Onun özverili çabası, bu yayının gerçeğe dönüşmesinde belirleyici olmuştur. Bu ilk sayının hazırlanmasında emeği geçen tüm öğrencilerimize, katkı sunan öğretim üyelerimize ve desteğini esirgemeyen mezunlarımıza içtenlikle teşekkür ediyorum.

Dilerim bu yayın, ilerleyen yıllarda daha da zenginleşerek, yalnızca matematiksel içeriğiyle değil, bölümümüzün ruhunu ve birikimini yansıtan bir gelenek haline gelir. Bu dergiye katkı sunan ya da sadece içinden bir cümleye göz atan herkes, bu kültürün bir parçasıdır. Derginin tüm okurlar için verimli, düşündürücü ve ilham verici bir deneyim olmasını temenni ederim.

Prof. Dr. İsmet Yurduşen
Matematik Bölüm Başkanı

Editörden Mektup



Değerli Okurlarımız,

Hacettepe Üniversitesi Matematik Bölümü bünyesinde yayımlanan *Hacettepe Lisans Matematik Dergisi*'nin ilk sayısına hoş geldiniz. Böyle bir ihtiyacın olup olmadığını tam olarak bilmiyorum; ancak bir yılı aşkın süredir aklımda lisans öğrencilerine yönelik bir dergi kurma fikri vardı. Temel amacım, matematik bölümü öğrencilerini sadece ders çalışıp sınavlara hazırlanmaktan biraz olsun uzaklaştırmak ve onları daha fazla düşünmeye, daha etkili yazmaya teşvik etmektir. Başlangıçta, sadece lisans öğrencilerinin yazılar yazdığı, akademik bir dergi modeli oluşturmayı hayal ediyordum. Yazılar, sistem üzerinden tarafımıza iletilecek, titiz bir değerlendirme sürecinin ardından yayımlanıp yayımlanmayacağına karar verilecekti. Ancak zamanla, yalnızca bu modele dayalı bir derginin sürdürülebilir olmayabileceği düşüncesiyle, derginin formatını daha kapsayıcı ve esnek bir yapıya dönüştürmeye karar verdim.

Dergi bu yeni haliyle, matematik ve matematik eğitimi üzerine farklı konuları anlaşılır ve lisans (hatta lise) düzeyindeki öğrencilere hitap eden bir dille ele alan akademisyen yazılarını; lisans öğrencilerinin merak edip araştırdıkları konular üzerine yazdıkları metinleri; bölümümüz mezunlarının hikayelerini; değişim programlarıyla yurt dışına giden öğrencilerimizin deneyimlerini, alanında uzman bilim insanlarıyla yapılan söyleşileri; ufkumuzu genişletecek kitap önerilerini ve bazı eğlenceli içerikleri bünyesinde barındırıyor.

Bu ilk sayı, örnek teşkil etmesi ve sonraki sayıların biçimini belirlemesi amacıyla hazırlandı. Özellikle öğrenci yazıları, bölümümüzde katkıda bulunacağını düşündüğümüz lisans öğrencilerinden ricada bulunularak temin edildi. Ancak önümüzdeki sayılarda dileyen lisans öğrencilerinin, iyi araştırdıkları ve farklı yönleriyle ele aldıkları konularla ilgili yazı göndermelerini ve bu sürece daha doğrudan katılmalarını bekliyorum. Bu yazıların uygunluğunun incelenebilmesi ve yayına hazır hale getirilebilmesi için tabii ki bir editör ekibi kuracağız.

Bir süre kafamda demlenmiş bu fikri anlatmaya başladığımda, anlattığım kişilerin de bu konuda heyecan duyduğunu gördüm. Herkes hem değerli fikirler sunuyor hem de nasıl destek olabileceğini paylaşıyordu. Bu motivasyonla derginin kapak ve iç tasarım çalışmalarına başladım. Sürecin her aşamasında, neredeyse her birine tek tek gidip nelerin iyi, nelerin kötü olduğunu sordum. Her defasında, böyle hocalarla tanışmış olmanın ne kadar büyük bir şans olduğunu yeniden hissettim. Hepsine ayrı ayrı teşekkür etmem zor. O yüzden bu süreçte destek olan tüm hocalarıma; yazılarıyla, önerileriyle, hikâyeleriyle derginin içeriğine katkıda bulunan tüm akademisyenlere, öğrencilere ve mezunlara teşekkür ederim.

Dergideki yazılar, mantık, geometri, analiz, sayılar kuramı, topoloji, cebir ve kriptoloji gibi matematiğin farklı alanlarına uzanıyor. Bunları her sayıda çeşitlendirmeyi hedefliyoruz. Şu an için yılda iki sayı olarak planladığımız Hacettepe Lisans Matematik Dergisi, çevrim içi ve ücretsiz bir şekilde okurlarıyla buluşuyor.

Herkese keyifli ve merak dolu okumalar diliyorum.

Dr. Orhan Oğulcan Tuncer
23 Temmuz 2025, Ankara

Bir Mantıkçının Gözünden Sıkça Sorulan Sorulara Yanıtlar

AHMET ÇEVİK

Jandarma ve Sahil Güvenlik Akademisi, Sosyal Bilimler Bölümü

✉ a.cevik@hotmail.com



Okul hayatında öğrencilere matematikte sayılarla ve kümelerle ilgili bir sürü bilginin ezberletildiğini biliyoruz. Liseden henüz mezun olup üniversitede matematik dersi alan öğrenciler (özellikle sayısal temelden gelmeyenler), ezberletilen bilgilerin ve formüllerin altında yatan gerekçelerini doğal olarak bilmeden geliyorlar. Öğretilmediği ama anlamadıkları için değil, zaten öğretilmediği için. Örneğin, ortaokullarda ya da liselerde, “Boş küme her kümenin altkümesidir” diye bir şey ezberletilir ama bunun neden gerçekten öyle olduğu hakkında mantıklı ya da anlamlı bir açıklama yapılmaz. Bu gibi benzer iddialar veya temel tanımlar için açıklama yapılması istendiğinde “İşimize öyle geliyor o yüzden” demek de çok tatmin edici gelmiyor bana. Ben bunun yerine “Öyle olmasaydı ne olurdu?” sorusunu sorduktan sonra bir saçmalık/anlamsızlık bulup, “Demek ki öyle olmalı” demenin daha ikna edici olduğuna inanıyorum. Sık kullanılan matematiksel gerçeklerin sebeplerini bilmek, bir kişinin matematik altyapısını mutlaka güçlendirir. Bu yazıda, hakkında sıkça sorulan bazı matematiksel gerçeklerin nedenlerini olabildiğince anlamlandırarak yazmaya çalışacağım.

■ Boş Küme Neden Her Kümenin Altkümesidir?

Boş kümenin $\emptyset$ ile gösterildiğini biliyoruz. “Boş küme her kümenin altkümesidir” demek, “Eğer A herhangi bir kümeysse, $\emptyset \subseteq A$ ” olduğunu söylemekle aynı şeydir. A herhangi bir küme olsun; $\emptyset \subseteq A$ ifadesinin doğru olması demek, “Eğer x ögesi boş kümenin içindeyse, x ögesi A ’nın da içindedir” demektir. Tırnak içindeki önerme, $p \rightarrow q$ biçiminde bir koşullu önermedir. Önermenin p yani öncül kısmı “ $x \in \emptyset$ ” ifadesine karşılık gelir, q yani ardıl kısmı da “ $x \in A$ ” ifadesine karşılık gelir. Demek ki $\emptyset \subseteq A$ ifadesinin doğru olması, belirtilen $p \rightarrow q$ biçimindeki önermenin doğru olmasıyla aynı şeydir. Peki buradaki $p \rightarrow q$ önermesi doğru mu? Evet! Çünkü p önermesi yanlış! Hiçbir zaman $x \in \emptyset$ doğru olmaz. Önermeler mantığından biliyoruz ki $p \rightarrow q$ önermesinin doğruluk tablosu gereği, eğer p yanlışsa, q ne olursa olsun, $p \rightarrow q$ doğru olur. Demek ki $\emptyset \subseteq A$ ifadesinin eşdeğeri olan “Her x için, x eğer boş kümenin içindeyse, x A ’nın içindedir” önermesi doğrudur. Çünkü hiçbir x için, x boş kümenin bir elemanı değildir, boş kümenin hiç elemanı yoktur. Boş kümenin içinde bir eleman olup bu eleman A kümesinde olmasaydı o zaman yanlış olurdu. Ama boş kümenin içinde bir eleman yok. Demek ki önerme yanlış değil. Yanlış değil demek doğru demektir. Yani $\emptyset \subseteq A$ ifadesi de böylece doğrudur.

■ 1 ve $0,9$ Sayıları Birbirine Neden Eşittir?

1’den küçük en büyük reel sayı $0,9$ (yani $0,999 \dots$) değil midir? Reel sayılarla ilgili mevcut tanımlarımıza, varsayımlarımıza ve ilkelerimize göre 1 ve $0,9$ aynı sayılardır. Aynı olmadığını kabul etmek zaten Arşimet özelliğine aykırıdır. *Arşimet özelliği*, verilen herhangi iki pozitif x ve y sayısı için, $xn > y$ özelliğini sağlayan bir n doğal sayısının var olduğunu söyler. Eğer bu iki sayı aynı olmasaydı, $1 - 0,9$ işleminin sonucunun *sonsuz küçük* sayı olması beklenirdi. Yani $0,9$ sayısı, 1’in altındaki en büyük öge olurdu. 1 ile $0,9$ arasında başka bir sayı var olamazdı. Ancak bu sezgilerimize de ters düşüyor. $0,9$ sayısı 1’in altındaki en büyük sayı olsaydı reel sayılarda bir *boşluk* söz konusu olurdu. Sonsuz küçük sayı diye bir şey yoktur. Arşimet ilkesi, sonsuz küçük sayının varlığını yasaklamıştır.

Bu sezgisel açıklama tatmin etmediyse 1’in $0,9$ sayısına eşit olduğunun çeşitli kanıtlarına bakılabilir. Birçok kanıt olmakla beraber, bunlardan biri *limit* tanımıyla şöyle yapılır:

$$0,\bar{9} = \lim_{n \rightarrow \infty} 0,\underbrace{999 \dots}_{n \text{ tane}} = \lim_{n \rightarrow \infty} \sum_{k=1}^n \frac{9}{10^k} = \lim_{n \rightarrow \infty} \left(1 - \frac{1}{10^n}\right) = 1 - \lim_{n \rightarrow \infty} \frac{1}{10^n} = 1 - 0 = 1.$$

Yine tatmin etmediyse basit cebirsel bir kanıt da şöyle verilebilir:

$x = 0,999 \dots$ olsun.

$$10x = 9,999 \dots$$

$$10x = 9 + 0,999 \dots$$

$$10x = 9 + x$$

$$9x = 9$$

$$x = 1.$$

■ Neden $0! = 1$ dir?

Cebirde faktöriyelin doğal sayılar için tanımlı bir fonksiyon olduğunu biliyoruz. Analiz dediğimiz alanda reel sayıların da “faktöriyeli” çeşitli yöntemlerle tanımlanabiliyor ancak biz doğal sayılar üzerinde tanımlanan faktöriyeli göz önünde bulunduralım. Faktöriyelin özyinelemeli tanımına bakalım. Aşağıda soru işaretli yere ne gelmesi gerektiğini bir örnek üzerinden giderek anlayacağız.

$$n! = n \times (n - 1)!$$

$$0! = ?$$

Örneğin, $5!$ ’i bu tanıma göre hesaplayalım.

$$5! = 5 \times 4!$$

$$\Rightarrow 4! = 4 \times 3!$$

$$\Rightarrow 3! = 3 \times 2!$$

$$\Rightarrow 2! = 2 \times 1!$$

$$\Rightarrow 1! = 1 \times 0!$$

Şimdi, bir sayının faktöriyelinin sıfır *olmaması* için hemen yukarıda son satırdaki ifadenin, yani $1!$ ’in sonucunun sıfır *olmaması* gerekir. Demek ki $0! = 0$ olarak tanımlarsak, her sayının faktöriyeli sıfır olur! Bu da anlamsız olur. En iyisi $1!$ ’i tanımlarken, eşitliğin sağında $1!$ ’i çarpmanın birim elemanıya, yani 1 ile çarpmak. Bu yüzden $0! = 1$ olarak tanımlamak, $1! = 1 \times 1$ eşitliğini verir ve diğer tüm sayıların faktöriyeli bize pozitif bir değer vereceği için $0! = 1$ tanımı anlamlı olur. Yani, $0! = 0$ olarak tanımlansaydı her sayının faktöriyeli sıfır olurdu ve bu da oldukça anlamsız olurdu.

■ 0 Neden Bir Doğal Sayıdır?

Matematik tanımlarla ve varsayımlarla başlar. Aritmetik kuramımızın varsayımları *Peano aksiyomları* diye bilinen varsayımlarla tanımlanmıştır. Peano aksiyomlarından burada bahsetmeyeceğiz. Bu aksiyomlar esasen doğal sayılar yapısının özelliklerine sahip tüm yapıların ortak özelliklerini belirten varsayımlardır. Peano aksiyomlarına göre, ‘0’ sembolüyle gösterilen sayı bir doğal sayıdır. Amasız fakatsız bunu kabul ederiz. Yani matematikte “0 bir doğal sayıdır” önermesi aksiyom gereği doğrudur. Doğal sayılar 1 ’den başlasaydı ne olurdu? Aslında bu çok büyük problemlere neden olmazdı. Bazı teknik tanımların ufak tefek değişmesi gerekirdi. Ama ortada bir yerdeki sayıyı (örneğin 2, 5, 29, 750 gibi) doğal sayı olarak kabul etmeseydik işte o zaman büyük sorunlar ortaya çıkardı. Çünkü 0 ’ı gözardı ederek doğal sayı *yapısını* yine koruyabiliriz. Yeter ki ortaya çıkan şey Peano aksiyomlarını sağlasın. Peano aksiyomlarını sağlayan matematiksel yapılara zaten *doğal sayı yapısı* diyoruz. Hepsinin ortak özelliği, hiçbir ögenin ardılı olmayan en küçük bir ögenin var olması. Diyelim ki 0 ’ı doğal sayı olarak kabul etmedik. Sorun değil; 1 ’den başlarız ve 0 ’ın doğal sayı yapısı içindeki “en küçük öge” olma rolünü 1 ’e vermiş oluruz. $0,1,2,3,\dots$ yerine $1,2,3,4,\dots$ diye devam eden bir yapı elde ederiz. Ne de olsa yine her sayı ardılık ilişkisi içinde ardışık olarak tanımlı. Yine herhangi

ardışık iki doğal sayının arasında başka bir doğal sayı yok. Yine en büyük doğal sayı diye bir şey yok.

Beyin jimnastiği yaptıracak bir şey söyleyeyim. Aslında Peano aksiyomlarını sağlayan yapının öğelerinin birer 'sayı' olmasına da gerek yok. 0'ın rolünü hiç çubuk, 1'in rolünü bir çubuk, 2'nin rolünü iki çubuk, 3'ün rolünü üç çubuk vs. alabilir. Bir çubuğun *ardılı*nı, o çubuğun yanına başka bir çubuk bitiştirmek olarak kabul edelim. Alın size doğal sayılar yapısı!

0 bir doğal sayıdır, aksiyom gereği böyle. Ancak gördüğümüz gibi, aksini düşünmek doğal sayılar yapısını bozan bir şey değildir. 0'ın kendisi olmasa da olur. Yeter ki yapı içinde 0'ın rolünü üstlenecek bir öge olsun. Diyebiliriz ki 0'ı kabul etmek zorunluluk değildir ama 0'ın rolünü alacak bir ögenin var olması bir zorunluluktur.

■ “Tanımsız” ile “Belirsiz” Arasındaki Fark Nedir?

Matematiğin tanımlarla ve aksiyomlarla başladığını söylemiştik. Bazen bir şey tanımlamak, mevcut kuramımızda çelişkilere neden olabilir. Örneğin, $\mathbb{R}$ (yani reel sayılar) üzerinde tanımlı olan $f(x) = 1/x$ fonksiyonunun tanım kümesi aslında $\mathbb{R} \setminus \{0\}$ kümesidir. Yani $f(0)$ tanımsızdır, çünkü $1/0$ tanımsız bir ifadedir. Verilen bir n sayısı için $n/0$ tanımlı olsaydı ne olurdu? Bir defa bu saçmalıklara sebep olurdu. Diyelim ki $a = b = 1$ olsun. Şimdi $a = b$ eşitliğinin her iki tarafını a ile çarpalım ve $a^2 = ab$ elde edelim. Her iki taraftan ab çıkaralım ve $a^2 - ab = 0$ elde edelim. Bu da $a(a - b) = 0$ ifadesine eşittir. Şimdi eşitliğin her iki tarafını $(a - b)$ ifadesine bölersek $a = 0$ olarak buluruz. Ama başta $a = 1$ olarak kabul etmiştik. Saçmalık elde ettik. $n/0$ ifadesi aritmetikte ya da cebirde anlamlı bir şekilde tanımlanamaz. Sıfıra bölmeyi geçerli kabul edersek işte böyle çelişkiler bulabiliriz. Analizde ise $n/0$ ifadesi ∞ olarak tanımlıdır, ancak orada fonksiyonların limitteki davranışını dikkate alırız.

Peki, $x^2 + 1 = 0$ denkleminin reel sayılarda çözümünün olmadığını biliyoruz. Ancak sonradan $i = \sqrt{-1}$ diye bir sayı tanımlamışız. Aynen bunun gibi $n/0$ ifadesinin sonucunu yapay bir şekilde tanımlayamaz mıyız? Tanımlayabiliriz elbette. Şimdi ben yeni bir “sayı” tanımlıyorum ve adına h diyorum. Bu bildiğimiz anlamda bir sayı değil, bir değer de değil, bir sabit olsun belki. Artık $n/0$ tanımlı bir ifade. Tamam ama ne işime yaradı bu? İşte, matematikte istediğiniz şeyi (mevcut kuramlarınızla tutarlı olmak kaydıyla) tanımlayıp kendi matematiğinizi yapabilirsiniz. Ancak bunu dünya kabul edecek diye bir şey yok. Tanımsız ifadeleri geleneksel anlamda tanımlamaya çalıştığımızda yukarıda yaptığımız kanıt gibi ortaya anlamsızlıklar çıkarabiliriz. Bir şeyin tanımsız olması demek, “anlamlı” bir açıklaması yapılamaz demektir. Elbette kafamızdan bir sembol uydurup, buna örneğin h ismi verip, bunu $n/0$ 'nin tanımı olarak kabul edebiliriz. Ancak bu hiçbir işimize yaramaz, en azından şu anda.

Belirsizlik ise biraz daha farklı bir kavram. Bir ifadenin tek değil, birçok (çoğunlukla sonsuz sayıda) anlamlı tanımı varsa ya da birçok çözümü varsa buna *belirsizlik* diyebiliriz. Örneğin, $\infty - \infty$ ifadesinin tek bir anlamlı sonucu yoktur. Olamayacağını burada sadece sezgisel olarak anlatmaya çalışacağım. Bu fark işleminin sonucu neden 1 olmasın? Ya da neden 2, 3, 4 vs. olmasın? Kümelerle anlamaya çalışalım. $A = \{0, 1, 2, 3, 4, \dots\}$ ve $B = \{1, 2, 3, 4, \dots\}$ olsun. Buna göre $A \setminus B = \{0\}$ olur ki bu da tek elemanlıdır. Ancak $B = \{2, 3, 4, 5, \dots\}$ olsaydı $A \setminus B = \{0, 1\}$ olurdu ki bu da bize 2 elemanlı bir küme verirdi. Şimdi $A = \{0, 1, 2, 3, 4, \dots\}$ ve $B = \{0, 2, 4, 6, 8, \dots\}$ olsun. Bu durumda $A \setminus B = \{1, 3, 5, 7, 9, \dots\}$ olur ki bu da sonsuz elemanlı bir küme verir. Demek ki kümelerle uygulandığında $\infty - \infty$ ifadesinin tek bir sonucu tanımlanamıyor. Analizde de durum farksız değildir.

■ 0^0 Neye Eşittir?

Negatif olmayan herhangi bir a sayısı için a^0 ifadesinin cebirsel olarak ne tür anlamlara karşılık geldiğine bakalım. a^0 ifadesi a sayısının 0 kez çarpımıdır; yani hiçbir şey çarpmamaktır. Çarpmanın birim elemanı 1 olduğu için, cebirde $0^0 = 1$ tanımı yapılmıştır. Küme kuramsal olarak da a^0 ifadesini yorumlamak mümkündür; şöyle ki a^0 ifadesi, 0 elemanlı bir kümeden a elemanlı bir kümeye olan fonksiyonların sayısıdır. Böyle sadece bir tane fonksiyon vardır, o da *boş fonksiyon* denilen fonksiyondur.

Öte yandan analizde 0^0 ifadesi belirsiz forma sahiptir. Yani, $f(x)$ ve $g(x)$ birer fonksiyon olsun ve $\lim_{x \rightarrow a} f(x) = 0$, $\lim_{x \rightarrow a} g(x) = 0$ olsun. Bu durumda $\lim_{x \rightarrow a} f(x)^{g(x)}$ ifadesinin sonucunu her zaman tek biçimde belirleyemeyiz. Örneğin, $\lim_{x \rightarrow 0^+} x^0 = 1$ iken, $\lim_{x \rightarrow 0^+} 0^x = 0$ oluyor. Bu yüzden 0^0 ifadesini

matematiğin bazı alanlarında 1 olarak tanımlamak anlamlıyken, analiz gibi diğer alanlarda anlamlı bir tanımlama yapmak mümkün olmayabiliyor.

■ Tam Sayıların Toplamı Sıfır Mıdır?

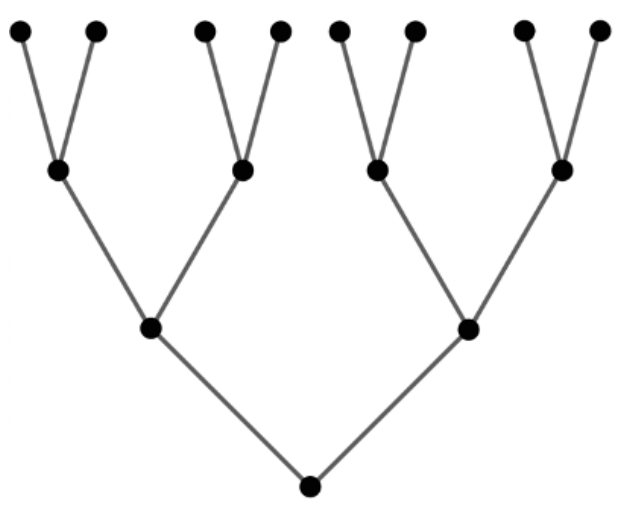
Pozitif ve negatif sayılar birbirini götürdüğü için bütün tam sayıların toplamının sıfır olduğunu zannedebilirsiniz. Ancak sonsuz toplamda işler sanıldığı gibi olmuyor. Elbette

$$0 + 1 + (-1) + 2 + (-2) + 3 + (-3) + \dots$$

gibi bir parantezleme yapılırsa pozitif sayılar ve negatif sayılar birbirini götürür ve sonuç sıfır olur diye düşünürsünüz. Ancak

$$(0 + 1) + (-1 + 2) + (-2 + 3) + (-3 + 4) + \dots$$

şeklinde bir parantezleme yapılırsa bu toplam sonsuza yaklaşır. İddia ediyorum ki başka türlü parantezleme yapıldığında toplam, eksi sonsuza yaklaşır. İşin özü, sonsuz toplam sonlu toplam sezgisiyle tanımlanabilecek bir işlem değildir. Sonlu şeyler arasındaki özellikleri, onlarla ilgili kullandığımız sezgileri sonsuz büyüklükteki şeylere her zaman uyarlayamayacağımızı gösteren bir başka örnek vermek istiyorum. Matematikteki ağaç yapılarını ele alalım.



Bu yapının sonsuza kadar yukarı doğru devam ettiğini düşünelim. En alttaki başlangıç noktasının hizası 0. kademe olsun. 1'inci kademe 2 nokta, 2'nci kademe 4 nokta, 3'üncü kademe 8 nokta var vs. Genellersek, n 'inci kademe 2^n nokta var. Hatta, n 'inci kademe kadarki dalların sayısı, n 'inci kademedeki noktaların sayısından daha fazla. Örneğin, 2'nci kademe 4 nokta varken bu kademenin altında toplamda 6 dal var. Matematiksel tümevarımla her sonlu n için bunun doğru olduğunu kanıtlayabiliriz. Ancak n sonsuza yaklaştığında aynı sonucu söylemek mümkün değil. Sonlu durumlar için olan bazı matematiksel gerçeklerin altındaki sezgilerimizi, sonsuzdaki ya da sonsuza yaklaşırken olan durumlara uygulamak bizi hataya sevk edebiliyor.

■ 1^∞ Neden Belirsizdir?

Herhangi bir n doğal sayısı için $1^n = 1$ olduğunu biliyoruz. Ancak analizde, $\lim_{x \rightarrow a} f(x) = 1$ ve $\lim_{x \rightarrow a} g(x) = \infty$ ise, $\lim_{x \rightarrow a} f(x)^{g(x)}$ değeri belirsizdir. Bunun sebebi, bu limit değerinin, taban olan $f(x)$ 'in 1'e ne kadar hızlı yaklaştığına ve üs olan $g(x)$ 'in sonsuza ne kadar hızlı büyüdüğüne bağlı olmasıdır. 1^∞ ifadesinin belirsiz olduğunu anlamak için önce şu örneğe bakalım: $c \in \mathbb{R}$ olsun. Buna göre $\lim_{x \rightarrow 0^+} (e^x)^{\frac{c}{x}}$ değeri ne olmalıdır? Taban 1'e yaklaşırken üs (pozitif veya negatif olmasına bağlı olarak) $\pm\infty$ 'a yaklaşır. 1^∞ formuna sahip bu limiti hesaplamak neyse ki zor değil. Üs özelliklerini kullanarak

$$\lim_{x \rightarrow 0^+} (e^x)^{\frac{c}{x}} = \lim_{x \rightarrow 0^+} e^{x \cdot \frac{c}{x}} = \lim_{x \rightarrow 0^+} e^c = e^c.$$

Herhangi bir $c \in \mathbb{R}$ için bu limitin değeri değişiyor. Elbette taban 1 ile sabit olduğu zaman $\lim_{x \rightarrow \infty} 1^\infty = 1$ olur. Ancak buradaki mesele, yukarıda söz ettiğimiz gibi, $f(x)$ fonksiyonunun 1'e soldan veya sağdan durumlarda $g(x)$ üs fonksiyonunun limit değerini farklı şekilde belirlemesidir. Örneğin, $\lim_{x \rightarrow \infty} 0,999^x = 0$ iken, $\lim_{x \rightarrow \infty} 1,001^x = \infty$ olur. Taban 1'e yaklaşırken üs sonsuza yaklaştığında bu uyumsuzluktan dolayı 1^∞ formu belirsizdir.

Belki de bu yüzden yalnızca cesurların işidir kanıt

ORHAN OĞULCAN TUNCER

Hacettepe Üniversitesi Matematik Bölümü

✉ otuncer@hacettepe.edu.tr



İngiliz Matematikçi Sir Michael Francis Atiyah'ın (1929-2019) sözleriyle,

“Kanıt, matematiği bir arada tutan yapıştırıcıdır.”

Bu ifadeyle Atiyah, etkileyici bir metafor yapmanın ötesinde, matematiğin en önemli yapıtaşının kanıt olduğuna işaret ediyordu. Elbette bu demek değil ki matematik yalnızca kanıttan ibarettir ya da bir matematikçi gününün her saatini önerme kanıtlayarak geçirir. Neticede matematik, teknik hesaplamalar yapmaktan karşıt örnekler oluşturmaya, algoritmalar bulmaktan özel durumlar incelemeye ya da modeller yapmaya kadar çok çeşitli uğraşlar da barındıran bir disiplindir. Yine de matematiği diğer disiplinlerden ayıran temel unsur, kanıt ve mantıksal gerekçelendirmeye sıkı sıkıya bağlı olmasıdır.

Kanıt, yalnızca bir sonucun doğruluğunu garanti altına almak için değil, aynı zamanda düşünce sürecindeki mantıksal yolculuğu aktarmak için de kullanılır. Bu sebeple matematik ve mantığı birbirinden tamamen ayırmak imkansızdır. Bu ilişkiyi belki de en iyi açıklayan, Filozof ve Matematikçi Bertrand Russell (1872-1970)'in şu sözleridir:

“Tarihsel olarak bakıldığında, matematik ve mantık tamamen farklı alanlar olarak görülmüştür. Matematik, bilimle ilişkilendirilirken; mantık, Antik Yunan’la bağdaştırılmıştır. Ancak her iki alan da modern zamanlarda önemli bir gelişim göstermiştir: mantık daha matematiksel bir nitelik kazanmış, matematik ise daha mantığa dayalı hâle gelmiştir. Sonuç olarak artık bu ikisi arasında kesin bir çizgi çekmek tamamen imkânsız olmuştur; gerçekte, ikisi bir ve aynıdır. Aralarındaki fark, çocuk ile yetişkin arasındaki fark gibidir: mantık, matematiğin gençliğidir; matematik ise mantığın olgunluk çağıdır.”

Bu yazının içinde birkaç önermenin bazı iyi bilinen kanıtlarından bahsedeceğiz. Ele alacağımız önermelerin kanıtları basit ve kolay anlaşılır olacaklar. Ancak bazı kanıtlar çok daha karmaşık olup sayfalarca hatta ciltlerce süren mantıksal ilerlemeler gerektirebilir. Dolayısıyla matematikte bir önermeyi kanıtlamak için, uzun ve soyut bir düşünme sürecine, sabırlı bir akıl yürütmeye ve kimi zaman detaylar içinde kaybolmadan ilerleyebilecek zihinsel bir dayanıklılığa hazır olmak gereklidir, ama tabii ki yeterli değildir. Nitekim bu zihinsel çabanın zorluğunu Charles Darwin şu şekilde ifade eder: “Soyut bir düşünce zincirini uzun süre takip etme gücüm sınırlı; bu yüzden metafizik ya da matematikte asla başarılı olamazdım.”

O halde esas sorumuza gelmiş bulunmaktayız: Matematiksel kanıt *tam olarak* nedir?

Russell herhangi bir önermeyi kanıtlamaya yeltenen bir matematikçinin asla muhakeme sürecinin tamamını kağıda dökemeyeceğini, bunun yerine uygun şekilde eğitilmiş bir zihni ikna etmeye yetecek kadar bir kanıt özeti ile yetinilmesi gerektiğini söylemiştir. Çünkü her önerme, daha önceki tanım ve önermelere dayanır. Onlar da başka tanım ve önermelere... Bir kanıtın, dayandığı tüm tanım ve kabulleri baştan sona eksiksiz biçimde içermesini şart koşmak, hem pratikte mümkün değildir hem de gereksiz bir çaba olur. Kendi önerilerini pek de ciddiye almadığı apaçık olan Russell, Alfred North Whitehead ile birlikte yazdığı *Principia Mathematica* kitabında, matematiğin tümünü en küçük ayrıntıları bile göz ardı etmeden temel mantıksal ilkelere indirgemeye çalışmıştır. Öyle ki $1 + 1 = 2$ ifadesini mantıksal ilkelerle elde etmeleri yüzlerce sayfa sürmüştür.

Dolayısıyla biz bu yazıda Russell’ın ilk önerisini dikkate alarak aklımıza mukayet olmaya çalışacağız. Bu bağlamda bir kanıt, bir önermenin doğruluğuna itiraz edilemeyecek şekilde ikna eden, mantık kuralları çerçevesinde inşa edilmiş tutarlı bir akıl yürütme olarak tanımlayabiliriz.¹

Alternatif olarak matematiksel bir kanıtın ne *olmadığını* da tartışabiliriz. Kanıt, sezgiye ya da sağduyuya yapılan başvurularla kurulmaz. “Bana mantıklı geliyor” ya da “herkes böyle düşünüyor” gibi ifadeler matematiksel geçerlilik taşımaz. Aynı şekilde, bir öğretmenin ya da otoritenin sözü de tek başına bir kanıt sayılmaz. Kanıt, yalnızca kuralları açık ve tutarlı biçimde tanımlanmış mantıksal bir sistem içinde geçerlidir.

Sonuç olarak, kanıt matematiksel düşüncenin omurgasıdır. Öğrenciler için bu, sadece kuralları uygulamak değil, bu kuralları neden uyguladığımızı sorgulamak anlamına gelir. Bir problemi çözmekle yetinmek değil, o çözümün neden ve nasıl çalıştığını görmek demektir. Matematiksel kanıt, sadece bilgi değil; düşünce üretmenin, paylaşmanın ve eleştirmenin en rafine yollarından biridir. Ve bu yönüyle matematik, yalnızca bir bilim değil, aynı zamanda bir düşünme biçimidir.

Şimdi yukarıda tartıştıklarımızı somut hale getirecek ve örneklerle destekleyeceğiz. Ayrıca bazı temel kanıt tekniklerinden bahsedeceğiz.

1. Belli durumlar için sağlanması yeterli değil.

Bir önermenin doğruluğunu göstermek üzere çıkılan yolda en sık yapılan hatalardan biri, önermenin birkaç özel durumda sağlandığını görüp bunu genel geçer bir doğru olarak kabul etmektir. Oysa matematikçiler için bu tür örnekler, ancak nihai kanıt inşa etmede yol gösterici olabilir; kendileri başlı başına bir kanıt sayılmaz. Bir örnek ele alalım:

İddia 1.

n , 1’den büyük bir tam sayı olsun. Eğer n asal sayı ise $2^n - 1$ de asal sayıdır.

Bu iddianın doğruluğu için ne dersiniz? Bunu görmek için bariz ve oldukça mantıklı olan bir yöntem birkaç asal sayı için yukarıdaki önermenin doğru olup olmadığını incelemektir.

- $n = 2$ asal sayısı için $2^n - 1 = 3$ olup 3 asal sayı olduğundan önerme gerçekleşir.
- $n = 3$ asal sayısı için $2^n - 1 = 7$ olup 7 asal sayı olduğundan önerme gerçekleşir.
- $n = 5$ asal sayısı için $2^n - 1 = 31$ olup 31 asal sayı olduğundan önerme gerçekleşir.
- $n = 7$ asal sayısı için $2^n - 1 = 127$ olup 127 asal sayı olduğundan önerme gerçekleşir.

Buraya kadar işler çok yolunda gidiyor. Dolayısıyla birçoğunuz önermenin doğru olduğunu düşünmeye başlamış bile olabilirsiniz. Şimdi $n = 11$ asal sayısını ele alalım. Bu durumda $2^{11} - 1 = 2047$ olup $2047 = 23 \cdot 89$ yazılabildiğinden, n asal olmasına rağmen $2^n - 1$ asal olmaz. Dolayısıyla birkaç durum için sağlanan bu önermeyi her n asal sayısı için doğru kabul edemeyiz. Yine de yalnızca 5. denemede önermenin sağlanmadığını görmüş olduk ve daha fazla deneme yapmamıza gerek kalmadı.

Şimdi başka bir örnek ele alalım:

İddia 2.

n negatif olmayan bir tam sayı olsun. Bu durumda $n^2 + n + 41$ bir asal sayıdır.

Bir önceki iddiayı incelerken yaptığımız gibi bir noktadan başlayarak denemeler yapalım. n bir negatif olmayan tam sayı olduğundan 0’dan başlamak uygun olacaktır.

- $n = 0$ için $0^2 + 0 + 41 = 41$ olup 41 bir asal sayıdır.
- $n = 1$ için $1^2 + 1 + 41 = 43$ olup 43 bir asal sayıdır.
- $n = 2$ için $2^2 + 2 + 41 = 47$ olup 47 bir asal sayıdır.
- $n = 3$ için $3^2 + 3 + 41 = 53$ olup 53 bir asal sayıdır.

¹Tabii bu tanım başka başka sorular doğurmaktadır. Ancak bunların detayına girmeyeceğiz.

- $n = 4$ için $4^2 + 4 + 41 = 61$ olup 61 bir asal sayıdır.
- $n = 5$ için $5^2 + 5 + 41 = 71$ olup 71 bir asal sayıdır.
- $n = 6$ için $6^2 + 6 + 41 = 83$ olup 83 bir asal sayıdır.
- $\vdots$
- $n = 39$ için $39^2 + 39 + 41 = 1601$ olup 1601 bir asal sayıdır.

Dolayısıyla 0 ile 39 arasındaki tüm tam sayılar için önerme gerçekleşmektedir. Yine de bu, önermenin doğru olduğu anlamına gelmez! Zira $n = 40$ için $40^2 + 40 + 41 = 1681 = 41 \cdot 41$ olup asal değildir. Bir önceki örneğin aksine burada önermenin doğru olmadığı sonucuna ulaşmak için 41 deneme yapmamız gerekti. Peki bu denemeyi nereye kadar yapabiliriz?

2. Yalnızca bir aksine örnek yeterlidir.

Bir önceki bölümde İddia 1’de verilen önermeyi ve İddia 2’de verilen önermeyi sağlamayan en az birer örnek olduğunu görmüş olduk. Buna matematikte *aksine örnek* (ya da karşı örnek, ters örnek; ing. counterexample) adı verilir. O halde, bir önermeyi kanıtlamak için istisnasız her durumu kapsayacak bir gerekçe ortaya koymak gerekirken, önermenin yanlışlığını göstermek için *yalnızca bir aksine örnek* yeterlidir. İddia 1’de $n = 11$ aksine örnek iken, İddia 2’de $n = 40$ aksine örnektir. Tabii ki başka aksine örnekler vermek mümkündür.

Dolayısıyla bir önermenin doğruluğunu kanıtlamak sayfalarca sürebilirken, tek satırlık bir aksine örnek önermenin yanlış olduğunu göstermeye yeterlidir. Ancak aksine örnek bulmak her zaman görüldüğü kadar kolay olmayabilir. Bu durumu bir örnekle görelim.

Euler² şu varsayımda bulunmuştur: *En az üç pozitif tam sayının küpleri toplanarak başka bir pozitif tam sayının kübü elde edilebilir.* Örneğin $3^3 + 4^3 + 5^3 = 27 + 63 + 125 = 216$ olup $216 = 6^3$ yazılabilir. Dolayısıyla bu örnekte üç tane pozitif tam sayının kübü toplanarak başka bir pozitif tam sayının kübü elde edilmiş oldu. Daha sonra Euler, iki tane pozitif tam sayının kübü toplanarak bir tam küp elde edilemeyeceğini kanıtladı³.

Bu durumu bir üst kuvvete taşırsak; dördüncü kuvvetlerinin toplamı bir başka tam sayının dördüncü kuvvetini verecek şekilde dört tane tam sayı bulabiliriz. Örneğin $30^4 + 120^4 + 272^4 + 315^4 = 353^4$ yazılabilir. Euler, üç tane tam sayının dördüncü kuvveti toplanarak başka bir tam sayının dördüncü kuvveti elde edilemeyeceğini iddia etti. Hatta varsayımını şu şekilde genelledi: $n \geq 2$ olmak üzere, *en az n tane pozitif tam sayının n -inci kuvvetleri toplanarak başka bir pozitif tam sayının n -inci kuvveti elde edilebilir.* Bir başka deyişle bir pozitif tam sayının n -inci kuvveti n ’den daha az pozitif tam sayının n -inci kuvvetlerinin toplamı olarak yazılamaz.

Euler’in bu iddiası 200 yıl boyunca ne kanıtlanabildi ne de çürütülebildi. Ta ki 1966 yılında iki matematikçi $27^5 + 84^5 + 110^5 + 133^5 = 144^5$ olduğunu gösterene kadar. Bu örnekle birlikte bir pozitif tam sayının 5. kuvvetinin dört tane pozitif tam sayının 5. kuvvetlerinin toplamı olarak yazılabildiği gösterilmiş oldu. Dolayısıyla Euler’in iddiasının $n = 5$ için yanlış olduğu aksine örnek ile kanıtlandı. Daha sonra bilgisayar gücüyle birlikte daha ilginç bir örnek olarak $95800^4 + 217519^4 + 414560^4 = 422481^4$ olduğu gösterildi. Dolayısıyla bir pozitif tam sayının 4. kuvvetinin üç tane pozitif tam sayının 4. kuvvetlerinin toplamı olarak yazılabildiği gösterilmiş oldu, ki bu Euler’in iddiasının $n = 4$ için de yanlış olduğu anlamına gelmekteydi.

Kıssadan hisse: Bazen önerme çürütmek, kanıtlamaktan daha zordur!

3. Nasıl başlayacağını bilmek...

Buraya kadar bir önermenin nasıl kanıtlanamayacağını ve nasıl çürütülebileceğini gördük. Şimdi ise bir önermenin nasıl kanıtlanabileceği hakkında konuşacağız.

Daha önce de söylediğimiz gibi, matematiksel bir kanıt yalnızca bir sonucun doğru olduğunu söylemek değildir; o sonucun neden doğru olduğunu, nasıl doğru olduğunu mantıklı, adım adım bir akıl yürütmeye göstermektir. Matematikte birçok kanıt tekniği mevcuttur. Ancak bu tekniklerin hepsini bilmek, karşılaştığınız her önermeyi kolayca kanıtlayabileceğiniz anlamına gelmez. Matematiği bu kadar ilgi çekici

²Leonhard Euler (1707–1783), modern matematiğin birçok alanının temellerini atan, üretkenliği ve derinliğiyle tanınan İsviçreli bir matematikçidir.

³Bu Fermat’ın son teoreminin bir özel halidir.

kılan şeylerden biri de budur. Bu nedenle, bu yazıda size kanıt yapmaya dair eksiksiz bir *reçete* sunmayı vaat etmediğimi belirtmek isterim! Yine de matematiksel kanıt sürecinde işleri kolaylaştırabilecek bazı yöntemlerden ve temel fikirlerden yazının ilerleyen bölümlerinde söz edeceğim. Bu yöntemlerin hangisinin elinizdeki önermeyi kanıtlamak için uygun olduğunu anlamak zamanla gelişen bir beceridir. Biraz alışkanlık, biraz sabır ve bolca deneme yanılma gerektirir. Ve tüm bunlara rağmen, bazen hangi yöntemle ilerleyeceğiniz hemen belli olmayabilir. Çinli filozof Lao Tzu’nun sözleriyle

“Binlerce kilometrelik bir yolculuk bile tek bir adımla başlar.”

Bir kanıtı binlerce kilometrelik bir yolculuk olarak düşünürsek, bu yolu tamamlamak için ilk adımı doğru atmak oldukça önemlidir. Ancak neyse ki matematik bize kanıtın herhangi bir anında en başa dönme, farklı yaklaşımlar deneme, hatta tamamen geri çekilip başka bir yoldan ilerleme imkânı sunar.

Aşağıda, kanıt yaparken size yardımcı olabilecek bazı temel öneriler vereceğim. Bu adımlar her zaman sıralı biçimde uygulanmak zorunda değil; ama genellikle bir önermeyle baş başa kaldığınızda işe yarayan yöntemlerdir. Yine de bu önerilerin her zaman yeterli olmayacağını bilmekte fayda var!

- *Önerme açık değilse, sadeleştirin.*
Eğer önerme size karmaşık geliyorsa ya da kullanılan terimlere tam olarak hâkim değilseniz, onu kendi anlayacağınız şekilde yeniden ifade edin. Gerekirse matematiksel dili geçici olarak bırakıp, günlük bir dille “ne demek isteniyor?” sorusunu kendinize sorun. Örneğin, türevle ilgili “türev operatörü lineerdir” ifadesi kulağa teknik gelebilir; ancak bunu “türevlerin toplamı, toplamın türevidir” biçiminde sadeleştirmek faydalı olabilir.
- *Hangi varsayımların verildiğini, hipotezin ne olduğunu, bir başka deyişle kanıtlanması istenen şeyin hangi koşullar altında verildiğini belirleyin.*
Birçok kanıt girişimi, yalnızca tanımlar üzerinden ya da hiçbir varsayım kullanılmadan yapılmaya çalışılır ve bu çoğu zaman başarısız olur. Size bir öncül verildiyse, örneğin “ n bir çift tam sayı olsun. Bu durumda ...” gibi, işe oradan başlayın.
- *İstenen şeyi açıkça belirleyin.*
Kanıtlamanız gereken ifadenin tam olarak ne olduğunu netleştirin. Ne zaman “Ben ne bulmaya çalışıyordum?” sorusunu sormaya başlarsanız, büyük ihtimalle yolunuzu kaybetmişsinizdir.
- *Konuya dair bildiklerinizi gözden geçirin.*
Kanıtlamaya çalıştığınız önermenin hipoteziyle ilgili (hatta bu hipotezi doğrudan içeren) ve bulmaya çalıştığınız sonucu da ilgilendirebilecek bilinen teoremleri gözden geçirin. Önermedeki matematiksel terimlerin tanımlarını iyi bilin ya da bu tanımları tekrar okuyun. Ayrıca hipotezi ve kanıtlanacak ifadeyi (ifadedeki terimlerin tanımlarıyla birlikte) iyi bir notasyon seçerek düzgün bir şekilde ifade edin.
- *Kendinize şu soruyu sorun: Bu ifade neden doğru olmalı?*
Bu soru, kanıt yapmanın en temel noktalarından biridir. Eğer bir ifadenin neden doğru olduğunu içten içe anlayamıyorsanız, onu kanıtlamaya çalışmak çok zordur. Bu durumda kendinize örnekler oluşturun, gerekirse bir şekil çizin, özel durumlar için önermenizi test edin. Anlamadan ispatlamak neredeyse imkânsızdır. Ama eğer içsel olarak doğru olduğuna ikna olduysanız, geriye kalan şey bunu teknik bir dille anlatmak olur. Bu teknik beceriler zamanla kazanılır; ama sezgisel anlayış çoğu zaman çok daha önceden gelişir.

Eminim ki bu listeye eklenecek çok şey var. Fakat unutmayalım ki bu listenin işe yarayıp yaramadığını denemeden, çabalamadan, vakit ayırmadan göremezsiniz. Bu listeye ünlü Fransız besteci ve piyanist Maurice Ravel’in şu sözüyle de bir katkıda bulunabiliriz:

“Kopyalayın. Eğer içinizde biraz özgünlüğünüz varsa, bu kopyaladıkça ortaya çıkar. Eğer yoksa, sorun değil.”

Gerçekten öğrenmenin ve gelişimin en doğal yollarından biri taklit etmek, kopyalamaktır. Benzer önermelerin kanıtlarını incelemek ve bu kanıtlarda izlenen yolları uyarlayarak elinizdeki önermeyi kanıtlamaya çalışmak oldukça öğreticidir. Eğer içinizde bir parça özgünlük varsa, bu zaten ortaya çıkacaktır. Yoksa bile

sorun değil, bunun bir öğrenme basamağı olduğunu bilip devam etmek gerekir. Son olarak, bu belki gereksiz bir tavsiye gibi görünebilir; ancak bence en önemlisi: YAZIN! Yazmadan matematik olmaz. Elinizde zaten yazılı bir şey varsa bile, onu tekrar yazın. Her çalıştığınızda gerekirse bir daha yazın. Çünkü düşünce, ancak kâğıda döküldüğünde gerçekten şekillenir.

Şimdi birkaç tane nispeten basit önermeyi sözlü bir şekilde anlatır gibi kanıtlamaya çalışacağım.

Teorem 1.

n bir pozitif tam sayı olmak üzere, $1 + 2 + \dots + n = \frac{n(n+1)}{2}$.

Kanıt. Teoremin ifadesini birlikte anlamaya çalışalım. n sayısının bir pozitif tam sayı olduğu verilmiş. Yani n sayısının $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ kümesinden *keyfi* bir sayı olduğu biliniyor. Bu durumda n sayısına kadar olan tüm pozitif tam sayıların toplamının, n sayısı ile 1 fazlasının çarpımının yarısına eşit olduğu iddia ediliyor. Birkaç örnekle durumu daha iyi anlamaya çalışalım:

$$\begin{aligned} n = 1 \text{ için } 1 &= \frac{1 \cdot 2}{2}, \\ n = 2 \text{ için } 1 + 2 &= 3 = \frac{2 \cdot 3}{2}, \\ n = 3 \text{ için } 1 + 2 + 3 &= 6 = \frac{3 \cdot 4}{2}, \\ n = 4 \text{ için } 1 + 2 + 3 + 4 &= 10 = \frac{4 \cdot 5}{2}. \end{aligned}$$

Yukarıdaki örnekler teorem için bir kanıt vermese de teoremin ifadesini anlamak için önemlidir. Şimdi verilen önermenin her n pozitif sayısı için doğru olduğunu kanıtlayalım.

$$1 + 2 + \dots + (n-1) + n = S$$

diyelim. Açıkça görülür ki

$$n + (n-1) + \dots + 2 + 1 = S$$

sağlanır. Çünkü tam sayılar için toplama işlemi değişmelidir, yani aynı tam sayıları hangi sırada topladığımızın bir önemi yoktur. O halde

$$\begin{aligned} 1 + 2 + \dots + (n-1) + n &= S, \\ n + (n-1) + \dots + 2 + 1 &= S \end{aligned}$$

bulunur. İki denklemi taraf tarafa toplarsak

$$(n+1) + (n+1) + \dots + (n+1) + (n+1) = 2S$$

elde ederiz. Bu denklemde n tane $(n+1)$ olduğunu görebildiniz mi? Buradan $n(n+1) = 2S$ olup dolayısıyla $S = n(n+1)/2$ bulunur. Sonuç olarak $1 + 2 + \dots + n = S = n(n+1)/2$ eşitliğine ulaşılır. $\square$

Teorem 2.

$Ax^2 + Bx + C$ ikinci dereceden bir polinom olmak üzere (yani $A \neq 0$), bu polinomun gerçel sayılar üzerinde ya kökü yoktur, ya $x = -\frac{B}{2A}$ ile verilen biricik kökü vardır ya da

$$x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$$

ile verilen iki farklı kökü vardır.

Kanıt. İkinci dereceden tek değişkenli bir polinomun kökleri için yukarıda verilen formülü birçoğunuzun

ezbere bildiğine yemin edebilirim, ama kanıtlayamam :) Fakat bu formülün nereden geldiğini kanıtlayabilirim.

$Ax^2 + Bx + C$ polinomunun köklerini aramak, $Ax^2 + Bx + C = 0$ denkleminin çözümlerini aramak ile aynı şeydir. Burada $A \neq 0$ olması, denklemin ikinci dereceden olması için gereklidir. Aksi takdirde $Bx + C = 0$ formunda x 'in kuvvetlerine göre en fazla birinci dereceden olan bir denklem elde edilir. Peki $Ax^2 + Bx + C = 0$ denkleminin çözümlerini nasıl bulabiliriz? En genel ikinci dereceden denklem yerine çok daha basit bir denklem ele alalım: $x^2 = a^2$. Bu denklemin çözümü için ne dersiniz? İki sayının karelerinin birbirine eşit olması için bu sayıların ya aynı ya da birbirlerinin zıt işaretlisi olması gerekir, değil mi? Yani $x = a$ ya da $x = -a$ olmalıdır. Şimdi $(x + b)^2 = a^2$ ikinci derece denklemini düşünelim. Biraz önceki duruma benzer şekilde $x + b = a$ ya da $x + b = -a$ olmalıdır. Yani bu denklemin çözümleri $x = a - b$ ve $x = -a - b$ biçimindedir. Dolayısıyla eğer denklemde x 'li terimlerin bir tam karesi varsa, bu durumda denklemi nasıl çözeceğimizi daha rahat kestirebiliriz!

Tekrar $Ax^2 + Bx + C = 0$ denkleminde x 'li terimlerin bir tam karesi olmadığı açıktır. Ancak tabii ki denklemin sol tarafını tam kareye tamamlamak mümkündür. Bu işleme geçmeden önce denklemin her iki tarafını A sayısına bölelim. A sayısı sıfırdan farklı olduğundan bunu yapabiliriz. Bunu yapmamızın sebebi tam kareye tamamlama işlemini basitleştirmektir. Böylece

$$x^2 + \frac{B}{A}x + \frac{C}{A} = 0$$

denkleminde ulaşırız. Bu denklem ile orijinal denklemimizin kökleri aynıdır. Şimdi denklemin sol tarafını tam kareye tamamlayalım:

$$x^2 + \frac{B}{A}x + \frac{C}{A} = \left(x + \frac{B}{2A}\right)^2 - \frac{B^2}{4A^2} + \frac{C}{A} = 0.$$

Buradan, neden ilk denklemi A sayısına böldüğümüz daha iyi anlaşılmış olmalı. Şimdi yukarıdaki denklemi düzenleyelim:

$$\left(x + \frac{B}{2A}\right)^2 = \frac{B^2 - 4AC}{4A^2}.$$

O halde bu denklemin kökleriyle orijinal denklemin kökleri aynıdır. Şimdi bu denklemin köklerini araştıralım. Denklemin sol tarafı bir gerçel sayının karesi olduğundan negatif bir sayı olamaz. Bu sebeple eğer denklemin sağ tarafı negatifse, yani $B^2 - 4AC < 0$ ise denklemin kökü yoktur! Eğer denklemin sağ tarafı sıfırsa, yani $B^2 - 4AC = 0$ ise bu durumda

$$\left(x + \frac{B}{2A}\right)^2 = 0$$

olup bu denklemin tek kökü $x = -\frac{B}{2A}$ 'dır. Diğer yandan $B^2 - 4AC > 0$ ise bu durumda yukarıda yaptığımız basit örneklere benzer şekilde

$$x + \frac{B}{2A} = \pm \frac{\sqrt{B^2 - 4AC}}{2A}$$

bulunur. Bu eşitlik düzenlenerek teoremden verilen ifade kolayca elde edilebilir. □

Teorem 3.

X ve Y iki küme ve $f : X \rightarrow Y$ bir fonksiyon olsun. Bu durumda aşağıdaki önermeler denktir.

- (i) f birebir fonksiyondur.
- (ii) Her $A \subseteq X$ için $A = f^{-1}(f(A))$ gerçekleşir.

Kanıt. Önce verilenleri anlayalım. X ve Y diye adlandırılan iki küme verilmiş, bu kümeler üzerinde herhangi bir kısıtlama yok. Dolayısıyla elimizde keyfi iki küme var. Bir de X kümesinden Y kümesine tanımlı keyfi bir fonksiyon mevcut.

Peki istenen ne? Basitçe (i) ve (ii)'de verilen iki önermenin birbirine denk olduğunu göstermemiz

isteniyor. Bu önermelerin detaylarına girmeden önce iki önermenin denk olmasının ne demek olduğunu anlayalım. İki önermenin denk olması demek, bu önermelerin birbirlerini *gerektirmesi* demektir. Bir başka deyişle, (i) önermesinin sağlandığı durumda (ii) önermesi de sağlanmalı ve (ii) önermesinin sağlandığı durumda (i) önermesi de sağlanmalıdır. Dolayısıyla iki önermenin denkliğini göstermek için, bu önermelerden birini kabul edip bu kabul altında diğerinin doğruluğunu göstermek gerekir ve bu iş her iki önerme için de yapılmalıdır.

İlk olarak (i)'nin (ii)'yi gerektirdiğini, yani (i)'yi kabul edip (ii)'nin gerçekleştiğini, gösterelim. f birebir fonksiyon olsun. Bu durumda her $A \subseteq X$ kümesi için $A = f^{-1}(f(A))$ olduğunu kanıtlamaya çalışacağız. Şimdiki sorumuz şu: İki kümenin eşitliği ne demek? Yani $A = f^{-1}(f(A))$ demekle neyi kastediyoruz? İki kümenin eşit olması aslında her iki kümenin birbirini kapsamaması (başka bir deyişle, birbirinin alt kümesi olması) anlamına gelir⁴. O halde $A \subseteq f^{-1}(f(A))$ ve $f^{-1}(f(A)) \subseteq A$ olduğunu göstermeliyiz.

Aslında ilk kapsama, yani $A \subseteq f^{-1}(f(A))$ ifadesi her zaman sağlanır. Yani bu kapsama, f birebir değilken de doğru zaten! Bu kısmın kanıtını alıştırma sorularında ödev olarak bırakacağım. Çünkü birazdan detaylarıyla kanıtlayacağımız ikinci kapsama, bu kısmı kendi kendinize yapmanızda çok faydalı olacak.

O halde ikinci kapsamayı gösterelim. Peki, $f^{-1}(f(A)) \subseteq A$ ne demek? $f^{-1}(f(A))$ kümesindeki her bir elemanın A kümesine de ait olması demek değil mi? O halde $f^{-1}(f(A))$ kümesinden keyfi bir eleman alıp bu elemanın A kümesine de ait olduğunu gösterelim: $x \in f^{-1}(f(A))$ olsun. Sıradaki soru şu: Bir elemanın, bir kümenin ön görüntüsünde olması ne demek?⁵ Bu bile yeni bir soru doğurdu: Bir kümenin ön görüntüsü ne demek?

Hemen ön görüntünün tanımına gidelim. $g : B \rightarrow C$ bir fonksiyon ve $E \subset C$ olmak üzere, $g^{-1}(E) = \{x \in B \mid g(x) \in E\}$ kümesine E kümesinin g fonksiyonu altındaki ön görüntüsü denir. Yani E kümesinin ön görüntüsü; fonksiyon altında görüntüsü E 'de olan elemanların kümesidir. O halde $x \in g^{-1}(E)$ ise, $g(x) \in E$ olmalıdır.

Şimdi kanıtımıza devam edelim. $x \in f^{-1}(f(A))$ olduğuna göre ön görüntü tanımı gereği $f(x) \in f(A)$ olmalıdır. Buraya kadar $f(x) \in f(A)$ olduğunu gördük ve f 'nin birebir olduğunu kullanmamıza gerek kalmadı. Ve unutmayalım ki $x \in A$ olduğunu göstermemiz gerekiyor. Bir kısmınız $f(x) \in f(A)$ ise $x \in A$ olmalıdır diye düşünebilir. Ancak bu doğru değil!

Örneğin; $f : \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}$ fonksiyonu $f(x) = x^2$ biçiminde tanımlansın. $A = (0, \infty) \subset \mathbb{R}$ alt kümesini düşünelim. $f(x) = 4 \in \mathbb{R}_{\geq 0}$ elemanını ele alalım. Bu durumda $f(x) \in f(A)$ olmasına rağmen $x \in A = (0, \infty)$ olmak zorunda değil! Çünkü $x = -2$ için de $f(x) = 4$ olur ve $-2 \notin (0, \infty)$.

Bu sebeple daha dikkatli ilerleyelim. $f(x) \in f(A)$ kısmında kalmıştık. Peki bu ne demek? Bir eleman bir kümenin görüntüsü kümesinde yatıyor. Görüntü kümesi tanımını hatırlayalım: $g : B \rightarrow C$ bir fonksiyon ve $D \subset B$ olmak üzere, $g(D) = \{g(x) \in C \mid x \in D\}$ kümesine D kümesinin g fonksiyonu altındaki görüntüsü adı verilir. Yani D kümesindeki elemanların g fonksiyonu altındaki görüntülerinin oluşturduğu kümeden bahsediyoruz. Dolayısıyla $y \in g(D)$ ise bu eleman $g(x)$ tipinde yazılabilir, yani $y = g(x)$ olacak şekilde $x \in D$ mevcut olmalıdır.

Dolayısıyla $f(x) \in f(A)$ demek, $f(x) = f(a)$ olacak şekilde bir $a \in A$ mevcut olması demektir. Artık birebirliği kullanma zamanı. Ne demek bir fonksiyonun birebir olması? Farklı elemanların görüntüleri farklı olmalıdır ya da denk olarak, görüntüleri aynı olan elemanlar aynıdır. f fonksiyonu birebir ve $f(x) = f(a)$ olduğundan $x = a$ olmalıdır. $a \in A$ olduğuna göre tabii ki $x \in A$ sağlanır. İşte bu!

Şimdi, (ii)'yi kabul edip (i)'nin gerçekleştiğini gösterelim. Her $A \subseteq X$ kümesi için $A = f^{-1}(f(A))$ olsun. Bu durumda f birebir midir? f 'nin birebir olması ne demektir: Görüntüleri aynı olan elemanlar aynıdır. Yani keyfi $x, x' \in X$ için $f(x) = f(x')$ ise $x = x'$ olmalıdır. O halde $f(x) = f(x')$ sağlanırken x ile x' eşit oluyor mu diye bakacağız değil mi? Diyelim ki $x, x' \in X$ için $f(x) = f(x')$ olsun. Bu aşamada kullanabileceğimiz başka bir yardımcı yok. Sadece (ii) önermesini kullanabiliriz. Görüyoruz ki (ii) önermesi kümelerin görüntü ve ön görüntülerinin içeren bir eşitlik. Ama elimizde küme yok. x ve x' elemanları var ve $f(x) = f(x')$ eşitliği var. Bu eşitlikten

$$f(\{x\}) = f(\{x'\})$$

⁴Yani A ve B kümeler olmak üzere, $A = B$ eşitliği demek $A \subseteq B$ ve $B \subseteq A$ kapsamalarının her ikisinin de sağlanması demektir.

⁵Burada f^{-1} size doğrudan fonksiyonun tersini çağırabiliriz. Ancak bilmelisiniz ki fonksiyonunun tersinin var olması için birebir ve örten olması gerekir.

olduğunu söyleyebiliriz. Artık elimizde birer elemanlı iki küme var ve bunların görüntüleri birbirine eşit. Bir fonksiyonun görüntü kümesi tabii ki değer kümesinin içinde olmalı. O halde $f(\{x\}) \subset Y$ ve $f(\{x'\}) \subset Y$ sağlanır. Dolayısıyla elimizde Y kümesinin içinde bulunan ve birbirine eşit iki küme var. Bu kümelerin ön görüntüleri de birbirine eşittir, yani

$$f^{-1}(f(\{x\})) = f^{-1}(f(\{x'\}))$$

olur. (ii)'den biliyoruz ki her $A \subseteq X$ kümesi için $A = f^{-1}(f(A))$ sağlanıyor. Bu sebeple $f^{-1}(f(\{x\})) = \{x\}$ ve $f^{-1}(f(\{x'\})) = \{x'\}$ olup $\{x\} = \{x'\}$ bulunur. Bu ise $x = x'$ demektir. O halde f fonksiyonu birebirdir. $\square$

4. -miş gibi yapmak

“Bir şeyin var olmadığını ya da sağlanmadığını nasıl kanıtlayabilirim?” sorusu öğrenciler için zaman zaman kafa karıştırıcı olabilir. Fakat matematikte böyle “olumsuz” ifadelerin de kanıtı mümkündür. Ve matematikçiler böyle önermelerin kanıtları için güzel bir strateji kullanır: -miş gibi yapmak. Mantıksal olarak bir nesnenin var olmadığını göstermek için, bu nesne varmış gibi yaparız (yani var olduğunu kabul ederiz) ve daha sonra bu kabulün yol açtığı sonuçları inceleriz. Eğer var olduğunu varsaymak ileride bir çelişkiye neden oluyorsa, bu durumda kabulümüz doğru olamaz. Dolayısıyla nesnenin varlığı imkânsız olup bu nesne yoktur diyebiliriz. Sizce de çok havalı değil mi?

Hemen bir teorem kanıtlayarak daha iyi anlamaya çalışalım.

Teorem 4.

$\sqrt{2}$ irrasyonel bir sayıdır.

Kanıt. Bir gerçel sayının irrasyonel olması rasyonel olmaması demektir. Dolayısıyla $\sqrt{2}$ sayısının rasyonel olmadığını göstereceğiz. Bir an için $\sqrt{2}$ sayısı rasyonelmiş gibi yapalım, bir başka deyişle bu sayının rasyonel olduğunu varsayalım. Bildiğimiz üzere rasyonel sayılar aslında iki tam sayının birbirine bölümü şeklinde yazılabilen kesirli sayılardır. Tabii ki payda sıfır olamaz. Eğer $\sqrt{2}$ sayısı rasyonel bir sayı ise, bu durumda

$$\sqrt{2} = \frac{a}{b}$$

olacak şekilde sıfırdan farklı ve aralarında asal a ve b tam sayıları vardır. Burada a ve b 'nin aralarında asal olması özel bir durum değildir, aksi takdirde kesirde sadeleştirme yapılarak aralarında asal hale getirilebilir. O halde $\sqrt{2} = a/b$ eşitliğinde her iki tarafın karesi alınıp düzenlenerek

$$2b^2 = a^2 \tag{1}$$

elde edilir. Demek ki a^2 tam sayısı 2'nin bir tam katıdır, bir başka deyişle a^2 bir çift tam sayıdır. Buradan a tam sayısının da çift olduğu sonucuna varırız. Çünkü tek tam sayıların karesi çift olamaz!⁶ Demek ki bir m tam sayısı için $a = 2m$ olur. Bu ifade (1) denkleminde yerine yazılırsa $2b^2 = (2m)^2 = 4m^2$ ve buradan da $b^2 = 2c^2$ elde edilir. O halde b^2 bir çift tam sayıdır. Bu da demektir ki b de bir çift tam sayıdır.

Sonuç olarak gösterdik ki a ve b 'nin her ikisi de çift tam sayıdır. Yani her ikisi de 2'ye tam bölünüyor. Bu durumda bir gariplik fark ettiniz mi? a ve b tam sayılarının aralarında asal olduğunu söylemiştik. Yani her ikisi de 2'ye bölünemez! O halde bu bir çelişkidir. Bu sebeple $\sqrt{2}$ sayısının rasyonel olduğunu kabulü yanlıştır. Bu da demektir ki $\sqrt{2}$ irrasyoneldir. $\square$

Başka bir teorem kanıtlayarak bu durumu pekiştirelim.

Teorem 5.

Sonsuz çoklukta asal sayı vardır.

⁶Kanıt. Bir tek tam sayı $2n + 1$ formundadır. $(2n + 1)^2 = 4n^2 + 4n + 1$ olup $4n^2 + 4n$ çift olduğundan 1 fazlası tektir.

Kanıt. Asal sayıların sonsuz çoklukta olduğunu kanıtlamak, aslında sonlu tane asal sayı olmadığını kanıtlamak demektir. O halde bir an için sonlu tane asal sayı varmış gibi yapalım ve bu asal sayıları $p_1, p_2, \dots, p_k$ ile gösterelim. Burada k ile tüm asal sayıların sayısı ifade edilmektedir.

Tüm asal sayıları çarpıp sonuca 1 ekleyerek

$$N = (p_1 p_2 \cdots p_k) + 1$$

sayısını oluşturalım⁷. Elde ettiğimiz N sayısı açıkça tüm asal sayılardan büyüktür, bu sebeple asal sayıların hepsinden farklı bir sayıdır. $p_1, \dots, p_k$ sayıları elimizdeki tüm asal sayılar olduğuna göre, bunlardan farklı olan N sayısı asal olamaz. Bu sebeple N sayısının, Aritmetiğin Temel Teoremi gereğince, bir asal çarpanı olmak durumundadır. Bu asal çarpan $p_1, \dots, p_k$ sayılarından biri olmak zorundadır, çünkü elimizdeki tüm asal sayılar bunlar! Diyelim ki bu asal çarpan $p_i, i \in \{1, 2, \dots, k\}$ olsun. O halde N sayısı p_i sayısının bir katı olmak zorunda. Diğer yandan açıkça $N - 1 = p_1 \cdots p_k$ sayısı da p_i sayısının bir katıdır. N ve $N - 1$ sayılarının her ikisi de p_i asalının bir katı olduğuna göre, bunların farkı da aynı asalın bir katı olmak zorundadır. Yani $N - (N - 1)$ sayısı da p_i asalının bir katıdır. Dolayısıyla 1 sayısı p_i asalının bir katı olur. Ancak bu imkansızdır, çünkü en küçük asal sayı 2'dir ve 1 sayısı 2'nin bile bir tam katı değildir. Bu bir çelişkidir! Bu sebeple sonlu tane asal sayının olduğu kabulümüz yanlıştır. Bu da demektir ki sonsuz çoklukta asal sayı vardır. $\square$

5. Doğal sayılardaki domino etkisi: Tümevarım

Bu bölümde, belirli türdeki matematiksel ifadeleri kanıtlamak için güçlü ve zarif bir yöntem olan *matematiksel tümevarım* kavramını ele alacağız. Tümevarım, temelde bir ifadenin tüm doğal sayılar için — ya da belirli bir noktadan itibaren tüm doğal sayılar için — doğru olduğu iddia edilen genel önermeleri kanıtlamak amacıyla kullanılır.

Bir P özelliğini tüm doğal sayılar için kanıtlamak istediğimizi düşünelim. Yani o P özelliğinin 0, 1, 2, ... için doğru olduğunu göstermek istiyoruz. Burada sonsuz çoklukta sayı olduğundan dolayı hepsi için tek tek P özelliğinin sağlandığını göstermek mümkün değildir. Aslında kanıtlamak istediğimiz özelliği (P) tek bir önerme olarak değil de, her n doğal sayısı için birer tane olmak üzere bir dizi önerme olarak görebiliriz:

- $n = 0$ için P özelliğinin sağlanması
- $n = 1$ için P özelliğinin sağlanması
- $n = 2$ için P özelliğinin sağlanması
- $\vdots$

Tümevarımdaki temel fikir, bu önermeler dizisindeki ilk önermeyi kanıtlamak ve ardından herhangi bir önermenin doğruluğu kabulü altında bir sonraki önermenin de doğru olduğunu göstermektir. Bu sayede dizideki tüm önermelerin doğru olduğu sonucuna varırız. Daha matematiksel bir şekilde ifade edecek olursak; eğer bir özelliğin her n doğal sayısı için doğru olduğu kanıtlanmak istenirse aşağıdakiler yapılmalıdır:

1. **Başlangıç adımı:** Bir başlangıç değeri için önermenin doğruluğunu kanıtla. Eğer kanıt tüm doğal sayılar üzerinde yapılacaksa, bu başlangıç değeri $n = 0$ olur. Eğer bir a doğal sayısı itibarıyla tüm doğal sayılar için bir ifade kanıtlanacaksa, başlangıç adımı $n = a$ olur.
2. **Tümevarım adımı:** Bir n doğal sayısı için önermenin doğru olduğunu varsayarak, $n + 1$ için de doğru olduğunu kanıtla. Burada, ifadenin belirli bir n için doğru olduğunu varsayan bu kabul, *tümevarım hipotezi* olarak adlandırılır.

Bu iki adım gerçekleştirildiğinde, elimizdeki önermenin her n (ya da her $n \geq a$) doğal sayısı için doğru olduğu sonucuna varabiliriz. Başlangıç adımında önermenin $n = 0$ (ya da $n = a$) için doğruluğunu kanıtıyoruz. Tümevarım adımından da biliyoruz ki bir n doğal sayısı için doğruysa bir sonraki için de doğru olmak zorunda. O halde, önerme $n = 0$ için doğru olduğundan $n = 1$ için de doğru olmalı. Yine tümevarım adımından $n = 1$ için doğru olan önerme, $n = 2$ için de doğru olmalı. Tekrar tümevarım adımından $n = 2$

⁷Elimizde sonlu tane asal sayı olduğundan dolayı burada yaptığımız çarpma anlamlıdır.

için doğru olan önerme, $n = 3$ için de doğru olmalı. Tümevarım adımında önermenin keyfi bir n için doğruluğu altında $n + 1$ için de doğru olduğunu gösterdiğimiz için bu böyle sonsuza kadar devam eder.

Matematiksel tümevarımı, güzel bir benzetme ile, doğal sayılardaki domino etkisi olarak düşünebiliriz. Bir sürü domino taşının uzunca dizildiğini düşünelim. Tüm domino taşlarının devrileceğinden nasıl emin olabiliriz? Bunun için iki şey gereklidir; ilk dominonun devrilmesi ve devrilen her dominonun bir sonraki dominoyu devirmesi. Aslında tümevarım adımı, “domino taşlarının birbirine yakın yerleştirilmesini, böylece bir tanesi devrilince bir sonrakinin de devrilmesini” garanti eder. Başlangıç durumu ise “ilk dominonun gerçekten itilmesi” demektir.

Teorem 6.

Her n doğal sayısı için $3, n^3 - n$ sayısını böler.

Kanıt. Her n doğal sayısı için bir ifade kanıtlamamız gerekiyor. Bu sebeple n üzerine tümevarım uygulayabiliriz.

1. *Başlangıç adımı:* $n = 0$ için önermeyi kanıtlayalım. Bu durumda $n^3 - n = 0 - 0 = 0$ olduğundan ve 3 sayısı 0 sayısını böldüğünden, bir başka deyişle 0 sayısı 3 sayısının bir tam katı olduğundan önerme gerçekleşir. Hatta benzer şekilde $n = 1$ için de $n^3 - n = 1 - 1 = 0$ olduğundan önerme gerçekleşir.
2. *Tümevarım adımı:* Şimdi keyfi bir n doğal sayısı için önermenin olduğunu, yani 3 sayısının $n^3 - n$ sayısını böldüğünü kabul edelim. Bu kabul altında önermeyi $n + 1$ için kanıtlamaya çalışacağız, yani 3 sayısının $(n + 1)^3 - (n + 1)$ sayısını böldüğünü göstereceğiz. Kabul gereği önerme n için sağlandığından dolayı, $n^3 - n$ sayısı 3'ün bir tam katıdır. Yani $n^3 - n = 3k$ olacak şekilde bir k tam sayısı vardır. Buradan

$$\begin{aligned}(n + 1)^3 - (n + 1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\ &= n^3 - n + 3n^2 + 3n \\ &= (n^3 - n) + 3(n^2 + n) \\ &= 3k + 3(n^2 + n) \\ &= 3(k + n^2 + n)\end{aligned}$$

elde edilir. O halde $(n + 1)^3 - (n + 1)$ sayısı 3'ün bir tam katıdır. Yani önerme $n + 1$ için de doğrudur.

Dolayısıyla önerme her n doğal sayısı için sağlanır. □

Teorem 7.

1'den başlayarak ilk n doğal sayının küpleri toplamı $\frac{n^2(n+1)^2}{4}$ ’e eşittir. Yani $1^3 + 2^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4}$.

Kanıt. n üzerine tümevarım uygulayalım.

1. *Başlangıç adımı:* $n = 1$ başlangıç durumunu inceleyelim. Bu durumda ise $1^3 = 1 = \frac{1^2(1+1)^2}{4}$ olup önerme $n = 1$ için gerçekleşir. Daha iyi anlayabilmek için $n = 2$ durumunu da gösterelim. Bu durumda $1^3 + 2^3 = 9$ olur. Ayrıca önermedeki ifadenin sağ tarafı da $\frac{2^2(2+1)^2}{4} = 9$ olduğundan, önerme $n = 2$ için de sağlanır.
2. *Tümevarım adımı:* Şimdi önermenin n doğal sayısı için doğru olduğunu kabul edelim. Bu kabul altında, önermenin $n + 1$ için doğru olduğunu kanıtlamaya çalışacağız. Yani $1^3 + 2^3 + \dots + (n + 1)^3 = \frac{(n + 1)^2(n + 2)^2}{4}$ olduğunu göstereceğiz. Tümevarım hipotezi kullanılarak

$$1^3 + 2^3 + \dots + n^3 + (n + 1)^3 = \frac{n^2(n + 1)^2}{4} + (n + 1)^3$$

$$\begin{aligned}
&= (n+1)^2 \left(\frac{n^2}{4} + (n+1) \right) \\
&= (n+1)^2 \frac{n^2 + 4n + 4}{4} \\
&= \frac{(n+1)^2 (n+2)^2}{4}
\end{aligned}$$

bulunur. O halde önerme $n+1$ için de gerçekleşir.

Dolayısıyla önerme her $n \geq 1$ doğal sayısı için sağlanır. $\square$

Tümevarım yoluyla bir kanıt yaparken, çoğu zaman tümevarım adımında ifadenin yalnızca n için doğruluğu, $n+1$ için doğruluğunu kanıtlamaya yeter. Ancak bazen biraz daha “güçlü” bir varsayıma ihtiyaç duyulur ve bu durumda tümevarım hipotezini güçlendirmek gerekir. Tümevarımın matematiksel ifadesindeki başlangıç adımı aynen kalırken, tümevarım adımı

2'. *Güçlü tümevarım adımı*: Bir n doğal sayısına kadar tüm doğal sayılar için önermenin doğru olduğunu varsayarak, $n+1$ için de doğru olduğunu kanıtla.

ile değiştirilsin. Bu yöntem *güçlü tümevarım* adı verilir. Ancak buradaki “güçlü tümevarım” ifadesi yukarıdaki klasik (ya da zayıf) tümevarımın bir genellemesi olduğu ya da bu yöntemle daha fazla önermenin kanıtlanabileceği anlamı taşımaz; sadece tümevarım adımında kullanılan varsayımın daha güçlü olmasına atıfta bulunur. Hatta temelde zayıf tümevarım kullanılan herhangi bir kanıt, doğrudan bir şekilde güçlü tümevarım kullanan bir kanıta dönüştürülebilir; aynı şekilde güçlü tümevarım kullanan bir kanıt da zayıf tümevarım kullanan bir kanıta dönüştürülebilir. Sadece, tümevarım hipotezini güçlendirmenin kolaylık sağladığı durumlar vardır.

Teorem 8.

2’den büyük her n doğal sayısı ya asaldır ya da asal sayıların çarpımı şeklinde yazılabilir.

Kanıt. n üzerine güçlü tümevarım uygulayalım. Neden bunu uyguladığımız gerektiği birazdan daha açık olacak.

1. *Başlangıç adımı*: $n=2$ başlangıç durumunu inceleyelim. 2 asal sayı olduğundan bu durum açıktır. Benzer şekilde 3 asal sayı olduğundan $n=3$ için de önermenin doğruluğu açıktır. Farklı bir örnek görmek adına $n=4$ durumunu da inceleyelim. Bu durumda $4=2 \cdot 2$ olduğundan ve 2 asal sayı olduğundan önermenin $n=4$ için sağlandığı da kolayca görülür.

2' *Güçlü tümevarım adımı*: Şimdi 2’den n doğal sayısına kadar tüm doğal sayılar için önermenin doğru olduğunu kabul edelim. Bu kabul altında, önermenin $n+1$ için doğru olduğunu kanıtlayacağız. Yani $n+1$ sayısının asal sayıların çarpımı şeklinde yazıldığını göstereceğiz. Bunu iki durumda inceleyelim:

- $n+1$ bir asal sayı olsun. Bu durumda kanıtlayacak bir şey yoktur.
- $n+1$ bir asal sayı olmasın. O halde $n+1 = a \cdot b$ olacak şekilde a ve b doğal sayıları vardır ve açıkça bu doğal sayılar $1 < a, b < n+1$ eşitsizliğini sağlar. Tümevarım hipotezinden a ve b doğal sayıları asal sayıların çarpımı olarak ifade edilebilir. O halde a doğal sayısı asal sayıların çarpımı olarak $p_1 p_2 \cdots p_i$ biçiminde ve b doğal sayısı asal sayıların çarpımı olarak $q_1 q_2 \cdots q_j$ biçiminde yazılabilir. Buradan $n+1 = p_1 p_2 \cdots p_i q_1 q_2 \cdots q_j$ olup, $n+1$ sayısı asal sayıların çarpımı biçiminde yazılmış olur.

O halde önerme $n+1$ için de doğru olur.

Dolayısıyla önerme her $n \geq 2$ doğal sayısı için gerçekleşir. $\square$

Yukarıdaki kanıtta güçlü tümevarım kullanmamızın en önemli sebebi a ve b doğal sayılarının asal sayıların çarpımı biçiminde yazıldığını söyleyebilmektir. Zayıf tümevarımda yalnızca n doğal sayısının önermeyi sağladığını kabul ederken, burada n ’den daha küçük olanların da önermeyi sağladığı kabulünü kullanmamız gerekti.

6. Önergelerin başka bir yüzü

“Eğer yağmur yağarsa dışarı çıkmam” önermesini düşünelim. Bu önermenin sözüne güvenilen bir insan tarafından söylendiğini ve bu kişinin dışarı çıktığını varsayalım. O halde yağmur yağmamıştır, öyle değil mi? Çünkü yağsaydı dışarı çıkmazdı. Dolayısıyla bu önerme ile “Dışarı çıktıysam yağmur yağmamıştır” önermesinin doğruluk değeri aynıdır. İlk koşullu önermeyi $p \rightarrow q$ ile ifade edersek, ikinci önerme $q' \rightarrow p'$ ile ifade edilir. Burada p' ile p önermesinin değili (olumsuzu) gösterilir. Bu iki koşullu önermenin doğruluk değerleri aynı olduğuna göre bu önermeler denktir: $p \rightarrow q \equiv q' \rightarrow p'$. O halde $p \rightarrow q$ önermesinin doğru olduğunu kanıtlamak yerine, $q' \rightarrow p'$ önermesinin doğru olduğunu kanıtlamakta yeterli olur. Çünkü bazen $q' \rightarrow p'$ koşullu önermesini kanıtlamak daha kolay olabilir. $q' \rightarrow p'$ koşullu önermesine $p \rightarrow q$ koşullu önermesinin karşıt tersi (ya da kontrapozitif), bu yöntem kullanılarak yapılan kanıtlara da *kontrapozitif ile kanıt* adı verilir.

Çok basit bir örnekle bu durumu anlamaya çalışalım.

Teorem 9.

Eğer n^2 çift tam sayı ise, n de çift tam sayıdır.

Kanıt. Önermeyi doğrudan kanıtlamaya çalışalım. n^2 tam sayısının çift olduğu durumda n nin de çift olduğunu göstermemiz gerek. Çift tam sayıların tanımı gereği; eğer n^2 çift tam sayı ise $n^2 = 2k$ olacak şekilde bir k tam sayısı mevcuttur. Hatta bu k tam sayısı negatif olamaz. O halde elimizde $n^2 = 2k$ gibi bir eşitlik var ve buradan n sayısının durumunu incelememiz gerekiyor. Ancak bu eşitlikten n hakkında fikir elde etmeye çalışırsak her iki tarafın karekökünü almak gerekir. Bu da bize $\sqrt{n^2} = \sqrt{2k}$ gibi bir eşitlik verir ve buradan n 'nin çift ya da tek olmasına karar veremeyiz. Dolayısıyla önermeyi doğrudan kanıtlamak biraz zorlu görünüyor. Bunun yerine koşullu önermenin karşıt tersini ele alalım: “ n çift tam sayı değilse, n^2 de çift tam sayı değildir.” Bu önerme, teoremin ifadesinde verilen önermeye denktir. O halde bu önermeyi kanıtlayalım.

n çift tam sayı olmasın. O halde n tektir ve $n = 2p + 1$ olacak şekilde p tam sayısı mevcuttur. Buradan $n^2 = (2p + 1)^2 = 4p^2 + 4p + 1 = 2(2p^2 + 2p) + 1 = 2m + 1$ olup n^2 tek tam sayıdır. Dolayısıyla n^2 çift tam sayı değildir. $\square$

■ Alıştırmalar

1. Teorem 1’de verilen önermeyi tümevarım kullanarak kanıtlayınız.
2. Aşağıdaki önermeleri kanıtlayınız.

- (a) X ve Y iki küme, $f : X \rightarrow Y$ bir fonksiyon ve $A \subseteq X$ olsun. Bu durumda $A \subseteq f^{-1}(f(A))$ olur.
- (b) A ve B iki küme olsun. Bu durumda $A \cap B = A$ olması için gerek ve yeter koşul $A \subseteq B$ olmasıdır. Not: Burada “gerek ve yeter koşul” demek aslında soldaki ve sağdaki önermelerin birbirine denk olması demektir. Bakınız Teorem 3.
- (c) A ve P , $n \times n$ tipinde matrisler ve P tersinir olsun. Her $k \geq 0$ tam sayısı için $(PAP^{-1})^k = PA^kP^{-1}$ olur.
- (d) Her $x \in [0, \pi/2]$ gerçel sayısı için, $\sin x + \cos x \geq 1$ sağlanır.

Yazıyı kapatırken, belki de zaten dikkatinizi çekmiş olabilecek bir şeyden bahsetmek istiyorum: $\square$. Bu kutucuk kanıtların sonuna konulan bir imzadır. Kanıtın bittiğini ifade etmek için kullanılır. Belki de bu işaret sadece bir sonu değil, aynı zamanda bir zafer ilanını temsil ediyordur. Eski kitapları ya da makaleleri karıştırırsanız, kanıtların sonunda genellikle Latince *quod erat demonstrandum* ifadesinin baş harflerinden oluşan Q.E.D. ifadesini görürsünüz. Bu ifade, “kanıtlanması gereken şey de buydu” anlamına gelir. Q.E.D. yerine $\square$ sembolünün matematikte ilk kullanımı Paul Halmos’a atfedilir.

İyi Temellendirilmemiş Kümeler

SEBAHATTİN EMRE ŞAHİN

Hacettepe Üniversitesi Matematik Bölümü, 4. Sınıf Öğrencisi

✉ emresahinmath@gmail.com



20. yüzyılın ortalarında Zermelo ve Fraenkel, matematiği tutarlı bir temele oturtmak amacıyla ZFC aksiyomatik sistemini ortaya atmışlardır. Aksiyomların ifade ettikleri kavramlar ilk bakışta basit görünse de, birçok matematikçi bu aksiyomlar üzerine derinlemesine düşünmüş ve bunları tartışmıştır. ZFC üzerine farklı amaçlara yönelik yeni aksiyom sistemleri önerilmiş, kümeler kuramının sınırları bu tartışmalar aracılığıyla genişlemiştir. Bu tartışmaların merkezinde, ZFC'nin bir aksiyomu olan Temellendirme Aksiyomu da yer almaktadır. Temellendirme Aksiyomu, en yalın ifadeyle, bir kümenin kendi içinde sonsuz bir elemanlık döngüsü oluşturmasını engelleyerek kümelerin "iyi temellendirilmiş" olmasını sağlar. Bu makalede, Temellendirme Aksiyomu'nun reddedilmesiyle ortaya çıkan iyi temellendirilmemiş kümeler üzerine bazı temel okumalar sunulmakta, bu kümelerin sahip olduğu ilginç özellikler tartışılmakta ve klasik küme kuramının ötesine geçen yaklaşımlara dair örnekler verilmektedir.

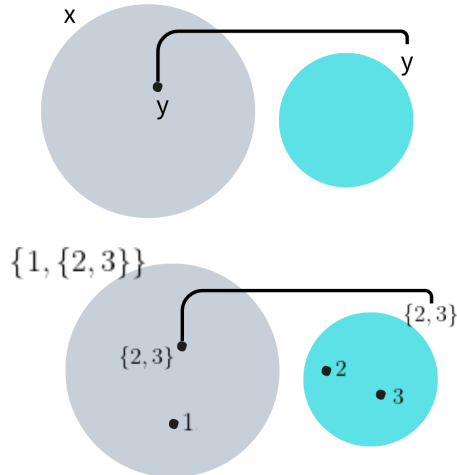
1. Temellendirme Aksiyomu

Bu yazıda, küme teorisi kitaplarındaki yerleşik notasyonlara sadık kalınarak, kümeler küçük harflerle (x, y, z gibi) ifade edilecektir. Ayrıca, klasik ZFC çerçevesine uygun olarak, kümelerin elemanlarının da yine kümeler olduğu varsayılacaktır.

Temellendirme Aksiyomu: $\forall x(x \neq \emptyset \rightarrow \exists y \in x (y \cap x = \emptyset))$.

Yukarıdaki ifade, Temellendirme Aksiyomu'nun doğrudan kendi ifadesidir. Daha anlaşılır biçimde ifade etmek istersek: "Boş kümeden farklı her kümenin, kendisiyle kesişmeyen bir elemanı vardır." Bu aksiyomu ilk gördüğümüzde akla şu sorular gelebilir: Aynı anda $y \in x$ ve $y \cap x = \emptyset$ nasıl mümkün olabilir? ZFC aksiyomatik sistemi çelişkili mi? Eğer öyleyse, dünya yok mu olacak?

Sakinleşip bir bardak su içtikten sonra bu kafa karışıklığının sebebini açıklayalım. Bunun nedeni alışık olduğumuz notasyondan farklı bir notasyon kullanıyor olmamız. y, x kümesini bir elemanı ve y de kendi başına ayrı bir kümedir.



Teorem 1.

Herhangi bir x kümesi için $x \notin x$ olur.

Kanıt. Aksine, $x \in x$ olacak şekilde bir x kümesi var olsun. Bu durumda $\{x\} \neq \emptyset$ olur. Temellendirme Aksiyomundan ötürü $x \cap \{x\} = \emptyset$ olmalı. Ancak, $x \cap \{x\} \neq \emptyset$. $\square$

Temellendirme Aksiyomu'nun bir sonucu olan bu teorem, doğrudan Russell Paradoksu'yla ilişkilidir. Bir sonraki alt başlıklarda Russell Paradoksu'nu daha ayrıntılı olarak inceleyeceğiz.

1.1. Russell Paradoksu

- $R = \{x \notin x\}$ kümesini inceleyelim. R kümesini, elemanları kendi kendini içermeyen kümeler olarak ifade edebiliriz. Fakat,

$$R \in R \Rightarrow R \notin R$$

$$R \notin R \Rightarrow R \in R$$

20. yüzyılda Russell tarafından ortaya atılan bu paradoksun temelinde, bir önermenin kendisine referans vermesi yatıyordu. Bu nedenle, matematiğin kendi içinde çelişkisizliğini sağlamak amacıyla, kendi kendine referans veren (döngüsel) yapılardan kaçınılması gerekiyordu. Bu yaklaşımın bir sonucu olarak, ZFC kümeler kuramında yer alan Temellendirme Aksiyomu, bu tür döngüsel kümelerle izin vermez (bkz. Teorem 1)

Ancak 20. yüzyılın sonlarına doğru, özellikle mantıksal paradokslar ve bilgisayar bilimi gibi alanlarda döngüsel yapılarla daha sık karşılaşmaya başlandı. Gerçekten de dikkatli bir şekilde ele alınmadıkla- rında bu tür döngüsellikler çelişkilere yol açabilir. Bununla birlikte, her döngüsel yapı çelişki doğurmaz. Dolayısıyla, uygun bir küme kuramı içerisinde bu yapıların temsil edilmesi gerekmektedir.

Temellendirme Aksiyomu olmadan kümeler kuramını araştıran birçok küme kuramcısı olmuştur; ancak bu çalışmalar, dönemin ana akım matematikçileri tarafından pek ciddiye alınmamıştır. Bu vizyoner isimler arasında M. Boffa, M. Forti, L. Gordeev ve F. Honsell yer almaktadır. Bununla birlikte, yakın döneme kadar bu alanda en sistemli yaklaşımı Peter Aczel'in çalışmaları sunmuştur. Bu yazının temel kaynağı da Peter Aczel'in *Non-Well-Founded Sets* kitabıdır.

İyi temellendirilmemiş bir kümeler kuramının gerekliliğini göstermek için bir örnek inceleyelim.

Örnek 1.**Veri Dizgisi/Akısı (Streams)**

Veri dizgisi (stream) kavramı genellikle bilgisayar bilimlerinde karşımıza çıkar ve özellikle sonsuz veri dizilerini tanımlamak için kullanılır.

Bir dizgi (stream), sezgisel olarak, bir sonlu değer a (örneğin bir sayı, karakter, sembol vb.) ile başka bir s' dizgisinin oluşturduğu sıralı çift $\langle a, s' \rangle$ şeklinde tanımlanır. Bu yapı, sonsuz veri dizilerini temsil etmekte kullanılır.

Tanım 1. (Kurtowski)

x ve y kümeler olmak üzere, $\langle x, y \rangle$ sıralı ikilisi şu şekilde tanımlanır:

$$\langle x, y \rangle = \{x, \{x, y\}\}.$$

Bir bilgisayar, bir veri dizgisini tanımlamak için genellikle özyinelemeli (rekürsif) fonksiyonlar kullanır. Örneğin, $f(n) = \langle n, f(n+1) \rangle$ biçimindeki bir tanım aracılığıyla, $n = 0$ için $\langle 0, \langle 1, \langle 2, \dots \rangle \rangle \rangle$ şeklinde bir veri dizgisi elde edilir.

Tanım 2.

A bir atomlar kümesi (sayılardan veya karakterlerden oluşan sonlu değerler) olmak üzere, $St(A)$ atomlardan oluşan tüm akışların kümesi olarak tanımlanır; eğer $s \in St(A)$ ise, o zaman $s = \langle a, s' \rangle$ olur, burada $a \in A$ ve $s' \in St(A)$ olur.

Teorem 2.

Temellendirme Aksiyomunu varsayalım. Herhangi iki x ve y kümeleri için, $x \neq \langle x, y \rangle$ ve $y \neq \langle x, y \rangle$.

Kanıt. Aksine, $x = \langle x, y \rangle = \{x, \{x, y\}\}$ veya $y = \langle x, y \rangle = \{x, \{x, y\}\}$ olsun. Bu durumda $x \in x$ veya $y \in y$ olur. Bu da Temellendirme Aksiyomu ile çelişir. $\square$

Teorem 3.

Temellendirme Aksiyomunu varsayalım. R ve S herhangi iki bağıntı olmak üzere, eğer bir a elemanı R bağıntısı altında S bağıntısına taşınıyorsa (aRS), o zaman hiçbir b elemanı yoktur ki b elemanı S bağıntısı altında R 'ye taşınınsın. (bSR).

Kanıt. Aksine, aRS ve bSR , yani $\langle a, S \rangle \in R$ ve $\langle b, R \rangle \in S$ olsun.

$$S \in \langle a, S \rangle \in R \in \langle b, R \rangle \in S.$$

Bu durum, Temellendirme Aksiyomu ile çelişir. $\square$

Sonuç 1.

Temellendirme Aksiyomunu varsayalım. O zaman $St(A) = \emptyset$.

Bu durum, sezgisel kavrayışımız ile matematiksel modelimiz arasında oldukça ciddi bir uyumsuzluk olduğunu gösterir. Sonuç olarak, eğer veri dizgiler gibi kendine referans veren sistemlerle çalışmak istiyorsak Temellendirme Aksiyomu çok da işimize yaramıyor.

2. Kümelerin Resmini Çizebilir misin, Abidin?

Burada çizmek istediğimiz kümeler, ilkokuldaki gibi elmalar, armutlar içeren Venn diyagramları değildir. Çünkü bu tür çizimler, “elma” kümesinin içindeki molekülleri, onların içindeki atomları ve atom altı parçacıkları bize gösteremez. Elma örneğini bir kenara bırakalım; çok daha iyi bildiğimiz bir kümenin resmini çizmeyi deneyelim.

Doğal sayıların inşasındaki ana fikir, n doğal sayısını, n elemanlı bir küme olarak tanımlamaktır. Bu fikri kullanırken, elimizdeki tek küme olan boş kümeye ardıl işlemi uygulayarak kümedeki eleman sayısını artırırız.

Tanım 3.

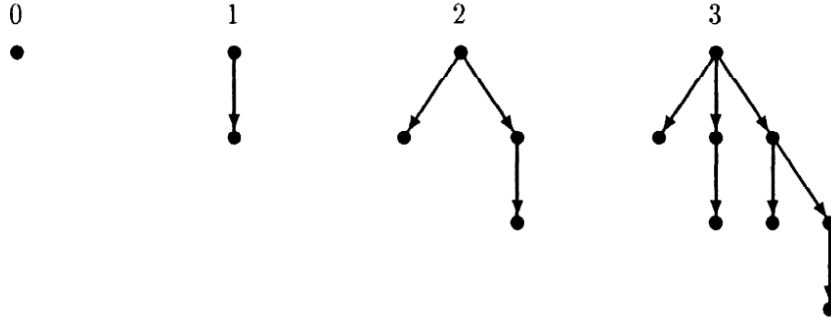
x bir küme olmak üzere $s(x) = x \cup \{x\}$.

$$0 = \emptyset$$

$$1 = s(0) = \{0\} \cup 0 = \{\emptyset\}$$

$$2 = s(1) = \{1\} \cup 1 = \{\emptyset, \{\emptyset\}\}$$

$$3 = s(2) = \{2\} \cup 2 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$



Kümelerin elemanlarını yönlendirilmiş doğru parçaları (oklar) ile temsil ettiğimizde ortaya çıkan yapı bir ağaç oluşturur. Örneğin, 2 kümesinden $\{1\}$ ve 1 kümelerine doğru çizilen oklar, 2 kümesinin tam olarak $\{1\}$ ve 1 elemanlarına sahip olduğunu gösterir.

2.1. Temellendirme Karşıtı Aksiyomu (TKA)

Karşıt Temellendirme Aksiyomuna geçmeden önce Aczel'in terminolojisindeki önemli tanımları verelim.

- Yönlü bir çizgede, herhangi bir n_0 noktasından başlayıp çizgenin her noktasına bir yol varsa **erişilebilir** (ing. accessible) olarak adlandırılır.

$$n_0 \rightarrow n_1 \rightarrow \dots \rightarrow n$$

- Bir çizge için **süsleme** (ing. decoration), çizgenin her noktasına bir kümenin atanmasıdır.

Bir erişilebilir çizge için eğer içinde sonsuz yollar veya döngüler yoksa **iyi temellendirilmiş** (ing. well-founded) olarak adlandırılır. Mostowski'nin Çökertme Lemması (ing. Collapsing Lemma), her iyi temellendirilmiş çizgenin tek bir süslemeye sahip olduğunu belirtir.

Karşıt Temellendirme Aksiyomu: Her işaretli erişilebilir çizge benzersiz bir kümeyi temsil eder.

Aczel'in Temellendirme Karşıtı Aksiyomu (TKA), her işaretli ve erişilebilir çizgenin, iyi temellendirilmiş olsun ya da olmasın, tekil bir kümenin resmini verdiğini belirtir. Temellendirme Karşıtı Aksiyomu'nun iki sonucu vardır: varlık ve tekillik.

- Her işaretli erişilebilir çizgenin bir süslemeye sahip olduğunu garanti eder (bu da iyi temellendirilmiş olanlar dışında kötü temellendirilmiş kümelerin de var olmasına yol açar)
- Hiçbir işaretli ve erişilebilir çizgenin birden fazla süslemeye sahip olamayacağını belirtir.

ZFC 'den Temellendirme Aksiyomu'nu çıkarıp (ve bu şekilde ortaya çıkan sisteme ZFC^- ile gösterilir) TKA'yı eklediğimizde Hiperküme Teorisi (ing. Hyperset Theory) elde edilir.

Örnek 2.

İki iyi temellenmemiş (non-well-founded) kümeyi ele alalım:

$$a = \{\text{Zermelo}, a\}, \quad b = \{\text{Zermelo}, b\}.$$

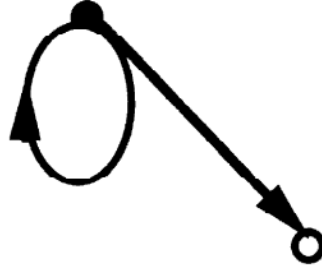
Peki, a ve b kümeleri eşit midir değil midir?

İyi temellenmiş küme kuramında, bu tür bir sorunun cevabı kolayca, Eşitlik Aksiyomu (ing. Axiom of Extensionality) uygulanarak elde edilir: İki küme, ancak ve ancak aynı elemanlara sahiplerse eşittir.

Ancak mevcut durumda, bu aksiyom yalnızca şu sonuca götürür:

$$a = b \text{ ancak ve ancak } a = b.$$

Dolayısıyla, iyi temellenmemiş kümeler söz konusu olduğunda Temellendirme Karşıtı Aksiyomundan yararlanmakta fayda var.



Zermelo

Her iki küme de aynı çizmeyi oluşturur. Sonuç olarak, bu iki küme (KTA) aynı tek kümedir.

2.2. Peki Russell Paradoksuna Ne Oldu?

Temellendirme Karşıtı Aksiyomundan sonra şu sorular aklımıza gelebilir:

Russell paradoksu ve kendini referans veren diğer paradokslar ne olacak? Temellendirme aksiyomu bizi bu tür şeylerden kurtarmak için alınmamış mıydı? Karşıt Temellendirme Aksiyomunu kabul edersek bunlar geri gelmez mi?

Kendini içeren bir küme örneği denilince akla genellikle “tüm kümelerin kümesi” gibi Russell kümeleri gelir. Ancak daha basit örnekler de vardır. Örneğin:

$$x = \{1, x\}$$

şeklinde kendini içeren daha basit kümeler de bulunur. Kendini içeren kümelere dair doğal örnekler vardır ve bu örnekler tanıdık hale geldikçe yapay olmaktan çıkarlar. Bu bölümde, iyi-temellendirilmemiş kümelerin tutarsız olmadığını, aksine tutarlı bir şekilde var olabileceklerini göstereceğiz.

Herhangi bir b kümesi verildiğini varsayalım, ister iyi-tanımlanmış ister iyi-tanımlanmamış olsun. Seçim Aksiyomu, b içindeki istediğimiz alt kümeleri seçmemize izin verir. b kümesi için Russell kümesini aşağıdaki biçimde oluşturabiliriz:

$$z_b = \{x \in b \mid x \notin x\}.$$

Russell’ın argümanına tekrar dönecek olursak, $z_b \in z_b$ ve $z_b \notin z_b$ arasında bir çelişki ortaya çıktığını biliyoruz. Ancak iyi temellendirilmemiş kümeleri içeren teorilerde, $z_b \in z_b$ mümkün olduğu için bu durumda bir çelişki oluşmaz. Çünkü artık $z_b \in z_b \Rightarrow z_b \notin z_b$ olması gerektiğine dair bir zorunluluk yoktur.

Aşağıdaki tabloda bazı iyi temellendirilmemiş kümeler için z_b kümelerini bulalım.

b	$z_b = \{x \in b \mid x \notin x\}$
$\Omega = \{\Omega\}$	$\emptyset$
$b = \{1, b\}$	$\{1\}$
$b = \{0, \{1, b\}\}$	$\{0, \{1, b\}\}$

Son örneğin biraz kafa karıştırıcı olduğunu kabul etmek gerekir. $b = \{0, \{1, b\}\}$ kümesi iyi temellendirilmemiştir; ancak buna rağmen, iyi temellendirilmiş bir küme gibi $z_b = b$ sonucu ortaya çıkmıştır. Bunun sebebi, diğer küme örneklerinde doğrudan kendilerini içerirken ($b = \{1, b\}$ gibi), $b = \{0, \{1, b\}\}$ kümesi dolaylı olarak kendisini içerir (elemanın elemanı olarak). Hatta böyle kümeleri incelemek için aşağıdaki gibi kümeler inşa edilebilir:

Tanım 4.

x ve z birer küme olsun. Bu durumda aşağıdaki koşullardan en az biri sağlanıyorsa, z kümesine x 'in bir bileşeni (ing. constituent) denir ve bu ilişki $z \in^* x$ şeklinde gösterilir.

- z, x kümesinin bir elemanıdır: $z \in x$,
- z, x kümesinin bir elemanının elemanıdır: $z \in t_0$ ve $t_0 \in x$,
- z, x kümesinin bir elemanının, bir elemanının, ..., bir elemanının elemanıdır; yani $z \in t_0 \in t_1 \in \dots \in t_n \in x$ olacak şekilde bir zincir mevcuttur ve bu zincir sonsuza kadar devam edebilir.

Bu tanım sayesinde, Russell kümelerini aşağıdaki şekilde revize ederek yeniden inceleyebiliriz.

$$w_b = \{x \in b \mid x \notin^* x\}$$

$$v_b = \{x \in^* b \mid x \notin^* x\}$$

Buradan z_b hakkında bazı çıkarımlarda bulunabiliriz.

Sonuç-1. b iyi temellendirilmemiş bir küme olmak üzere, $z_b \notin b$.

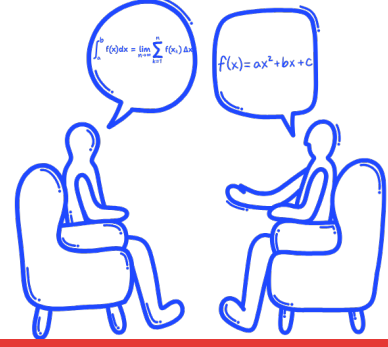
Sonuç-2. b iyi temellendirilmemiş bir küme olmak üzere, hiçbir küme tüm alt kümelerini eleman olarak içeremez.

Sonuç-3. b iyi temelli bir küme olmak üzere $z_b = b$.

■ Kaynaklar

- [1] J. Bell, “Peter aczel. non-well-founded sets. with a foreword by jon barwise. csli lecture notes, no. 14. center for the study of language and information, stanford1988, also distributed by the university of chicago press, chicago, xx+ 131 pp.,” The Journal of Symbolic Logic, vol. 54, no. 3, pp. 1111–1114, 1989.
- [2] M. Boffa, “Peter aczel, jon barwise, non-well-founded sets,” 1989.
- [3] M. Pakkan and V. Akman, “Hypersolver: A graphical tool for commonsense set theory,” Information Sciences, vol. 85, no. 1-3, pp. 43–61, 1995.
- [4] J. Barwise and L. Moss, “Hypersets,” The Mathematical Intelligencer, vol. 13, no. 4, pp. 31–41, 1991.
- [5] A. Nesin, “Kümeler kuramı 1,” Nesin Yayıncılık, pp. 21–22, 2010.
- [6] B. Kaya, “MATH 320: Set Theory Lecture Notes,” Middle East Technical University, Ankara, Turkey, Lecture Notes, 2018, Spring 2018, used Hrbacek & Jech as main reference. [Online]. Available: <https://users.metu.edu.tr/burakk/lecturenotes/320lecturenotes.pdf>
- [7] R. Grausi, “Non well-founded set theory,” Universit“ at Hamburg, Project on Alternative Set Theories, Lecture notes / preprint, 2025, Consistent proof of ZF + AFA based on graphical systems. [Online]. Available: <https://www.math.uni-hamburg.de/home/khomskii/ALST/romain.pdf>

Matematik Söyleşileri



Bilimsel yolculuklar çoğu zaman formüllerle, teoremlerle, araştırmalarla anlatılır. Ama bazen bir insan, bir mektup, bir jest, ya da bir tesadüf; o yolculuğun en dokunaklı duraklarından biri olur. Türkiye'nin önde gelen matematikçilerinden, Orta Doğu Teknik Üniversitesi Matematik Bölümü Öğretim Üyesi Prof. Dr. Mahmut Kuzucuoğlu ile gerçekleştirdiğimiz bu söyleşide, yalnızca matematik değil; aynı zamanda bir vefa hikâyesine, bilimsel dayanışmalara, kültürel etkileşimlere ve profesör olma yolculuğuna da tanık oluyoruz. Kendisiyle geçmişe uzanan samimi bir sohbet gerçekleştirdik. Okuyan herkese, kendi yolculuğu için bir ışık tutmasını umuyoruz.

Selcan Şenyurt/Talha Tin: Hocam, öncelikle matematikle nasıl tanışmanızdan bahsedelim. İçinizde ilk kıvılcımı yakan neydi? Bir ispat mı, bir film mi, bir öğretmen mi? Yani "Ben bu işi sevdim, matematikle uğraşmalıyım" dediğiniz anı merak ediyoruz.

Mahmut Kuzucuoğlu: Benim hikâyem biraz eski. Türkiye'nin modern matematiğe geçiş sürecinin ilk öğrencilerindenim diyebilirim. Denizli Lisesi'nde okurken bize modern matematik dersi veriliyordu. O derste bize ders veren hocamız Zeki Çetinkaya da o yıl bir kursa gitmişti, nereye gitmiş hatırlamıyorum ama, oldukça hevesli ve gerçekten matematik öğreten biriydi. Bence biraz ondan etkilendim. Biraz da çevreden ve babamdan. Babamın matematiği de iyiydi. Açıkçası birazda cahillikten.

SŞ/TT: Cahillikten mi?

Evet. O zamanlar mesela endüstri mühendisliği ne demek, bilmiyordum. Makine falan biliyorduk ama bilgisayar yoktu, Denizli'de hiç yoktu zaten. Yani benim çevremde, 1976'larda üniversiteyi bitiren de pek yoktu. Hiç yoktu diyemem belki bir kişi çıkabilir falan diye. Bu yüzden seçilecek konular hakkında çok da fikir sahibi değildim. Kimyaya, fiziğe de fazla ilğim yoktu. Matematik herkesin bildiği, oturup kitapla çalışabileceğin bir şeydi. Kendi başına yapılabilirdi, bir defter, bir kitap yeterliydi. Bu yüzden matematiği tercih ettim.

Ama esas olarak matematiği tanımam, ne olduğu hakkında fikrim olması, doğru dürüst nerede yapılır sonradan öğrendim. Hatta ODTÜ'de lineer cebir dersindeydik, ikinci sınıftaydım. Her hocanın bir odası olduğunu bile bilmiyordum. Her teneffüste hocaya soru sormaya çalışıyorum. O zamanlar hocamız, şimdi Doğuş Üniversitesi'nde olan Prof. İsmail Güloğlu'ydu. Herhalde usandığından bir gün dedi ki: "Benim odam var, niye gelip orada sormuyorsun bu soruları?" Sonradan öğrendim her hocanın bir odası olduğunu. Yani o kadar cahil geldik buraya.

SŞ/TT: Peki, sizi yönlendiren kimse oldu mu?

Burada çok oldu. ODTÜ'ye gelince birçok yeni şeyle karşılaştım. Bilmediğim şeyler hakkında fikir sahibi olunca, değişik konularda dersler alınca tabii biraz da başarabildiği dersi seviyor insan. Ben biraz cebiri sevdim. O zaman iyi hocalarımız da vardı burada. Cebiri seçmeye karar verdim ve öyle devam etti. Hep bir sonraki basamak... Master nedir bilmiyordum ODTÜ'ye geldiğimde, öyle söyleyeyim.

SŞ/TT: Peki hocam, akademik hayatınızda sizi derinden etkileyen bir dönüm noktası oldu mu? Bu dönüm noktası sizi nasıl değiştirdi?

ODTÜ’de bir sürü şey öğrendik ama üniversite bitince yurt dışına gitmem gerektiğini öğrendim. O konuda çok net bir karar verdim. Çünkü burada aldığım eğitim sırasında, çocukça belki ama, gitmenin gerekli olduğunu anladım okuduğum kitaplardan, buradaki izlenimlerden, derslerden... Bir de biz, okulu bitirir bitirmez asistan olduk. Alt katta oturuyorduk o zaman, orası ikinci bir eğitim yuvası gibiydi. Hep benden tecrübeli asistanlarla oturur, kalkar, konuşurduk. O zamanlar yemeklere birlikte gidilirdi. Oralarda çok şey öğrendim. Onlardan biri de İrfan Altaş’tı, o da asistandı. Şimdi Avustralya’da bilgisayar, nümerik analiz konularında profesör olarak çalışıyor. Onunla birlikte Amerika’ya müracaat ettik.

O zamanlar e-mail falan yok. Mektupla başvuru yapıyoruz. Mektup da pahalı. İki asistan birleşip, başvurularımızı aynı zarfa koyardık. Hem daha ucuz olurdu hem de o kadar az paramız vardı ki mecburduk. Bir de başvuruların çoğu kayıt parası isterdi. O zamanlar Türkiye’de cebinde dolar taşımak yasaktı. Doları gerekçesiz bulunduramazdın. Merkez Bankası’ndan gerekçeli olarak 20-30 dolar alabilirdin. Ben üniversiteye mektup yazdım, halimizi anlattım. Anladılar ama affetmediler. Amerika’ya gittikten sonra yine de o kayıt parasını aldılar benden. :)

Türkiye’deyken İngiltere’deki Manchester Üniversitesi’ne de doktora yapmak için müracaat etmiştim. Burs alabilmem için de bana master tezini yaz gönder dediler. Ama o tarihe kadar tezim yetişmedi. Amerika’daki Toledo Üniversitesi’nden asistanlık alınca da onlara bir mektup gönderdim:

"Kusura bakmayın, tezim zamanında yetişmedi. Tezim ektedir. Toledo Üniversitesi’ne gidiyorum, adresim şudur." dedim ve Amerika’ya gittim. Christmas zamanıydı. Bir mektup geldi Manchester’dan: "Tezinizi gördük. Hâlâ gelmek ister misiniz? Bursunuz hazır." dediler. Hemen atladım tabii. Çünkü orada benim çalışmak istediğim Prof. Dr. Brian Hartley vardı, dünya çapında bir profesördü. Sonradan da tez hocam oldu. Hemen kabul ettim.

Manchester Üniversitesi’nin kabulü eylül ayı için geçerliydi. Toledo’da aralıktan sonra da işlemler devam etti. Ben de Toledo’da yüksek lisansa başlamıştım, master yapıyordum; ardından doktora yapacaktım. Orada ayrıca şöyle bir program vardı: belirli dersleri alırsanız, belirli sınavlara girerseniz, tezsiz bir yüksek lisans programı kapsamında size bir diploma veririz deniyordu. Benim de köylülüğüm tuttu. Bana "Sen Amerika’da bir yıl kaldın, ne yaptın?" diye sorulduğunda, hiç olmazsa "master yaptım" diyebileyim istedim. Bu haberi duyduktan sonra, ikinci dönemde sanırım, o programı tamamlama kararı verdim. Biraz fazla sayıda ders aldım. O yıl sonunda da gerekli sınavlara girdim. Ve hemen ardından İngiltere’ye direkt geçiş yaptım.

Bu kadar uzun anlatmamın sebebi şu: Türkiye’den Amerika’ya gitmek büyük bir kültür şoku yaratıyor. Amerika’da adece kültürel değil, matematiksel bir fark da var. Disiplin çok başka. Haftalık ödev veriyorlar, topluyorlar, okuyorlar. Biz Türkiye’de ödev vermeyi iyi biliyoruz, okumayı az biliyoruz, geri vermeyi hiç bilmiyoruz. Buradaki hocalara haksızlık olmasın, Amerika’da sistem oturmuş, asistanlar sayesinde bunun sürekliliği sağlanıyor. Bizde bu yoktu. Ben de gençliğimde bir iki heveslendim de sonra sonra enerji kalmıyor.

İngiltere’ye geçtiğimde ise bambaşka bir atmosfer vardı. Amerika’daki gibi değildi fakat orada da başka bir disiplin ve matematik kültürü vardı. Bursu aldık ama karşılığında beklenen talebin büyüklüğünü de ilk günden gördük. Kaydımı yaparken biri şöyle dedi: "Aldığın bursun kıymetini bil. Onu bekleyen binlerce öğrenci var bu ülkede." Kimdi bilmiyorum ama uyanmama vesile oldu diyebilirim.

"Orada, araştırmamanın kıymetini; tez hocamla her hafta yapılan görüşmelere hazırlıksız gitmemenin gerekliliğini; 'Bu haftalık böyle oluversin' dememenin önemini öğrendim. Gerçek bir disiplin vardı. O kültürü yaşarken anlamıyorsun ama sonradan hayatının bir parçası olduğunu fark ediyorsun. Bir çocuk ailesinden nasıl kültür alırsa biz de oralarda öyle bir kültür aldık.

SŞ/TT: Kültür şoku yaşadığınızı söylediniz. Genç yaşta denizaşırı bir yere gitmek, yeni kültürler tanımak, bir de üzerine matematiğin zorluğu... Bütün bunların altından nasıl kalktınız?

Açıkçası denize düşmek gibiydi. Boğulmamaya çalıştık. Üzerinde düşünecek pek fırsat olmadı. Yapmamız gerekenleri yetiştirmeye çalıştık, yaptık. Kolay değildi. Ama benim özelimde, matematiğin doyuruculuğu birçok şeyi hallediyordu. Özlem duyuluyor elbette ama karalara bağlayacak vakit olmuyor. Her hafta ödev veriyorlar, onları okuyorlar, geri getiriyorlar. Neyin yanlış, neyin doğru olduğunu gösteriyorlar. Matematik bölümünde çok temiz insanlar vardı. Kültürel olarak da iyi gördüm. Oda arkadaşım Amerikalıydı mesela. Evlendi, düğününe gittik, Amerikalıların düğünü nasıl oluyormuş gördük. :)

Zaten Türkiye’de, mesela Denizli’den Ankara’ya gelince bile bir kültür değişimi yaşanıyor. Benim için İngiltere’ye gitmek bu değişimlerin ortasında daha dengeli bir yerdeydi. Orada akademik olarak çok güzel bir ortam vardı. Oralarda okurken de çağrıldığım her yere gittim, ilgilenen herkesle konuştum. Dolayısıyla kafamda var olan soru işaretleri gitti ve dünyanın öyle çok da büyük olmadığını gördüm. Almam gereken kültürü aldım ve yapmak istediğimi yapıp istemediklerimi yapmadım. Yaşarken ne olup bittiğini anlamıyorsun ama bir çocuk büyürken ailesinden nasıl kültür alıyorsa biz de oralarda öyle bir kültür aldık.

SŞ/TT: Şu anki öğrencilerle kendi öğrenciliğinizi kıyasladığınızda ne söylemek istersiniz?

Herkesin bulunduğu dönem kendine zor. Şimdiki öğrencilerin olanaklarının daha fazla olduğunu düşünüyorum. Bizim zamanımızda internet yoktu, bilgiye erişim bu kadar yaygın değildi. Şimdi internette çok bilgi var ama doğrusunu seçmek zor. Bizim zamanımızda bilgi yoktu, biz bilgiye açtık. ODTÜ’nün kütüphanesi çok iyiydi. Biz iyi bir ham maddeydik; bizi bir şekle sokmaya çalıştılar.

Amerika çok disiplinliydi, bizi bir şekle soktular. İngiltere kendi başına ayrı bir kültürdü. Matematiksel kültürün izlerini oradaki matematikçilerde hissediyordunuz. O izler seni ister istemez etkiliyor ve öğreniyorsun.

Şimdiki öğrenciler de bence çok aç. Ama biz öğrencilere yeterince erişemiyoruz. Bunun kasıtlı bir nedeni yok. Hocaların da öğrencilerin de pek imkânı yok birbirine ulaşmak için. Ben ancak seçmeli derslerde 25-30 kişilik sınıflarda öğrencilerin tavırlarını, sınav kağıtlarını okuyarak bir fikir sahibi olabiliyorum. Ama 100 kişilik sınıfta bu mümkün olmuyor. Kimseyi suçlamıyorum tabii, bu zaman da böyle işte. Bizim zamanımızda sınıflar daha küçüktü. Hocalar daha çok ilgileniyordu. Ben özellikle matematiği seçtikten sonra çok küçük sınıflarda ders aldım. Hocalar bizi tanırdı. Sorduğumuz sorulardan, sınıftaki oturmuş kalkışımızdan... Emek veren çok hocamız oldu.

SŞ/TT: Peki hocam, gelecek kaygısı açısından bakalım bir de. Matematik bir adanmışlık istiyor. Geleceği çok da düşünmüyorsun, matematikle ilgilenmek seni o an için yeterince tatmin ediyor. Ama siz kendi öğrenciliğinizde “tünelin sonunda bir ışık var” diyebiliyor muydunuz?

Bu zor bir soru. Kaygı her zaman vardı. Özellikle saf matematikte bu daha yoğun. Çünkü uygulamalı matematikten endüstriye geçmek mümkün ama saf matematikte tek hedef akademisyenlik. Asistan olacaksın, sonra öğretim üyesi... Bizim zamanımızda bu rotayı tamamlarsan Türkiye’de iş bulma ihtimalin vardı. Şimdi bu olasılık daha düşük. Sadece Türkiye’de değil, dünyada da öyle.

Ben artık öğrencileri cebire veya grup teorisine yönlendirme konusunda eskisi kadar hevesli değilim. Nihayetinde aç karnına matematik olmuyor. Zengin olmak istemiyoruz ama en azından karnımızı doyuracak bir maaş olmalı. Bu da şu anda uygulamalı matematikte daha mümkün. Kriptoloji olabilir, finansal matematik olabilir.

Ben saf matematikçiyim, tabii ki aynı zevk olur mu dersiniz, olmaz derim. Ama hangi branş olursa olsun, doğru dürüst matematik yapmak hâlâ mümkün. Yeter ki kolaya kaçmayın. Ali, Ayşe kolay yoldan gidiyor ben de oradan gidip “profesör” olayım demeyin. Matematiğe gönül ilişkisiyle bağlanırsanız, hangi konuda olursa olsun kaliteli matematik yapmak mümkün.

SŞ/TT: Türkiye'ye dönme kararınızda ne etkili oldu? Yurt dışında kalmayı hiç düşündünüz mü?

Hayır, kalmak istemedim. Bunun sebebini tam bilmiyorum. Belki kültürel, belki ailevi. Başka bir ülkede bir hedef uğruna kalabilirsin, ama o hedef bitince orada kalmanın anlamı yok. Ben o hedefi Türkiye'de gerçekleştirmeyi tercih ettim.

SŞ/TT: Sizin için başarı ne demek hocam? Akademik başarı ile kişisel tatmin arasında nasıl bir ilişki var sizce?

Akademik başarı hissi zor bir şey. Kendi kendine "başardım" demekle olmaz. Bu başarı, dünyada senin konunda çalışan insanlar arasında nerede olduğunu sormadan gelmez. Yerel başarı insanı ancak kibirlendirir.

SŞ/TT: Dinlediğim bir röportajda Aziz Sancar da benzer bir şey söylüyordu. İstanbul Üniversitesi'ni birincilikle bitirmiş ama Amerika'ya gidince kendini, kendi tabiriyle, bir şey zannetmeye başlamış. Saygın bir üniversitenin tıbbından birincilik alması onu üstün hissettirmiş. Sonra üstünlük kurduğunu sandığı ülkenin insanların uzaya vızır vızır araç gönderdiğiyle yüzleşince anlamış kimle mücadele ettiğini. Sizin de dediğiniz gibi.

Evet, ben de benzer bir şeyi İngiltere'de yaşadım. Amerika'daki sistemden farklıydı. Amerika'da belli dersleri alman lazım ama İngiltere'de seminerler vardı. Hocalar ve öğrenciler birlikte katılırdı. Manchester Üniversitesi'nde doktora öğrencileri olarak bir seminer başlatmıştık, hocama danışarak kitap seçtik. Tony Springer'ın Linear Algebraic Groups kitabını okuduk. Hocalardan katılmak isteyenler oldu ama biz, "sizin yanınızda soru soramayız, tartışmaya çekiniriz" deyip kibarca yalnız kalmayı tercih ettik.

Sonra bir dönem Cambridge'den bir sayılar teorisi hocası geldi. Yanında 4-5 asistan getirmişti. Seminerde bir anda seviye yükseldi. Gerçek bir mücadele başladı. Daha bilgili insanlarla olmak seni geliştiriyor. Onlardan çok şey öğrendim. Alt katta asistanlıkta öğrendiklerim gibi. Daha bilgili ve tecrübeli, daha vizyonluydular. Seviye yükselten bir şeydi.

SŞ/TT: Matematiksel olgunluk hakkında ne düşünüyorsunuz? Hayata bakışınızı nasıl etkiledi?

Ben hayatımdan çok memnunum. Sanatçıların dediği gibi, yani matematikle bir daha karşılaşsam yine yaparım. Problem çözme sanatını hayatın içinde kullanabilirsen mutlu olmak daha kolay. Ama matematik zor bir iş. Severek yapmazsan çekilmez. Matematik bir yerde hayatınızın akışı başka bir yerdeyse çok zor. Birleştiremeyenler çok mutsuz oluyor.

SŞ/TT: Peki hocam, yaşın yaratıcılığa etkisi hakkında ne dersiniz? Derler ya, 25 yaşa kadar yaratıcılığın zirvesidir diye, matematikte böyle midir hakikaten yoksa matematik olgunlukla mı olur?

Yaratıcılık Tanrı vergisi değil bence. Aklıma ırmak geliyor. Bir kaynaktan doğar ve yeni kollar eklendikçe büyüyerek ilerler. Yaratıcılık da o nehrin ivmesi gibi artar. Biz de sürekli bir şeyler eklemesek, bilgi ve beceriyi artırmazsak durgun bir su gibi kalırız. Matematikçilerin hiçbiri ilahi insanlar değil.

Ben, İngiltere'nin en iyi matematikçilerinden biri olan Prof. Dr. Brian Hartley ile çalıştım, tez hocam olur kendisi. İtalya'dan, Rusya'dan, Beyaz Rusya'dan, Almanya'dan, Ukrayna'dan çok iyi matematikçilerle; değişik insanlarla çalıştım ve onları günlük hayatlarında da gözlemledim. Çalıştığım insanlar çok mutluydu. Çünkü yukarıda bahsettiğim birleştirmeyi yapabilmişlerdi. En gıptayla baktığım matematikçilerin hepsi benden en az iki kat fazla çalışıyordu. Ucuzdan yaratıcı olunmaz.

SŞ/TT: Şansa bağlı mı peki? Yoksa her an hazır olmak mı lazım?

Hazır olacaksın. Fırsat geldiğinde değerlendireceksin. Mesela Amerika'da havuzlu evde kalıyordum. İyi bir bursum vardı. Ama İngiltere'den cevap gelince, bursum neredeyse yarısı kadar olmasına rağmen hiç düşünmeden kabul ettim. Matematiksel olgunluk doğru tercihe yönlendirmelidir dediğim de buydu işte. Doğru da yaptığımı düşünüyorum.

SŞ/TT: Hocam, peki hobileriniz var mıydı? Film, müzik, kitap?

Benim en sevdiğim şey yürüyüş yapmak. İngilizlerden öğrendim. Hocam beni ailesiyle dağa yürüyüşe çağırmıştı. O zamanlar Türkiye’de yoktu öyle şeyler. Dedim ben köylü çocuğuyum, biz dağa bahçeye ancak tarlamız falan varsa gideriz, yürümeye gitmeyiz. :)

Gel sen beğenmezsen devam etmezsin dedi ve ben ilk gün çok memnun kaldım. Bütün sorularımı sorabilmişim. Dedim böyle olacaksa ben hep gelirim. Sonra her hafta gittim. Yanıma sorularımı yazdım: Sağ cebe en önemliler, sol cebe orta önemliler, arka cebe sıradakiler. Yolda hepsini sordum. Çok şey öğrendim oralarda.

SŞ/TT: 20’li yaşlarınıza ne söylemek isterdiniz?

İlkyar (ilköğretim) öğrencilerine ODTÜ’de seminerler verirken şöyle başlardım: Resmini gördüğünüz köy evinde doğdum, şimdi profesörüm. :)

Ama önemli olan ne istediğine karar vermek. Gerçekten seviyor musun? Seviyorsan devam et. Gözünün yaşına bakma. Mücadelenin gerektirdiği yarışlara da girmekten kaçınmamak lazım ama.



Prof. Dr. Mahmut Kuzucuoğlu’nun 1958’de Denizli’nin Çal ilçesinin Ortaköy kasabasında doğduğu ev

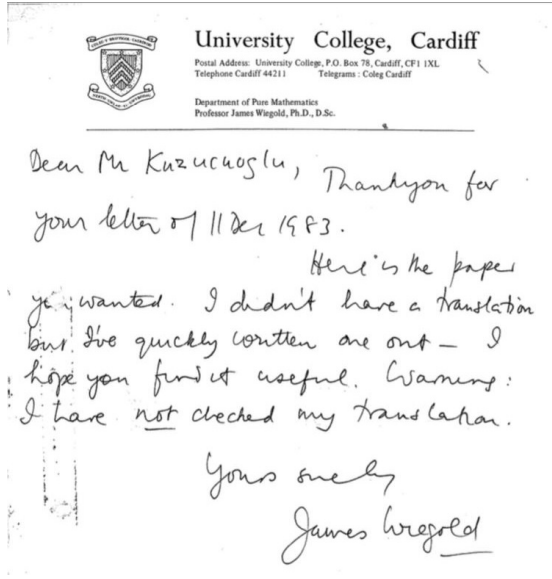
SŞ/TT: Hocam bir de matematikçiyle evli olmak nasıl bir şey?

Çok güzel bir şey. Yabancı bir ülkede aynı dili konuşan iki kişi gibi oluyorsun.

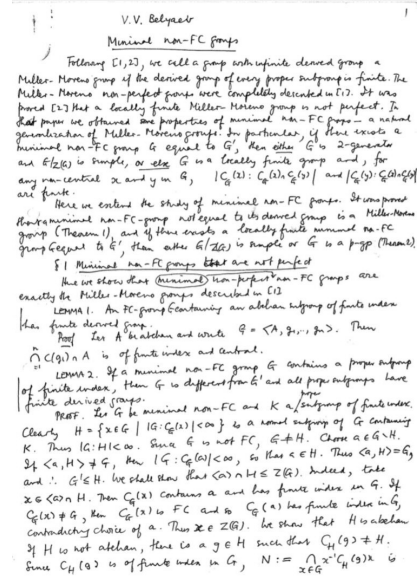
SŞ/TT: Son olarak size ilham olan bir olaydan bahseder misiniz?

İngiltere’nin Cardiff şehrindeki bir üniversiteden çok meşhur bir matematikçi vardı, James Wiegold. Benim web sayfamda da bahsettiğim bir isim. Size kısaca özetleyeyim: Ben o zamanlar sizin yaşlardayım, hatta bir yaş büyüğünüzdüm. Yüksek lisans tezimi yazıyordum. Tez hocam bana bir makale gösterdi ve “Bunu bul” dedi. Gittim baktım, makale Rusça. Yıl 1982 civarı. Türkiye’de o zamanlar Rusça bilen neredeyse yok. Sovyetler dağılmamış. Ama hocam ısrar etti. Ben de üniversite kütüphanesine gittim. O dönem internet yok tabii. “Mathematical Reviews” diye bir kaynak vardı, oradan makalelerin özetlerini bulabiliyorduk. Bu Rusça makaleyi kimin okuduğunu oradan tespit ettim. O kişiye bir mektup yazdım: “Bu makale Rusça. Sizin okuduğunuzu görüyorum. Elinizde çevirinin kopyası varsa bana gönderebilir misiniz?”

O zamanlar mektup 15 günde gider, 15 günde gelir. Bir ay sonra cevap geldi. Diyor ki: “Mahmut, kusura bakma. Ben Rusça bildiğim için okudum geçtim, yazılı bir çeviri yapmamıştım. Ama senin için çeviriyorum şimdi. Daktilo edemedim, el yazısıyla yolluyorum. Kusura bakma.” Ve gerçekten, el yazısıyla makalenin çevirisini göndermiş.



James Wiegold'dan gelen mektup



James Wiegold'un el yazısı makale çevirisi

Yıllar sonra beni İtalya'ya, Ischia adasındaki bir konferansa davet ettiler. Konferansa gitmeden 15-20 gün önce dediler ki: "Şu gün James Wiegold anısına ayrıldı. O gün konuşma yapmak ister misin?" Wiegold ismi bana tanıdık geldi ama çıkaramadım. Eski dosyalarımı karıştırmaya başladım. Meğer o, yıllar önce bana Rusça makaleyi çevirip gönderen kişiymiş. Vefat etmiş. O gün de onun anısına konuşma yapmışlar. Ne beni çağıranlar bunu biliyordu ne de ben. Tam bir tesadüf. Elimde hâlâ onun el yazısıyla gönderdiği mektup ve çeviriler duruyor. O belgeleri alıp konferansta gösterdim. Dedim ki: "Bugün James Wiegold'un günüyümüş. Benim de onunla böyle bir anım var."



2012 yılında İtalya'nın Ischia adasında yapılan konferanstan

Oradakiler çok etkilendi. Meğer kendisi zaten böyle incelikli davranışlarıyla da tanınan biriymiş. Bu olayı hayatımın felsefesi haline getirdim. O beni hiç tanımadığı hâlde bunu yaptıysa, ben de bir başkasına yardım etmeyi görev bilmeliyim.

Size özellikle bu hikâyeyi anlatmak istedim. Umarım ilham olur.

SŞ/TT: Evet hocam, çok teşekkür ederiz. Gerçekten büyük bir zevkti bizim için.

■ Hazırlayanlar

SELCAN ŞENYURT

Hacettepe Üniversitesi Matematik Bölümü, 2. Sınıf Öğrencisi

✉ senyurtselcan409@gmail.com

TALHA TİN

Hacettepe Üniversitesi Matematik Bölümü, 3. Sınıf Öğrencisi

✉ talhatin@gmail.com



Karmaşık Sayılar ve Düzlem Geometrisi

UĞUR GÜL

Hacettepe Üniversitesi Matematik Bölümü

✉ gulugur@hacettepe.edu.tr



Bu yazıda Kartezyen düzlem $\mathbb{R}^2$ 'deki herhangi bir $(x, y) \in \mathbb{R}^2$ noktasını karmaşık düzlemdeki $z := x + iy \in \mathbb{C}$ noktasına eşleyerek ve karmaşık sayıların üzerindeki standart toplama ve çarpma işlemlerinin özelliklerini kullanarak düzlem geometrisindeki birtakım sonuçları elde edeceğiz. Bu sonuçlar bir üçgenin alanını kenar uzunlukları cinsinden veren Heron formülü, köşeleri aynı çember üzerindeki bulunan bir dörtgenin kenar uzunluklarının sağlaması gereken şartı belirten Batlamyus Teoremi ve herhangi bir dörtgeninin kenarları üzerinde kurulan karelerin merkezleri karşılıklı birleştirildiğinde oluşan doğru parçalarının uzunluklarının eşit olduğunu ve birbirlerine dik olduklarını söyleyen Van Aubel Teoremidir.

1. Karmaşık Sayılar

1.1. Karmaşık Sayıların Tanımı

Bu kısımda karmaşık sayıların tanımını yapacağız. Karmaşık sayıları oluşturan temel fikir gerçel sayı sistemi $\mathbb{R}$ 'ye $i^2 = -1$ denklemini sağlayan bir sayı ilave etmektir. Hiçbir gerçel sayının bu denklemi sağlayamayacağı aşikardır, zira $x \in \mathbb{R}$ ise $x^2 \geq 0$ olduğundan $x^2 + 1 \geq 1 > 0$ olur. Yani $x \in \mathbb{R}$ olduğunda hiçbir zaman $x^2 + 1 = 0$ olamaz. Gerçel sayılar kümesine dahil olmayan bu “farazi” i sayısına **sanal (imajiner) sayı** denir.

Gerçel sayılar kümesi $\mathbb{R}$ 'ye $i^2 = -1$ denklemini sağlayan sanal bir i sayısı eklersek

$$\mathbb{R}[i] := \left\{ \sum_{k=0}^n a_k i^k : a_k \in \mathbb{R}, i^0 = 1 \right\}$$

halkasını elde ederiz. Bir $p(x) = \sum_{k=0}^n a_k x^k$ polinomunun derecesi $\deg(p) \geq 2$ ise bölme algoritması uygulayarak

$$p(x) = (x^2 + 1)q(x) + r(x)$$

elde edilir ki burada q bir polinom ve r derecesi en fazla 1 olan bir polinomdur, yani $a, b \in \mathbb{R}$ olmak üzere, $r(x) = bx + a$ şeklindedir. Bu durumda

$$p(i) = \sum_{k=0}^n a_k i^k = (i^2 + 1)q(i) + r(i) = r(i) = a + ib$$

sağlanır. O hâlde

$$\mathbb{R}[i] := \left\{ \sum_{k=0}^n a_k i^k : a_k \in \mathbb{R}, i^0 = 1 \right\} = \{a + ib : a, b \in \mathbb{R}\}$$

dir. Bu sayı sistemine

$$\mathbb{C} := \mathbb{R}[i] = \{x + iy : x, y \in \mathbb{R}\}$$

karmaşık sayılar sistemi denir.

Bir $z \in \mathbb{C}$ karmaşık sayısının, $a, b \in \mathbb{R}$ olmak üzere, $z = a + ib$ şeklinde tek bir gösterimi vardır, yani $a_1, b_1, a_2, b_2 \in \mathbb{R}$ iken $z = a_1 + ib_1 = a_2 + ib_2$ ise $a_1 = a_2$ ve $b_1 = b_2$ sağlanır ki bu da $a, b \in \mathbb{R}, a + ib = 0 \Rightarrow a = b = 0$ olmasına denktir: Varsayalım ki $a + ib = 0$ fakat $a \neq 0$ veya $b \neq 0$ olsun, genelliği kaybetmeden

$b \neq 0$ varsayabiliriz, o halde $ib = -a \Rightarrow i = -\frac{a}{b} \Rightarrow \frac{a^2}{b^2} = -1 = (\frac{a}{b})^2$, yani bir $r = \frac{a}{b} \in \mathbb{R}$ için $r^2 = -1$ olur ki bu da bir çelişki doğurur. O halde $a + ib = 0$ ise $a = b = 0$ olmalıdır.

Karmaşık sayılar kümesinde iki tane $x_1 + iy_1, x_2 + iy_2$ sayıları aldığımızda onların toplamını aşağıdaki gibi yaparız:

$$(x_1 + iy_1) + (x_2 + iy_2) = (x_1 + x_2) + i(y_1 + y_2).$$

Örnek 1.

$z_1 = 1 + 3i$ ve $z_2 = 4 - 2i$ ise

$$z_1 + z_2 = (1 + 4) + i(3 + (-2)) = 5 + i$$

olur.

Çarpmayı da en doğal şekliyle aşağıdaki gibi yapabiliriz:

$$(x_1 + iy_1)(x_2 + iy_2) = x_1x_2 + ix_1y_2 + iy_1x_2 + i^2y_1y_2 = (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1)$$

Örnek 2.

$z_1 = 2 + 3i$ ve $z_2 = 3 + 4i$ ise

$$z_1z_2 = (2 \cdot 3 - 3 \cdot 4) + i(2 \cdot 4 + 3 \cdot 3) = -6 + 17i$$

olur.

Bu işlemlerle $(\mathbb{C}, +, \cdot)$ kümesi bir cisim oluşturur: Yani $(\mathbb{C}, +)$ değişmeli bir gruptur, aynı şekilde $(\mathbb{C} - \{0\}, \cdot)$ de değişmeli bir gruptur ve toplama işlemi çarpma işlemi üzerinden dağılma özelliğine sahiptir:

$$z_0(z_1 + z_2) = (z_1 + z_2)z_0 = z_0z_1 + z_0z_2 \quad \forall z_0, z_1, z_2 \in \mathbb{C}$$

denklemini sağlar.

Bir $z = x + iy$ karmaşık sayısı için x 'e z 'nin **gerçel kısmı**(İng. real part), y 'ye de **sanal kısmı**(İng. imaginary part) denir ve

$$x = \Re(z) \quad y = \Im(z)$$

şeklinde gösterilir. İki karmaşık sayı eşittir ancak ve ancak gerçel ve sanal kısımları birbirine eşittir. Bir $z = x + iy$ karmaşık sayısı verildiğinde $\bar{z} = x - iy$ karmaşık sayısına z 'nin **karmaşık eşleniği**(İng. complex conjugate) denir. Karmaşık eşlenik almanın toplama üzerinde dağıldığı aşikardır:

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$$

Karmaşık eşlenik alma çarpma üzerinde de dağılır:

$$\begin{aligned} \overline{(z_1z_2)} &= \overline{(x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1)} = (x_1x_2 - y_1y_2) - i(x_1y_2 + x_2y_1) \\ &= (x_1x_2 - y_1y_2) + i(x_1(-y_2) + x_2(-y_1)) = (x_1 - iy_1)(x_2 - iy_2) = \bar{z}_1\bar{z}_2 \end{aligned}$$

Bir karmaşık sayı gerçeldir ancak ve ancak karmaşık eşleniği kendisine eşittir. Daha genel olarak bir karmaşık sayının gerçel ve sanal kısımlarının kendisi ve eşleniği cinsinden ifadesi aşağıdaki gibidir:

$$\Re(z) = \frac{z + \bar{z}}{2}, \quad \Im(z) = \frac{z - \bar{z}}{2i}. \quad (1)$$

Karmaşık eşlenik iki karmaşık sayıyı birbirine bölmek istediğimizde çok işimize yarar, çünkü $z = x + iy$ için

$$z \cdot \bar{z} = (x + iy)(x - iy) = x^2 + y^2 \in \mathbb{R} \quad (2)$$

olduğundan $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$ verildiğinde eğer $z_2 \neq 0$ ise

$$\frac{z_1}{z_2} = \frac{x_1 + iy_1}{x_2 + iy_2} = \frac{(x_1 + iy_1)(x_2 - iy_2)}{(x_2 + iy_2)(x_2 - iy_2)} = \frac{(x_1x_2 + y_1y_2) + i(x_2y_1 - x_1y_2)}{x_2^2 + y_2^2}$$

gerçekleşir.

Örnek 3.

$z_1 = 3 + 4i$ ve $z_2 = 2 + i$ ise

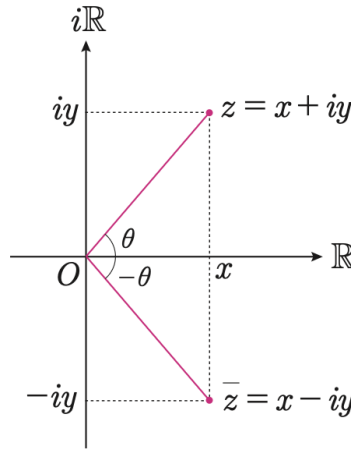
$$\frac{z_1}{z_2} = \frac{(3.2 + 4.1) + i(4.2 - 3.1)}{2^2 + 1^2} = 2 + i$$

olur.

Karmaşık sayılar kümesi $\mathbb{C}$ 'yi Kartezyen düzlem $\mathbb{R}^2$ olarak görmek çoğu zaman büyük avantaj sağlar. Bu aşağıdaki eşleştirmeye sağlanır:

$$x + iy \in \mathbb{C} \longleftrightarrow (x, y) \in \mathbb{R}^2$$

Bu eşleştirmeye $\mathbb{R}^2$ Kartezyen düzlemindeki y eksenini sanal eksene dönüştür. Karmaşık sayılar kümesi $\mathbb{C}$ 'nin bu eşleştirme kullanılarak yapılan geometrik gösterimine **karmaşık düzlem** (İng. complex plane) denir.



1.2. Mutlak Değer

Karmaşık sayılar kümesi $\mathbb{C}$ 'yi $\mathbb{R}^2$ Kartezyen düzlemi ile özdeşleştirdikten sonra $\mathbb{R}^2$ 'ye konulan norm $\mathbb{C}$ 'nin üzerine de doğal olarak konulabilir:

$z = x + iy \in \mathbb{C}$ olsun,

$$|z| = \|(x, y)\| = \sqrt{x^2 + y^2}$$

şeklinde tanımlanan $|z|$ niceliğine z 'nin **mutlak değeri** (İng. absolute value) denir. Mutlak değer en önemli özelliği pozitif bir nicelik olmasıdır. Yani $|z| \geq 0$ eşitsizliği bütün $z \in \mathbb{C}$ için sağlanır. Ayrıca $|z| = 0$ dır ancak ve ancak $z = 0$ dır. Bir önceki kısımdaki (2) no'lu denklemden $|z|$ ile z 'nin karmaşık eşleniği arasındaki aşağıdaki münasebet anında farkedilir:

$$|z|^2 = z \cdot \bar{z}$$

Bu denklemden ve (2) numaralı denklemden $|\cdot|$ niceliğinin de çarpma üzerinden dağıldığını rahatlıkla görebiliriz:

$$|z_1 z_2|^2 = (z_1 z_2) \overline{z_1 z_2} = (z_1 z_2) \bar{z}_1 \bar{z}_2 = z_1 \bar{z}_1 z_2 \bar{z}_2 = |z_1|^2 |z_2|^2 \quad (3)$$

Ayrıca

$$|\bar{z}| = |z|$$

olduğunu görmek zor değildir.

Örnek 4.

$z_1 = 3 + 4i$ ve $z_2 = 2 + i$ ise

$$|z_1| = |3 + 4i| = \sqrt{3^2 + 4^2} = \sqrt{9 + 16} = \sqrt{25} = 5$$

ve

$$|z_2| = |2 + i| = \sqrt{2^2 + 1^2} = \sqrt{4 + 1} = \sqrt{5}$$

dir.

Bu $|\cdot|$ niceliğine mutlak değer denilmesi tesadüf değildir zira $\mathbb{R}$ 'deki mutlak değer bir nevi genişlemesidir: Eğer $z = x + iy$ 'de $y = 0$ alınırsa $|z| = \sqrt{x^2} = |x|$ olur. Gerçek sayılar $\mathbb{R}$ 'deki mutlak değer üçgen eşitsizliği dediğimiz aşağıdaki eşitsizliği sağlar:

$$|x + y| \leq |x| + |y| \quad \forall x, y \in \mathbb{R}$$

Aynı eşitsizliğin doğru olmasını karmaşık sayılarda da bekleyebiliriz:

Teorem 1. (Üçgen Eşitsizliği)

$$|z_1 + z_2| \leq |z_1| + |z_2| \quad \forall z_1, z_2 \in \mathbb{C}$$

Kanıt.

$$|z_1 + z_2|^2 = (z_1 + z_2)(\bar{z}_1 + \bar{z}_2) = |z_1|^2 + z_1\bar{z}_2 + z_2\bar{z}_1 + |z_2|^2$$

Bir önceki kısımdaki (1) no'lu denklemden ($z = z_1\bar{z}_2$ alınarak)

$$z_1\bar{z}_2 + z_2\bar{z}_1 = 2\Re(z_1\bar{z}_2)$$

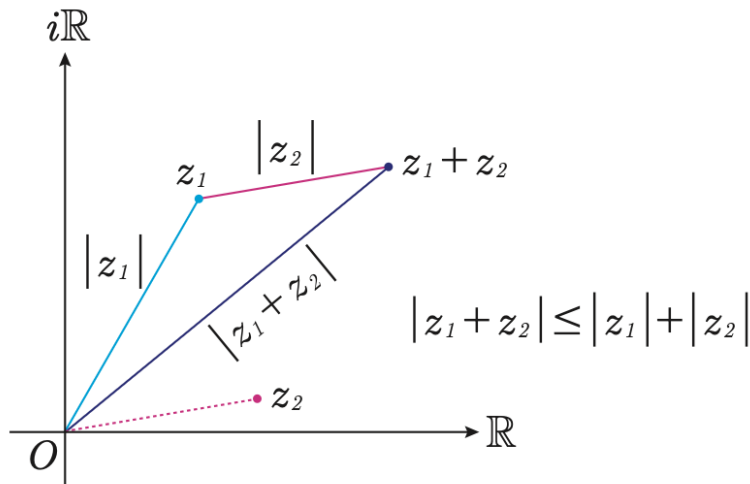
ve her $z \in \mathbb{C}$ için

$$|\Re(z)| \leq \sqrt{(\Re(z))^2 + (\Im(z))^2} = |z|$$

olduğundan ve (3) no'lu denklemden

$$\begin{aligned} |z_1 + z_2|^2 &= |z_1|^2 + |z_2|^2 + 2\Re(z_1\bar{z}_2) \leq \\ &|z_1|^2 + |z_2|^2 + 2|z_1\bar{z}_2| = \\ &|z_1|^2 + |z_2|^2 + 2|z_1||z_2| = (|z_1| + |z_2|)^2 \end{aligned} \quad (4)$$

elde edilir ki bu da üçgen eşitsizliğini kanıtlar. $\square$



1.3. Kutupsal Gösterim

Karmaşık sayılar kümesi $\mathbb{C}$ 'yi Kartezyen düzlem $\mathbb{R}^2$ ile özdeşleştirdikten sonra $\mathbb{R}^2$ üzerindeki kutupsal koordinatları $\mathbb{C}$ üzerine de koyabiliriz. İlk önce kutupsal koordinatları hatırlayalım: $(x, y) \in \mathbb{R}^2$ için

$$x = r \cos \theta, \quad y = r \sin \theta$$

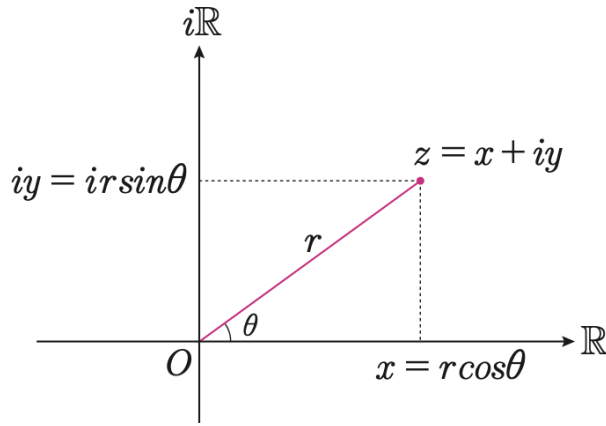
olarak yazdığımızda $r = \sqrt{x^2 + y^2}$, (x, y) 'nin orjine olan uzaklığını ve θ ise x -ekseni ile yaptığı açığı verir. Eğer $z = x + iy$ için yukarıdaki denklemden x ve y 'yi yerine koyacak olursak

$$z = x + iy = r \cos \theta + ir \sin \theta = r(\cos \theta + i \sin \theta)$$

elde edilir. $r = \sqrt{x^2 + y^2} = |z|$ olduğu hatırlanırsa

$$z = |z| (\cos \theta + i \sin \theta)$$

olur.



Bir karmaşık sayının bu şekilde yazılmasına onun **kutupsal gösterimi** (İng. polar representation) denir. Kutupsal gösterimdeki $\cos \theta + i \sin \theta$ karmaşık sayısına z 'nin kutupsal kısmı denir, θ niceliğine ise z 'nin **argümanı** (İng. argument) denir, $\theta = \arg z$ şeklinde gösterilir. Burada birkaç karmaşık sayının kutupsal gösterimlerini örnek olarak vermekte fayda vardır:

Örnek 5.

En basit karmaşık sayı $z = 1$ ile başlayalım:

$$z = 1 = 1(\cos(0) + i \sin(0))$$

olduğundan 1'in kutupsal gösterimi

$$1 = \cos(0) + i \sin(0)$$

şeklindedir. Sonraki doğal örneğimiz $z = i$ imajiner sayısıdır:

$$z = i = 1(\cos(\frac{\pi}{2}) + i \sin(\frac{\pi}{2}))$$

olduğundan i 'in kutupsal gösterimi

$$i = \cos(\frac{\pi}{2}) + i \sin(\frac{\pi}{2})$$

şeklindedir. Bir başka örnek de $z = 1 + i$ sayısıdır. Onun da kutupsal gösterimi

$$1 + i = \sqrt{2}(\cos(\frac{\pi}{4}) + i \sin(\frac{\pi}{4}))$$

şeklindedir.

Bir z karmaşık sayısının kutupsal kısmı olan $\cos \theta + i \sin \theta$ karmaşık sayısını bir sonraki bölümde daha ayrıntılı inceleyeceğiz. Bu $z = \cos \theta + i \sin \theta$ karmaşık sayısının mutlak değerinin 1 olduğu açıktır. Kutupsal koordinatları kullanarak tersini de söyleyebiliriz: Mutlak değeri 1 olan her z karmaşık sayısı $\cos \theta + i \sin \theta$ şeklinde yazılabilir.

1.4. Euler Formülü

Bu kısımda $\cos \theta + i \sin \theta$ sayısını inceleyeceğiz. Trigonometrik fonksiyonlar $\cos \theta$ ve $\sin \theta$ 'yı Analiz derslerinden hatırlayalım: Her iki fonksiyon da sonsuz kere türevlenebilir ve her yerde mutlak yakınsayan Taylor serisine sahiptir. Taylor seri açılımları aşağıdaki gibidir.

$$\cos \theta = \sum_{k=0}^{\infty} (-1)^k \frac{\theta^{2k}}{(2k)!}$$

$$\sin \theta = \sum_{k=0}^{\infty} (-1)^k \frac{\theta^{2k+1}}{(2k+1)!}$$

Yukarıdaki Taylor serileri mutlak yakınsadığı için toplam sıralarını değiştirebiliriz. Serileri $\cos \theta + i \sin \theta$ ifadesine koyarsak

$$\cos \theta + i \sin \theta = \left(\sum_{k=0}^{\infty} (-1)^k \frac{\theta^{2k}}{(2k)!} \right) + i \left(\sum_{k=0}^{\infty} (-1)^k \frac{\theta^{2k+1}}{(2k+1)!} \right)$$

elde edilir. Terimleri θ 'nın kuvvetlerine göre yeniden sıralarsak

$$\left(\sum_{k=0}^{\infty} (-1)^k \frac{\theta^{2k}}{(2k)!} \right) + i \left(\sum_{k=0}^{\infty} (-1)^k \frac{\theta^{2k+1}}{(2k+1)!} \right) = 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + \dots$$

$$= \sum_{k=0}^{\infty} \frac{(i\theta)^k}{k!}$$

elde edilir.

Üstel fonksiyon e^x 'i hatırlayalım: Üstel fonksiyonun da Taylor serisi mutlak yakınsaktır ve Taylor seri açılımı aşağıdaki gibidir:

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

O halde yukarıdaki son üç denklemi birleştirirsek aşağıdaki **Euler¹ Formülünü** elde ederiz:

$$e^{i\theta} = \cos \theta + i \sin \theta$$

Euler Formülünü bir diferansiyel denklemin çözümü olarak elde etmek de mümkündür:

$$z(\theta) = \cos(\theta) + i \sin(\theta)$$

fonksiyonunun türevi

$$z'(\theta) = -\sin(\theta) + i \cos(\theta) = i(\cos(\theta) + i \sin(\theta)) = iz(\theta)$$

verir. Yani

$$z'(\theta) - iz(\theta) = 0$$

diferansiyel denklemi sağlanır. Bir 'c' sabiti için

$$z'(\theta) - cz(\theta) = 0$$

¹Leonard Euler(1707-1783):Matematiksel Analiz ve Mekanik sahalarına önemli ve derin katkıları ile bilinen büyük İsviçreli matematikçi

diferansiyel denklemini çözerken eşitliğin her iki tarafını ' $e^{-c\theta}$ ' ile çarpıp denklemi

$$e^{-c\theta}(z'(\theta) - cz(\theta)) = (e^{-c\theta}z(\theta))' = 0$$

haline getirdiğimiz gibi burada da $c = i$ alıp

$$e^{-i\theta}(z'(\theta) - iz(\theta)) = (e^{-i\theta}z(\theta))' = 0$$

elde ederiz. Bu durumda $e^{-i\theta}z(\theta)$ fonksiyonunun türevi 0 olduğundan sabit fonksiyon olmalıdır ki bu da

$$e^{-i\theta}z(\theta) = C \Rightarrow z(\theta) = Ce^{i\theta}$$

verir. Buradaki C sabiti $\theta = 0$ değeri konularak bulunabilir:

$$z(0) = \cos(0) + i \sin(0) = 1 = Ce^{i0} = C$$

Yani $C = 1$ olmalıdır. Buradan da

$$z(\theta) = \cos(\theta) + i \sin(\theta) = e^{i\theta}$$

elde edilir.

Euler Formülünde $\theta = 2\pi$ alınırsa

$$e^{2\pi i} = 1$$

elde edilir. Bu denklemden

$$e^0 = e^{2\pi i - 2\pi i} = e^{2\pi i} e^{-2\pi i} = 1 = e^{-2\pi i}$$

elde edilir. Son iki denklemi öteleysek, yani defalarca kendi kendine uygularsak

$$e^{2\pi ni} = 1 \quad \forall n \in \mathbb{Z} \quad (5)$$

elde ederiz. Kutupsal gösterimdeki $\cos \theta + i \sin \theta$ yerine Euler Formülünden $e^{i\theta}$ konulursa

$$z = |z| e^{i\theta}$$

elde ederiz. Yukarıdaki (5) no'lu denklemden dolayı $\arg z = \theta + 2\pi n$, $n \in \mathbb{Z}$ alınabilir, yani argüman çok değerli bir nicelik olur ki bu da onun iyi tanımlı olmasını engeller. Bu tuhaf durum genelde argüman için uzunluğu 2π olan bir aralık belirlemek yoluyla düzeltilir. Genelde $-\pi < \arg z \leq \pi$ olarak belirlenen argümana **Asli Argüman** (İng. principal argument) denir ve $\theta = \text{Arg}(z)$ notasyonu ile gösterilir.

Örnek 6.

$z = i$ karmaşık sayısının mutlak değeri $|i| = 1$ ve asli argümanı $\text{Arg}(i) = \frac{\pi}{2}$ dir. Aynı şekilde $z = -i$ karmaşık sayısının da mutlak değeri $|-i| = 1$ ve asli argümanı $\text{Arg}(-i) = \frac{-\pi}{2}$ dir.

İki karmaşık sayı $z_1, z_2 \in \mathbb{C}$ 'nin argümanları eşittir ancak ve ancak bir $n \in \mathbb{Z}$ için $\arg z_1 - \arg z_2 = 2\pi n$ dir. İki karmaşık sayı $z_1, z_2 \in \mathbb{C}$ alalım:

$$z_1 = |z_1| e^{i\theta_1}, \quad z_2 = |z_2| e^{i\theta_2}$$

olduğundan

$$z_1 z_2 = |z_1| |z_2| e^{i(\theta_1 + \theta_2)} = |z_1 z_2| e^{i(\theta_1 + \theta_2)}$$

olur. O hâlde

$$\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$$

olur. Yani iki karmaşık sayıyı çarpmak geometrik olarak mutlak değerlerini çarpıp, argümanlarını toplamak demektir. Dikkat ediniz ki "arg" fonksiyonu da tıpkı $\mathbb{R}$ 'deki logaritma fonksiyonu gibi çarpımları toplamalara dönüştürür. Aynı şekilde iki karmaşık sayı z_1 ve z_2 'nin ($z_2 \neq 0$ olmak üzere) oranlarının argümanı argümanlarının farkıdır:

$$\text{Arg}\left(\frac{z_1}{z_2}\right) = \text{Arg}(z_1) - \text{Arg}(z_2)$$

sağlanır. Euler formülünün bir sonucu da “De Moivre”(dö muavr) formülü olarak bilinen aşağıdaki formüldür:

$$(\cos \theta + i \sin \theta)^n = e^{in\theta} = \cos(n\theta) + i \sin(n\theta) \quad \forall n \in \mathbb{N}$$

2. Karmaşık Düzlemde Geometri

2.1. Çapraz Oran

Aynı doğru üzerinde bulunmayan üç noktadan bir çember geçtiğini biliyoruz. Bu durumda verilen ve aynı doğru üzerinde olmayan z_1, z_2 ve $z_3 \in \mathbb{C}$ noktalarını alalım. Burada z_1, z_2 ve $z_3 \in \mathbb{C}$ noktalarının aynı doğru üzerinde bulunmaması koşulunun $z_3 - z_1$ 'in $z_2 - z_1$ 'in gerçel katı olmaması şartına yani $\frac{z_3 - z_1}{z_2 - z_1} \notin \mathbb{R}$ şartına denk olduğunu görmek okur için zor olmamalıdır. Bu şart ise

$$\overline{\left(\frac{z_3 - z_1}{z_2 - z_1}\right)} \neq \frac{z_3 - z_1}{z_2 - z_1}$$

$\Rightarrow$

$$A := (z_3 - z_1)(\bar{z}_2 - \bar{z}_1) - (\bar{z}_3 - \bar{z}_1)(z_2 - z_1) \neq 0$$

olmasına denktir. Bu z_1, z_2 ve $z_3 \in \mathbb{C}$ noktalarından geçen çember üzerinde bir $z \in \mathbb{C}$ noktası alalım. Çember geometrisinden bildiğimiz üzere zz_2 doğrusu ile z_1z_2 doğrusu arasındaki açı zz_3 doğrusu ile z_1z_3 arasındaki açıya eşit olmalıdır. Burada zz_2 doğrusu ile z_1z_2 doğrusu arasındaki açı

$$\text{Arg}\left(\frac{z_2 - z}{z_2 - z_1}\right)$$

dir. Aynı şekilde zz_3 doğrusu ile z_1z_3 doğrusu arasındaki açı

$$\text{Arg}\left(\frac{z_3 - z}{z_3 - z_1}\right)$$

dir. O hâlde bu iki sayının asli argümanlarının eşit olması için oranlarının gerçel olması gerekir, yani

$$\left(\frac{z - z_2}{z_1 - z_2}\right) : \left(\frac{z - z_3}{z_1 - z_3}\right) \in \mathbb{R}$$

olmalıdır. Yani z, z_1, z_2 ve $z_3 \in \mathbb{C}$ aynı çember üzerindedir ancak ve ancak

$$O(z, z_1, z_2, z_3) := \left(\frac{z - z_2}{z - z_3}\right) : \left(\frac{z_1 - z_2}{z_1 - z_3}\right) \in \mathbb{R}$$

sağlanır. Burada

$$O(z_0, z_1, z_2, z_3) := \left(\frac{z_0 - z_2}{z_0 - z_3}\right) : \left(\frac{z_1 - z_2}{z_1 - z_3}\right)$$

oranına z_0, z_1, z_2 ve $z_3 \in \mathbb{C}$ 'nin **çapraz oranı** (İng. “cross ratio”) denir. Bu durumda z, z_1, z_2 ve $z_3 \in \mathbb{C}$ aynı çember üzerindedir ancak ve ancak $O(z, z_1, z_2, z_3) \in \mathbb{R} \Leftrightarrow$

$$O(z, z_1, z_2, z_3) = \overline{O(z, z_1, z_2, z_3)}$$

$\Leftrightarrow$

$$\left(\frac{z - z_2}{z - z_3}\right) : \left(\frac{z_1 - z_2}{z_1 - z_3}\right) = \overline{\left(\frac{z - z_2}{z - z_3}\right) : \left(\frac{z_1 - z_2}{z_1 - z_3}\right)}$$

$\Leftrightarrow$

$$\left(\frac{z - z_2}{z_1 - z_2}\right)\left(\frac{\bar{z} - \bar{z}_3}{\bar{z}_1 - \bar{z}_3}\right) = \left(\frac{\bar{z} - \bar{z}_2}{\bar{z}_1 - \bar{z}_2}\right)\left(\frac{z - z_3}{z_1 - z_3}\right)$$

olur.

2.2. Batlamyus Teoremi

Verilen herhangi $z_1, z_2, z_3, z_4 \in \mathbb{C}$ karmaşık sayıları için

$$\begin{aligned} (z_1 - z_2)(z_3 - z_4) + (z_3 - z_2)(z_4 - z_1) &= \cancel{z_1 z_3} - z_1 z_4 - z_2 z_3 + \cancel{z_2 z_4} + z_3 z_4 - \cancel{z_1 z_3} - \cancel{z_2 z_4} + z_2 z_1 \\ &= z_1 z_2 - z_1 z_4 + z_3 z_4 - z_2 z_3 = z_1(z_2 - z_4) - z_3(z_2 - z_4) = (z_1 - z_3)(z_2 - z_4) \end{aligned}$$

özdeşliğinin geçerli olduğunu görmek zor değildir.

Bu

$$(z_1 - z_2)(z_3 - z_4) + (z_3 - z_2)(z_4 - z_1) = (z_1 - z_3)(z_2 - z_4)$$

özdeşliğini üçgen eşitsizliği ile birleştirirsek her $z_1, z_2, z_3, z_4 \in \mathbb{C}$ için sağlanan

$$|z_1 - z_2| |z_3 - z_4| + |z_3 - z_2| |z_4 - z_1| \geq |z_1 - z_3| |z_2 - z_4|$$

eşitsizliğini elde ederiz. Bunun geometrik anlamı $z_1, z_2, z_3, z_4 \in \mathbb{C}$ karmaşık sayılarını sırasıyla $A(x_1, y_1)$, $B(x_2, y_2)$, $C(x_3, y_3)$, $D(x_4, y_4) \in \mathbb{R}^2$ noktaları ile özdeşleştirirsek

$$|AB| |CD| + |BC| |AD| \geq |AC| |BD|$$

şeklinde elde edilen “**Batlamyus² eşitsizliği**” dir. Bu eşitsizliğin eşitlik hâli, A, B, C ve D noktaları aynı çember üzerinde ise sağlanır ki buna da “**Batlamyus Teoremi**” denir:

Teorem 2. (Batlamyus Teoremi)

Birbirlerinden farklı $z_1, z_2, z_3, z_4 \in \mathbb{C}$ karmaşık sayıları verilsin öyle ki $z_2, z_3, z_4 \in \mathbb{C}$ sayıları aynı doğru üzerinde bulunmasın. O hâlde $z_1, z_2, z_3, z_4 \in \mathbb{C}$ karmaşık sayıları aynı çember üzerindedir ancak ve ancak

$$|z_1 - z_2| |z_3 - z_4| + |z_3 - z_2| |z_4 - z_1| = |z_1 - z_3| |z_2 - z_4|$$

sağlanır.

Kanıt. Yukarıdaki

$$(z_1 - z_2)(z_3 - z_4) + (z_3 - z_2)(z_4 - z_1) = (z_1 - z_3)(z_2 - z_4)$$

özdeşliği ile başlayalım. Bu özdeşlikte her iki tarafı $(z_3 - z_2)(z_4 - z_1)$ ile bölersek

$$\frac{(z_1 - z_2)(z_3 - z_4)}{(z_3 - z_2)(z_4 - z_1)} + 1 = \frac{(z_1 - z_3)(z_2 - z_4)}{(z_3 - z_2)(z_4 - z_1)}$$

elde edilir. Bu denklem ise

$$-O(z_1, z_3, z_2, z_4) + 1 = O(z_1, z_2, z_3, z_4)$$

denkleminde denktir ki burada

$$O(z_1, z_2, z_3, z_4) := \left(\frac{z_1 - z_3}{z_2 - z_3} \right) : \left(\frac{z_1 - z_4}{z_2 - z_4} \right)$$

$z_1, z_2, z_3, z_4 \in \mathbb{C}$ karmaşık sayılarının çarpıraz oranını göstermektedir. Bu durumda z_2, z_3, z_4 aynı doğru üzerinde olmadığından, $z_1, z_2, z_3, z_4 \in \mathbb{C}$ aynı çember üzerindedir ancak ve ancak $O(z_1, z_2, z_3, z_4) \in \mathbb{R}$ ve $O(z_1, z_3, z_2, z_4) \in \mathbb{R}$. Burada $\text{Arg}(O(z_1, z_2, z_3, z_4)) = 0$ olduğundan $O(z_1, z_2, z_3, z_4) > 0$ yani pozitif bir gerçel sayıdır. O hâlde $\text{Arg}(O(z_1, z_3, z_2, z_4)) = \pi$ olur ki bu da $O(z_1, z_3, z_2, z_4) < 0$ ve $-O(z_1, z_3, z_2, z_4) > 0$ olması demektir. Yani eğer z_1, z_2, z_3 ve z_4 aynı çember üzerinde iseler

$$|-O(z_1, z_3, z_2, z_4) + 1| = |-O(z_1, z_3, z_2, z_4)| + 1 = |O(z_1, z_2, z_3, z_4)|$$

sağlanır ki bu da

$$|z_1 - z_2| |z_3 - z_4| + |z_3 - z_2| |z_4 - z_1| = |z_1 - z_3| |z_2 - z_4|$$

olmasına denktir. Tersine olarak eğer

$$|z_1 - z_2| |z_3 - z_4| + |z_3 - z_2| |z_4 - z_1| = |z_1 - z_3| |z_2 - z_4|$$

sağlanırsa

$$|-O(z_1, z_3, z_2, z_4) + 1| = |-O(z_1, z_3, z_2, z_4)| + 1 = |O(z_1, z_2, z_3, z_4)|$$

gerçeklenir ki buradan da üçgen eşitsizliğinin tersi kullanılarak (yani eğer $|z_1 + z_2| = |z_1| + |z_2|$ ise $\frac{z_1}{z_2} \in \mathbb{R}^+$

²Batlamyus ya da Ptolemy(MS100-170): Küresel geometrinin temellerini ortaya koyduğu “Almagest” adlı eseriyle ünlü İskenderiyeli matematikçi

olduğundan) $-O(z_1, z_3, z_2, z_4) \in \mathbb{R}^+$ elde edilir. Bu ise z_1, z_2, z_3 ve z_4 noktalarının aynı çember üzerinde olması demektir. Yani $z_1, z_2, z_3, z_4 \in \mathbb{C}$ aynı çember üzerindedir ancak ve ancak

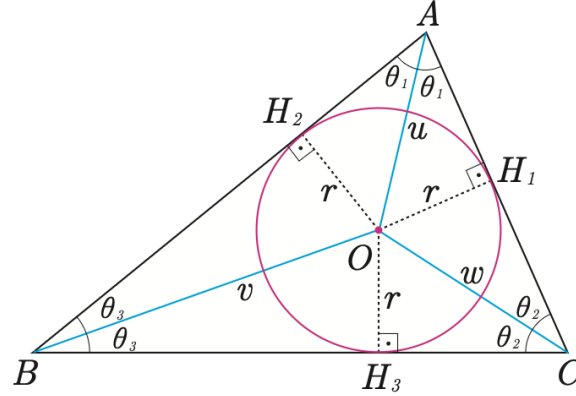
$$|-O(z_1, z_3, z_2, z_4)| + 1 = |O(z_1, z_2, z_3, z_4)|$$

sağlanır ve bu da ancak ve ancak

$$|z_1 - z_2| |z_3 - z_4| + |z_3 - z_2| |z_4 - z_1| = |z_1 - z_3| |z_2 - z_4|$$

eşitliği sağlanırsa gerçekleşir. □

2.3. Heron Formülü



Şekildeki ABC üçgenine bakalım. Heron³ formülü ABC üçgeninin alanını kenar uzunlukları cinsinden aşağıdaki gibi verir:

$$A(ABC) = \sqrt{s(s-a)(s-b)(s-c)}$$

ki burada $a = |BC|$, $b = |AC|$, $c = |AB|$ ve $s = \frac{a+b+c}{2}$ dir.

İç yarıçap r ve yarıçevre s cinsinden ABC üçgeninin alanını veren daha kolay bir formül aşağıdaki gibi elde edilir:

$$A(ABC) = A(BOC) + A(AOC) + A(AOB) = \frac{ra}{2} + \frac{rb}{2} + \frac{rc}{2} = r\left(\frac{a+b+c}{2}\right) = rs$$

Bu kısımda karmaşık sayıları kullanarak, dahiyane bir fikir vasıtasıyla r 'yi a, b, c ve s cinsinden bulacağız:

Karmaşık sayılar düzlemimizi merkezi A noktasında ve pozitif gerçel eksenini AC doğrusu olacak şekilde yerleştirdiğimizi tahayyül edelim: O hâlde $\overrightarrow{AO}$ vektörü bir u karmaşık sayısı olarak görülüp,

$$\overrightarrow{AO} = u = |AH_1| + ir = |u| e^{i\theta_1}$$

şeklindedir. Aynı şekilde

$$\overrightarrow{BO} = v = |BH_2| + ir = |v| e^{i\theta_2}$$

ve

$$\overrightarrow{CO} = w = |CH_3| + ir = |w| e^{i\theta_3}$$

elde edilir.

Şimdi bu u, v ve w karmaşık sayılarını çarptığımızda, $\theta_1 + \theta_2 + \theta_3 = \frac{\pi}{2}$ olduğundan dolayı

$$\begin{aligned} uvw &= (|AH_1| + ir)(|BH_2| + ir)(|CH_3| + ir) = |u| |v| |w| e^{i(\theta_1 + \theta_2 + \theta_3)} \\ &= |u| |v| |w| e^{i\frac{\pi}{2}} = i |u| |v| |w| \end{aligned}$$

elde edilir.

Aşağıdaki denklemlerden

$$|AH_1| + |CH_3| = b$$

³Heron(MS10-70): Geometri ve Mekaniğe katkılarıyla bilinen İskenderiyeli matematikçi

$$|BH_2| + |CH_3| = a$$

$$|AH_1| + |BH_2| = c$$

$|AH_1| + |BH_2| + |CH_3| = s$ ve $|AH_1| = s - a$, $|BH_2| = s - b$ ve $|CH_3| = s - c$ elde edilir.

O hâlde

$$\Re(uvw) = \Re(((s-a) + ir)((s-b) + ir)((s-c) + ir)) = 0$$

dır. Bu üç karmaşık sayı u, v ve w 'nin çarpımına bakalım:

$$\begin{aligned} & ((s-a) + ir)((s-b) + ir)((s-c) + ir) \\ &= [((s-a)(s-b) - r^2) + i(r(s-a) + r(s-b))][(s-c) + ir] \\ &= [((s-a)(s-b) - r^2)(s-c) - r(r(s-b) + r(s-a))] \\ &\quad + i[(r(s-b) + r(s-a))(s-c) + r((s-a)(s-b) - r^2)] \end{aligned}$$

O hâlde buradan

$$\Re(uvw) = (s-a)(s-b)(s-c) - r^2(s-a+s-b+s-c) = 0$$

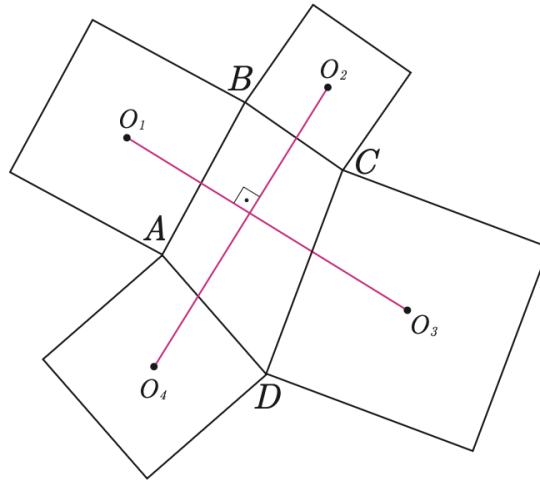
elde edilir. Burada $s-a+s-b+s-c = 3s - (a+b+c) = 3s - 2s = s$ olduğundan

$$(s-a)(s-b)(s-c) - r^2s = 0 \Rightarrow r^2 = \frac{(s-a)(s-b)(s-c)}{s}$$

elde edilir. Bu da Heron formülünü verir:

$$A(ABC) = rs = \sqrt{\frac{(s-a)(s-b)(s-c)}{s}}s = \sqrt{s(s-a)(s-b)(s-c)}$$

2.4. Van Aubel Teoremi



Belçikalı matematikçi Henri Van Aubel⁴ 1878 yılında, düzlemde verilen herhangi bir dörtgenin kenarları üzerine kurulan karelerin merkezlerini karşılıklı olarak birleştiren doğru parçalarının eşit uzunlukta olduğunu ve bu doğruların birbirlerine dik olduklarını ispatladı. Bu kısımda bu teoremin karmaşık sayılarla yapılan bir ispatını göreceğiz: Yukarıdaki şekildeki $ABCD$ dörtgenini karmaşık düzlemimize A noktası orjin 0 noktasına gelecek şekilde yerleştirelim. Burada B noktası $2a \in \mathbb{C}$ karmaşık sayısı, C noktasının B noktasından farkı $2b \in \mathbb{C}$ karmaşık sayısı, D noktasının C noktasından farkı $2c \in \mathbb{C}$ karmaşık sayısı ve A noktasının D noktasından farkı $2d \in \mathbb{C}$ karmaşık sayısı olsun. Bu durumda

$$2a + 2b + 2c + 2d = 0 \Rightarrow a + b + c + d = 0$$

sağlanır.

⁴Henricus Hubertus (Henri) Van Aubel (1830-1906): Sentetik Düzlem Geometrisiyle ilgili ilginç teoremleri ile bilinen Belçikalı matematikçi

Bu teoremi ispatlarken düzlemde iki doğru parçasının aynı uzunlukta ve birbirine dik olmasının karmaşık sayılar cinsinden karakterizasyonunu kullanıyoruz: Bir AB doğru parçası, eğer A noktasının düzlemde karşılık geldiği karmaşık sayı z_1 ve B noktasının düzlemde karşılık geldiği karmaşık sayı z_2 ise $AB = z_2 - z_1$ olur. Ayrıca $CD = z_4 - z_3$ olsun. O halde eğer $z_2 - z_1 = i(z_4 - z_3)$ ise $z_2 - z_1 = r_1 e^{i\theta_1}$ ve $z_4 - z_3 = r_2 e^{i\theta_2}$ için

$$z_2 - z_1 = r_1 e^{i\theta_1} = e^{i\frac{\pi}{2}} r_2 e^{i\theta_2} = r_2 e^{i(\theta_2 + \frac{\pi}{2})}$$

olduğundan $r_1 = r_2$ ve $\theta_1 = \frac{\pi}{2} + \theta_2$ olmalıdır. Yani eğer $z_2 - z_1 = i(z_4 - z_3)$ ise AB doğru parçası CD doğru parçasına dik ve bu iki doğru parçası eşit uzunlukta olmalıdırlar. Benzer şekilde eğer $z_4 - z_3 = i(z_2 - z_1)$ ise de aynı durum gerçekleşir yani AB ve CD aynı uzunlukta ve birbirlerine diktirler. Terside doğrudur yani AB doğru parçasının uzunluğu CD doğru parçasınıninkine eşit ve bu iki doğru parçası birbirlerine dik iseler $z_2 - z_1 = i(z_4 - z_3)$ veya $z_4 - z_3 = i(z_2 - z_1)$ olmalıdır. Burada i ile çarpma bir karmaşık sayıyı kendisine dik olacak şekilde saat yönünün tersi yönde döndürür.

Şimdi yukarıdaki şekle geri dönelim: A noktası 0 yani orijin noktasında olduğundan AB kenarı üzerindeki karenin merkezi O_1 noktası $a + ia \in \mathbb{C}$ karmaşık sayısına karşılık gelir. Aynı şekilde BC kenarı üzerindeki karenin merkezi O_2 noktası $2a + b + ib \in \mathbb{C}$ karmaşık sayısına, CD kenarı üzerindeki karenin merkezi O_3 noktası $2a + 2b + c + ic \in \mathbb{C}$ karmaşık sayısına ve AD kenarı üzerindeki karenin merkezi O_4 noktası ise $-d + id \in \mathbb{C}$ karmaşık sayısına karşılık gelir. O hâlde O_1O_3 doğru parçası

$$O_1O_3 = 2a + 2b + c + ic - (a + ia) = a + 2b + c + i(c - a) \in \mathbb{C}$$

ve O_4O_2 doğru parçası

$$O_4O_2 = 2a + b + ib - (-d + id) = 2a + b + d + i(b - d) \in \mathbb{C}$$

karmaşık sayılarına karşılık gelirler. Burada O_1O_3 doğru parçasını i ile çarparsak

$$iO_1O_3 = i(a + 2b + c + i(c - a)) = (a - c) + i(a + 2b + c) \in \mathbb{C}$$

elde ederiz. Şimdi $a + b + c + d = 0$ olduğunu hatırlayalım:

$$a + b + c + d = 0 \Rightarrow a + b + d = -c$$

ve buradan da

$$2a + b + d = a + (a + b + d) = a - c$$

elde edilir. Aynı şekilde $a + b + c = -d$ ve

$$a + 2b + c = b + (a + b + c) = b - d$$

elde edilir. Buradan da

$$iO_1O_3 = (a - c) + i(a + 2b + c) = 2a + b + d + i(b - d) = O_4O_2$$

sonucu çıkar ki bu da O_1O_3 doğrusunun O_2O_4 doğrusuna dik olduğu ve $|O_1O_3| = |O_2O_4|$ olduğunu verir. Böylece Van Aubel Teoremini ispatlamış olduk.

■ Kaynaklar

- [1] Ahlfors, L. V. Complex Analysis: An Introduction to the Theory of Analytic Functions of One Complex Variable, Prentice Hall 1953.
- [2] Deaux, R. Introduction a la geometrie des nombres complexes, F. Ungar Pub. Co. 1956.
- [3] Needham, T. Visual Complex Analysis, Oxford University Press 1997.
- [4] Schwerdtfeger, H. Geometry of Complex Numbers: Circle Geometry, Moebius Transformation, Non-Euclidean Geometry, Dover Pub. 1980.
- [5] Yaglom, I. M. Complex Numbers in Geometry, Academic Press 1968.

Matematiksel Düşünmeyi Anlamak: Kavramsal Temellerden Öğrenme Ortamlarına

ŞENOL DOST

Hacettepe Üniversitesi Matematik ve Fen Bilimleri Eğitimi Bölümü
Matematik Eğitimi Ana Bilim Dalı

✉ dost@hacettepe.edu.tr



Matematiksel bilgi, yalnızca doğru sonuçlara ulaşmayı sağlayan bir araç değil; kavramların, matematiksel yapıların ve aralarındaki ilişkilerin düşünsel olarak inşa edildiği tutarlı ve anlamlı bir sistemdir. Bu sistem içinde matematiksel düşünme, işlem yapmanın çok ötesine geçerek anlam kurma, genelleme, gerekçelendirme, soyutlama ve temsil etme gibi üst düzey bilişsel süreçleri kapsar. Matematiği öğrenmek ve öğretmek, farklı bağlam ve düzeylerde gerçekleşse de, özünde ortak bir düşünme kültürünün ve akıl yürütme geleneğinin parçası olarak biçimlenir. Bu yazı, matematiksel düşünmenin temel bileşenlerini inceleyerek, bu süreçlerin bireysel öğrenme deneyimlerinde ve öğretimsel ortamlarda nasıl yapılandığını, ne tür bilişsel dönüşümlere zemin hazırladığını tartışmayı amaçlamaktadır.

Matematiksel düşünme, birbirini besleyen ve farklı düzeylerde işleyen bilişsel süreçlerin bir bütünüdür. Bu süreçlerin yapısını anlamak, yalnızca bireyin matematiksel bilgiyi nasıl edindiğini ve dönüştürdüğünü kavramak açısından değil, aynı zamanda etkili öğretim yaklaşımlarını geliştirmek açısından da kritik öneme sahiptir. Literatürde bu düşünme biçimlerine dair çeşitli kuramsal çerçeveler ve sınıflandırmalar yer almakla birlikte, bu yazıda matematiksel düşünmenin temel bileşenleri olarak kavramsal düşünme, işlemsel düşünme, temsillerle düşünme, genelleme, soyutlama, kanıtlama ve gerekçelendirme gibi süreçler ele alınacaktır. Her bir bileşen, öğrencilerin matematiksel anlam oluşturma yollarını ve problem çözme stratejilerini derinlemesine incelemek için birer odak noktası olarak değerlendirilecektir.

1. Kavramsal ve İşlemsel Düşünme

Kavramsal düşünme, bir matematiksel kavramın altında yatan anlamı, yapısal özellikleri ve bu kavramın farklı temsilleri arasındaki ilişkileri anlamayı içerir. Öğrencinin kavramlar arasında bağlantılar kurarak genel geçer ilkeleri keşfetmesi ve bu ilkeleri esnek biçimde farklı durumlara uygulayabilmesi, bu düşünme biçiminin temel göstergelerindendir. Örneğin, kesirlerle çarpmayı yalnızca işlem adımlarıyla değil, “bir bütünün belirli bir kısmını almak” şeklinde kavramsal olarak yorumlayabilmek, derin bir matematiksel anlayışı yansıtır.

Buna karşılık, işlemsel düşünme daha çok prosedürel bilgilere, yani bir matematiksel işlemin nasıl yapılacağına ilişkin adımları bilmeye ve uygulamaya dayanır. Aynı örnek üzerinden gidersek, bir öğrencinin $\frac{2}{3} \times \frac{3}{4}$ işlemini doğru bir şekilde $\frac{6}{12}$ sonucuna ulaştırması, işlemsel becerinin bir göstergesidir.

Bu iki düşünme biçimi birbirine karşıt değil, aksine birbirini destekleyen ve öğrenme sürecinde iç içe geçen yapılarıdır. Kavramsal bilgi, işlemsel stratejilerin anlamlı biçimde seçilmesini ve kullanılmasını yönlendirirken; işlemsel uygulamalar da öğrencinin kavramlara dair sezgilerini ve anlayışını sınama ve pekiştirme fırsatı sunar. Örneğin, işlemsel akıcılık kazanmış bir öğrenci, farklı sayı türleriyle yapılan işlemlerde benzerlikleri fark ederek daha derin kavramsal genellemelere ulaşabilir.

Bu karşılıklı ilişki, özellikle yapılandırmacı öğrenme kuramları ve APOS (Eylem–Süreç–Obje–Şema) teorisi bağlamında da ele alınmaktadır. Yapılandırmacı yaklaşımlar, öğrenmenin aktif bir süreç olduğunu ve bireylerin bilgiyi kendi deneyimleriyle yapılandırdıklarını vurgular. APOS teorisi ise, matematiksel kavramların öğrenilme sürecini eylemden şemaya doğru gelişen aşamalarla açıklar; bu süreçte işlemsel bilgiler kavramsal anlayışa dönüşerek daha karmaşık zihinsel yapılar oluşturur. Böylece, kavramsal ve

işlemsel düşünme sadece farklı bilgi türleri değil, aynı zamanda öğrenmenin dinamik evreleri olarak görülebilir.

2. Temsillerle Düşünme

Matematiksel kavramlar genellikle sembolik, grafiksel, sözel ve somut modeller gibi çoklu temsiller aracılığıyla ifade edilir. Bu temsillerin her biri, kavramın farklı bir yönünü görünür kılar ve öğrenenin anlam kurma sürecine farklı açılardan katkı sağlar. Etkili matematiksel düşünme, bu temsiller arasında esnek bir şekilde geçiş yapabilme, bir temsildeki bilginin diğerine nasıl dönüştüğünü kavrayabilme ve temsil biçimlerinin sınırlılıklarını fark edebilme becerisini içerir. Örneğin, ikinci dereceden bir fonksiyonun cebirsel (sembolik) biçimi olan $f(x) = x^2 - 4x + 3$, grafiksel temsilde bir parabol olarak, somut modellerle fiziksel bir yörünge olarak ya da sözel olarak bir problem bağlamında ifade edilebilir. Bu temsiller arasında geçiş yapabilmek, kavramın çok boyutlu bir şekilde anlaşılmasına olanak tanır.

Temsiller yalnızca bilgiyi sunan sabit görünümüler değil, aynı zamanda kavramsal düşünmeyi yapılandıran dinamik araçlardır. Özellikle yapılandırmacı yaklaşımlarda, öğrenenin bir temsilden diğerine geçerken kurduğu anlamlar, kavramsal gelişimin temelini oluşturur. Temsiller arası geçişler, öğrenme sürecinde kavramsal anlayışın oluşmasında belirleyici bir rol oynar. Temsilsel yeterlilik kazanmış bir öğrenci, örneğin bir grafik üzerinde bir fonksiyonun artan azalan bölgelerini okuyabilir, bu bilgiyi cebirsel biçime taşıyabilir ve bir problem durumunda sözel olarak açıklayabilir.

Bu nedenle, matematiksel temsillerle düşünme becerisi yalnızca farklı formatlarda bilgi sunmayı değil, aynı zamanda temsiller arasında anlamlı bağlar kurabilme yetisini içerir ve derinlemesine kavrayışın vazgeçilmez bir bileşeni olarak görülmelidir.

3. Genelleme ve Soyutlama

Genelleme, öğrencilerin belirli örneklerden hareketle daha geniş matematiksel yapıları, örüntüleri ve ilişkileri fark ederek soyutlamalar yapma sürecidir. Bu süreçte birey, benzer durumlar arasındaki ortak özellikleri ayırt eder ve bu ortaklıklardan yola çıkarak genellenmiş matematiksel ifadeler geliştirir. Örneğin, ardışık tek sayıların kareleri arasındaki farkın her zaman 8'in katı olduğunu fark eden bir öğrencinin, bu durumu $(2n + 1)^2 - (2n - 1)^2 = 8n$ olarak ifade etmesi genelleme sürecine verilebilecek güçlü bir örnektir. Böyle bir genelleme, öğrencinin örnekler arasında bağlantılar kurarak daha derin bir kavramsal anlayış geliştirdiğine işaret eder.

Soyutlama ise, yapılan genellemelerin bağlamdan ve somut örneklerden bağımsız biçimde düşünülmesi ve temsil edilmesi sürecidir. Bu aşamada öğrenci, yalnızca belirli durumları değil, bu durumların altında yatan yapısal örüntüleri zihinsel olarak kavrar ve bunları soyut kavramlar (örneğin, değişkenler, fonksiyonlar, cebirsel yapılar) aracılığıyla ifade edebilir. Örneğin, bir aritmetik dizideki terimlerin genel yapısını $a_n = a + (n - 1)d$ biçiminde ifade edebilen bir öğrencinin, hem genelleme hem de soyutlama becerilerine ilişkin güçlü bir kavrayış geliştirdiği söylenebilir. Bu tür bir ifade, yalnızca sayıların ardışıklığını görmekle kalmayıp, altta yatan yapının değişkenler aracılığıyla modellenmesini de içerir.

Genelleme ve soyutlama süreçleri, özellikle cebirsel düşünmenin gelişiminde merkezi bir rol oynar. Bu bağlamda, öğrencilerden yalnızca işlemsel örnekleri tekrar etmeleri değil, bu örneklerdeki yapısal örüntüleri fark etmeleri ve genelleyerek yeniden yapılandırmaları beklenir. Sfard'ın nesneleşme (reifikasyon) kuramına göre, bir matematiksel süreç zamanla zihinsel bir nesneye dönüşür; bu dönüşüm ise büyük ölçüde soyutlama yoluyla gerçekleşir. Dolayısıyla genelleme ve soyutlama, yalnızca üst düzey bilişsel beceriler değil, aynı zamanda kavramsal gelişimin temel yapı taşlarıdır.

Öğretimsel Ortamda Genelleme ve Soyutlamayı Destekleyen Etkinlikler:

- **Örüntü Tamamlama ve Genelleme:** Öğrencilere sayı örüntüleri (örneğin 3, 6, 9, 12, ...) verilerek genel kuralı ifade etmeleri istenebilir. Bu etkinlikler, genellenmenin başlangıç düzeyini oluşturur.
- **Temsiller Arası Geçiş:** Bir durumu tablo, grafik ve cebirsel ifadeyle temsil etme çalışmaları, öğrencinin yapıyı genelleyip soyutlamasına yardımcı olur.

- **Açık Uçlu Problem Çözme:** “Her zaman doğru olur mu?” türünden sorularla öğrencilerden çeşitli örnekler üretmeleri ve ardından bir genelleme yapmaları beklenebilir.
- **Karşıt-örnek Oluşturma:** Genellemenin sınırlarını sorgulamak ve soyut düşünmeyi pekiştirmek için “Bu genelleme hangi durumlarda geçerli değildir?” gibi sorular sorulabilir.
- **Sözlü Gerekçeleştirme:** Öğrencilerin kendi genellemelerini açıklamaları ve arkadaşlarının genellemelerine dönüt vermeleri, soyutlamaya geçiş sürecini hızlandırır.

Etkili öğretim ortamlarında genelleme ve soyutlama süreci sadece teşvik edilmez; aynı zamanda yapılandırılır, sorgulanır ve yeniden şekillendirilir. Bu da öğrencilerin yüzeysel işlem bilgisiyle yetinmeyip matematiksel yapının derinliklerine inmelerini sağlar.

4. Kanıtlama ve Gerekçeleştirme

Matematiksel düşünmenin belki de en ayırt edici özelliği, doğruluğun otoriteye ya da geleneksel kabullere değil; akıl yürütmeye, mantıksal tutarlılığa ve kanıta dayanmasıdır. Bu bağlamda kanıtlama, yalnızca sonuçları haklı çıkarmanın bir aracı değil; aynı zamanda düşünceyi yapılandırmanın, kavramları ilişkilendirmenin ve matematiksel anlamı derinleştirmenin bir yoludur. Kanıtlama süreci, öğrencilerin geçici sezgilerini sorgulamalarını ve genellemelerini gerekçeli bir şekilde test etmelerini sağlar. Bu süreç, aynı zamanda matematiksel doğruluğun neye dayandığına dair epistemolojik bir farkındalık kazandırır.

Gerekçeleştirme ise, sınıf içi öğrenme bağlamında öğrencilerin kendi düşüncelerini başkalarına açık ve tutarlı bir biçimde sunmalarını; aynı zamanda arkadaşlarının düşüncelerini değerlendirme ve sorgulama becerilerini geliştirmelerini sağlar. Bu yönüyle gerekçeleştirme, matematiksel akıl yürütmenin yalnızca bireysel değil, aynı zamanda etkileşimli bir süreç olduğunu ortaya koyar. Öğrencilerin “Neden böyle düşündün?” veya “Bu kural her zaman geçerli mi?” gibi sorularla birbirlerinin düşünce yapılarını sınamaları, derin öğrenmenin ve anlamlı etkileşimin temelidir.

■ Matematiksel Düşünmenin Sosyal Boyutu

Matematiksel bilgi, bireysel bir zihinsel edinimin ötesinde, sosyal ve kültürel bir bağlamda inşa edilir. Bu bağlamda matematik öğrenmek, sadece kavramları ve prosedürleri edinmek değil; aynı zamanda bu kavramların hangi durumlarda, hangi amaçlarla ve nasıl kullanılacağını anlamak anlamına gelir. Öğrenmek, anlamın inşasına yönelik aktif bir süreçtir; öğretmek ise bu süreci başkaları için yeniden tasarlamak ve öğrenenin dünyasına rehberlik edebilecek araçlar sunmaktır. Bu yönüyle öğretmen, yalnızca bilgi aktarıcısı değil; anlam oluşturmaya destekleyen bir öğrenme ortamının yöneticisidir.

Matematiği öğrenme ve öğretme süreçleri, farklı bilişsel yönelimler taşısa da her ikisi de matematiksel düşünmenin temel bileşenlerini etkin biçimde kullanmayı gerektirir. Öğrenen, kavramların doğasını ve ilişkilerini keşfederken; öğreten, bu keşfi destekleyecek uygun temsil biçimlerini, problem durumlarını ve etkileşim ortamlarını tasarlar. Bu açıdan bakıldığında, öğretmek yalnızca bildiğini aktarmak değil; bilgiyi yeniden düşünmek, dönüştürmek ve öğrenenin zihninde yeniden yapılandırılmasını sağlamaktır.

Matematik öğretimi üzerine yapılan araştırmalar, öğretmenlerin sahip olduğu derin kavramsal anlayışın, öğrencilerin düşüncelerini anlama, yönlendirme ve yeniden şekillendirme süreçlerinde kritik bir rol oynadığını göstermektedir. Bu bağlamda, matematiksel düşünmenin öğretim süreçlerinde görünür kılınması, yalnızca öğretmenin içerik bilgisiyle değil, aynı zamanda pedagojik duyarlılığıyla da doğrudan ilişkilidir. Öğrencilerin neyi nasıl düşündüğünü anlamaya dönük bir öğretmen bakışı, öğrenme sürecine dönük daha esnek, anlamlı ve etkili müdahaleleri mümkün kılar.

Matematik öğrenen bireylerin zamanla öğretmen bakış açısını da geliştirmeleri, kavramların doğasına dair daha derin bir farkındalık kazanmalarını sağlar. Öte yandan, öğretmenlerin öğrenme süreçlerine ilişkin edindikleri içgörüler, öğrencilerin anlam dünyalarına daha yakınlaşmalarına olanak tanır. Bu karşılıklı anlayış, matematiksel anlamın ortak bir zeminde inşa edilmesine katkıda bulunur. Böylece süreç, yalnızca bilgi aktarımıyla sınırlı kalmayıp, anlamın paylaşılması ve matematiksel düşünmenin kültürel bir pratik olarak gelişimi yönünde ilerler.

■ Matematiksel Düşünmenin Gelişimi ve Öğrenme Ortamlarının Rolü

Matematiksel düşünmenin gelişimi, büyük ölçüde öğrenme ortamlarının yapısına ve niteliğine bağlıdır. Sınıf, öğrencilerin yalnızca bilgi alıcısı değil; aynı zamanda matematiksel kavramları keşfeden, yapılandıran, sorgulayan ve anlamı birlikte inşa eden bireyler olarak yer aldığı dinamik bir öğrenme topluluğudur. Bu bağlamda etkili bir öğretim tasarımı, yalnızca içerik aktarımıyla sınırlı kalmamalı; öğrencilerin düşünmesini, bağlantılar kurmasını, alternatif çözüm yolları üretmesini ve matematiksel anlamı derinleştirmesini sağlayan zengin bir öğrenme ekosistemi sunmalıdır.

Öğrenenlerin aktif katılımını önceleyen ve onları düşünmeye, sorgulamaya ve yeniden yapılandırmaya teşvik eden öğretim stratejileri bu süreçte kritik öneme sahiptir. Açık uçlu sorular, keşfetmeye dayalı problem çözme etkinlikleri, işbirlikli öğrenme ortamları, yapılandırılmış matematiksel tartışmalar ve çoklu temsillere dayalı materyaller, öğrencilerin düşünme becerilerini geliştiren ve sınıf içerisinde entelektüel bir merak kültürünü besleyen güçlü araçlardır. Bu tür stratejiler, öğrenmeyi bireysel bir çabanın ötesine taşıyarak, sosyal ve bilişsel etkileşimlerin merkezi olduğu bir sürece dönüştürür.

Öğretmenlerin, öğrencilerin düşünce süreçlerine yönelik farkındalığı ve bu süreçleri tanıma ile yönlendirme becerisi, matematiksel anlam inşasında belirleyici bir rol oynar. Öğretmen, yalnızca doğru cevaba ulaşmayı amaçlayan bir rehber değil; öğrencilerin farklı düşünme biçimlerini dikkate alan, anlam kurma yollarına saygı gösteren ve bu yolları destekleyici yönlendirmelerde bulunan bir kolaylaştırıcıdır. Bu yaklaşım, öğrencilerin öğrenme süreçlerine aktif katılımını desteklerken, daha derin ve kalıcı bir kavramsal farkındalık geliştirmelerini de sağlar.

Sonuç olarak, sınıf ortamı matematiksel düşünmenin uygulamaya döküldüğü canlı bir öğrenme sahası olarak görülmelidir. Bu ortamda öğretmen ve öğrenciler, yalnızca bilgi paylaşan bireyler değil; birlikte öğrenen, düşünen ve sorgulayan bir topluluk oluştururlar. Bu topluluk, matematiksel bilgiye yönelik daha içselleştirilmiş, bağlamsal ve kalıcı bir anlayışın temelini atarken; öğrenmenin duygusal boyutunu da destekleyerek öğrencilerin matematikle daha olumlu ve sürdürülebilir bir ilişki kurmalarını sağlar.

■ Sonuç ve Öneriler

Bu yazıda, matematiksel düşünmenin temel bileşenleri ele alınarak hem bireysel öğrenme süreçlerinde hem de öğretim ortamlarında nasıl yapılandığı incelenmiştir. Matematiksel düşünme; anlam kurma, soyutlama, genelleme, temsillerle ilişkilendirme ve gerekçelendirme gibi çok katmanlı bilişsel süreçleri içeren bir yapı olarak değerlendirilmiştir. Bu yapı yalnızca bireysel zihinsel bir etkinlik değil, aynı zamanda sosyal, kültürel ve pedagojik bağlamlarda biçimlenen bir öğrenme sürecidir.

Matematiksel düşünmenin gelişimi, yalnızca öğrencinin bireysel çabasıyla değil; bu çabayı destekleyen öğrenme ortamlarının niteliğiyle de yakından ilişkilidir. Bu bağlamda sınıf, öğrencilerin düşüncelerini özgürce ifade edebildikleri, farklı bakış açılarını tartışabildikleri ve birlikte anlam inşa edebildikleri bir öğrenme topluluğuna dönüşmelidir. Etkili öğretim stratejileri, öğrencilerin aktif katılımını ön planda tutmalı ve onları eleştirel, yaratıcı ve bağlantı kurarak düşünmeye teşvik etmelidir.

Öğretmenin rolü bu süreçte merkezi bir öneme sahiptir. Derinlemesine kavramsal bilgiye sahip, öğrencilerin düşünme yollarını tanıyabilen ve bu süreçleri yönlendirebilen öğretmenler, öğrenmenin niteliğini doğrudan etkiler. Bu bağlamda öğretmen, yalnızca bilgi aktaran değil; anlamı birlikte yapılandıran, öğrencilerin düşünme becerilerini destekleyen ve öğrenme sürecini kolaylaştıran bir rehberdir.

Sonuç olarak, matematik eğitimi yalnızca “öğretmek” değil; “düşündürmek” ve “düşünmeyi görünür kılmak” temel hedef olmalıdır. Matematiksel bilgiye yönelik yaklaşımımız; bu bilginin nasıl üretildiğini, nasıl kullanıldığını ve nasıl paylaşıldığını şekillendirir. Bu nedenle, hem öğrencilerin öğretim süreçlerine yönelik farkındalık kazanmaları hem de öğretmenlerin öğrenme süreçlerine dair derinlemesine içgörü geliştirmeleri, matematiksel düşünmenin anlamlı ve kalıcı biçimde gelişmesini sağlayacaktır.

■ Kaynaklar

- [1] Dubinsky, E. & McDonald, M. A. (2001). APOS: A constructivist theory of learning in undergraduate mathematics education. In D. Holton (Ed.), *The teaching and learning of mathematics at university level* (pp. 275–282). Dordrecht: Springer.

- [2] Lesh, R., Post, T., & Behr, M. (1987). Representations and translations among representations in mathematics learning and problem solving. In C. Janvier (Ed.), *Problems of representation in the teaching and learning of mathematics* (pp. 33–40). Hillsdale, NJ: Lawrence Erlbaum Associates.
- [3] Hiebert, J. & Lefevre, P. (1986). Conceptual and procedural knowledge in mathematics: An introductory analysis. In J. Hiebert (Ed.), *Conceptual and procedural knowledge: The case of mathematics* (pp. 1-27). Hillsdale, NJ: Erlbaum
- [4] Sfard, A. (1991). On the dual nature of mathematical conceptions: Reflections on processes and objects as different sides of the same coin. *Educational Studies in Mathematics*, 22(1), 1–36. DOI: 10.1007/BF00302715.

Paranoyak Bir Matematikçi: Kurt Gödel

ALİ BERK KOYUNCU

Hacettepe Üniversitesi Matematik Bölümü, 3. Sınıf Öğrencisi

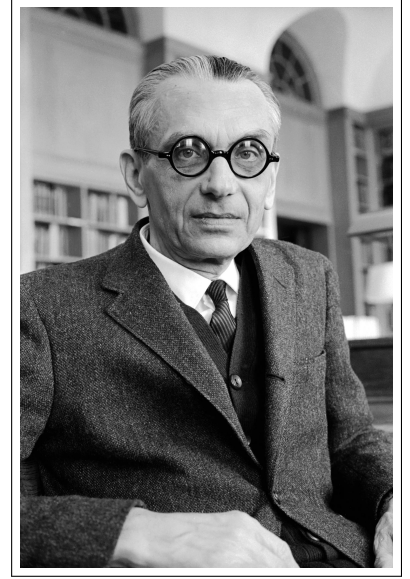
✉ aliberkkync@gmail.com



Bu yazıda size Einstein'ın yakın bir dostundan bahsetmek istiyorum. Tabii ki kendisinin tek özelliği Einstein'ın dostu olması değil. Matematik tarihinin altın isimlerinden biri olarak kabul edilen Kurt Gödel, Aristo'dan bu yana en büyük mantıkçı olarak anılır. Yaptığı çalışmalarla 20. yüzyıl matematiğinin seyrini değiştiren Gödel'in teoremleri matematikçiler kadar matematikçi olmayanların da ilgisini çekmiştir. 28 Nisan 1906 yılında bugün Çek Cumhuriyeti'nin olduğu Avusturya-Macaristan bölgesindeki Brünn kentinde dünyaya geldi. Tekstil işiyle uğraşan Rudolf Gödel ve Marianne Gödel çiftinin 2 oğlundan küçük olanıydı. Gençliğinde etrafındakileri sonu gelmez sorularla bunalttığı için kendisine 'Der Herr Warum' yani 'Bay Neden' lakabı takıldı.

1. Eğitim Hayatı

18 yaşında abisinin arkasından Viyana Üniversitesi'nde eğitim görmeye başladı. Burada Furtwängler, Hahn, Wirtinger, Menger, Helly gibi öğretmenlerden dersler aldı. Üniversitenin başlarında hangi alanla ilgileceği konusunda oldukça kararsız olan Kurt, Furtwängler'in derslerinden çok etkilenmiş ve matematiğe yönelme kararı almıştır. 1929 yılında, henüz 23 yaşındayken Hans Hahn'ın danışmanlığında doktora derecesini aldı. Birinci derece yüklem mantığının eksiksiz (tam) olduğunu gösterdiği doktora tezi, daha sonra Gödel'in Tamlık Teoremi olarak anılacaktır.



Kurt Gödel (1906-1978)

Doktorasını tamamladığı yıl babasını kaybeden Gödel, Viyana Üniversitesi'nde Öğretim Üyesi olarak çalışmaya devam etti, taa ki Avrupa'da dünya savaşının çanları çalmaya başlayana kadar. O da diğer çoğu bilim insanı gibi Avrupa'dan Amerika'ya kaçtı. 1940 yılında Princeton İleri Araştırma Enstitüsü'nde çalışmaya başladı. Princeton'da ileride sıkı bir dostluk kuracağı, hatta bu dostunun ölümünden sonra onun adını taşıyan bir ödülün ilkinde layık görüleceği Albert Einstein ile tanıştı. Gödel, Einstein'ın genel görelilik kuramı üzerine de önemli çalışmalar yapmıştır. Einstein'ın kütleçekim alan denklemlerine, ekseni etrafında dönen bir evreni tanımlayan bir çözüm getirir. Bu çözümde evrenin dönüşü, ışığı da birlikte sürükler; dolayısıyla bir maddesel cismin, ışık hızını aşmaksızın uzay-zaman içinde kapalı bir zaman-benzeri eğri (ing. timelike curve) izlemesi, yani zamanda geriye gitmesi mümkün hale gelir. Bu model, görelilik kuramının belirli koşullarda zamanda yolculuğa izin verebileceğini göstermesi bakımından çarpıcıdır. Gödel'in bu çözümü, "Gödel evreni" olarak bilinir ve dönen, homojen ama gözlemlenebilir evrenimizle tutarsız bir yapıya sahiptir. Nitekim bu model, gökbilimcilerin gözlemlendiği kütleçekimsel kıvrıma kayma verileriyle çeliştiği için fiziksel evrenin gerçek yapısı olarak kabul edilmez. Yine de bu çözüm, genel görelilik kuramının zaman kavramına dair sınırlarını gözler önüne serdiği için teorik fizikte büyük yankı uyandırmıştır. Einstein ise, kuramının böyle sıra dışı çözümlere izin vermesinden rahatsızlık duymuştur.

Zaman zaman ilgi alanı felsefeye kayan Gödel, Leibniz ve Kant'ın çalışmalarını okuduğunda bu kişilere hayran olur. Kendisinin Tanrı varlığına dair ispatı da vardır¹. Hatta ünlü mantıkçı Solovay, 1985'te yapılan

¹Gödel'in ontolojik ispatı olarak bilinir.

bir toplantıda, Gödel'den 'therefore G exists' yani 'demek ki G vardır' sözleriyle biten mektuplar almıştır. Burada G İngilizce 'God' (Tanrı) kelimesinin baş harfi olması dışında Gödel'in de baş harfi olması oldukça ilgi çekici.

2. Temellerin Sarsılışı ve Eksiklik Teoremleri

Dönemin matematikçileri, sağlam ve tutarlı bir temel arayışı içindeydiler. Bu temel, hiçbir çelişkiye yol açmamalı ve matematiksel gerçeklerin yapı taşını oluşturmalıydı. Öyle ki Russell ve Whitehead, *Principia Mathematica* adlı eserlerinde, matematiği mantıksal paradokslardan arındırmayı amaçlayan, ‘Tipler Kuramı’ adında bir kuram geliştirmişlerdi. Kitap o kadar temelden başlıyordu ki ‘ $1 + 1 = 2$ ’ önermesinin kanıtından ancak 362. sayfada bahsedebilmişlerdi. Bir süreliğine de olsa, bu dev çalışmanın amacına ulaştığı düşünülmüştü. Ta ki Gödel’in Eksiklik Teoremleri bu yapının temellerini sarstığı ana kadar...

362 PROLEGOMENA TO CARDINAL ARITHMETIC [PART II]

*54.42. $\vdash :: \alpha \in 2. \supset : \beta \subset \alpha. \supset ! \beta. \beta \neq \alpha. \equiv. \beta \in \iota' \alpha$
Dem.
 $\vdash. *54.4. \supset \vdash :: \alpha = \iota' x \cup \iota' y. \supset :$
 $\beta \subset \alpha. \supset ! \beta. \equiv : \beta = \Lambda. \vee. \beta = \iota' x. \vee. \beta = \iota' y. \vee. \beta = \alpha : \supset ! \beta :$
[*24.53-56.*51.161] $\equiv : \beta = \iota' x. \vee. \beta = \iota' y. \vee. \beta = \alpha$ (1)
 $\vdash. *54.25. \text{Transp.} *52.22. \supset \vdash : x \neq y. \supset. \iota' x \cup \iota' y \neq \iota' x. \iota' x \cup \iota' y \neq \iota' y :$
[*13.12] $\supset \vdash : \alpha = \iota' x \cup \iota' y. x \neq y. \supset. \alpha \neq \iota' x. \alpha \neq \iota' y$ (2)
 $\vdash. (1). (2). \supset \vdash :: \alpha = \iota' x \cup \iota' y. x \neq y. \supset :$
 $\beta \subset \alpha. \supset ! \beta. \beta \neq \alpha. \equiv : \beta = \iota' x. \vee. \beta = \iota' y :$
[*51.235] $\equiv : (\supset z). z \in \alpha. \beta = \iota' z :$
[*37.6] $\equiv : \beta \in \iota' \alpha$ (3)
 $\vdash. (3). *11.11.35. *54.101. \supset \vdash. \text{Prop}$

*54.43. $\vdash :: \alpha, \beta \in 1. \supset : \alpha \cap \beta = \Lambda. \equiv. \alpha \cup \beta \in 2$
Dem.
 $\vdash. *54.26. \supset \vdash :: \alpha = \iota' x. \beta = \iota' y. \supset : \alpha \cup \beta \in 2. \equiv. x \neq y.$
[*51.231] $\equiv. \iota' x \cap \iota' y = \Lambda.$
[*13.12] $\equiv. \alpha \cap \beta = \Lambda$ (1)
 $\vdash. (1). *11.11.35. \supset$
 $\vdash :: (\supset x, y). \alpha = \iota' x. \beta = \iota' y. \supset : \alpha \cup \beta \in 2. \equiv. \alpha \cap \beta = \Lambda$ (2)
 $\vdash. (2). *11.54. *52.1. \supset \vdash. \text{Prop}$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

Principia Mathematica adlı eserde $1 + 1 = 2$ önermesinin kanıtından bahsedilen yer

Hilbert'in öncülüğünde çalışan matematikçiler, tüm matematiği sağlam, çelişkisiz ve eksiksiz bir biçimsel sistem olarak kurmayı hedefliyorlardı. Hilbert'in ünlü “Bilmeliyiz, bileceğiz” sloganı, bu iyimser arayışın simgesiydi.

Ancak henüz 25 yaşındayken genç Kurt Gödel'in 1931'de yayımladığı Eksiklik Teoremleri, bu programı sarsıcı biçimde altüst etti. Matematiğin temelini oluşturması umulan bu eşsiz yapının içinden konuşarak, onun sınırlarını gösterdi. Gödel, yeterince güçlü herhangi bir biçimsel sistemin kaçınılmaz olarak eksik olacağını, yani bazı doğru önermelerin sistem içinde ispatlanamayacağını kanıtladı (*Birinci Eksiklik Teoremi*). Ayrıca, böyle bir sistemin kendi tutarlılığını yine kendi içinde kanıtlamasının imkânsız olduğunu da gösterdi (*İkinci Eksiklik Teoremi*).

Daha matematiksel olarak ifade etmek istersek, Gödel'in birinci eksiklik teoremi şunu söyler: Doğal sayıları, toplama ve çarpma (yani aritmetiğin tamamını) ifade edecek güçte olan ve neyin aksiyom olup olmadığı anlaşılabilen çelişkisiz (tutarlı) bir sistemde², doğru olan ama sistem içinde kanıtlanamayan bir önerme olmak zorundadır. Dolayısıyla sistem eksiktir. Bu teorem basit ve akıllıca bir temel fikre dayanır. Gödel'in temelde yaptığı iş biçimsel dilin aritmetikleştirilmesidir. Yani Gödel, biçimsel sistemin dilinde oluşturulabilecek bütün önermeleri (doğru ya da yanlış), terimleri, formülleri, kanıtları (hatta her cümleyi) doğal sayılar, toplama ve çarpma kullanarak yazmanın bir yöntemini sunmuştur. Bunu nasıl yaptığını bir sonraki bölümde değineceğiz. Bu fikirden yola çıkan Gödel, "Bu önerme kanıtlanamaz" cümlesini

²Bkz. Peano Aritmetiği

aritmetik ile ifade etmeyi başarır. Dolayısıyla matematiğe indirgenen bu önermenin artık bir matematiksel önerme olduğunu söyleyebiliriz. O halde bu önerme ya doğru ya da yanlış olmalıdır. İlk olarak önermenin yanlış olduğunu düşünelim. Bu durumda verilen önerme kanıtlanabilir olmalıdır. Biliyoruz ki matematikte bir önerme kanıtlanabiliyorsa doğrudur. Ancak önermenin yanlış olduğunu kabul etmiştik. Dolayısıyla bir çelişki elde ettik. Çelişkisiz bir sistemde olduğumuza göre, önerme doğru olmalıdır. Önermenin ne dediğine tekrar bakalım: "Bu önerme kanıtlanamaz". O halde elimizde doğru bir önerme var ve bu önerme kanıtlanamaz!³

Şimdi ikinci eksiklik teoremine matematiksel olarak bakalım: Doğal sayıları, toplamayı ve çarpmayı ifade edecek güçte tutarlı bir sistemin tutarlı olduğu gerçeği sistemin içinde kanıtlanamaz. Bu teorem aslında birinci eksiklik teoreminden elde edilir. Tutarlı bir S sisteminin tutarlılığının kendi içinde kanıtlanamayacağını göstereceğiz. G önermesi Birinci Eksiklik Teoremi'nde bahsedilen kanıtlanamaz bir önerme olsun. S sisteminin tutarlılığının kendi içinde kanıtlanabildiğini varsayalım. Yani bu, " S sistemi tutarlıdır" önermesini kanıtlamak demektir. Şimdi, "Eğer S sistemi tutarlıysa, bu durumda G önermesi kanıtlanamaz" ile verilen önermeyi ele alalım. Bu önerme sistem içinde biçimselleştirilebilir. S sisteminin tutarlılığının kendi içinde kanıtlanabildiğini varsaydığımızdan dolayı, bu önermeyle birlikte G 'nin kanıtlanamazlığı da sistem içinde kanıtlanmış olur. G önermesi kanıtlanamayacağını söylüyordu ve biz bu önermeyi sistem içinde kanıtlamış olduk. Bu durum Birinci Eksiklik Teoremi ile çelişir. Dolayısıyla varsayımımız yanlış olup, tutarlı bir sistem kendi tutarlılığını kanıtlayamaz, sonucuna varırız.

3. Gödel Numaralandırması

Gödel numaralandırması, bir aksiyomlar sistemi hakkındaki ifadeleri sistem içindeki ifadelerle, yani sayılarla ilgili ifadelerle eşleyerek sistemin *bir anlamda* kendisiyle konuşmasını sağlar. Bu süreçteki ilk adım, herhangi bir olası matematiksel ifadeyi veya bir dizi ifadeyi *Gödel numarası* adı verilen biricik sayıya eşlemektir.

Öncelikle, biçimsel sistemin dilindeki her bir ilkel sembole, sabite, fonksiyon sembollerine ve değişken sembollerine birer doğal sayı atanır. Bu sayıya o sembolün *sembol numarası* denir. Hangi sembole hangi sayının atanacağı ve hangi sırayla yapılacağı önemli değildir; bu atama keyfidir. Ancak bir kez yapıldıktan sonra sabit kalmalıdır. Örneğin aritmetiğin standart dili göz önüne alınırsa, bir şeyin var olduğu ifadesi $\exists$ sembolü ile, toplama ise $+$ ile ifade edilir. Daha da önemlisi, "ardılı" ifade eden S sembolü, sayıları belirtmenin bir yolunu verir; örneğin $SS0$, 2'yi (0'ın ardılının ardılı) ifade eder. Örneğin Nagel ve Newman, tam olarak 12 tane sabit sembol olduğunu kabul etmiş ve bu sembollere aşağıdaki doğal sayıları atamıştır.

Sabit Sembol	Sembol Numarası	Anlamı
$\neg$	1	değil
$\vee$	2	veya
$\rightarrow$	3	eğer... ise
$\exists$	4	... vardır
$=$	5	eşittir
0	6	sıfır
S	7	ardıl (bir sonraki sayı)
(	8	sol parantez
)	9	sağ parantez
,	10	noktalama işareti (virgül)
$+$	11	toplama
$\times$	12	çarpma

Tablo 1. İlkel sabit sembollerin Gödel numaraları

Bu on iki sembolden sonra, x , y ve z gibi sayısal değişkenleri temsil eden harfler, 12'den büyük asal sayılara (yani 13, 17, 19, ...) eşlenir. Bu biçimsel dilde yazılabilecek sayılabilir sonsuz çoklukta cümle var.

³Bazıları şu soruyu sorabilir: Şimdi biz önermenin doğru olduğunu kanıtlamış olmadık mı? Cevap: Hayır. Teoremin ifadesine dönecek olursak burada anahtar ifade "sistem içinde kanıtlanamayan" ifadesidir.

Bu cümlelerin hepsi kurala uygun olmayabilir, ancak bunu kontrol edebileceğimiz bir algoritma mevcuttur. Yukarıdaki atamaları yaptıktan sonra bu sembollerin ve değişkenlerin herhangi bir kombinasyonu — yani oluşturulabilen herhangi bir aritmetik formül veya formül dizisi — kendi Gödel sayısını alır. Örneğin, $0 = 0$ formülünü ele alalım. Bu formülün üç sembolü, Gödel sayıları sırasıyla 6, 5 ve 6'ya karşılık gelir. Gödel'in bu üç sayı dizisini, başka hiçbir simge dizisinin üretemeyeceği tek ve benzersiz bir sayıya dönüştürmesi gerekir. Bunu yapmak için ilk üç asal sayıyı (2, 3 ve 5) alır; aynı konumdaki sembole karşılık gelen sayıyı bu asal sayının kuvvetine yazar ve bunları birbiriyle çarpar:

$$2^6 \times 3^5 \times 5^6 = 243,000,000$$

Bu eşleme oldukça işe yarar, çünkü *Aritmetiğin Temel Teoremi* sayesinde her önerme tek bir sayıyla ve her sayı da tek bir önerme ile eşleşir. Gödel sayıları tam sayılardır ve tam sayılar asal sayıların etkisine yalnızca tek bir şekilde açıktır. Yani 243.000.000 sayısının asal çarpanlara ayrılması yalnızca şu şekilde mümkündür:

$$2^6 \times 3^5 \times 5^6$$

Dolayısıyla, bu Gödel sayısına karşılık gelen formül yalnızca $0 = 0$ olabilir.

Gödel daha sonra bir adım daha ileri giderek her formül dizisine de benzersiz bir Gödel numarası verdi. Bu durumda, daha önce olduğu gibi asal sayılar listesiyle başladı. Daha sonra her bir asalı dizideki aynı konumdaki formülün Gödel sayısına yükseltti. Örneğin $0 = 0$ önce geliyorsa, bu dizinin sayısı şu şekilde olur:

$$2^{243,000,000}$$

Sonuç olarak Gödel, bu yöntemi kullanarak her mantıksal ifadeyi bir doğal sayıya çevirmeyi başardı; buna Gödel numaralandırması denir. Bu sayede formüller aritmetiğin diliyle temsil edilebildi. Bu tekniklerle, kendi anlamına gönderme yapan, yani "bu önerme kanıtlanamaz" diyen en az bir önerme kurmayı başardı. Böyle bir önerme, sistem tutarlıysa ne ispatlanabilir ne de çürütülebilir. Bir önceki bölümde de ifade ettiğimiz gibi bu, Gödel'in birinci eksiklik teoreminin özüdür: Tutarlı ve yeterince güçlü her biçimsel sistemde, doğruluğu sistem içinde kanıtlanamayan önermeler vardır.

4. Kapanış

Eksiklik teoremlerinin sonuçları çok yıkıcıydı. Mantıksal-pozitivist olan Viyana Çevresi, Hilbert'in biçimcilik projesi başta olmak üzere matematiğin temelleri sorununu çözmeye çalışan herkesi yerle yeksan etmişti. Peki bu teoremler gerçekten elimizi kolumuzu bağlıyor mu? Matematik tutarsız olabilir mi? O halde bunca şeyi üstüne inşa ettiğimiz, medeniyetimizin direği, matematik eksik olabilir mi? Teoremler insanın aklında bolca soruya yol açıyor ve ne yazık ki bu soruların birçoğu zihnimizce yanlış cevaplanıyor. Ben de ilk başta oldukça yanlış cevaplamıştım ve derinden üzen bir yola sokmuştu. Fakat bir gün Ahmet Çevik'in 'Matematik Felsefesi ve Matematiksel Mantık' isimli kitabında bir sonraki alt başlıkta yazdığım şeyleri okuyuncaya kadar.

■ Eksiklik teoremlerinden ne anlamamalıyız?

- Hiçbir biçimsel sistem tam ve tutarlı olamaz.

Gödel'in teoremi her biçimsel sistem için geçerli değildir. Tam ve tutarlı bir sisteme örnek: burulmasız bölünebilen Abel grupları.

- Matematik tutarsızdır veya tutarlı olduğu bilinemez.

Gödel'in teoremleri matematiğin tutarsız olduğunu söylemez. Sadece yeterince güçlü sistemlerin kendi tutarlılığını sistemin aksiyomlarından kanıtlamayacağını söyler.

- Gödel'in teoremi yanlıştır ve matematikçiler arasında kabul görmez.

Gödel'in özgün teoreminden bu yana, eksiklik olgusu kapsamlı bir şekilde incelenmiş ve oldukça iyi anlaşılmıştır. Matematik camiası Gödel'in teoremlerini kabul etmiş ve değerini takdir etmiştir.

- Matematik biçimsel bir sistem haline getirilemez.

Burada olağan matematik-gerçek matematik ayrımı yapmak gerekir. Yapmış olduğumuz matematik biçimselleştirilebilir, ancak yapıyor olduğumuz matematik aktivitesi biçimselleştirilemez.

Matematik tarih boyunca birçok krizle karşı karşıya geldi. Büyük çoğunluğunu çözmüş olsak da, en önemli krizi hâlâ çözmek bir yana tam olarak anlamış bile bulunmuyoruz. Gödel'i kendini aç bırakıp, paranoyalarına teslim eden karanlık da bu olsa gerek. Hayatının son yıllarında çevresindeki herkesin onu zehirleyeceğine inanan Gödel, sadece eşi tarafından hazırlanmış yemekleri yemeyi kabul ediyordu. Eşi hastalanıp hastaneye kaldırıldığında ise tamamen yemek yemeyi reddetti ve 1978'de, yalnızca 29 kilo ağırlığındayken açlıktan hayatını kaybetti.

Cantor, Turing, John Nash ve Kurt Gödel – Tüm bu matematikçiler sıra dışı denilebilecek hayatlar sürdüler ve aynı sıra dışılığa son nefeslerini verdiler. Fakat onların açtığı o daracık yol sayesinde matematik dünyamıza ışık tutabiliyor. Bir süredir okuyup araştırdığım, anlamaya çalıştığım, Einstein'ın yakın dostu olan bu 'deli' matematikçilerden paranoyak matematikçimiz Kurt Gödel'i umarım anlatabilmişimdir. Tuhaf bir adamdı ama bu tuhaf adamın olağanüstü düşleri vardı. Bu düşler sayesinde içinde yaşadığımız düşü daha iyi anlayabiliyoruz ya da en azından anlamaya çalışıyoruz.



Einstein ve Gödel, New Jersey, Princeton'daki düzenli yürüyüşlerinden birinde.

■ Kaynaklar

- [1] Ali Nesin & Ali Törün, Matematikçi Portreleri (7. Baskı), Nesin Yayıncılık, 2023.
- [2] Ahmet Çevik, Matematik Felsefesi ve Matematiksel Mantık, Nesin Yayıncılık, 2019.
- [3] Janna Levin, Tuhaf Bir Adamın Olağanüstü Düşleri, Çev. Nedim Çatlı, Nora Kitap, 2021.
- [4] Ernest Nagel & James R. Newman, Gödel Kanıtlaması, Çev. Bülent Gözkan, Alfa Yayıncılık, 2020.
- [5] Bekir S. Gür, Matematik Belası Üzerine, Nesin Yayıncılık, 2020.
- [6] https://nesinkoyleri.org/wp-content/uploads/2019/09/226_232_kurtgodel.pdf
- [7] Matthias Baaz, Kurt Godel and the Foundations of Mathematics: Horizons Of Truth, Cambridge, 2021.

Matematiğin İzinde Kitaplar

PINAR AYDOĞDU

Hacettepe Üniversitesi Matematik Bölümü

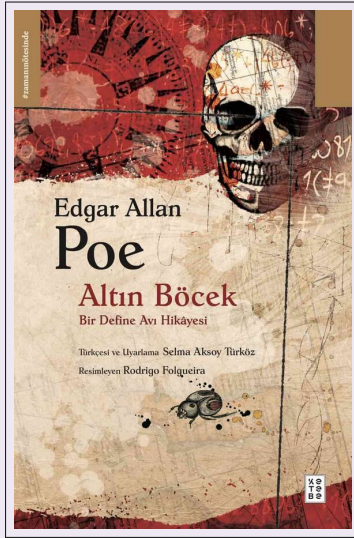
✉ paydogdu@hacettepe.edu.tr



Bir düşünce eylemi olarak matematik, kendini ifade etmenin yaygın ve etkin yollarından biri olan yazmakla iç içedir. Bu nedenle, sanılanın aksine, resim, müzik gibi görsel ve işitsel sanat dallarının yanı sıra edebiyatla da sıkı bir dostluğu vardır. Bu köşemizde, matematiğin izinden giderek ilgimizi çeken ve öğrencilerimizin mutlaka okuması gerektiğini düşündüğümüz popüler bilim, roman, şiir, öykü vs. elimizin vardığı tüm kitapları kısaca tanıtmaya çalışacağız.

■ Edebiyatın Şifresi: Poe ve Altın Böcek

Altın Böcek – Edgar Allan Poe (Çev. Selma Aksoy Türköz), Ketebe Yayınları (2025)



Edgar Allan Poe'nun 1843'te kaleme aldığı Altın Böcek adlı öyküsü, gotik atmosferi ve gizemli anlatımıyla tanınsa da, aynı zamanda matematiksel düşünme biçimlerini barındıran nadir edebi metinlerden biridir. Poe, hazine avı temasını sıradan bir macera kurgusu olmaktan çıkarıp, bir şifre çözme problemine dönüştürür. Ana karakter William Legrand, bir parşömente karşılaştığı şifreli metni, yalnızca dilsel değil, matematiksel yöntemlerle çözerek okuyucuyu şaşırtır. Bu yönüyle Altın Böcek, yalnızca bir öykü değil, aynı zamanda (basit) bir kriptografi dersi gibidir. Öyküdeki gizli mesaj, klasik bir yerine koyma şifresi ile yazılmıştır. Bu, her harfin başka bir harfle (veya sembolle) değiştirildiği basit ama tarihsel olarak etkili bir şifreleme yöntemidir. Legrand, şifreyi çözmek için İngilizce dilinde en sık kullanılan harfleri (özellikle E, T, A gibi) analiz eder. Bu yöntem, modern kriptografinin temel taşlarından biri olan frekans analizinin ilk uygulamalarından biri olarak değerlendirilebilir. Poe'nun öyküsünde Legrand'ın şu cümlesi dikkat çekicidir:

“Kriptografik yazının yaratıcılığı şifrenin kendisinde değil, onu kıran zihinde yatmaktadır.”

Legrand'ın burada ifade ettiği gibi, matematiksel düşünce yalnızca formüllerde değil, çözüm stratejilerinde ve sabırla ilerletilen analizlerde de kendini gösterir.

Altın Böcek, bir matematikçinin gözünden yalnızca bir şifreli mesaj değil, bir problem çözme sürecinin dramatik bir sunumu olarak da okunabilir. Poe, karakterine yalnızca zekâ değil, sistematik düşünme ve gözlem yeteneği de verir. Bu yönüyle öykü, matematiksel akıl yürütmenin edebiyattaki temsiline güzel bir örnek oluşturur. Günümüzde siber güvenlikten yapay zekâya kadar pek çok alanda kullanılan kriptografinin, bir yazarın hayal gücüyle nasıl birleştiğini görmek, hem ilham verici hem de düşündürücüdür.

Gotik edebiyatın önemli temsilcilerinden biri olan Poe, polisiye edebiyatın kurucusu ve bilim kurgu türünün de ilk temsilcilerinden biri olarak kabul edilir. Öykülerinde kullandığı şifreleme tekniği ile ilgili

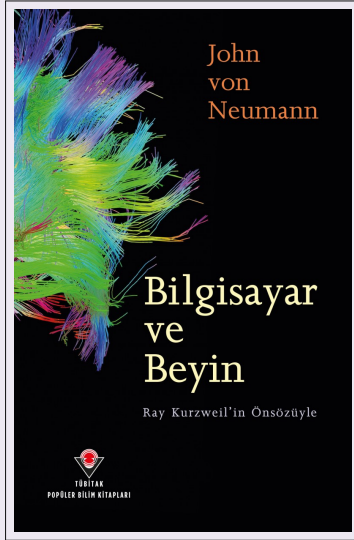
yazılmış makaleler de vardır. Onu esas üne kavuşturan Kuzgun şiirini de özellikle okumanızı tavsiye ederim.

Ek Okuma Önerisi: Şifreleme konusuna ilgi duyanlar için, çok iyi bir bilim yazarı olan Simon Singh’in, Buzdağı Yayınları’ndan Ali Atav çevirisi ile 2020’de yayımlanan “Şifre Kitabı: Antik Mısır’dan Kuantum Bilgisayarlara Gizlilik Bilimi” kitabını da öneririm.

Film Önerisi: The Pale Blue Eye, 2022

■ Bir Matematikçinin Beyni: Von Neumann, Bilgisayar ve Düşünce

Bilgisayar ve Beyin – John von Neumann (Çev. Zekeriya Aydın), TÜBİTAK Popüler Bilim Kitapları (2023)



Matematik tarihine adını altın harflerle yazdıran Macar-Amerikalı matematikçi John von Neumann, 20. yüzyılın dahilerinden biri olarak bilinir. Henüz çocuk yaşlarda kendini belli eden parlak zekası sayesinde matematikten fiziğe, ekonomiden bilgisayara pek çok alanda önemli izler bıraktı. Von Neumann, atom bombasının yanı sıra modern bilgisayarların gelişmesine ön ayak olmuş isimlerden biridir. Ne var ki, atom bombası çalışmalarına katıldığı Manhattan Projesi’nde yer alması daha sonraki yıllarda kanser olmasına yol açtı ve henüz 53 yaşında, daha pek çok bilimsel katkı verebileceği bir dönemde bu dünyadan ayrıldı. Ancak, onun zekası ölüm döşeginde de kendini gösterdi: Ölümünden kısa bir süre önce, hasta yatağında kaleme aldığı Bilgisayar ve Beyin adlı kitabı, makineyle zihni karşılaştıran felsefi ve bilimsel bir sorgulamanın ürünü. Sağlığı el verseydi bir konferansta sunacağı kitaplaştırılmış bu yazı, yalnızca soyut kuramlarla değil, modern bilgisayarın mimarisiyle de bugün hâlâ etkisini sürdürüyor. Von Neumann’ın tamamlanamamış bu notları, temelinde beyni bir makine olarak nasıl görebileceğimizi

tartışıyor. Von Neumann’ın eşi Klara Dan von Neumann’ın duygusal bir girişiyle başlayan kitabın dili-mize çevrilirken de baz alınan üçüncü baskısında bilgisayar bilimci Ray Kurzweil’in uzun ve açıklayıcı bir önsözü bulunuyor. Ayrıca, ikinci baskıdan sonra eklenen, nörobilim felsefesi üzerine çalışan Paul Churchland ve Patricia Churchland ikilisine ait bir önsöz de var. Bu önsözlerle birlikte, kitabın felsefi ve bilimsel yanlarının daha anlaşılır olduğunu söylemek mümkün.

Von Neumann, beynin ve bilgisayarın bilgi işleme süreçlerini karşılaştırırken, her ikisinin de elektriksel sinyallerle çalışmasına rağmen temelde farklı yapılar olduğunu savunur: Bilgisayarlar düzenli, merkezi ve dijitaldir; beyin ise paralel, dağınık ve büyük ölçüde analog. Beyin ve bilgisayar karşılaştırmasını aşağıdaki tabloda özetleyebiliriz:

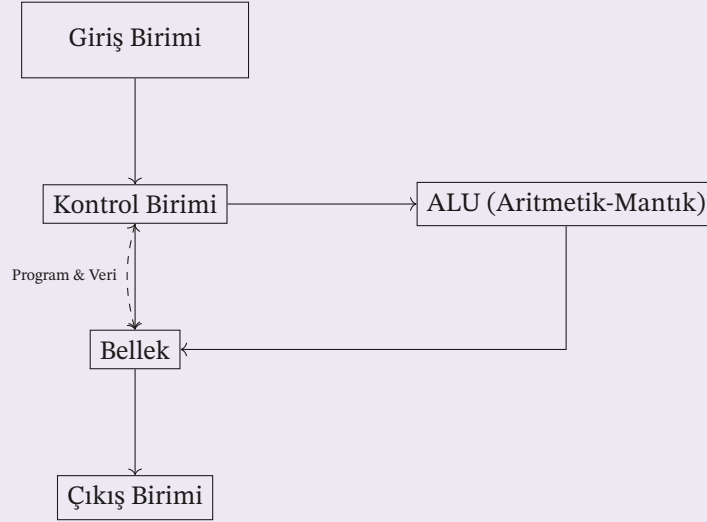
Özellik	Bilgisayar	Beyin
Yapı	Merkezi, sabit	Dağınık, dinamik
İşlem	Sıralı	Paralel
Sinyal Tipi	Dijital (0/1)	Elektrokimyasal
Bellek	Adresli	İlişkilendirici
Esneklik	Sınırlı	Öğrenebilir
Hata Toleransı	Düşük	Yüksek

Tablo 1. Beyin ile bilgisayarın temel farkları

Kitap, yalnızca hesaplama biliminin temel taşlarını değil, insan zihninin ne kadar "hesaplanabilir" olduğunu da sorgular. Von Neumann'ın net ve sistematik anlatımı, okuyucular için hem kavramsal hem ilham verici bir keşif sunar. Bu kısa ama yoğun metin, modern matematiksel düşüncenin nerelere uzanabileceğini görmek isteyenler için kaçırılmaması gereken bir eserdir.

Bugün kullandığımız bilgisayarlar, "Von Neumann mimarisi" olarak bilinen bir yapı üzerinde kurulmuştur. Bellek, işlemci ve veri akışını düzenleyen ilk kişi von Neumann'dır. Onun oluşturduğu bu yapı, halen cep telefonu, diz üstü bilgisayar ve hatta süper bilgisayarların temelini oluşturmaktadır.

Von Neumann'ın 1945'te oluşturduğu mimari şema aşağıdaki şekilde ifade edilebilir:



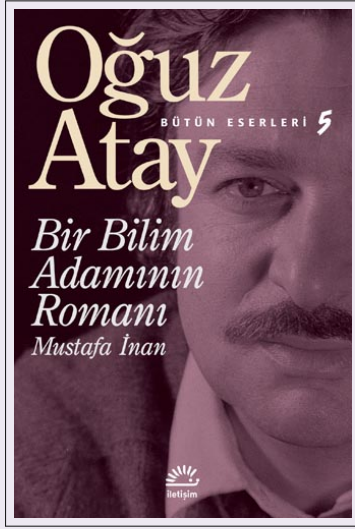
Bu aşamadan sonra, 1950'de Turing'in ünlü Computing Machinery and Intelligence makalesi yayımlanmıştır. İlk kez 1958 yılında yayımlanan Bilgisayar ve Beyin kitabının ardından 1960'larda manyetik çekirdek hücreli bellekler kullanılmaya başlanmıştır.

Bu bölümü, Cahit Arf'ın, von Neumann ile ilgili sözleri ile noktalamak istiyorum. Bir sohbet sırasında bir arkadaşı Cahit Arf'a, "Sen Türkiye'nin von Neumann'ısın." der. Bunun üzerine, Arf arkadaşına von Neumann ile karşılaşmış karşılaşmadığını sorar. Arkadaşı karşılaşmadığını söyleyince Cahit Arf şöyle devam eder: "Ben karşılaştım. Adam o kadar hızlı düşünüp, o kadar hızlı konuşuyor ki söylediklerini anlayıp takip edemedim, hem de bildiğim ya da bildiğimi sandığım matematikti sohbet konumuz."

Film Önerisi: Adventures of a Mathematician, 2020.

■ Mustafa İnan: Bilimle Yaşayan Bir Öncünün Romanı

Bir Bilim Adamının Romanı – Oğuz Atay, İletişim Yayınları (2024)



Türkiye'nin modern bilim ve mühendislik tarihinin mihenk taşlarından biri olan Mustafa İnan, bilimsel azmi ve vizyonu ile ülkemizde bilim kültürünün gelişmesine büyük katkı sağlamıştır. Yaşam öyküsü, TÜ-BİTAK'ın Bilim Adamı Yetiştirme Grubu'na ait bir proje kapsamında, öğrencisi Oğuz Atay'ın kaleme aldığı *Bir Bilim Adamının Romanı* (1975) adlı biyografik romana konu olmuştur. Önsözünü Cahit Arf'ın yazdığı roman, her ne kadar ısmarlama olarak yazılmış olsa da hem akademisyen hem de başarılı bir yazar olan Atay'ın güçlü kalem sayesinde bilim tarihine önemli bir katkı sunulmuştur. Atay, bu değerli bilim insanının hayatını ve iç dünyasını edebi bir dille gözler önüne sermiştir. Mustafa İnan'ı yalnızca başarılı bir mühendis ve akademisyen olarak değil, aynı zamanda bilimsel ideallerle yoğrulmuş bir insan olarak tasvir eder. Kitapta İnan'ın disiplinli çalışmaları, Türkiye'nin kalkınması için verdiği mücadele ve akademik yaşamındaki zorluklar derinlikli bir şekilde ele alınır. Bu yönüyle eser, bilim insanı olmanın yalnızca teknik bilgi birikimi değil, aynı zamanda büyük bir sabır, inanç ve toplumsal sorumluluk gerektirdiğini ortaya koyar. İnan'ın teknik başarısının ötesinde, onun bilimsel sürece yaklaşımını, araştırma etiğini ve insanî yönlerini de okuyucuya aktarır. Akademik bürokrasi, kaynak sıkıntısı ve zaman zaman yalnızlık gibi zorluklar, bilimsel tutkusu karşısında küçük kalır.

Mustafa İnan bir inşaat mühendisi idi. Ancak, kendisi gibi inşaat mühendisi ve akademisyen olan öğrencisi Atay'ın kaleminden çıkan bu romanda da görülebileceği gibi İnan'ı bir matematikçi olarak anmak kesinlikle yanlış değildir. Kendisi ülkemizde yapılan matematik çalışmalarının gelişmesi için katkıda bulunmaya sürekli çaba göstermiştir. Uzmanlık alanından önce matematiğin doğru bir şekilde yerleşmesi için çalışmıştır. Hatta arkadaşları kendisinden Kerim Erim'in doçenti olarak bahsederler. (Kerim Erim, Türkiye'nin ilk doktoralı matematikçisidir ve Cumhuriyet tarihimizin önemli matematikçilerindendir.) Ayrıca, edebiyat ve dil başta olmak üzere, pek çok konuya ilgi duyan İnan, Dil ve Matematik başlığı ile bir makale de yayımlamıştır (dil çalışmalarına devam etmek istese de ne yazık ki ömrü vefa etmemiştir). Bu bağlamda roman, özellikle matematik ve fen bilimleri öğrencileri için yol gösterici bir nitelik taşır. Mustafa İnan'ın hayatı, genç bilim insanlarına sadece mesleki başarı için değil, aynı zamanda bilime ve topluma karşı duyulan sorumluluğun önemini de hatırlatır. Oğuz Atay'ın etkileyici anlatımı, bilim dünyasının soğuk yüzünün ardındaki insanî dokuyu başarıyla ortaya koyar. Mustafa İnan'ın bilimsel mirası, Atay'ın kalem ile nesilden nesile aktarılırken, okuyucuda bilimin yalnızca bir meslek değil, bir yaşam biçimi olduğu bilinci pekişir. Kısaca, *Bir Bilim Adamının Romanı*, matematiğe ve bilime gönül veren herkes için ilham verici, düşündürücü ve öğretici bir başvuru kaynağıdır.

Şunu da ifade etmek gerekir ki, Adana'nın bir köyünden yola çıkarak, ülkesini kalkındırmak için önemli adımlara ve büyük başarılarla imza atmış olan İnan, o dönemki genç cumhuriyetimizin çok önemli bir kazanımıdır. Tübitak'ın ve Türk Matematik Derneği'nin kurucuları arasında yer alan Mustafa İnan'ın eşi Jale İnan da Türkiye'nin ilk kadın arkeoloğudur.

Ek Okuma Önerisi: Ne yazık ki ülkemizdeki arşiv yetersizliğinden, değerli matematikçimiz Prof. Dr. Kerim Erim hakkında detaylı bir biyografi yazılamamış olsa da, bilim tarihçilerimizden Osman Bahadır'ın kaleme aldığı, Anahtar Kitaplar tarafından 2006'da yayımlanan “Matematikte Bir Öncü Kerim Erim” biyografisini okumanızı da tavsiye ederim.

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– yanıtı giden yolun kendisi de tümüyle yepyeni teorilerin doğmasına neden olabilmektedir. **Fermat’ın 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’ın 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’ın 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’ın 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. Matematğin 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) ayrıştırılabilmesidir. 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 türdür. 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 parçalandığı ile 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 (gerçek veya karmaşık katsayılı) polinomlar da benzer bir özelliğe

sahiptir. Buna göre sıfırdan farklı sabit olmayan her polinom ilerde *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 · 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 · 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 $p \nmid a$ veya $p \nmid b$ 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 indirgenemezdır. 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 şekilde 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 ayrılabiliriyorsa, bu işlemi ortaya çıkan tüm yeni çarpanlar için tekrarlayabiliriz. Bu işlemi tekrarladığımızda eğer bir adımdan sonra hiçbir çarpanın daha fazla birimsel olmayan çarpana ayrılmadığını 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 yazılabilmek konusudur. Eğer bu türden her yazım bir anlamda tek türlü ise o zaman tek türlü çarpanlara ayırma özelliği adı verilen özellik ortaya çıkar. Peki bu tek türlülüğü nasıl tanımlayacağız? Elbette ki bazı yazımları eşdeğer kabul ederek. Öncelikle çarpanın 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 türlüliğini 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 $p_1, \dots, p_n \in R$ indirgenemez elemanlar, u birimsel eleman ve $k_1, \dots, k_n$ pozitif tam sayılar olmak üzere $x = u p_1^{k_1} \dots p_n^{k_n}$ biçiminde çarpanlarına ayrılabilir ve
- (2) $k_1, \dots, k_n, l_1, \dots, l_m$ 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 ayrılıştaki ikiye ikiye 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'ın **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. $\square$

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. $N(p) > N(r_1) > N(r_2) > \dots > N(r_i) > N(r_{i+1}) \geq 0$ 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 $r_{n-1} \mid r_{n-2}, r_{n-1} \mid r_{n-3}, \dots, r_{n-1} \mid p, r_{n-1} \mid a$ 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:

$$\begin{aligned} ab &= pbq_1 + r_1b \\ pb &= r_1bq_2 + r_2b \end{aligned}$$

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

$p \mid ab$ 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. $\square$

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 $k_1, \dots, k_n, l_1, \dots, l_m$ pozitif tam sayıları, herhangi ikisi ilgili olmayan indirgenemez elemanlardan oluşan $\{p_1, \dots, p_n\}$ ve $\{q_1, \dots, q_m\}$ kümeleri ile u ve v birimsel elemanları için $z = u p_1^{k_1} \dots p_n^{k_n}$ ve $z = v q_1^{l_1} \dots q_m^{l_m}$ biçiminde iki farklı çarpanlara ayırma yazımı bulunsun. Teorem 2'den p_1 indirgenemez elemanı aynı zamanda asal elemandır. $p_1 \mid q_1^{l_1} \dots q_m^{l_m}$ 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 $z = u p_1^{k_1} \dots p_n^{k_n} = v u_1^{l_1} p_1^{l_1} \dots q_m^{l_m}$ olur. $\mathbb{Z}[i]$ bir tamlık bölgesi olduğundan, sadeleşme işlemi yapabiliriz. Genelliği bozmadan $k_1 \geq l_1$ olduğunu varsayalım. Bu durumda

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

elde edilir. Bu yazımda $k_1 - l_1$ bir pozitif tam sayı ise o zaman p_1 asal elemanı $q_2^{l_2} \dots q_m^{l_m}$ çarpımını böleceği için $q_2, \dots, q_m$ indirgenemez elemanlarından biri ile ilgili olur. Fakat q_1 de p_1 ile ilgili olduğundan, bu durumda $q_2, \dots, q_m$ 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 $u p_2^{k_2} \dots p_n^{k_n} = v' q_2^{l_2} \dots q_m^{l_m}$ 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. $\square$

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'ın 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.

Bilgisayarlar Nasıl Çalışabilir?

MURAT ERŞEN ÜNAL

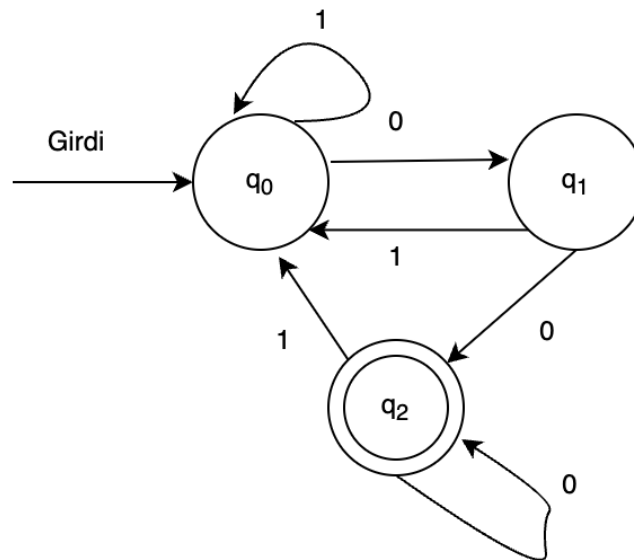
Hacettepe Üniversitesi Matematik Bölümü, Yüksek Lisans Öğrencisi

✉ mersenunal@gmail.com



Evde, işte, okulda, otobüste... kısaca her yerde karşımıza çıkıyor bilgisayarlar. Bazen bir masanın üzerinde bazen içini görmediğimiz bir kutuda. Hepsine bilgisayar diyoruz ama aslında hepsi başka bir iş yapıyor. Hatta bir bilgisayarla farklı zamanlarda farklı işler yapıyoruz. Akşamları okuldan gelince oyun oynarken gece yatmadan ödevi yapmadığımızı fark edip sabaha kadar ödev yapıyoruz. Sonra da sabah derste uyuyoruz... Farklı işler yapması bakımından beynimize benziyor bilgisayarlar. Örneğin, beynimiz uyurken rüyalarla meşgulken, sabah sabah okula giderken metroda, otobüste veya sokakta gördüğümüz kimi insanları inceler hatta bazılarıyla ilgili hayaller bile kurar. O sırada reklam tabelalarında gördüğü bir yazıyı da okumayı ihmal etmez. Çok ilginçtir insan okuyabildiği bir kelimeyi görünce okur. Neyse konuyu dağıtmayalım, Aynı bilgisayarın farklı işlemleri yapabilmesi programlanabilir olmasının sonucudur. Günümüzde kullandığımız ortalama bir diz üstü bilgisayar saniyede yaklaşık olarak 10^9 adet işlem yapabilmektedir. Bunu en ama en kaba haliyle şöyle düşünebilirsiniz, bir bilgisayar bir saniyede 1 milyar tane toplama işlemi yapabilmektedir. Ancak bu bahsettiğimiz bilgisayarın nasıl çalıştığını tam olarak anlayabilmek için; otomat teoriden yarı iletken fiziğine, bilgisayar programlamadan dijital devre tasarımına kadar birçok alanda derinlemesine bilgi sahibi olmak gerekir. Bu yüzden başlığımız “Bilgisayarlar Nasıl Çalışır?” değil. Biz bu yazıda belli bir kurala göre davranan bir mekanizma ile basit bir problemi nasıl çözebiliriz onu göstereceğiz. Ve böylece bu yazıyı okuyan biri üzerinde, bilgisayarların nasıl çalışabileceğine dair bir önsezi yaratabiliriz. Birazdan anlatacağımız şimdiden gözünüzü korkutmasın herkesin anlayabileceği şeylerden söz edeceğiz.

Otomatalardan söz edeceğiz. Otomataların önemli olmasının bir sebebi, Otomataları basit dijital devre elemanlarıyla gerçekleyebiliyor olmamız. Yani verilen bir otomata gibi davranan bir dijital devre oluşturabilen mekanizmalarımız var. Bu mekanizmalara da belki ileride değiniriz. Öncelikle otomataları inceleyelim.



Şekil 1. 4 ile bölünebilme kuralını tanıyan otomata

Şekil 1’de bir otomatanın basit bir görseli görülmektedir. Bu otomata q_0 konumunda başlamaktadır ve girdi olarak 0 ve 1 harflerinden oluşan bir dizi kabul etmektedir. Bir otomata bulunduğu konum ve girdisinin incelediği elemanına göre bir sonraki konumunu güncellemektedir. Bu güncelleme yöntemi şekil üzerinde oklarla gösterilmiştir. Örneğin q_2 konumunda olan bir otomata; 1 harfi geldiğinde q_0 konumuna gidecek, 0 harfi geldiğinde ise yine q_2 konumunda kalacaktır. Girdinin tüm elemanları incelendiğinde otomatanın son olarak bulunduğu konum ise o girdiye verdiği cevap olarak adlandırılır. Örneğin şekildeki otomataya 01001 dizisini girdi olarak verdiğimizde otomata aşağıda adım adım anlatıldığı şekilde hareket edip cevap verecektir. Burada dikkat edilmelidir ki okumayı soldan sağa doğru yapıyoruz. Bu durum farklı kaynaklarda farklılıklar göstermektedir. Fakat genel durumu değiştiren herhangi bir yargı yoktur, sadece sıralamanın tersten yapılması olasıdır ve şaşıracak bir durum değildir. Yukarıda belirtildiği üzere makul dillerin sıralama farklılığı ile oluşturulduğu düşünülebilir. Buradaki dil kavramı insanlar tarafından konuşulan dil olarak algılanmamalıdır. Nasıl insanlar bildikleri bir dili anlıyor ise otomatalarda çeşitli dilleri anlayacak şekilde inşa edilir.

Şimdi az önce bahsettiğimiz girdiyi alan Şekil 1’de tasfir edilmiş otomatanın çalışma adımlarını verelim.

1. Otomata q_0 konumunda başlayacaktır.
2. Girdinin ilk elemanı 0 harfi olduğu için otomata q_0 konumundan q_1 konumuna okla belirtildiği gibi gidecektir.
3. Otomata artık q_1 konumundadır.
4. Girdinin sonraki elemanı 1 harfi olduğundan otomata q_1 konumundan q_0 konumuna gidecektir.
5. Otomata artık q_0 konumundadır.
6. Girdinin sonraki elemanı 0 harfi olduğundan otomata q_0 konumundan q_1 konumuna gidecektir.
7. Otomata artık q_1 konumundadır.
8. Girdinin sonraki elemanı 0 harfi olduğundan otomata q_1 konumundan q_2 konumuna gidecektir.
9. Otomata artık q_2 konumundadır.
10. Girdinin sonraki elemanı 1 harfi olduğundan otomata q_2 konumundan q_0 konumuna gidecektir.
11. Otomata artık q_0 konumundadır.
12. Girdinin bütün elemanları incelendiğinden ve otomata q_0 konumunda olduğundan otomatanın girdiye verdiği cevap q_0 olacaktır.

Otomataları ilkel bilgisayarlar olarak düşünebiliriz. Günümüzde bilgisayarları, bilgisayarın tasarım aşamasında tanımlanmış prosedürleri kullanarak farklı türden problemleri çözmek için kullanabilmekteyiz. Örneğin optimizasyon problemlerini çözmek ve incelemek bilgisayar programlarının en önemli görevlerindendir ve optimizasyon problemlerinin önemini kavramak sezgisel olarak kolaydır. Biz bu yazıda karar problemleriyle ilgileneceğiz. Okur herhangi bir karar problemini şu şekilde düşünebilir: verilen bir karar probleminin cevabı ya evettir ya da hayırdır. Tabii bu noktada belirtmeliyiz ki bu problemler objektif problemler yani bir cevabı olan problemler olmalıdır. Bir cevabının olmasından kastımız, problemin cevabının sorulan kişiye, yere, zamana veya sorudan başka bir şeye bağlı olmamasıdır. Örneğin, “Bal güzel midir?” sorusu bu bağlamda gerçek bir karar problemi değildir. Çünkü sorunun cevabı kişiye ya da bazı durumlara göre farklılık gösterebileceğinden kesin bir cevabı yoktur. Ama “2 sayısı 3 sayısından büyük müdür?” sorusu gerçek bir karar problemidir. Çünkü soruda verilen her şeyin net bir tanımı olduğu gibi sorunun net ve kesin bir cevabı da vardır. Karar problemleri birçok fenomeni ifade etmek için kullanılabilir ve karar problemlerinin çözümü başka birçok problemin de çözümünün bulunmasında da yardımcı olur. Örneğin verilen bir optimizasyon probleminin optimum değerine “Bu optimum değer herhangi bir x değerinden büyük mü?” gibi karar problemleriyle de yaklaşabiliriz.

Yukarıda bir problemin, karar problemi olarak kabul edilebilmesi için gerçek bir cevabının olması gerektiğini belirtmiştik. Şimdi biraz daha temel bir durumdan bahsedelim: Bir problemin var olması için önce o problemi yazılı olarak ifade edebilmemiz gerekir. Bir problemi yazılı olarak ifade etmek ise basitçe uygun bir alfabe, genelde binary alfabe $\{0, 1\}$, kullanarak ifade etmektir. Detaylar için okuyucular [1] kaynağını inceleyebilirler.

Şimdi otomatalara geri dönelim. Otomataya verdiğimiz girdiyi belirli bir karar probleminin yazılı hali, otomatanın verdiği cevabı ise otomatanın problem için bulduğu cevap olarak düşünebiliriz. Şekil 1’de görülebileceği gibi q_0 ve q_1 konumları tek çemberden oluşmaktayken q_2 konumu çift çemberden oluşmaktadır. Bunu şöyle düşünebiliriz; eğer otomata tek çemberden oluşan bir konumu cevap olarak veriyorsa soruya “Hayır” cevabını veriyor, çift çemberden oluşan bir konumu cevap olarak veriyorsa soruya “Evet” cevabını veriyordur. Bir otomata sonlu sayıda tek veya çift çemberli konumlardan oluşabilir. Buradaki önemli hususlardan biri, bir otomatanın her konumu için ve kabul ettiği alfabenin her harfi için gideceği yeni konumun tanımlanmış olmasıdır. Ayrıca kolayca anlaşılabilirliği gibi otomata farklı uzunlukta girdileri de kabul edebilmektedir. Kısacası vereceği cevap, girdinin uzunluğuna değil girdinin temsil ettiği karar problemine bağlı olmasıdır.

Aslında Şekil 1’de görselleştirdiğimiz otomata verilen bir doğal sayının 4 sayısı ile bölünüp bölünemeyeceğinin cevabını vermektedir. Girdi olarak da ilgili doğal sayının 2’lik tabandaki yazılımını kabul etmektedir. Bu örneği vermemizin en önemli sebebi okura otomataların basit ve anlaşılır bir şekilde karar problemlerini çözmek için nasıl kullanılabileceğini aktarmaktır.

Artık otomataların resmi ve matematiksel tanımını verebiliriz.

Tanım 1.

Bir $D = (Q, \Sigma, \delta, q_0, F)$ 5’lisi,

- Q : Konumlar kümesi,
- q_0 : Başlangıç konumu,
- Σ : Alfabe,
- $F \subseteq Q$: Evet cevaplı konumlar,
- $\delta: Q \times \Sigma \rightarrow Q$, geçiş fonksiyonu,

olmak üzere kararlı bir otomata olarak adlandırılır.

Bu tanımı daha iyi anlayabilmek için Şekil 1’i inceleyelim. Şekildeki otomatanın: Konumlar kümesi $Q = \{q_0, q_1, q_2\}$ kümesi, alfabesi $\Sigma = \{0, 1\}$ kümesi, başlangıç konumu q_0 , evet cevaplı konumları $F = \{q_2\}$ kümesidir. Geçiş fonksiyonu δ ise aşağıdaki tabloda belirtildiği biçimde tanımlıdır.

Anlık Konum \ Giren harf	0	1
q_0	q_1	q_0
q_1	q_2	q_0
q_2	q_2	q_0

Görüldüğü üzere evet ya da hayır cevabı veren konumların varlığı ve herhangi bir konumdan girdinin ilgili konumundaki alfabe elemanına göre hangi konuma gideceği kesin olarak belirlidir. Bu durum en basit otomatadan en karmaşık otomataya değişmeyen bir gerçektir.

Şimdi Şekil 1’deki otomatayı daha detaylı inceleyelim. Örneğin bu otomataya 1100 girdisini verirse, otomata, ilk konum başlangıç konumu q_0 olmak üzere sırasıyla: q_0, q_0, q_0, q_1, q_2 konumlarında bulunur ve sonuç olarak q_2 konumu bu girdiye verdiği cevap konumu olur. Veya otomataya 00 girdisini verirse, otomata ilk konum başlangıç konumu olmak üzere sırasıyla : q_0, q_1, q_2 konumlarında olur. Bu gözlemler ile hangi konumda olursa olsun iki ardışık 0 okunduğu anda yeni konum q_2 olacaktır. Kısacası okurların da kolayca fark edebileceği üzere bu otomata, son iki harfi 0 olan bütün girdilere “Evet” cevabını verir. Diğer taraftan hangi konumda olursa olsun herhangi bir konumda bulunan bu otomataya 01, 10 veya 11 girdi parçaları için q_2 dışındaki bir konumda bulunacaktır. Bir başka deyişle son iki harfi 0 olmayan tüm girdilere de “Evet” cevabını vermiyordu. 4’e bölünen bütün sayıların ikilik tabanda son iki hanesi 0 olduğunu biliyoruz. Dolayısıyla bu otomata 4’e bölünen sayıların 2’lik tabandaki yazılışlarına “Evet” cevabını veriyorken diğer durumlarda “Hayır” cevabını vermektedir. Yani bu basit otomata örneği bir sayının 4’e bölünüp bölünemeyeceğini belirleyebilmektedir.

Otomatlar günlük hayatta karşımıza çıkan bazı basit problemleri çözmek için kullanılmaktadır. Örneğin, kütüphanede su almak için kullandığımız otomat makineleri aslında birer otomatadır. Bilgisayarlar çalışma prensibi bakımından otomatalara göre biraz, ama çok fazla değil, daha karışık makinelerdir. Ama bu çalışma prensibini gerçek hayatta işe yarayan bir sisteme dönüştürmek kocaman bir endüstridir ve birçok farklı disiplini içinde barındırır. Biz bu yazımızda basit bir problemi matematiksel mekanizmalar kullanarak nasıl çözebileceğimizi otomatalar üzerinden anlattık. Bilgisayarlar aynı yolun ileri bir safhası olarak düşünülebilir.

■ Kaynaklar

- [1] Michael R. Garey and David S. Johnson. Computers And Intractability A Guide to Theory of NP-Completeness. W. H. Freeman and Company, 1979

Nizami İki Karma Metodunun Matematiksel İzahı

TALHA TİN

Hacettepe Üniversitesi Matematik Bölümü, 3. Sınıf Öğrencisi

✉ talhatin@gmail.com



1. Grup Kavramı

Bu yazıda bir iskambil destesi üzerine tanımlanacak karma metotları üzerinde durulacak, bu sebeple de simetri gruplarından bahsetmemiz gerekecek. Bir deste üzerinde tanımlanabilecek bir karma metodunun simetri grupları ile ilişkisini ilk bakışta göremeyecek, matematiksel olgunluğu yüksek olmayan okuyucular endişelenmesin. Ancak tanımları verilecek olan bu kavramların bizim ne işimize yarayacağı yazının ilerleyen kısımlarında anlam kazanacaktır.

Soyut Cebir derslerini almış okuyucular grup kavramını ilk kez duymuyordur. Ancak grup kavramı ile ne kastediyoruz biraz bundan bahsedelim. Bir G kümesi alalım. Bu küme boştan farklı olsun. Bu küme üzerine bir ikili işlem tanımlayalım. İkili işlem ile kastımız tam olarak aşağıdaki gibi bir fonksiyondur:

$$\begin{aligned} *: G \times G &\rightarrow G \\ (x, y) &\mapsto * (x, y) = x * y \end{aligned}$$

Yani G kümesinden aldığımız iki elemanı bir işleme tâbi tutuyoruz ve bu işlemin görüntüsü (başka bir deyişle sonucu) yine G kümesinde oluyor. Bir küme ve bir işlem ile bir grup yapısını inşa etmek için, bu yapının aşağıdaki özellikleri sağlamasını bekleriz.

1. $\forall a, b, c \in G$ için $(a * b) * c = a * (b * c)$ (Birleşme)
2. $\exists e \in G$ öyle ki $\forall a \in G$ için $e * a = a * e = a$ (Birim eleman)
3. $\forall a \in G, \exists a^{-1} \in G$ öyle ki $a * a^{-1} = a^{-1} * a = e$ (Ters eleman)

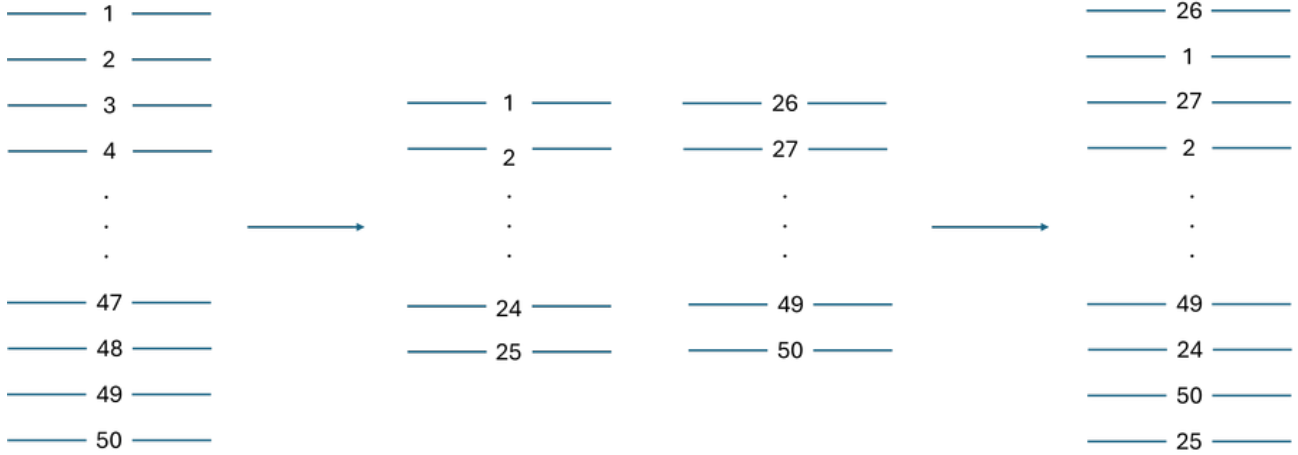
Oluşturduğumuz bu yapıyı ve sonuçlarını açıklamak ayrı bir yazının konusu. Biz simetri gruplarının gösteriminden faydalanacağımız için bu yapıyı yalnız bu açıdan ele almakla yetineceğiz. Ancak bir grubun ne olduğunu hiç duymamış okuyucular için de şu ana kadar bir sezi oluşturmayı umuyoruz.

Simetri grupları için çok formel bir tanım vermektense, kavramsal bir sezi hissettirmeye çalışacağız. Simetri kelimesinin günlük kullanımı ve etimolojisi üzerine düşündüğümüzde zaten mevzunun aşına olduğumuz simetrilerle ilgili olacağını kestirebiliriz. Yine de gruplar teorisinin mertebe kavramı ile simetri grubu elemanlarının dairesel temsilleri üzerinde ön bilgiye sahip olmak faydalı olacaktır.

2. Faro Karması

Faro ismi İspanya'da meşhur olan bir iskambil oyunundan gelir. Bu karma metodunun ilginç sonuçlar oluşturduğunu gören matematikçiler bu karma metodunu mükemmel karma olarak da isimlendirmiştir. Neden ilginç sonuçlar oluşturduğunu analiz etmeden önce karma metodunu tanımlayalım. $2n$ tane karta sahip bir deste alalım. Bu desteyi tam ortadan iki parçaya bölelim. Oluşan iki parçayı öylesine nizami karacağız ki, bir kart ilk parçadan bir kart ikinci parçadan gelecek. Bu durumda aslında bir değil iki karma metodu tanıttık; çünkü bir karmanın sonunda oluşacak destenin en altındaki kart, oluşturduğumuz parçaların herhangi birinden gelebilir. Biz *iç faro karması* olarak adlandırılan karma ile çalışacağız. Bu karma yönteminde, karma sonunda destenin en altında bulunan kart, ilk destenin üst yarısındaki parçasından

gelir. Bu karmayı her kartın konumunun değiştiği karma olarak da görebiliriz, çünkü dış faro karmasında ilk ve son kartın konumu hep aynı kalır. Her iki karma metodunun ilgi çekici sonuçları olsa da biz bu yazımız boyunca iç faro karması ile çalışacağız.



Şekil 1. 50 Kart İçin Faro Karması

Karma metodunu ve oluşturduğu grup yapısını (her ne demekse artık!) analiz etmek adına bir soru soralım: 50 kartlık bir desteye kaç kez faro karması uygularsak deste tekrar ilk konumuna ulaşır? Bu soruya cevap verebilmek adına destemizdeki kart sayısını küçülterek bir analiz yapalım. Sadece hesap yaparak çift sayıda karta sahip desteler için soruyu cevaplandırdığımızda; tablonun solunda destedeki kart sayısı, sağında ise ilk konuma dönmek için gereken faro karma sayısı olmak üzere şu tabloyu elde ederiz.

2	2
4	4
6	3
8	6
10	10
12	12
14	4
...	...
50	?

Cevabımıza ulaşmak adına bir fonksiyon tanımlayacağız. Bu fonksiyonun işlevi, bir faro karması sonucunda bir kartın kaçınıcı kart olduğunu bize söylemek olacak. Yani x 'inci kartın bu f fonksiyonu altındaki görüntüsü, yani $f(x)$ bir kez faro karmasına tabii tutulan destede x 'inci kartın kaçınıcı kart olduğu olacaktır. 50 kartlık bir deste için fonksiyonun tanım kümesindeki tüm elemanların (yani 1'den 50'ye kadar olan tüm sayıların) görüntülerine bakalım.

$1 \mapsto 2$	$26 \mapsto 1$
$2 \mapsto 4$	$27 \mapsto 3$
$3 \mapsto 6$	$28 \mapsto 5$
$\vdots$	$\vdots$
$24 \mapsto 48$	$49 \mapsto 47$
$25 \mapsto 50$	$50 \mapsto 49$

50 elemanlı bir kümeden 50 elemanlı bir kümeye, bize bu görüntüleri verecek bir fonksiyon tanımlamak istiyoruz. Bu kısımda yeterli olgunluğa sahip okuyucu simetri gruplarının neden işimize yarayacağını sezmış olacaktır.

İlk 25 kart için fonksiyon kuralını yazmak kolay, $f_{50}(x) = 2x$ fonksiyonu ilk 25 kart için işimizi görecektir. Ancak 26'ncı karttan 50'nci karta kadar fonksiyon kuralını yazmak bu kadar kolay değil. Yine de her bir kartın görüntüsünü analiz ettiğimizde destenin altındaki kısım için de $f_{50}(x) = 2(x - 26) + 1$

olduğunu görebiliriz. O halde bu fonksiyonu bir parçalı fonksiyon olarak şu şekilde ifade edebiliriz:

$$f_{50}(x) = \begin{cases} 2x & ; x \leq 25 \\ 2x - 51 & ; x > 25 \end{cases}$$

Simetri gruplarının gösterimi sayesinde bu fonksiyon kuralı aşağıdaki biçimde yazılabilir:

$$\begin{aligned} & (1\ 2\ 4\ 8\ 16\ 32\ 13\ 26)(3\ 6\ 12\ 24\ 48\ 45\ 39\ 27) \\ & (5\ 10\ 20\ 40\ 29\ 7\ 14\ 28)(11\ 22\ 44\ 37\ 23\ 46\ 41\ 31) \\ & (9\ 18\ 36\ 21\ 42\ 33\ 15\ 30)(17\ 34)(19\ 38\ 25\ 50\ 49\ 47\ 43\ 35) \end{aligned}$$

Burada, her parantezde bir çevrimsel atamalar dizisi tarif edilir; örneğin ilk parantez bize f_{50} fonksiyonunun

$$1 \mapsto 2 \mapsto 4 \mapsto 8 \mapsto 16 \mapsto 32 \mapsto 13 \mapsto 26 \mapsto 1$$

şeklinde atamalar yaptığını söyler. Takip eden diğer parantezlerle birlikte değerlendirildiğinde f_{50} fonksiyonunun nasıl çalıştığı tam olarak belirli olur.

Simetri Gruplarında Mertebe Hesaplama

Sorumuzu artık

“Bir deste, belirli bir karma yönteminin art arda uygulanması ile ne zaman ilk konumuna döner?”

şeklinde netleştirebiliriz. Dikkat edilirse f_{50} fonksiyonu, 7 döngünün bileşkesi tarafından oluşuyor. Tüm fonksiyonun mertebesini bulabilmek için, onu oluşturan döngülerin mertebelerini (yani ne zaman başlangıç konumuna döneceklerini) hesaplayalım. İlk olarak

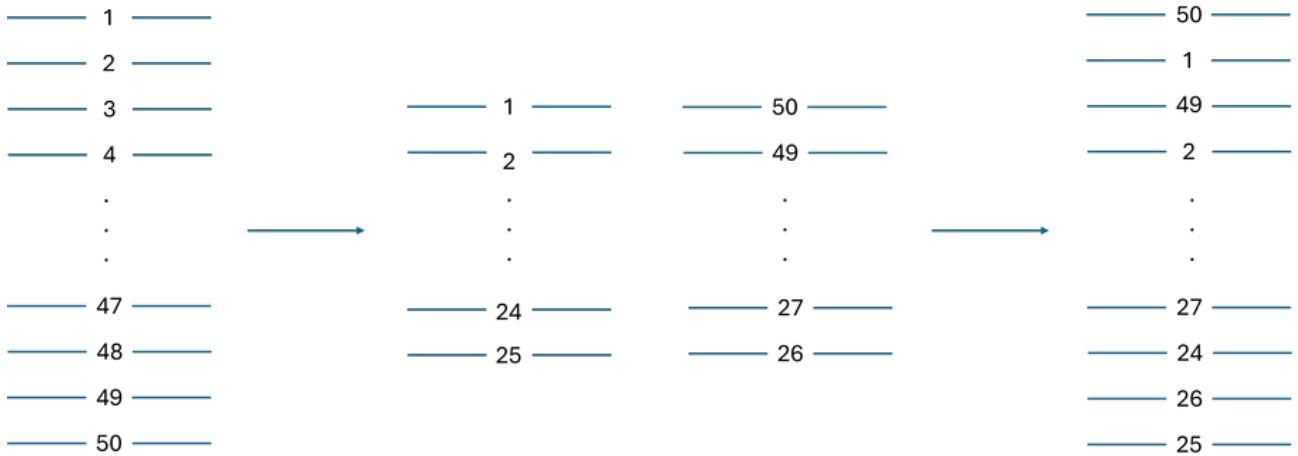
$$(1\ 2\ 4\ 8\ 16\ 32\ 13\ 26)$$

döngüsü ile başlayalım. 8 elemanı olan bu döngünün mertebesini hesaplarken, bir sekizgenin dönme simetrilerini incelemek bu döngünün ilk konumuna ne zaman ulaşacağını görmemizi sağlayacaktır. Bir sekizgeni sekiz kez döndürdüğümüzde ($\pi/4$ radyanlık dönmelerden bahsediyoruz) sekizgen tekrar ilk konumuna gelecektir. O halde bu döngünün mertebesi 8'dir. 8 elemanı olan diğer döngüler için de aynı hesap yapılacaktır. 2 elemanı olan döngü için bu hesabı yaptığımızda sonuç 2 çıkacaktır. Çünkü bir doğruyu iki kez π radyan döndürdüğümüzde ilk konumuna ulaşacaktır. Bir desteye faro karmasını bir kez uyguladığımızda bu döngülerin her birini birer kez uygulamış oluruz. O halde bir desteye iki kez faro karması uyguladığımızda 2 elemanı olan döngü ilk konumuna dönmüş olsa da (yani 17. ve 34. kartlar tekrar 17. ve 34. kartlar olur) diğer altı döngüden hiçbirisi ilk konumuna ulaşmış değildir. Ancak faro karmasını sekiz kez uyguladığımızda, mertebesi sekiz olan altı döngü başlangıç konumuna dönmüş olur. Bu sırada mertebesi iki olan döngü ise 4 kez ilk konumuna dönmüş olur. Daha sezgisel açıklanmaya çalışılsa da aslında f_{50} fonksiyonunun mertebesi, bu yedi döngünün mertebelerinin en küçük ortak katına eşittir.

Soruyu iskambil destelerinden aşına olduğumuz 52 kartlık desteler için sormamamızın sebebi, 52 kartlık destenin tek bir döngü vereceğidir. Yani destemiz 52 tane karta sahipse, ona 52 kez faro karması uygulamamız gerekecektir. Bizi daha ilginç bir sonuca ulaştırdığını düşündüğümüzden 50 kartlık bir deste için cevap aradık.

3. Tersyüz Karması

Çift sayıda karta sahip bir deste üzerine tanımlanabilecek yeni bir karma metodu tanıtalım. Bu karma metodunda, faro karmasında olduğu gibi deste tam ortadan ikiye bölünür ve oluşan parçalardan kart numaraları büyük olan parça (ilk destenin altındaki parça) ters çevrilir. Ardından aşına olduğumuz faro karması uygulanır. Bu karma metodu *flip shuffle* olarak adlandırılır ve tersyüz karması adıyla Türkçeleştirilebilir.



Şekil 2. 50 Kart İçin Tersyüz Karması

Önceki karma metodu için yaptığımız analizi, tersyüz karması için de yapacağız. 50 kartlık bir destede her bir kartın bir tersyüz karması sonucunda kaçınıcı kart olduğunu şu şekilde inceleyebiliriz:

$$\begin{array}{ll} 1 \mapsto 2 & 26 \mapsto 49 \\ 2 \mapsto 4 & 27 \mapsto 47 \\ 3 \mapsto 6 & 28 \mapsto 45 \\ \vdots & \vdots \\ 24 \mapsto 48 & 49 \mapsto 3 \\ 25 \mapsto 50 & 50 \mapsto 1 \end{array}$$

Tersyüz karması için de fonksiyon kuralını öncekine benzer bir mantıkla yazabiliriz. Bu fonksiyon 50 kartlık bir destede x 'inci kartın bir karma sonrası kaçınıcı kart olduğunu veren fonksiyondur.

$$g_{50}(x) = \begin{cases} 2x & ; x \leq 25 \\ 101 - 2x & ; x > 25 \end{cases}$$

Az önce faro karması için cevapladığımız soruyu, yani 50 kartlık bir deste kaç karma sonunda ilk konumuna döner sorusunu tersyüz karması için de soralım. Ancak burada sorunun cevabını bulmak amacıyla, faro karması için yaptığımız gibi yazdığımız fonksiyonu kullanmak yerine; faro karmasının ve tersyüz karmasının oluşturduğu grup yapıları arasında bire-bir bir eşleme bulalım.

4. Faro Karmasının ve Tersyüz Karmasının Karşılaştırılması

Teorem 1.

Faro karmasını $4n$ tane karta sahip bir desteye uyguladığımızda oluşan grup yapısı ile tersyüz karmasını $2n$ tane karta sahip bir desteye uyguladığımızda oluşan grup yapısı aynı olur.

Kanıt. Öncelikle, $4n$ kartlık bir deste ile $2n$ kartlık bir deste arasında bire bir bir dönüşüm tanımlayacağız. $4n$ kartlık destenin ilk $2n$ kartını alalım; bu, bizim bire bir dönüşümümüz olacak. Yani $4n$ karta sahip destenin ilk $2n$ kartı ile $2n$ karta sahip destenin tamamı arasında bir eşleme olduğunu göstereceğiz. Ayrıca, bu dönüşümün tersi, $2n$ kartlık bir desteyi kopyalayıp, oluşan iki desteden birini ters çevirerek birleştirip $4n$ kartlık desteyi elde etmek şeklinde düşünülebilir. Bu dönüşümü $4n = 20$ kart için görselleştirelim.

Aşağıdaki şemada üzeri çizgili olan numaralar, çevrilmiş kartları simgelemektedir.

$$\begin{array}{cccccccccccc}
 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \overline{10} & \overline{9} & \overline{8} & \overline{7} & \overline{6} & \overline{5} & \overline{4} & \overline{3} & \overline{2} & \overline{1} & \longleftrightarrow & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
 \overline{10} & \overline{1} & \overline{9} & \overline{2} & \overline{8} & \overline{3} & \overline{7} & \overline{4} & \overline{6} & \overline{5} & \overline{5} & \overline{6} & \overline{4} & \overline{7} & \overline{3} & \overline{8} & \overline{2} & \overline{9} & \overline{1} & \overline{10} & \longleftrightarrow & \overline{10} & \overline{1} & \overline{9} & \overline{2} & \overline{8} & \overline{3} & \overline{7} & \overline{4} & \overline{6} & \overline{5} \\
 \overline{5} & \overline{10} & \overline{6} & \overline{1} & \overline{4} & \overline{9} & \overline{7} & \overline{2} & \overline{3} & \overline{8} & \overline{8} & \overline{3} & \overline{2} & \overline{7} & \overline{9} & \overline{4} & \overline{1} & \overline{6} & \overline{10} & \overline{5} & \longleftrightarrow & \overline{5} & \overline{10} & \overline{6} & \overline{1} & \overline{4} & \overline{9} & \overline{7} & \overline{2} & \overline{3} & \overline{8} \\
 8 & \overline{5} & \overline{3} & \overline{10} & \overline{2} & \overline{6} & \overline{7} & \overline{1} & \overline{9} & \overline{4} & \overline{4} & \overline{9} & \overline{1} & \overline{7} & \overline{6} & \overline{2} & \overline{10} & \overline{3} & \overline{5} & \overline{8} & \longleftrightarrow & 8 & \overline{5} & \overline{3} & \overline{10} & \overline{2} & \overline{6} & \overline{7} & \overline{1} & \overline{9} & \overline{4}
 \end{array}$$

Bu dönüşüm değişmelidir. Yani önce $4n$ karta faro karması uygulayıp dönüşümü uygulamakla, dönüşümü uygulayıp $2n$ karta tersyüz karması uygulamak aynıdır.

Genel olarak gözlemleyebiliriz ki, $4n$ karta sahip bir desteyi alıp ortadan ikiye böldüğümüzde, destenin altta kalan kısmı üstteki destenin ters çevrilmiş haline karşılık gelir. $\square$

Bu teorem sayesinde $4n$ tane karta sahip bir desteye faro karması uygulamakla $2n$ tane karta sahip bir desteye tersyüz karması uygulamak arasında matematiksel bir fark olmadığını, yani destenin ilk konumuna ne zaman döneceğini iki karma metodu ile de aynı yöntemle hesaplayabileceğimizi gördük.

■ Teşekkür

Bu çalışmanın ortaya çıkmasında katkı sağlayan ve fikir aşamasından yazım sürecine kadar her adımda değerli geri bildirimleriyle katkı sunan Prof. Dr. Bülent Saraç'a minnettarım.

■ Kaynaklar

- [1] Butler, S., Diaconis, P., & Graham, R. (2016). *The mathematics of the flip and horseshoe shuffles*. The American Mathematical Monthly, **123**(6), 542–556.
- [2] Demaine, E. D., & Demaine, M. L. (2018). *Juggling and card shuffling meet mathematical fonts*. Connections in Discrete Mathematics: A Celebration of the Work of Ron Graham, 297.
- [3] Diaconis, P., Graham, R. L., & Kantor, W. M. (1983). *The mathematics of perfect shuffles*. Advances in Applied Mathematics, **4**(2), 175–196.

Esnek Çokgenler (Fleksagonlar) ve Biraz Sihir

CANSU BETİN ONUR¹, ELİF MEDETOĞULLARI²

¹Başkent Üniversitesi Bilgisayar Mühendisliği Bölümü

²TED Üniversitesi Matematik ve Fen Bilimleri Eğitimi Bölümü
Matematik Eğitimi Ana Bilim Dalı

✉ cbetinonur@baskent.edu.tr, elif.medetogullari@tedu.edu.tr



■ Fleksagonların Keşfi: Tesadüften Matematiksel Büyüye

1939 yılında, Princeton Üniversitesi'nde yüksek lisans öğrencisi olan Arthur H. Stone, Amerikan standardında üretilmiş bir defteri İngiliz yapımı bir dosyaya yerleştirmekte zorlanınca, defterin kenarlarından taşan bölümleri şeritler halinde kesmek zorunda kaldı. Bu artan kağıt parçaları, Stone'un ellerinde sıradan bir atık olmaktan çıkıp yaratıcı bir yapıya dönüştü. Kağıt şeritlerini katlamaya başlayan Stone, katladığı şekillerden birinin beklenmedik biçimde döndürülebilir —yani yüzeyleri çevrilerek farklı yüzlerin ortaya çıkarılabilir— olduğunu fark etti. Bu yapıların her bir yüzü düzgün çokgenlerden oluşuyordu ve dinamik olarak yeniden şekillendirilebilmeleri, onları hem görsel olarak etkileyici hem de matematiksel olarak son derece ilginç kılıyordu.

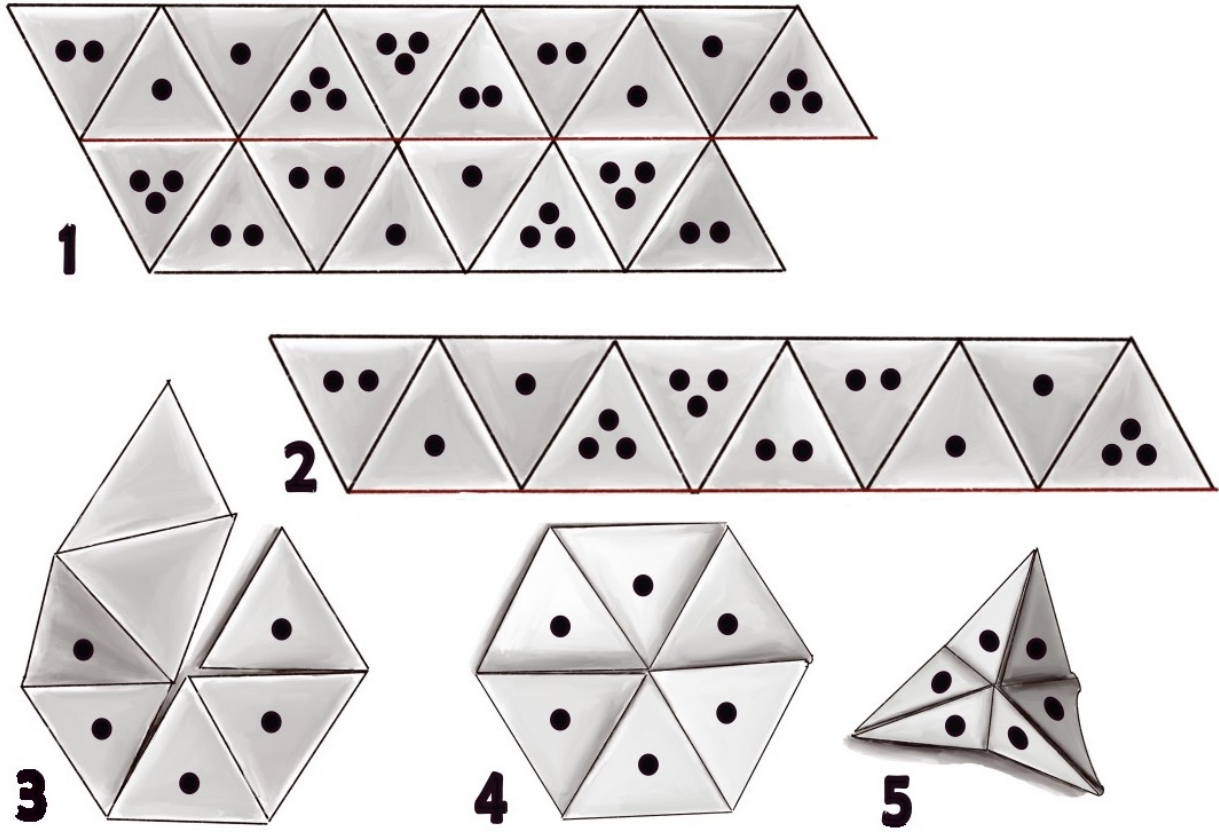
Stone'un bu keşfi kısa sürede dikkat çekti. Princeton Matematik Kulübü'ndeki arkadaşları arasında yer alan genç Richard P. Feynman —ki ileride kuantum elektrodinamiği konusundaki çalışmalarıyla Nobel Fizik Ödülü'ne layık görülecektir— bu yeni yapıların cazibesine kapılan ilk kişilerden biri oldu. Kulüpteki bir diğer isim olan Bryant Tuckerman ise fleksagonların sistematik olarak modellenmesini sağlayan matematiksel araçları geliştirdi. Bugün *Tuckerman diyagramları* olarak bilinen bu gösterimler, fleksagonların katlama ve çevirme dizilerini analiz etmek için hâlâ kullanılmaktadır.

"Fleksagon" terimi, bu yapıların esnekliğini (flexibility) ve çokgenliğini (polygon) yansıtan bir bileşik kelime olarak türetilmiştir. Biz de bu nedenle bu yapılara esnek çokgen diyeceğiz. Önce yüz sayısı, sonra kaç gen olduğu söylenerek isimlendirilirler. İlk geliştirilen örnekler genellikle altıgen şeklindeki *heksafleksagonlar* idi. Bunları zamanla farklı geometrik ve yapısal özelliklere sahip diğer türler izledi. Örneğin: **Triheksafleksagon**: Üç görünür yüzü olan en basit heksafleksagon türüdür.

Esnek çokgenler, 1950'li yıllarda Martin Gardner'ın Scientific American dergisinde yayımlanan yazılarıyla geniş kitlelere ulaştı. Gardner'ın 1956 tarihli "Flexagons" başlıklı makalesi, bu yapıların yalnızca eğlenceli oyuncaklar değil, aynı zamanda topoloji, kombinatorik ve simetri teorileriyle yakından ilişkili matematiksel nesneler olduğunu vurguladı. Bu yazıyla birlikte esnek çokgenler hem matematiksel araştırmaların hem de eğitim materyallerinin konusu haline geldi.

Bugün esnek çokgenler, matematiğin görsel ve deneysel doğasını ön plana çıkaran güçlü araçlar olarak kabul edilir. Katlamalı yüzeylerin topolojik ve kombinatorik yapıları üzerine çalışan araştırmacılar için ilham verici bir model sunarken; sınıf ortamlarında simetri, grup teorisi ve dönüşüm kavramlarını öğretmek için de etkili bir materyaldir.

Hadi hep beraber esnek çokgenler katlayalım.



Şekil 1

Esnek Altıgen (Heksafleksagon): Arthur'un keşfi olan ilk fleksagonu yapacağız. Şekil 1'de bulunan 1. resimdeki gibi, üzerinde 3 farklı desen olan toplam 18 eşkenar üçgen yer alan bir kağıt şerit oluşturalım. Sonra ortadan katlayarak yapıştıralım ve 2. resmi elde edelim. 2. resimdeyken, tüm üçgenlerin kenarlarını her iki yöne de katlayarak kat izi yapalım. Bu daha sonra esnek altıgenimizin kullanımını kolaylaştıracaktır. Şimdi üçgenleri, tümünde aynı desen aynı yöne bakacak şekilde katlayalım ve 3. resmi elde edelim (tek noktalı üçgenler bir yüzde bir araya getirilmiştir, siz isterseniz iki noktalı ya da üç noktalı üçgenleri de bir araya getirebilirsiniz). İki boş üçgen açıkta kalıyor. Bunları üst üste getirip yapıştıralım ve 4. resmi elde edelim. Esnek altıgenimiz tamamlandı. 5. resimdeki gibi parmaklarınızla içeri doğru iterek ve belki tepesinden yaprakları ayırmayı deneyerek diğer yüzlerini keşfetmeye hazırsınız? Sahi neden trihexaflexagon diyorduk buna?

İkinci esnek çokgenimiz, zaten büyüğü olan bu matematiksel oyuncuğa bir de sihir katıyor. Önce kısaca meşhur sihirli karelerden bahsedelim.

■ Sihirli Kareler

Kenar uzunluğu n olan bir karenin içine 1'den n 'ye kadar n^2 doğal sayı yerleştirelim. Eğer karenin içindeki her satırın, her sütunun ve her köşegenin toplamı aynı sayı ise bu kareye **sihirli kare** denir.

8	1	6
3	5	7
4	9	2

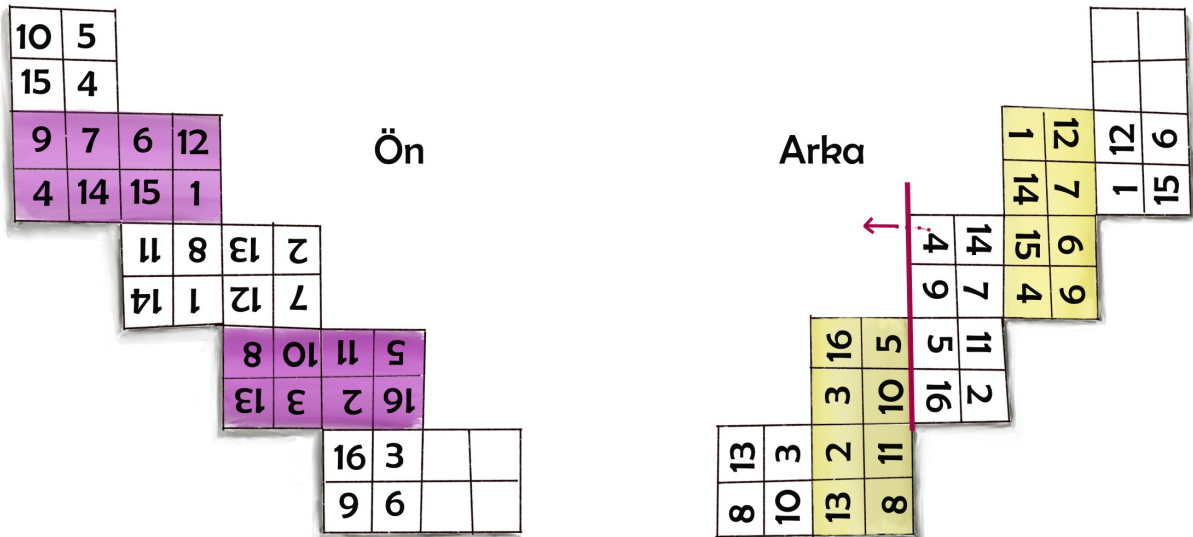
Şekil 2

Şekil 2'deki karenin herhangi bir satırını toplayın. Kaç buldunuz? Peki şimdi de sütunları deneyin. Hep 15 mi buluyorsunuz? Gelin bir de köşegenlerdeki sayıları deneyelim. $8 + 5 + 2 = 15$ ve $6 + 5 + 4 = 15$. Bunlar da 15 çıktı. Sihir gibi değil mi? İşte bu özelliğe sahip karelere sihirli kareler diyoruz. Sihirli karelerin binlerce yıllık bir geçmişi var.



Şekil 3. Rönesans dönemi ünlü Alman ressam Albrecht Dürer'in Melankoli 1 isimli resminde sağ üst köşede gizemli bir sihirli kare görünmekte. Burada yapacaklarımızdan biri belki de.

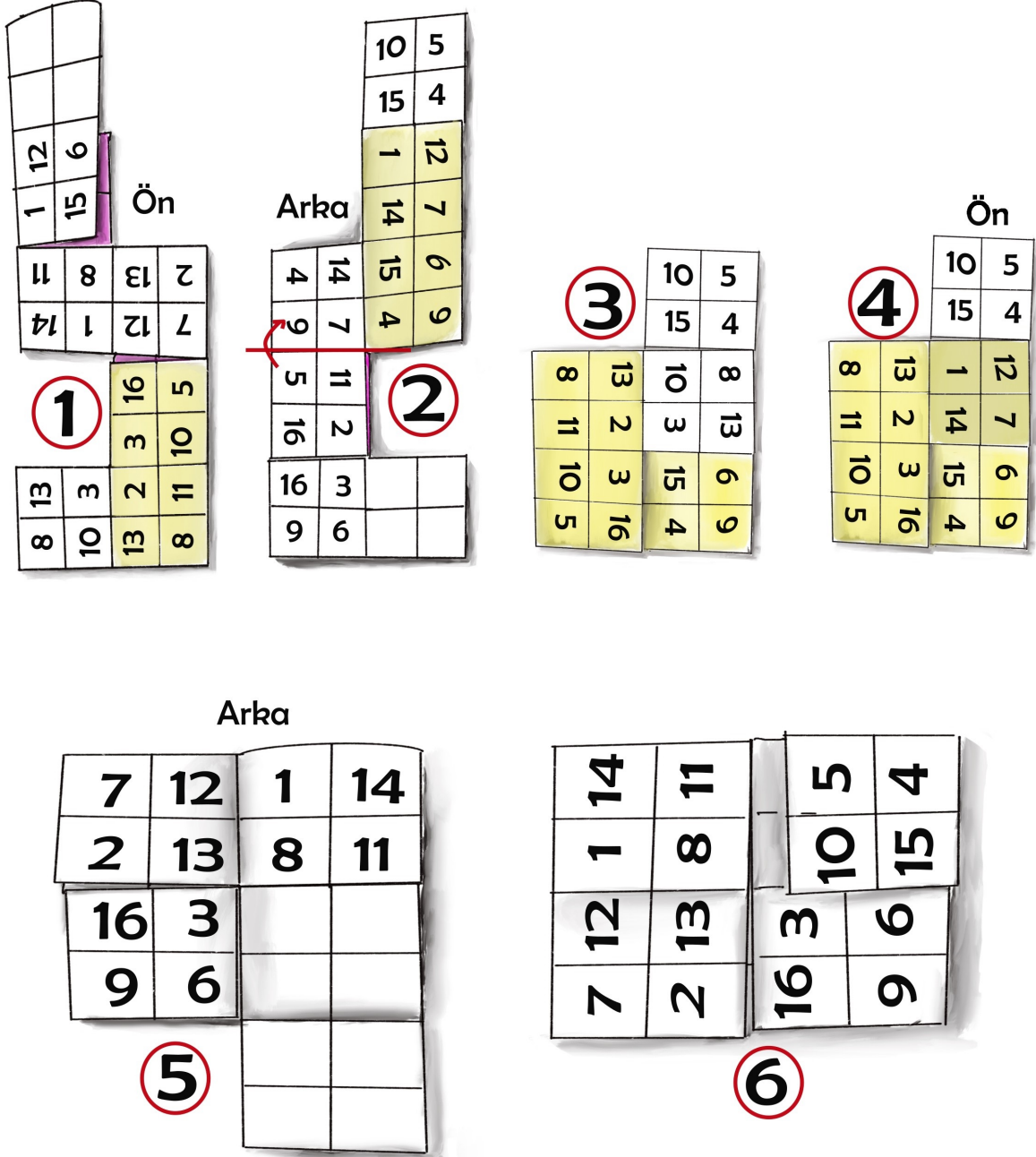
Hadi her yüzü açıldıkça sihir ortaya çıkan bir esnek çokgen yapalım.



Şekil 4

Bir kâğıt, renkli kalemler ve bir cetvel alıp Şekil 4'te "ön" yazan resimdeki gibi küçük karelere bölelim ve mümkünse belirtilen bölgeleri farklı renklerle boyayalım. Arka yüzünü çevirelim ve Şekil 4'te arka

ile belirtilen resimdeki gibi rakamları yerleştirelim ve yine belirtilen yerleri ön kısımdakinden farklı bir renk ile boyayalım. Son olarak Şekil 4'teki arka ile belirttiğimiz resimdeki gibi şeridimizi işaretli yerden arkadan saat yönünde pembe kareler üst üste gelecek şekilde katlayalım. Şekil 5'teki 1. resmi elde etmemiz gerekiyor.



Şekil 5

Şekil 5'teki 1. resmin arka yüzünü çevirelim, Şekil 5'teki 2. resmi elde edelim. Kâğıdın alt kısmını kırmızı ile işaretli çizgiden saat yönünde üç sarı kare ön yüzde buluşacak şekilde katlayalım ve Şekil 5'teki 3. resmi elde edelim. Altta kalan sarı kareleri de üst yüzeye çıkaralım ve 16 sarı kare de bize bakıyor olsun, böylece Şekil 5'teki 4. resmi elde edelim. 4. resmin arka yüzünü çevirelim ve 5. resmi elde edelim. Burada iki boş dörtlü küçük kare parçası göreceksiniz, onları yapıştıralım ve 6. resmi elde edelim (5. resmin saat yönünün tersi yönde 90 derece döndürülmüş hali resmedilmiştir.).

1'den 16'ya kadar sayıların yerleştirildiği bir sihirli kare görüyorsunuz.

Sorular: Ama her şey bu kadar mı sizce? Bu esnek çokgenin içinde başka sihirli kareler gizli olabilir mi? Kaç tane dersiniz? Buna göre bu esnek çokgenin adı ne olmalı? Sadece 4 kareden oluşan yani 1'den 4'e kadar rakamların yazıldığı ve altı farklı sihirli kare içeren bir sihirli esnek çokgen katlayabilir misiniz?

■ Kaynaklar

- [1] Martin Gardner, Hexaflexagons and other mathematical diversions, The University of Chicago Press, 1988.
- [2] <http://www.flexagon.net/index.php/magic-flexagons>
- [3] <http://mathworld.wolfram.com/MagicSquare.html>

Kategori Teorisi: Temel Kavramlar, Tarihsel Gelişim ve Matematiksel Düşünceye Katkısı

SULTAN EYLEM TOKSOY

Hacettepe Üniversitesi Matematik Bölümü

✉ eylemtoksoy@hacettepe.edu.tr



Bilimsel teorilerin temel işlevlerinden biri, geçmiş deneyimleri sistematik olarak organize ederek, bir sonraki kuşağın bu bilgi birikimini daha az zahmetle içselleştirmesini sağlamaktır. Bu, bilimsel etkinliğin sürdürülebilir ve kümülatif şekilde ilerleyebilmesi için gereklidir. Matematiksel düşüncede bu ihtiyaca cevap veren araçlardan biri de kategori teorisidir. Kategori teorisi bazı ünlü matematikçiler tarafından "benzetme bilimi" olarak tanımlanan matematik bilimindeki benzetmeleri sistemli biçimde ele alan disiplinler arası bir dildir. Bu dil, farklı matematiksel yapılardaki ortak özellikleri ortaya çıkararak düşünceyi derinleştiren bir soyutlama sunar. Matematiksel nesnelerle bu nesneler arasındaki dönüşümleri (morfizmaları) sistematik biçimde ele alır.

Tarihsel olarak kategori teorisine dair ilk fikirler Samuel Eilenberg ve Saunders MacLane tarafından 1942 yılında grup teorisi üzerine yazdıkları bir makalede ([2]) ortaya konmuş, ancak kavramlar tam anlamıyla bu yazarların 1945 tarihli çalışmalarında ([3]) tanıtılmıştır. Bu makalede fonktörler, doğal dönüşümler ve kategoriler kavramsallaştırılmış; kategori teorisinin cebirsel topolojiye uygulamaları ilk kez tartışılmıştır. Bu gelişme, sezgisel ve geometrik homolojiden, homolojik cebire geçişin kritik bir adımı olmuştur. Yazarlar, amaçlarının doğal dönüşümleri anlamak olduğunu belirtmiş ve bunun önce fonktörlerin ardından da kategorilerin tanımlanmasını gerektirdiğini ifade etmişlerdir. Bu çalışmalar, Emmy Noether'in soyut yapıların anlaşılması için süreçleri (özellikle homomorfizmaları) analiz etme yaklaşımının bir devamı niteliğindedir. Eilenberg ve MacLane'in çalışması, topolojik yapıların cebirsel yapılar aracılığıyla analiz edilmesini amaçlamış ve bu hedefle kategorik dili geliştirmiştir.

Bu yazıda yukarıda bahsi geçen kategori, fonktör ve doğal dönüşüm kavramları tanımlanacak ve bazı temel örnekler verilecektir. Daha ayrıntılı bilgi edinmek isteyen okurlara [4], [5] nolu kaynaklar önerilebilir. Öncelikle kategori teorisi kitaplarının çoğunda bulunan, küme-teorik bir arka plana ve dile sahip olan kategori tanımını verelim:

Tanım 1.

Bir $\mathcal{C}$ kategorisi

1. $Ob(\mathcal{C})$ ile göstereceğimiz nesneler sınıfından;
2. Her sıralı (A, B) nesneler çifti için $Mor_{\mathcal{C}}(A, B)$ ile göstereceğimiz ve farklı (A, B) ve (C, D) çiftleri için $Mor_{\mathcal{C}}(A, B) \cap Mor_{\mathcal{C}}(C, D) = \emptyset$ olacak şekildeki morfizmalar kümesinden;
3. $f \in Mor_{\mathcal{C}}(A, B), g \in Mor_{\mathcal{C}}(B, C)$ olmak üzere her (g, f) çiftine bunların bileşkesi denilen $g \circ f \in Mor_{\mathcal{C}}(A, C)$ morfizmasını karşı getiren $Mor_{\mathcal{C}}(B, C) \times Mor_{\mathcal{C}}(A, B) \longrightarrow Mor_{\mathcal{C}}(A, C)$ fonksiyonlarından oluşur; öyle ki
 - (a) Her A, B, C, D nesneleri ve $f \in Mor_{\mathcal{C}}(A, B), g \in Mor_{\mathcal{C}}(B, C), h \in Mor_{\mathcal{C}}(C, D)$ morfizmaları için birleşme kuralı yani $h \circ (g \circ f) = (h \circ g) \circ f$ eşitliği sağlanır.
 - (b) Her $A \in Ob(\mathcal{C})$ nesnesinin, her $f \in Mor_{\mathcal{C}}(A, B), g \in Mor_{\mathcal{C}}(B, A)$ için $f \circ 1_A = f, 1_A \circ g = g$ eşitliklerini gerçekleyen bir $1_A \in Mor_{\mathcal{C}}(A, A)$ birim morfizması vardır.

Örnek 1.1. **Set:** Kümeler kategorisi

- (a) **Nesneler:** Bütün kümeler.
- (b) **Morfizmalar:** Kümeler arasındaki bütün fonksiyonlar. Morfizmaların bileşkesi fonksiyonların alışılmış bileşkesidir.

2. **Vect_F:** Bir F cismi üzerindeki vektör uzayları kategorisi

- (a) **Nesneler:** Bir F cismi üzerindeki tüm vektör uzaylar.
- (b) **Morfizmalar:** F cismi üzerindeki vektör uzaylar arasındaki doğrusal dönüşümler. Morfizmaların bileşkesi doğrusal dönüşümlerin bileşkesidir.

3. **Grp:** Gruplar kategorisi

- (a) **Nesneler:** Bütün gruplar.
- (b) **Morfizmalar:** Bütün grup homomorfizmaları. Morfizmaların bileşkesi grup homomorfizmalarının alışılmış bileşkesidir.

4. **Ab:** Abel gruplar kategorisi

- (a) **Nesneler:** Abel gruplar.
- (b) **Morfizmalar:** Abel grup homomorfizmaları. $\text{Mor}_{\text{Ab}}(A, B) = \text{Hom}(A, B)$ ile gösterilir. Morfizmaların bileşkesi grup homomorfizmalarının alışılmış bileşkesidir.

5. **Top:** Topolojik uzaylar kategorisi

- (a) **Nesneler:** Bütün topolojik uzaylar.
- (b) **Morfizmalar:** Sürekli Fonksiyonlar. Morfizmaların bileşkesi fonksiyonların alışılmış bileşkesidir.

6. **hoTop:**

- (a) **Nesneler:** Bütün topolojik uzaylar.
- (b) **Morfizmalar:** Homotopik fonksiyonların denklik sınıfları. Morfizmaların bileşkesi fonksiyonların alışılmış bileşkesidir. Bu kategori cebirsel topolojinin merkezinde yer alır ve morfizmaların yapıyı koruyan fonksiyonlar olmadığı bir kategori örneğidir.

7. **Ring:** Halkalar kategorisi

- (a) **Nesneler:** Bütün birimli halkalar ($1 \neq 0$).
- (b) **Morfizmalar:** Birimi koruyan halka homomorfizmaları. Morfizmaların bileşkesi halka homomorfizmalarının alışılmış bileşkesidir.

8. **R-Mod:** Sol R -modüller kategorisi

- (a) **Nesneler:** R birimli bir halka olmak üzere tüm sol R -modüller.
- (b) **Morfizmalar:** Modül homomorfizmaları. $\text{Mor}_{R\text{-Mod}}(A, B) = \text{Hom}_R(A, B)$ ile gösterilir. Morfizmaların bileşkesi modül homomorfizmalarının alışılmış bileşkesidir.

9. **Farklı bir $\mathcal{C}$ kategorisi:**

- (a) **Nesneler:** Tüm pozitif tam sayılar.
- (b) **Morfizmalar:** İki $n, m \in \mathbb{Z}^+$ için $\text{Mor}_{\mathcal{C}}(m, n)$ kümesi n sayısı m ile bölünmediğinde boş küme, bölündüğünde ise tek bir $f_{m,n}$ elemanından oluşsun.

$\mathcal{C}$ bir kategoridir: Öncelikle morfizmaların bileşkesini tanımlayalım. $m, n, k \in \mathbb{Z}^+$ olmak üzere $f_{m,n} \in \text{Mor}_{\mathcal{C}}(m, n)$ ve $f_{n,k} \in \text{Mor}_{\mathcal{C}}(n, k)$ olsun. $f_{m,n} \in \text{Mor}_{\mathcal{C}}(m, n)$ olduğundan $m|n$ ve $f_{n,k} \in \text{Mor}_{\mathcal{C}}(n, k)$ olduğundan $n|k$ olup dolayısıyla $m|k$ olur. Yani bir $f_{m,k} \in \text{Mor}_{\mathcal{C}}(m, k)$ morfizması vardır. Bu morfizmayı $f_{m,n}$ ve $f_{n,k}$ morfizmalarının bileşkesi olarak alalım. Yani $f_{n,k} \circ f_{m,n} = f_{m,k}$. Her $n \in \mathbb{N}$ için $n|n$ olduğundan $f_{n,n}$ morfizması vardır ve $n|k$ durumunda $\text{Mor}_{\mathcal{C}}(n, k)$ 'da tek bir $f_{n,k}$ morfizması var olduğundan $f_{n,k} \circ f_{n,n} = f_{n,k}$ elde edilir. Benzer şekilde $m|n$ durumunda $\text{Mor}_{\mathcal{C}}(m, n)$ 'de tek bir $f_{m,n}$ morfizması var olduğundan $f_{n,n} \circ f_{m,n} = f_{m,n}$ elde edilir. O halde n nesnesinin birim morfizması olarak $1_n = f_{n,n}$ alınabilir. Ayrıca her m, n, k, l nesneleri ve $f_{m,n} \in \text{Mor}_{\mathcal{C}}(m, n)$, $g_{n,k} \in \text{Mor}_{\mathcal{C}}(n, k)$, $h_{k,l} \in \text{Mor}_{\mathcal{C}}(k, l)$ morfizmaları için birleşme kuralı sağlanır. Yani $h_{k,l} \circ (g_{n,k} \circ f_{m,n}) = (h_{k,l} \circ g_{n,k}) \circ f_{m,n}$ eşitliği sağlanır ([1]).

Örneklere bakıldığında bir kategorinin, nesneleriyle değil, morfizmalarıyla karakterize edildiğine dikkat edilmelidir. Örneğin $\mathcal{T}\text{op}$ kategorisinin kategorik özellikleri ile $ho\mathcal{T}\text{op}$ kategorisinin kategorik özellikleri birbirinden farklıdır. Bir $\mathcal{C}$ kategorisinde bir $f : A \longrightarrow B$ morfizması için $g \circ f = 1_A$ ve $f \circ g = 1_B$ olacak şekilde bir $g : B \longrightarrow A$ morfizması bulunursa f 'ye izomorfizma denir. Örneğin Set kategorisinde izomorfizmalar birebir örten fonksiyonlar, $\mathcal{A}b$ kategorisinde grup izomorfizmaları, $\mathcal{T}\text{op}$ kategorisinde homeomorfizmalardır.

Kategori teorisi, matematiksel yapıları iki farklı şekilde birleştirir. İlk olarak, yukarıda gördüğümüz gibi, teorik olarak tanımlanmış ve uygun morfizma kavramına sahip hemen hemen her matematiksel yapı kümesi bir kategori oluşturur. Bu, küme-teorik bir ortamda sağlanan bir birleştirmedir. İkinci olarak ve belki de daha da önemlisi, bir yapı türü tanımlandıktan sonra, verilen yapıdan nasıl yeni yapıların oluşturulabileceğini belirlemek zorunludur. Örneğin A ve B gibi iki küme verildiğinde küme teorisi bunların kartezyen çarpımı dediğimiz $A \times B$ kümesini oluşturmamızı sağlar. Ayrıca verilen yapıların daha temel alt yapılara nasıl ayrıştırılabileceğini belirlemek de zorunludur. Örneğin, bir sonlu Abel grup verildiğinde, bu grup belirli alt gruplarının (dik) çarpımına nasıl ayrıştırılabilir? Her iki durumda da, belirli türdeki yapıların nasıl birleşebileceğini bilmek gerekir. Bu kombinasyonların doğası, salt küme-teorik bir bakış açısıyla bakıldığında oldukça farklı görünebilir. Kategori teorisi, bu yapıların çoğunun aslında "evrensel özelliğe" sahip bir kategorideki belirli nesneler olduğunu ortaya koymaktadır. Nitekim, kategorik bir bakış açısından, küme teorisindeki kartezyen çarpım, grupların (Abel veya değil) dik çarpımı, topolojik uzayların çarpımı ve mantık sistemlerindeki önermelerin birleşimi evrensel özelliğe sahip bir kategorideki çarpım nesnesinin özel durumlarıdır. Bir $\mathcal{C}$ kategorisinde verilen X ve Y nesnelerinin çarpımı olarak adlandırılan nesne projeksiyon morfizmaları olarak adlandırılan $p : P \longrightarrow X$ ve $q : P \longrightarrow Y$ morfizmalarıyla birlikte bir P nesnesidir ve bu evrensellik özelliğini sağlar. Yani her W nesnesi ve $f : W \longrightarrow X$, $g : W \longrightarrow Y$ morfizmaları için $p \circ h = f$ ve $q \circ h = g$ olacak şekilde tek bir $h : W \longrightarrow P$ morfizması vardır. Bu çarpım nesnesi izomorfizma farkıyla tektir. Dolayısıyla kategori teorisinde, belirli bir yapıyı oluşturan unsurların doğası önemsizdir. Önemli olan, bir nesnenin kategorideki diğer nesnelerle nasıl ilişkili olduğudur. Kategori teorisi, farklı yapı türlerinin birbirleriyle nasıl ilişkili olduğunu ortaya koyar. Örneğin, cebirsel topolojide, topolojik uzaylar gruplarla (modüller, halkalar vb.) çeşitli şekillerde (homoloji, kohomoloji, homotopi, K-teorisi gibi) ilişkilidir. Kategori teorisi tam da bu bağlantıları açıklığa kavuşturmak ve karşılaştırmak için Eilenberg ve Mac Lane tarafından icat edilmiştir. İşte bu amaç doğrultusunda en önemli kavramlardan biri, fonktörler olarak adlandırılan kategoriler arasındaki morfizmalardır. Detaylı tanımı verilmeden önce fonktörler kategoriler arasında yapı koruyan dönüşümler olarak adlandırılabilir.

Tanım 2.

$\mathcal{C}$ ve $\mathcal{D}$ iki kategori olsun. Bir kovaryant $F : \mathcal{C} \longrightarrow \mathcal{D}$ fonktörü $\mathcal{C}$ 'nin her A nesnesine $\mathcal{D}$ 'nin bir $F(A)$ nesnesini, $\mathcal{C}$ 'deki her $f \in \text{Mor}_{\mathcal{C}}(A, B)$ morfizmasına $\mathcal{D}$ 'de bir $F(f) \in \text{Mor}_{\mathcal{D}}(F(A), F(B))$ morfizmasını karşı getiren ve aşağıdaki koşulları gerçekleyen bir kuraldır:

1. $f \in \text{Mor}_{\mathcal{C}}(A, B)$, $g \in \text{Mor}_{\mathcal{C}}(B, C)$ ise $F(g \circ f) = F(g) \circ F(f)$ 'dir.
2. $\mathcal{C}$ 'nin her A nesnesi için $F(1_A) = 1_{F(A)}$ 'dir.

Tanım 3.

$\mathcal{C}$ ve $\mathcal{D}$ iki kategori olsun. Bir *kontravaryant* $F : \mathcal{C} \longrightarrow \mathcal{D}$ *funktoru* $\mathcal{C}$ 'nin her A nesnesine $\mathcal{D}$ 'nin bir $F(A)$ nesnesini, $\mathcal{C}$ 'deki her $f \in \text{Mor}_{\mathcal{C}}(A, B)$ morfizmasına $\mathcal{D}$ 'de bir $F(f) \in \text{Mor}_{\mathcal{D}}(F(B), F(A))$ morfizmasını karşı getiren ve aşağıdaki koşulları gerçekleyen bir kuraldır:

1. $f \in \text{Mor}_{\mathcal{C}}(A, B), g \in \text{Mor}_{\mathcal{C}}(B, C)$ ise $F(g \circ f) = F(f) \circ F(g)$ 'dir.
2. $\mathcal{C}$ 'nin her A nesnesi için $F(1_A) = 1_{F(A)}$ 'dir.

Örnek 2.

1. $U : R\text{-Mod} \longrightarrow \text{Set}$ dönüşümünü her $A \in \text{Ob}(R\text{-Mod})$ için $U(A) = A$ ve $R\text{-Mod}$ 'daki herhangi bir f homomorfizması için $U(f) = f$ olarak tanımlayalım. U bir kovaryant funktordur. U 'ya *unutkan funktor* denir. Bunun nedeni $U(A) = A$ 'nın bir küme olarak düşünülmesi yani A 'nın modül yapısının unutuluyor olması ve $U(f)$ 'nin de kümeler arasında bir fonksiyon olarak görülmesidir.
2. Bir $\mathcal{C}$ kategorisi ve $\mathcal{C}$ 'nin bir A nesnesini alalım. $F_A = \text{Mor}(A, -) : \mathcal{C} \longrightarrow \text{Set}$ dönüşümünü aşağıdaki gibi tanımlayalım:

- (a) Her $B \in \text{Ob}(\mathcal{C})$ için $F_A(B) = \text{Mor}(A, B)$.
- (b) $g : B \longrightarrow C$ için $F_A(g) : \text{Mor}(A, B) \longrightarrow \text{Mor}(A, C)$ morfizmasını $F_A(g)(f) = g \circ f$.

F_A bir kovaryant funktordur.

3. Bir $\mathcal{C}$ kategorisi ve $\mathcal{C}$ 'nin bir B nesnesini alalım. $F^B = \text{Mor}(-, B) : \mathcal{C} \longrightarrow \text{Set}$ dönüşümünü aşağıdaki gibi tanımlayalım:

- (a) Her $A \in \text{Ob}(\mathcal{C})$ için $F^B(A) = \text{Mor}(A, B)$.
- (b) $g : A \longrightarrow C$ için $F^B(g) : \text{Mor}(C, B) \longrightarrow \text{Mor}(A, B)$ morfizmasını $F^B(g)(f) = f \circ g$.

F^B bir kontravaryant funktordur.

4. $H_n : \mathcal{T}op \longrightarrow \mathcal{A}b$ dönüşümünü aşağıdaki gibi tanımlayalım:

- (a) Her X topolojik uzayına n . homoloji grubu olarak adlandırılan $H_n(X)$ grubunu karşılık getirsin.
- (b) Her $f : X \longrightarrow Y$ sürekli fonksiyonuna $H_n(f) : H_n(X) \longrightarrow H_n(Y)$ grup homomorfizmasını karşılık getirsin.

H_n bir kovaryant funktordur. Bu funktor *tekil homoloji funktor* olarak adlandırılır.

Tanım 4.

Verilen $F : \mathcal{A} \longrightarrow \mathcal{B}$ ve $G : \mathcal{A} \longrightarrow \mathcal{B}$ fonktörleri için *doğal dönüşüm* olarak adlandırılan $\eta : F \longrightarrow G$ fonksiyonu, $\mathcal{A}$ 'nın her A nesnesine $\mathcal{B}$ 'nin bir $\eta(A) : F(A) \longrightarrow G(A)$ morfizmasını karşılık getiren bir fonksiyondur öyle ki $\mathcal{A}$ 'daki her $f : A \longrightarrow A'$ morfizması için aşağıdaki diyagram değişmelidir. Yani $G(f) \circ \eta(A) = \eta(A') \circ F(f)$ 'dir.

$$\begin{array}{ccc} F(A) & \xrightarrow{\eta(A)} & G(A) \\ F(f) \downarrow & & \downarrow G(f) \\ F(A') & \xrightarrow{\eta(A')} & G(A') \end{array}$$

$\mathcal{A}$ 'daki her A nesnesi için $\eta(A)$ morfizması bir izomorfizma ise η 'ya *doğal izomorfizma* denir.

Bir doğal dönüşüm ilgili kategorilerin morfizmaların bileşkesi gibi iç yapısını bozmadan bir funktoru diğerine dönüştürmenin yolunu sağlar. Bu nedenle bir doğal dönüşüm fonktörlerin morfizması olarak düşünülebilir. Doğal dönüşümlerin birçok örneği [4]'te verilmektedir.

Örnek 3.

1. Bir $F : \mathcal{A} \longrightarrow \mathcal{B}$ fonktoru için $\mathcal{A}$ 'nın her A nesnesine $1_{F(A)}$ morfizmasını karşılık getiren $1_F : F \longrightarrow F$ bir doğal izomorfizmadır.
2. Verilen iki $U : \mathcal{G}rp \longrightarrow \mathcal{S}et$ ve $F : \mathcal{S}et \longrightarrow \mathcal{G}rp$ fonktörleri için $\eta : 1_{\mathcal{S}et} \longrightarrow U \circ F$ ve $\eta' : F \circ U \longrightarrow 1_{\mathcal{G}rp}$ fonksiyonları birer doğal dönüşümdür.

Önerme 1.

İki doğal dönüşümün (dikey) bileşkesi bir doğal dönüşümdür.

Kanıt. Verilen $F, G, H : \mathcal{A} \longrightarrow \mathcal{B}$ fonktörleri için $\eta : F \longrightarrow G$ ve $\xi : G \longrightarrow H$ iki doğal dönüşüm ve $f : A \longrightarrow B$ morfizması $\mathcal{A}$ kategorisinde bir morfizma olsun. O zaman aşağıdaki diyagramı oluşturabiliriz:

$$\begin{array}{ccccc}
 F(A) & \xrightarrow{\eta(A)} & G(A) & \xrightarrow{\xi(A)} & H(A) \\
 F(f) \downarrow & & \downarrow G(f) & & \downarrow H(f) \\
 F(B) & \xrightarrow{\eta(B)} & G(B) & \xrightarrow{\xi(B)} & H(B)
 \end{array}$$

η ve ξ doğal dönüşüm olduğundan, sol kare ve sağ kare değişmelidir. Yani

$$G(f) \circ \eta(A) = \eta(B) \circ F(f)$$

ve

$$H(f) \circ \xi(A) = \xi(B) \circ G(f).$$

Buradan

$$H(f) \circ \xi(A) \circ \eta(A) = \xi(B) \circ G(f) \circ \eta(A) = \xi(B) \circ \eta(B) \circ F(f)$$

elde edilir. Bu $\xi \circ \eta$ 'nin doğal dönüşüm olduğu anlamına gelir. □

Eilenberg ve Mac Lane'in ilk gözlemlediği gibi, fonktoru tanımlayabilmek için kategori, doğal dönüşümü tanımlayabilmek için de fonktor tanımlanmıştır ([4, §I.4]). Kategori teorisi, matematiğin farklı dallarındaki yapılar arasında derin birleştirici ilişkiler kurar. Fonktörler ve doğal dönüşümler sayesinde, kümelerden gruplara, topolojik uzaylardan cebirsel yapılara kadar geniş bir yelpazede yapısal dönüşümler anlam kazanır. Bu teori, hem soyut hem de uygulamalı matematiğin pek çok alanında temel bir rol oynar.

■ Kaynaklar

- [1] Alizade, R. ve Pancar, A., *Homoloji Cebire Giriş*, Yeniden Düzenlenmiş Baskı 2016. https://www.researchgate.net/publication/312136271_Homoloji_Cebire_Giris
- [2] Eilenberg, S. ve MacLane, S., Group Extensions and Homology, *Annals of Mathematics* **43** (4), (1942) 757–831.
- [3] Eilenberg, S. ve MacLane, S., General Theory of Natural Equivalences, *Transactions of the American Mathematical Society* **58** (2), (1945) 231–294.
- [4] Mac Lane, S., *Categories for the Working Mathematician*, Springer, Second Edition 1998.
- [5] Reihl, E., *Category Theory in Context*, Dover Publications 2016.

Düğüm Teorisine Giriş: Temel bir değişmez "Bağlanma Sayısı" üzerine

SİNEM ONARAN

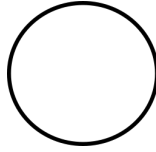
Hacettepe Üniversitesi Matematik Bölümü

✉ sonaran@hacettepe.edu.tr



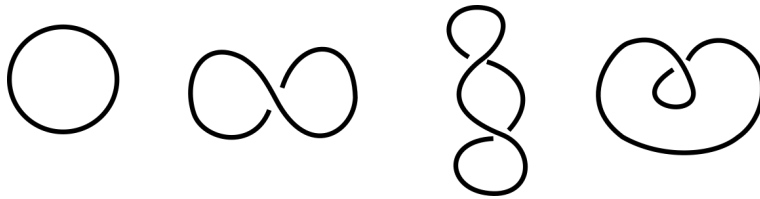
Düğüm, insanlık tarihinin en eski araçlarından. Giysi yapımından balıkçılığa, zaman ölçümünden inşaatla kadar pek çok alanda kullanılmıştır. Matematikte topolojinin bir dalı olarak çalışılan düğüm teorisi ile ilgili ilk çalışmalar 18. ve 19. yüzyıllarda Vandermonde, Gauss ve Listing tarafından yapılmıştır. 20. yüzyılda Alexander ve Reidemeister önemli adımlar atmış, Jones'un 1984'te tanımladığı polinom ise teoriyi derinleştirmiştir. Bugün düğüm teorisi; matematik dışında fizik, kimya ve özellikle DNA topolojisi gibi biyoloji alanlarında da uygulanmaktadır.

Düğüm, kendi kendini kesmeyen kapalı eğriler olarak düşünebiliriz. Matematiksel açıdan ise bir düğüm, $\mathbb{R}^3$ içinde birim çember $S^1 = \{(x, y) \mid x^2 + y^2 = 1\}$ 'e homeomorfik olan altkümeleri olarak tanımlanabilir. Burada, iki topolojik uzay arasında tanımlı bir $f : X \rightarrow Y$ fonksiyonu birebir, örten, sürekli ve tersi f^{-1} de sürekli ise, bu fonksiyona bir homeomorfizma denir. Böylece X ve Y uzayları birbirine homeomorfik, yani topolojik olarak eşdeğer kabul edilir.



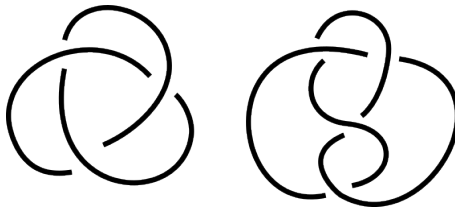
Şekil 1. Çözük düğüm.

Şekil 1'de düğüm diyagramı verilen çözük düğüm, en basit düğüm örneğidir. $\mathbb{R}^3$ uzayı içerisindeki bir düğümün diyagramı, düğümün xz -düzlemine olan izdüşümüdür. Bir düğümün birden fazla izdüşümü yani birden fazla diyagramı olabilir.



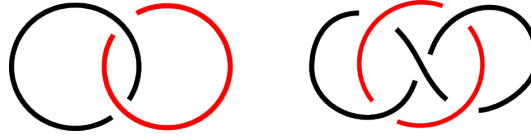
Şekil 2. Çözük düğümün birden fazla izdüşümü.

Çözük düğümden sonraki en basit düğüm örnekleri trefoil düğümü ve Sekiz düğümüdür.



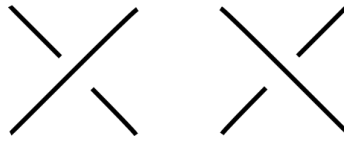
Şekil 3. Trefoil düğümü ve Sekiz düğümü.

Düğümün ayrı birleşimlerini alırsanız bir *link* elde edilir. Linki oluşturan her bir düğüm, linkin bir *bileşenidir*. 2-bileşenli linke Hopf link ve Whitehead link örneklerini verebiliriz.



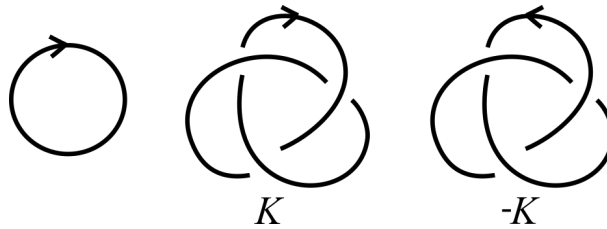
Şekil 4. Hopf link ve Whitehead link.

Bir düğüm diyagramında yayların birbirini üzerinden geçtiği yerlere *düğüm çaprazlaması* denir. Düğüm diyagramlarında iki tip çaprazlama görülebilir.



Şekil 5. Düğüm diyagramındaki çaprazlamalar.

Bir düğüm diyagramı üzerinde belirli bir nokta seçerek, bu noktadan başlayıp saat yönünde ya da saat yönünün tersine hareket edebiliriz. Diyagram üzerinde bu yönün açıkça belirtildiği düğüm ya da linke yönlü düğüm ya da yönlü link adı verilir. Yönlü düğüm örneklerini Şekil 6'de görebilirsiniz.

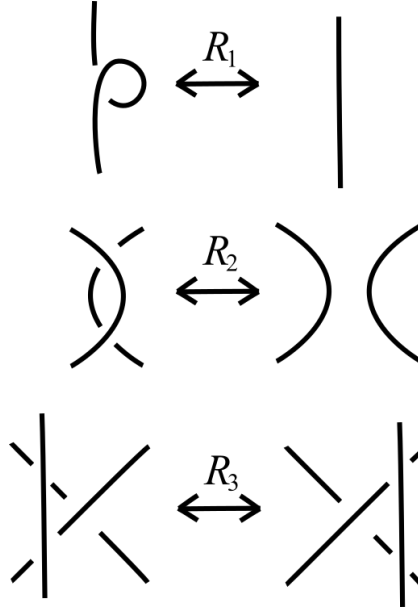


Şekil 6. Yönlü düğümler.

Peki, verilen iki düğümün birbirinden farklı olup olmadığını nasıl anlayabiliriz? Örneğin, çözükle düğüm ile trefoil düğümünün farklı olduğu nasıl ispatlanır? Bu tür soruları yanıtlatabilmek için düğüm değişmezleri adı verilen matematiksel araçlara ihtiyaç duyarız.

Düğüm değişmezleri, bir düğümün farklı diyagramlarla gösterilmesine rağmen değişmeden kalan, düğüme ait temel karakteristik özellikleri ortaya koyan niceliklerdir. Başka bir deyişle, düğüm üzerinde yapılan topolojik dönüşümlerle değişmeyen, düğümün yapısal özelliklerini koruyan ölçütlerdir. Polinom değişmezleri (örneğin Alexander, Jones veya HOMFLY polinomları), bağlantı sayısı, minimum çaprazlama sayısı ve cebir teorisi kullanarak düğüm grubu gibi birçok farklı düğüm değişmezi tanımlanmıştır. Bu değişmezler, farklı düğümleri ayırt etmenin yanı sıra, düğüm teorisinde sınıflandırma yapabilmenin de temel araçlarıdır. Aynı zamanda yön kavramı da birçok değişmezin tanımında kritik bir rol oynar; çünkü bazı düğüm değişmezleri yönlü düğümler üzerinde tanımlanır ve düğümün yönü değiştirildiğinde elde edilen değer değişebilir. Bu nedenle, yön bilgisi ve değişmezlerin birlikte kullanımı, düğüm teorisinde vazgeçilmez bir öneme sahiptir.

İki düğümün aslında aynı düğüm olup olmadığını, yani izotopik olup olmadıklarını göstermek için Reidemeister hareketlerini kullanabiliriz. Bu hareketler, düğüm diyagramı üzerinde yapılan lokal değişikliklerle, düğümün topolojik özelliğini bozmadan şeklinin değiştirilmesini sağlar. Üç temel Reidemeister hareketi vardır ve bu hareketler Şekil 7'de gösterilmiştir.



Şekil 7. Reidemeister hareketleri.

Reidemeister hareketleri, düğüm diyagramları arasında geçiş yapmanın ve eşdeğerlik göstermenin temel yollarındandır. Aşağıdaki teorem, iki diyagramın aynı düğümü temsil etmesi için bu hareketlerin yeterli olduğunu ifade eder:

Teorem 1. (Reidemeister-Markov)

İki düğüm (veya link) diyagramının aynı düğümü (veya linki) temsil etmesi için gerekli ve yeterli koşul, bu iki diyagramın sonlu sayıda R_1 , R_2 , R_3 Reidemeister hareketleri, bu hareketlerin tersleri ve düzlem izotopileri yoluyla birbirine dönüştürülebilir olmasıdır.

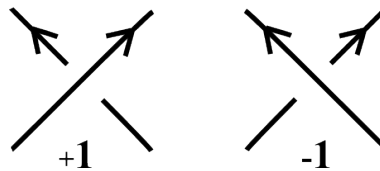
Burada izotopi, düğüm yayının sürekli bir biçimde deformasyona uğraması anlamına gelir. Düzlem izotopisi ise, bu deformasyonun düğüm yayının kendini kesmeden gerçekleştirdiği sürekli hareketlerdir.

Bir düğüm için tanımlanan bir nicelik, eğer tüm Reidemeister hareketleri altında değişmeden kalıyorsa, bu nicelik düğüm değişmezi olarak adlandırılır.

Şimdi, düğümler ve linkler için tanımlanmış önemli bir değişmez olan bağlanma sayısı üzerinde duralım. Bağlanma sayısını tanımlayabilmek için öncelikle düğüme veya linke bir yön vermemiz ve çaprazlamalarını incelememiz gerekir. Verilen yönlü düğüm veya yönlü link diyagramında her bir çaprazlama için, Şekil 8'de gösterildiği şekilde bir sayı atanır. Bu atamaya göre:

+1 -değeri verilen çaprazlamalara pozitif çaprazlama,

−1 -değeri verilen çaprazlamalara ise negatif çaprazlama denir.

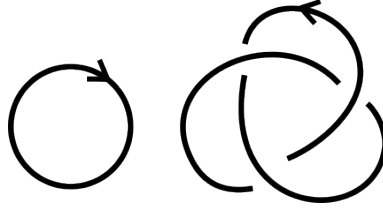


Şekil 8. Pozitif ve negatif çaprazlama.

K_1 ve K_2 olmak üzere iki yönlü bileşene sahip bir link diyagramı ele alalım. Bu iki bileşen arasında oluşan çaprazlamalardaki +1 ve −1 değerlerinin toplamının yarısı, K_1 ile K_2 bileşenleri arasındaki bağlanma sayısı

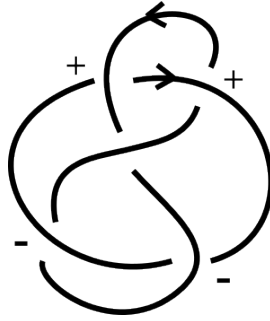
olarak tanımlanır ve $bs(K_1, K_2)$ şeklinde gösterilir. Bağlanma sayısı, Reidemeister hareketleri altında sabit kaldığından, diyagramın seçimine bağlı değildir ve bu nedenle yönlü linkler için bir topolojik değişmezdir.

Sıradaki adımda, bağlanma sayısının bazı örnek linkler üzerinde nasıl hesaplandığını birlikte inceleyelim. Örneğin; aralarında hiç çaprazlama olmadığı için Şekil 9'da verilen linkin bileşenleri için bağlanma sayısı $bs(K_1, K_2) = 0$ 'dır.



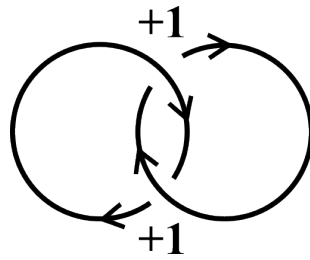
Şekil 9. Bağlanma sayısı $bs(K_1, K_2) = 0$.

Şekil 10'da verilen Whitehead linkin bileşenleri arasındaki bağlanma sayısını hesaplarken sadece aralarındaki çaprazlamalardan gelen $+1$ ve -1 sayıları hesaba katılır ve $bs(K_1, K_2) = \frac{1}{2}(-2 + 2) = 0$ 'dır.



Şekil 10. Whitehead linkin bileşenlerinin bağlanma sayısı $bs(K_1, K_2) = 0$.

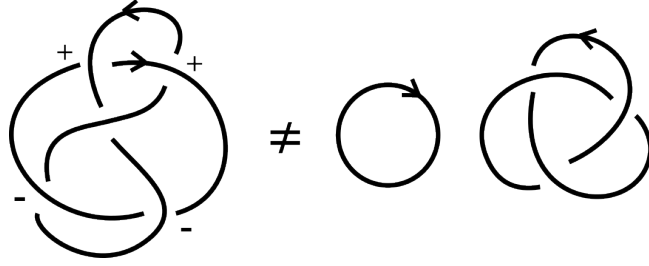
Hopf linkin bileşenleri arasındaki bağlanma sayısını ise $bs(K_1, K_2) = \frac{1}{2}(+1 + 1) = +1$ olarak hesaplarız.



Şekil 11. Pozitif Hopf link, bağlanma sayısı $bs(K_1, K_2) = +1$.

Whitehead link ile Hopf link'in bileşenleri arasındaki bağlanma sayıları farklı olduğundan, bu iki linkin birbirinden farklı olduğu sonucuna varabiliriz. Ancak, bağlanma sayısı aynı olan her iki linkin mutlaka aynı olması gerekmez. Örneğin, ilk bağlanma sayısını hesapladığımız link örneği ile Whitehead link'in bileşenleri arasındaki bağlanma sayısının her iki durumda da 0 olduğunu gördük. Buna rağmen, bu iki link topolojik olarak farklıdır. Bu durum, bağlanma sayısının bazı linkleri ayırt etmekte yetersiz kaldığını ve daha güçlü değişmezler ihtiyacı duyulduğunu göstermektedir. Bu tür değişmezlerin incelenmesi ise başlı başına ayrı bir yazının konusu olabilir.

Düğüm teorisinin temel hedeflerinden biri, tüm düğümleri belirli kurallara göre sınıflandırmaktır. Bu sınıflandırma sürecinde, düğüm değişmezleri önemli bir rol oynar; çünkü aynı düğümü temsil eden farklı



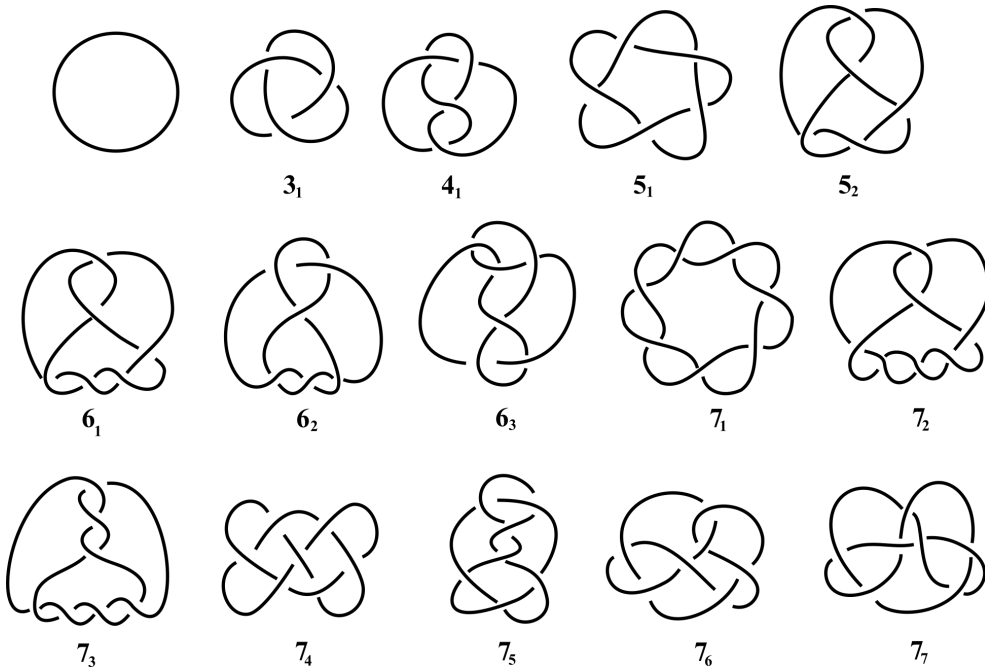
Şekil 12. Bağlanma sayıları aynı olan iki farklı link.

diyagramlar olsa bile, değişmezler sabit kalır ve düğümler arasındaki farkları ortaya koymaya yardımcı olur. Düğüm tablosu, belirli bir çaprazlama sayısına kadar olan düğümlerin sistematik şekilde listelendiği, sınıflandırmayı görselleştiren önemli bir araçtır. Bu tablolar sayesinde düğümler kolayca tanımlanabilir, karşılaştırılabilir ve topolojik yapıları üzerine analiz yapılabilir.

Son olarak, yazımızı sadece bilgiyle değil, biraz da merakla bitirelim:

Bağlanma sayısı neden daima tam sayıdır?

Bu sorunun cevabını düşünürken, aşağıdaki düğüm tablosu size ilham verebilir.



Bu düğüm tablosunda, çaprazlama sayısı en fazla yedi olan düğüm diyagramları listelenmiştir. Düğümlerin adlandırılması ve sıralanmasında Alexander ve Briggs'in 1926 yılında geliştirdikleri notasyon sistemi esas alınmıştır.

■ Kaynaklar

- [1] A. Adams, *The knot book, an elementary introduction to the mathematical theory of knots*, American Mathematical Society.
- [2] K.Reidemeister, *Knotentheorie*, Berlin: Springer-Verlag, 1932.
- [3] D. Rolfsen, *Knots and links*, Berkeley, California: Publish or Perish Press, 1976.

Diffie-Hellman Anahtar Değişimi

SÜMEYYE SOYLU

Hacettepe Üniversitesi Matematik Bölümü, 4. Sınıf Öğrencisi

✉ sumeyyesoylu1101@gmail.com



Öncelikle biraz bilgisayar çağı öncesine dönelim; hatta yazının icat edildiği zamana kadar gidebiliriz. Çünkü gizli bilgilere sahip olma kavramının uygarlığın başlangıcına kadar dayandığı düşünülmektedir. Savaşlarda, politik entrikalarda veya kişisel mesajlarda bilgilerin yalnızca istenilen kişi tarafından anlaşılması her zaman büyük önem taşımıştır. Bu amaçla geliştirilen kriptografi, yani şifreleme bilimi, binlerce yıllık bir geçmişe sahiptir.

Örneğin Roma İmparatorluğu'nda Julius Caesar, mesajlarını gizli tutabilmek için her harfi alfabede belirli bir sayıda kaydırarak başka bir harf ile değiştirdiği basit bir şifreleme yöntemi kullanmıştır. Mesela her harf 3 birim sağa kaydırıldığında, şifreli metni çözmek isteyen kişinin de her harfi 3 birim sola kaydırması gerekir. Burada 3 sayısı anahtar olarak kullanılır ve mesajın doğru şekilde çözülebilmesi için bu anahtarın alıcı tarafından bilinmesi şarttır. Eğer bu bilgi (anahtar) gizli tutulmazsa, şifreleme amacına ulaşmaz ve ayrıca anahtar olmadan şifre çözülemez, çünkü alıcı her harfi kaç birim geri kaydıracağını yalnızca anahtar sayesinde bilebilir.

O zamandan itibaren uygarlıklar, harflerin başka harf veya sembollerle değiştirilmesine dayanan yerine koyma şifreleri (örneğin Caesar şifresi) ve harflerin yerlerinin değiştirilmesine dayanan yer değiştirme şifreleri yöntemlerini geliştirerek şifreleme tekniklerini çeşitlendirmiştir. Kullanılan tekniklerin karmaşıklık seviyesi ise dönemden döneme ve ülkeden ülkeye farklılık göstermiştir. Örneğin, Amerika Birleşik Devletleri 1917'de I. Dünya Savaşı'na girerken, İtalya'da 1600'lü yıllarda kullanılan şifrelerden bile daha basit yöntemler kullanıyordu.

Tarih boyunca, 20. yüzyıla kadar geliştirilen şifreleme yöntemlerinin tamamı, bugün simetrik şifreleme olarak adlandırdığımız yapıya dayanıyordu. Zamanla bu yöntemler, polialfabetik şifreleme gibi daha karmaşık tekniklerle gelişmiş, 20. yüzyılda ise II. Dünya Savaşı sırasında kullanılan Enigma gibi mekanik rotor makinelerinden, günümüzde kullanılan modern simetrik şifreleme yöntemleri olan blok ve akış şifreleme algoritmalarına evrilmiştir.

Simetrik şifrelemede hem şifreleme hem de şifre çözme işlemi için aynı gizli anahtar kullanılır. Bu anahtar, algoritmanın en önemli bileşenidir. Peki neden bu kadar önemli olduğunu bir örnekle açıklayalım, çünkü temel mantığı her zaman aynıdır. Örneğin blok şifrelemede, mesaj önce belirli uzunluktaki parçalara bölünür ve her parça, anahtarın belirlediği karmaşık matematiksel işlemlerden geçirilerek şifrelenir. Çözme algoritması ise aynı anahtarı kullanarak bu işlemleri tersine çevirir ve orijinal mesajı ortaya çıkarır. Burada asıl önemli olan, tüm matematiksel dönüşümlerin anahtara bağlı olmasıdır. Anahtar değiştiğinde, algoritmanın tüm adımlarındaki matematiksel işlemler de değişir. Bu nedenle yanlış anahtar kullanan biri, ortaya çıkan karışıklıktan hiçbir anlamlı bilgi elde edemez.

Tabii simetrik şifrelemenin büyük bir sıkıntısı vardır; en büyük sorun anahtarın güvenli bir şekilde paylaşılmasıdır.

İşte bu soruna çözüm arayışıyla birlikte, 1976 yılında Whitfield Diffie ve Martin Hellman, “**New Directions in Cryptography**” başlıklı makalelerini yayımladıklarında, kriptografi dünyasında yeni bir dönem başlamış oldu [1]. Çünkü Diffie-Hellman protokolü, tarihte ilk kez yayımlanan asimetrik algoritma olarak, daha önce mümkün olmadığı düşünülen bir şeyi başardı: İki tarafın, önceden hiç karşılaşmadan ortak bir gizli anahtar oluşturabilmesini sağladı. Bu gelişme, asimetrik kriptografinin diğer adıyla açık anahtarlı kriptografinin doğuşuna zemin hazırladı.

Asimetrik şifreleme sistemlerinde her kullanıcının bir açık anahtarı ve bir de gizli anahtarı bulunur. Açık anahtar herkesle paylaşılabilirken, gizli anahtar yalnızca sahibinde kalır. Gönderici, alıcının açık anahtarını kullanarak mesajı şifreler ve bu mesajı yalnızca alıcı, kendi gizli anahtarıyla çözebilir. Böylece güvenli iletişim için önceden gizli anahtar paylaşımı yapmaya gerek kalmaz.

Burada not olarak belirtmek gerekir ki, ele alacağımız Diffie-Hellman bir asimetrik şifreleme algoritması değil, bir anahtar paylaşım protokolüdür.

Şimdi, anahtar değişim problemini daha iyi kavrayabilmek için bir senaryo hayal edelim. Daha önce hiç iletişim kurmamış iki tarafın, aralarındaki iletişimi gizli tutarak haberleşmek istediklerini varsayalım. İletişim kanalı üzerinde bir saldırganın bulunabileceği ihtimalini bilerek, taraflar mesajlarını saldırgan tarafından çözülemeyecek ve tamamen okunamaz hâle getiren bir şifreleme sistemi kullanmaktadır.

Ancak bu şifreleme sisteminde, gönderici mesajı şifrelemek için bir anahtar (gizli bilgi) kullanmakta ve alıcının da bu şifreli mesajı çözebilmesi için aynı anahtara sahip olması gerekmektedir. Göndericinin bu anahtarı güvenli olmayan iletişim kanalı üzerinden doğrudan alıcıya iletmesi durumunda, saldırganın anahtara erişme ve böylece şifreli mesajı çözme riski ortaya çıkar.

İşte bu noktada, taraflar arasında güvenli bir şekilde ortak bir anahtarın paylaşılması sorunu, yani anahtar değişim problemi, karşımıza çıkmaktadır.

1976 yılında Whitfield Diffie ve Martin Hellman tarafından önerilen **Diffie-Hellman Anahtar Değişimi**, anahtar dağıtım problemlerine bir çözüm sunar. Yani, iki tarafın daha önce birbirleriyle tanışmadan, güvensiz bir kanal üzerinden ortak bir gizli anahtar üzerinde anlaşmasını sağlar. Bu sayede, ortak üretilen anahtar ile gönderici mesajını şifreleyip güvensiz ağ üzerinden alıcıya iletebilirken, alıcı da aynı anahtarı kullanarak bu şifreli mesajı çözebilir.

Diffie-Hellman anahtar değişim protokolü, p bir asal sayı olmak üzere, mod p altında tanımlı sonlu cisim $\mathbb{Z}_p$ 'nin sıfır dışı elemanlarının oluşturduğu çarpımsal bir grup olan $\mathbb{Z}_p^*$ üzerinde tanımlanmıştır. Burada

$$\mathbb{Z}_p = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p-1}\}, \quad \mathbb{Z}_p^* = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$$

şeklinde dir.

$(\mathbb{Z}_p^*, \cdot)$ sonlu grubu, abelyen (değişmeli) ve devirli bir gruptur. Devirli oluşuna açıklık getirelim:

Bir $g \in \mathbb{Z}_p^*$ için, eğer

$$\{g^1 \pmod{p}, g^2 \pmod{p}, \dots, g^{p-1} \pmod{p}\} = \mathbb{Z}_p^*$$

eşitliği sağlanıyorsa, yani $\mathbb{Z}_p^*$ kümesinden aldığımız bir eleman g 'nin mod p altındaki $g^1, g^2, \dots, g^{p-1}$ kuvvetleri, $\mathbb{Z}_p^*$ 'deki tüm elemanları hiçbir tekrar olmadan veriyorsa, bu durumda g sayısına mod p için bir **ilkel kök**, $\mathbb{Z}_p^*$ grubuna da devirli grup denir.

Şimdi bu protokolün işleyiş sürecini ele alalım. Tarafları gönderici olarak Ayşe ve alıcı olarak Burak şeklinde adlandıralım. Ardından, taraflar arasında anahtar değişiminin nasıl gerçekleştiğini adım adım inceleyelim.

Adım 1: Taraflar, herkes tarafından bilinebilecek şekilde yeterince büyük bir asal sayı p ve mod p altında ilkel bir kök g üzerinde anlaşılır.

Adım 2: Gönderen (Ayşe), rastgele bir a tam sayısı seçer ve bu değeri gizli tutar. Alıcı (Burak), rastgele bir b tam sayısı seçer ve o da bu değeri gizli tutar.

Adım 3: Ayşe $A \equiv g^a \pmod{p}$ ifadesini hesaplar ve bu değeri Burak'a gönderir. Burak ise $B \equiv g^b \pmod{p}$ değerini hesaplayıp Ayşe'ye gönderir.

Adım 4: Ayşe, Burak'tan kendisine gelen B değerini kullanarak $B^a \pmod{p}$ hesaplamasını yapar. Burak ise Ayşe'den aldığı A değerini kullanarak $A^b \pmod{p}$ işlemini gerçekleştirir.

4. adımın sonunda Ayşe, $B^a \equiv g^{ba} \pmod{p}$ hesaplamış, Burak ise $A^b \equiv g^{ab} \pmod{p}$ hesaplamış oldu. $ab = ba$ olduğundan her iki taraf da aynı gizli anahtara ulaşmış olur. Artık bu anahtar, daha sonra simetrik şifreleme sistemlerinde kullanılabilir.

Somutlaştırarak anlatmak gerekirse:

Burak, yeni bir yemek bloguna abone olur. Bu blogda, dünya çapındaki şefler gizli tariflerini takas etmek amacıyla iletişim kurmaktadır. Bir gün Burak, blog üzerinden “AyseChef06” adlı kullanıcıdan bir mesaj alır.

Ayşe, Akdeniz mutfağına ait çok özel bir sos tarifini paylaşmak istediğini, ancak blogun mesajlaşma sistemine güvenmediğini belirtir.

Bunun üzerine Burak, bu sorunu birlikte çalışarak çözebileceklerini söyler. Önerisi şudur: Blogun herkese açık kanalını kullanarak, sadece kendilerinin bileceği ortak bir gizli anahtar oluştursunlar. Daha sonra bu anahtar, bir simetrik şifreleme sisteminde (örneğin AES, 3DES) kullanılarak, sos tarifi güvenli bir şekilde şifrelenebilir. Böylece tarifi içeriği blog üzerinden iletile bile, üçüncü şahıslar tarafından okunamaz hâle gelecektir.

Şimdi bu süreci nümerik bir örnek ile açıklayalım:

Adım 1: Burak, herkese açık blog kanalında iki bilgi paylaşır: Asal sayı $p = 71$ ve $g = 7$ ilkel kök üzerinde anlaşalım.

Adım 2: Ayşe gizli tam sayı olarak 6 değerini seçiyor ve Burak 60'ı seçiyor.

Adım 3: Ayşe $A \equiv 7^6 \pmod{71} \equiv 2$ değerini hesaplıyor ve Burak'a gönderiyor. Burak $B \equiv 7^{60} \pmod{71} \equiv 30$ değerini hesaplıyor ve Ayşe'ye gönderiyor.

Adım 4: Ayşe, Burak'tan gelen $B = 30$ değerini kullanarak: $K \equiv 30^6 \pmod{71} \equiv 45$ hesaplıyor. Burak ise Ayşe'nin gönderdiği $A = 2$ değerini kullanarak: $K \equiv 2^{60} \pmod{71} \equiv 45$ hesaplıyor.

Yani, $K = 45$ ikisinin de kullanacağı ortak gizli anahtar olur.

Peki, bu iletişimi izleyen bir kulak misafiri neden ortak anahtara ulaşamaz? Bu sorunun yanıtını açıklayalım.

Diffie-Hellman anahtar değişiminin güvenliği, *ayrık logaritma problemine* dayanır ve bu problemin çözülmesi zor olduğu düşünülmektedir.

$\mathbb{Z}_p^*$ kümesinde tanımlı **Ayrık Logaritma Problemi** şu şekilde ifade edilir:

p asal sayı olmak üzere, $\mathbb{Z}_p^*$ grubunda bir ilkel kök g ve bir sayı h verildiğinde,

$$g^x \equiv h \pmod{p}$$

eşitliğini sağlayan x tam sayı değerine, h 'nin g tabanına göre **ayrık logaritması** denir.

Burada asıl mesele şudur: Eğer g , x ve p biliniyorsa, h 'yi bulmak kolaydır. Ancak g , h ve p biliniyorken x 'i bulmak yeterince büyük sayılar için oldukça zordur. Bu probleme **ayrık logaritma problemi** adı verilir.

Şimdi protokole geri dönelim. Burada kulak misafiri, herkese açık olan asal sayı p ve ilkel kök g gibi bilgilere sahiptir. Adım 3'te Ayşe'nin Burak'a ve Burak'ın da Ayşe'ye açık ağ üzerinden direkt gönderdikleri $A \equiv g^a \pmod{p}$ ve $B \equiv g^b \pmod{p}$ değerlerini okusa da, burada Ayşe ve Burak tarafından gizli tutulan a ve b değerlerini bulmak için yukarıda tanımlanan ayrık logaritma problemini çözmesi gerekir.

Eğer saldırgan bu problemi çözebiliyorsa, yani tarafların gönderdikleri $A \equiv g^a \pmod{p}$ ve $B \equiv g^b \pmod{p}$ ifadelerinden a ve b 'yi çıkarabilirse, bu durumda Ayşe ve Burak'ın ortak gizli anahtarı olan $g^{ab} \pmod{p}$ değerini hesaplaması kolay olur ve böylece Ayşe ile Burak'ın paylaştığı ortak anahtara erişebilir.

Verilen nümerik örneğe bakıldığında, $7^6 \pmod{71} \equiv 2$, $7^{30} \pmod{71} \equiv 30$ eşitliklerinde ayrık logların hesaplanması, küçük asal sayılar ile çalışıldığından deneme-yanılma yöntemiyle kolaylıkla gerçekleştirilebilir.

Bununla birlikte, ayrık logların hesaplanması için: Yaklaşık 20 veya daha az ondalık basamağa sahip asal sayılar için çalışan Bebek-Adım Dev-Adım yöntemi, 20 veya daha fazla ondalık basamağa sahip asal sayılar için ise İndeks Hesabı yöntemi tercih edilebilir.

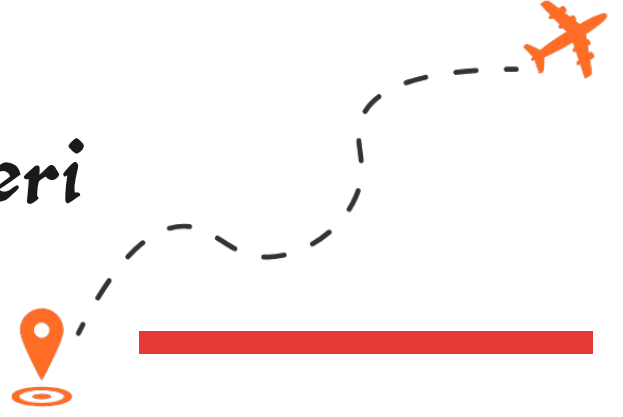
Ancak gerçek hayattaki Diffie-Hellman uygulamalarında kullanılan asal sayı p , genellikle 2048 bit (yaklaşık 617 basamak) uzunluğunda, ilkel kök g , 2, 3, 5 veya 7 gibi küçük sayılar seçilirken, gizli tutulan a ve b de en az 256-512 bit uzunluğunda seçilmektedir. Bu durumda, ayrık logaritmanın hesaplanması için klasik bilgisayarlar üzerinde her ne kadar algoritmalar geliştirilmiş olsa da, kullanılan asal sayıların oldukça büyük olması nedeniyle bu algoritmalar üstel zaman gerektirmektedir ve dolayısıyla klasik bilgisayarlar üzerinde makul sürede hesaplama yapılamamaktadır.

Diğer yandan, kuantum bilgisayarlar için geliştirilen Shor algoritmasının ayrık logaritma problemini logaritmik zamanda çözebileceği teorik olarak gösterilmiştir [2]. Ancak mevcut teknoloji düzeyinde kuantum bilgisayarlar, büyük asal sayılar üzerinde işlem yapabilecek yeterli kapasiteye sahip değildir. Yine de teorik olarak mümkün görülmesi, gelecekte Diffie-Hellman protokollerinin kuantum tehditlere karşı savunmasız kalabileceğini göstermektedir. Bu doğrultuda, kuantum tehditlere karşı dirençli kriptografik sistemlerin geliştirilmesine yönelik çalışmalar kuantum sonrası (post-quantum) kriptografi alanında devam etmektedir.

■ Kaynaklar

- [1] Diffie, W., & Hellman, M. (1976). *New Directions in Cryptography*. *IEEE Transactions on Information Theory*, 22(6), 644–654. <https://doi.org/10.1109/TIT.1976.1055638>
- [2] Shor, P. W. (1994). *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE. <https://doi.org/10.1109/SFCS.1994.365700>
- [3] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.
- [4] Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.
- [5] Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). *An Introduction to Mathematical Cryptography*. Springer.
- [6] Smart, N. (2016). *Cryptography: An Introduction* (3rd ed.).
- [7] Wood, D. (2021). *Real-World Cryptography*. Manning Publications, Shelter Island.
- [8] Kraft, J., & Washington, L. C. (2015). *Kriptografi ile Sayılar Teorisine Giriş* (Çev. A. Yavuz). Palme Yayıncılık.
- [9] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Erasmus Günlükleri



■ Nurten Ünlerşen – *Częstochowa Teknoloji Üniversitesi, Polonya*



Ekim 2024 ve Şubat 2025 ayları arasında, Polonya'nın Częstohova şehrinde bulunan Politechnika Częstochowa Üniversitesi'nde Erasmus hareketliliği kapsamında bulundum. Bu süreç, hem akademik hem de kişisel gelişimim açısından oldukça değerli ve dönüştürücü bir deneyim oldu.

Erasmus programı sayesinde ilk kez ailemden ve alıştığım çevreden uzak bir yerde, tamamen kendi başıma yaşadım. Bu durum bana hem sorumluluklarımı daha iyi yönetmeyi hem de ani gelişen durumlara karşı çözüm üretmeyi öğretti. Farklı bir ülkede bağımsız bir şekilde yaşamayı deneyimlemek, özgüvenimi artırdı ve bana büyük bir kişisel olgunluk kazandırdı.

Konaklama açısından şanslıyım; okulun yurdu olduğu için bu konuda herhangi bir sorun yaşamadım. Polonya, yaşam maliyetleri bakımından oldukça avantajlı bir ülkedir. Verilen Erasmus hibesi, günlük harcamalarımı karşılamak açısından büyük ölçüde yeterli oldu. Yalnızca ekstra seyahatlerim için kendi birikimlerimi kullandım. Bu sayede gündelik ihtiyaçlarımı rahatça karşılayabildim.

Polonya, Avrupa'nın merkezinde yer aldığı için seyahat etmek oldukça kolaydı. Bu fırsatı değerlendirerek sekiz farklı ülkeye gittim. Her bir ülke, kendine has bir atmosfer ve kültürel miras sunuyordu. Farklı şehirlerde kaybolmak, yeni yerler keşfetmek ve yerel halkla iletişim kurmak, kendi sınırlarımı zorlamamı ve daha cesur adımlar atmamı sağladı. Seyahat etmek sadece yeni yerler görmeme değil, aynı zamanda kendimi daha iyi tanımama yardımcı oldu.

Erasmus sürecindeki en büyük kazanımlarımdan biri de çok kültürlü bir çevrede bulunmak ve farklı ülkelerden gelen öğrencilerle tanışmak oldu. Onlarla vakit geçirmek, yaşam tarzlarını, düşünme biçimlerini ve geleneklerini öğrenmemi sağladı. Sürekli İngilizce iletişim kurmak durumunda olduğum için dil pratiği yapma fırsatı da buldum. Bununla birlikte, günlük hayatta Polonya halkının İngilizce konusunda çok yetkin olmaması zaman zaman iletişim zorlukları yaşamama neden oldu.

Akademik açıdan da verimli bir dönem geçirdim. Politechnika Częstochowa Üniversitesi'nde toplam altı ders aldım. Bu dersler arasında zorunlu derslerimden olan Diferansiyel Denklemler ve Ayrık Matematik'in yanı sıra, Nümerik Analiz, Matematiksel Programlamaya Giriş ve Fuzzy Modeling gibi laboratuvar ağırlıklı seçmeli matematiksel programlama dersleri de vardı. Ayrıca, alan dışı seçmeli olarak Mikroekonomi dersi aldım. Tüm dersler İngilizce işlendiği için hem içerikleri takip etmekte hem de öğretim üyeleriyle iletişim kurmakta herhangi bir zorluk yaşamadım. Dönem sonunda aldığım altı dersin tamamını başarıyla tamamladım ve bu derslerin tümünü Hacettepe Üniversitesi'nde saydırabildim.

Derslerin işleniş biçimi, Hacettepe Üniversitesi'ndekine oldukça benziyordu. Genellikle haftada bir saat teorik ve bir saat uygulamalı oturumlar şeklinde yürütülüyordu. Eğer dersin laboratuvar içeriği varsa, her hafta bir laboratuvar projesi hazırlamamız bekleniyordu. Ders içerikleri de genel olarak benzerdi, bu nedenle akademik anlamda uyum sağlamakta zorlanmadım.

Kısacası, Erasmus deneyimi bana yalnızca akademik ve dil gelişimi değil, aynı zamanda kültürel farkındalık ve özgüven kazandırdı. Farklı kültürlerden insanlarla tanışmak, yeni ülkeler keşfetmek ve

bağımsız bir şekilde yaşamayı öğrenmek hayatımın en değerli deneyimlerinden biri haline geldi. Bu süreç, bakış açımı genişletti ve kendimi birçok farklı ortamda daha rahat ifade edebilmemi sağladı. Hayatım boyunca unutamayacağım anılar biriktirme fırsatı yakaladım.

■ Tolga Topçuoğlu – Tübingen Üniversitesi, Almanya



Hacettepe Üniversitesi Matematik Bölümü öğrencisiyim. 2024 bahar döneminde Erasmus+ öğrenci değişim programı kapsamında, dördüncü dönemimi Almanya'nın Tübingen şehrindeki Eberhard Karls Üniversitesi'nde geçirdim. Bu süreç, akademik, sosyal, kültürel ve ekonomik yönleriyle oldukça öğretici ve geliştirici bir deneyim oldu.

Akademik açıdan, Almanya'daki sistemin daha esnek ve öğrenci odaklı olduğunu gözlemledim. Ancak ders seçimi süreci kolay olmadı; İngilizce verilen derslerin çoğu yüksek lisans düzeyindeydi, Almanca verilen dersler ise benim mevcut dil seviyemi aşıyordu. Neyse ki, hem Hacettepe'deki hem de Tübingen'deki koordinatörlerimin desteğiyle seviyeme ve ilgi alanıma uygun dersleri seçebildim.

Bazı derslerde başarılı oldum, bunda hocalarımın anlayışlı ve destekleyici yaklaşımı büyük rol oynadı. Örneğin, Doğrusal Cebir dersinden çekilmek zorunda kaldım çünkü ders tamamen Almanca işleniyordu ve bu benim alışık olduğum, dersi derste öğrenme yöntemlerimle uyuşmuyordu. Ayrıca, her hafta verilen ödevlerin dili

ve kapsamı nedeniyle bu dersi takip etmek oldukça zordu.

Buna karşılık, Almanca dil dersimi yüksek motivasyonla tamamladım; günlük hayatta pratik yapma imkânım da olduğu için başarılı bir şekilde geçtim. Dinamik Sistemler dersi ise farklıydı; yüksek lisans seviyesindeydi ve içeriği zorluydu. Ancak hocam zorlandığımı fark edip bireysel destek sağladı. Final sınavında ergodik teori kısmını kendi anlayabildiğim düzeyde ifade ettim ve bu sayede dersi geçtim.

Genel olarak değerlendirdiğimde, lisans eğitiminin erken döneminde Erasmus'a gitmenin akademik açıdan oldukça zorlayıcı olabileceğini düşünüyorum. Yeterli Almanca seviyem olsaydı bile, sistemin yapısı ve derslerin işleniş tarzı bana oldukça farklı geldi. Alman eğitim sisteminde büyümemiş olmak, temel yaklaşımlarına aşina olmamak önemli bir dezavantaj oluşturdu. Daha bireysel, araştırma odaklı bir sistemleri var ve bu, benim alışık olduğum öğrenme tarzından oldukça farklıydı.

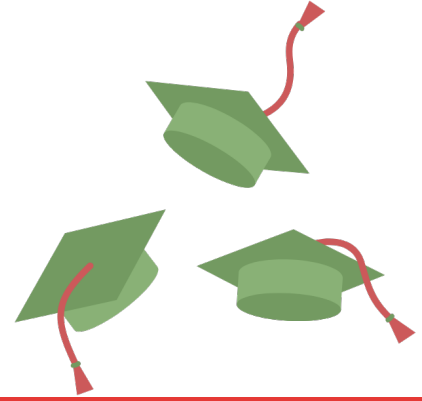
Sosyal ve kültürel açıdan, Erasmus süreci bana birçok farklı milletten insanla tanışma ve dostluk kurma fırsatı sundu. Ortak iletişim dilimiz İngilizceydi; bu, yabancı dil pratiği yapmam açısından çok faydalı oldu. İtalyan ve İngiliz arkadaşarımla düzenlediğimiz kültürel yemek geceleri gibi etkinlikler sayesinde sadece farklı kültürleri tanımakla kalmadım, aynı zamanda kendi kültürümü de paylaşma şansı yakaladım. Beş aylık süreçte Avrupa'nın farklı köşelerini gezme fırsatım oldu ve bu seyahatler bana unutulmaz anılar kazandırdı.

Ekonomik açıdan, Almanya'daki yaşam bizim için Türkiye'ye göre oldukça pahalıydı. Erasmus hibesi elbette destek sağladı ama özellikle konaklama ve temel ihtiyaçlar için ek bütçe yönetimi gerektirdi. Bu durum bana finansal sorumluluk bilinci ve bütçe planlama alışkanlığı kazandırdı. Ucuz marketlerden alışveriş yaparak, öğrenci indirimlerinden faydalanarak ve bisikletli ulaşımı tercih ederek ekonomik dengeyi sağladım.

Karşılaştığım zorluklar arasında bürokratik süreçlerin yavaşlığı, dil bariyerleri ve yalnızlık hissi öne çıkıyordu. Ancak bu zorluklar bana sabırlı olmayı, kendi ayaklarım üzerinde durmayı ve yeni ortamlara daha kolay adapte olmayı öğretti. Başlangıçta çekindiğim dil meselesi zamanla avantaja dönüştü; hem İngilizcemi geliştirdim hem de Almanca konusunda kendime güven kazandım.

Sonuç olarak Erasmus, yalnızca bir öğrenim hareketliliği değil; kendimi keşfetme, kültürler arası anlayış geliştirme ve dünyaya daha açık bir birey olma yolculuğuydu. Bu sürece katkı sağlayan tüm koordinatörlerime, hocalarıma, AB ofisine ve aileme teşekkür ederim. Her üniversite öğrencisinin bu deneyimi yaşamasını içtenlikle tavsiye ederim.

Mezun Hikâyeleri



Matematik bölümünden mezun olan öğrencilerimizin yolları farklı yönlere uzanıyor: akademi, özel sektör, yurt dışı deneyimleri ve daha fazlası... Bu köşemizde, mezunlarımızın hem öğrencilik anılarına hem de mezuniyet sonrası yaşadıklarına kulak veriyoruz. Onların hikâyeleri, hem geçmişe bir selam hem de gelecek öğrencilere ilham niteliğinde.

■ ERSAN KAVAFOĞLU '05 – Meta, Yazılım Mühendisi



 ersan-kavafoglu

Çocukluğumdan beri programlamaya meraklıydım. Hobi olarak başladığım bu ilğim, hayatımın yönünü belirledi. Hacettepe Matematik'ten mezun olduktan yaklaşık bir ay sonra, Maliye Bakanlığı Bilgi İşlem biriminde yazılımcı alımı ilanı açılmıştı. Açıkçası başvuru yaparken “Bilgisayar mühendisleri varken beni neden alsınlar ki?” diye düşündüm. Ancak ailemin “Başvur, en azından bir deneyim olur” ısrarıyla şansımı denedim. Tamamen Java odaklı yazılı sınav ve mülakatlardan geçerek yazılımcı olarak işe alındım.

Belki şaşırtıcı olabilir ama 2007 yılında, Maliye Bakanlığı'nda birçok uluslararası şirketten çok daha güncel yazılım teknolojileri kullanılıyordu. Yüz binlerce kullanıcıya hizmet veren e-devlet sistemini, çağdaş teknolojilerle sıfırdan inşa etmek hem öğretici hem de geliştiriciydi. İki yıl içinde teknoloji takım liderliğine yükseldim. O dönemde birlikte çalıştığım bazı arkadaşlarım bugün Apple, Oracle, Amazon gibi firmalarda mühendislik yapıyor (benden başka bir matematikçi daha var :)).

Maliye Bakanlığı'ndaki görevim sırasında hobi olarak 3D uygulamalar ve oyunlar geliştireyordum. 2010 yılında, boş zamanlarımda Unity için bir sürükle-bırak arayüz geliştirme aracı yazdım.

Bu aracın, Unity için yayımlanan ilk sürükle-bırak editör olduğunu o zaman fark etmemiştim. Hiçbir ticari beklentiyle yola çıkmadan ürünü Unity Asset Store'a gönderdim. Aynı gece, Unity yöneticilerinden gelen beş ayrı e-postayı görünce heyecandan ne yapacağımı şaşırdım. Ürünü çok beğenmişlerdi; görselleri yetersiz bulmalarına rağmen yine de dayanamayıp ana sayfaya koymuşlardı. İlk birkaç saat içinde beş lisans satıldı ve bu, o zamanki aylık maaşıma neredeyse eşdeğerdi. Sonraki birkaç yıl içinde ürün yaklaşık 10.000 geliştirici ve stüdyo tarafından lisanslandı. Electronic Arts, Bioware, Gameforge ve hatta US Air Force gibi kuruluşlar da bu müşteriler arasında yer aldı.

2013 yılında Maliye Bakanlığı'ndan istifa ederek bağımsız mobil oyunlar geliştirmeye başladım. Birkaç yıl içinde beş oyun yayımladım. Ticari başarı elde edemesem de bu süreçten büyük deneyim kazandım.

Daha sonra çevre mühendisliği simülasyonları geliştirmek üzere bir ortağımla birlikte Çınar Yazılım'ı kurduk. Beş kişilik ekibimizle çevre laboratuvar otomasyonu ve Çevre Bakanlığı için hava kirliliği simülasyon yazılımları üzerine çalıştık.

2020 yılında Amazon'un Türkiye işe alım etkinliğine davet edildim. Başarılı geçen mülakat süreci sonunda Dublin'de çalışmaya başladım. 2022 yılında ise Meta'nın Londra ofisine geçiş yaptım ve hâlen burada görev yapmaktayım. Gizlilik sözleşmem nedeniyle projeler hakkında detay veremiyorum; ancak temel olarak artırılmış gerçeklik ve giyilebilir teknolojiler üzerine çalışıyorum. Merak edenler Orion projesine göz atabilir (<https://about.fb.com/news/2024/09/introducing-orion-our-first-true-augmented-reality-glasses/>).



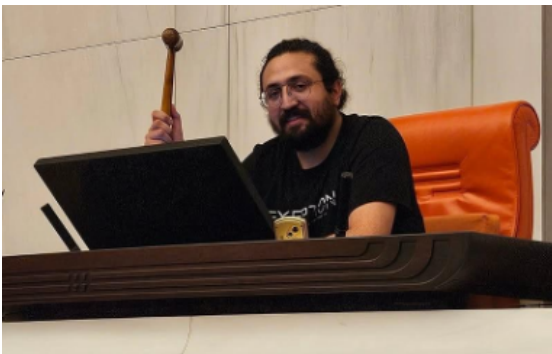
Tüm bu süreçte matematik eğitiminin bana sağladığı altyapı çok büyük bir avantaj sağladı. Özellikle oyun geliştirme ve makine öğrenmesi gibi alanlarda karşılaşılan denklemleri ve yapıları rahatlıkla anlayıp uygulayabiliyorum. Pek çok bilgisayar mühendisinin mesafeli yaklaştığı matematiksel kavramlara aşina olmak, beni öne çıkardı. Özellikle Lineer Cebir ve Diferansiyel Geometri dersleri, 3 boyutlu uygulamalar geliştirirken sıkça karşılaştığım problemlerin çözümünde kilit rol oynadı. Matrisler, vektörler, kuaterniyonlar gibi yapılar bu alanda kullanmanız gereken temel araçlar arasında yer alıyor.

Öğrenci arkadaşlara kendi deneyimlerimden edindiğim ve işe yarayacağına inandığım birkaç önerim var:

- “Bilgisayar mühendisleri benden daha iyidir” gibi düşüncelere kapılmayın. Yazılım öğrenilebilir, ama matematiksel düşünme yeteneği çok daha değerlidir ve nadirdir.
- Başvurun. Ulaşılmaz görünen pozisyonlara bile başvurmaktan çekinmeyin.
- Yaptıklarınızı açık kaynak projelerle ya da küçük ürünler olarak paylaşmaktan çekinmeyin. Sizin ihtiyacınız olmuşsa, muhtemelen başkalarının da ihtiyacı olmuştur.
- Özellikle yapay zeka ve 3 boyutlu yazılımlar gibi matematik temelli alanlarda avantaj sizde olacak. Bu gücünüzü kullanın.
- Hobi projeleri üretmek, bir şeyleri gerçekten anlamanın ve öğrenmenin en iyi yollarından biridir.
- Halen devam ediyor mu bilmiyorum fakat bölümümüzde Java, C, Pascal ve veri yapıları gibi harika temel yazılım dersleri veriliyordu¹. Bu dersler yazılıma başlamak veya geliştirmek için harika bir fırsat.

Matematik eğitimi bana sadece teknik bilgi değil, problem çözme alışkanlığı, sabır ve analitik düşünce kazandırdı. Hacettepe’de aldığım eğitim, bu uzun yolculuğun temel taşlarından biriydi.

■ BURAK ŞİMŞEK '19 – 4HERA Yazılım ve Donanım Sistemleri, Yazılım Geliştirme Yöneticisi



 brokolililer

Üniversite yolculuğum, 2014 yılında Mersin’den Ankara’ya gelmemle başladı. 1 yıl isteğe bağlı hazırlık okudum. Yarım dönem okulu uzatarak 4,5 yılda lisansı tamamladım.

Şu an ses ve görüntü sistemleri üzerine donanım ve yazılım geliştiren bir firmada Yazılım ve Ar-Ge Yöneticisi pozisyonunda çalışıyorum. Videowall Controller, Digital Signage, Otomasyon çözümlerimiz; askeri ve savunma, kamu, güvenlik, bankacılık, kurumsal ve ulaşım gibi pek çok sektörde kullanılmaktadır. Ayrıca, Parlamento ve toplantı odası konferans çözümleri geliştiriyoruz.

Bölümün ilk yılı gerçekten acı vericiydi. Hazırlık okumanın faydası, Ankara’ya adaptasyon ve okula alışmak

konusunda oldu. Eğer Ankara’da ilk seneniz ve Matematik Bölümü okuyorsanız hayat gerçekten çok zor (Cedric). İlk ders seçimi yaptığımda hangi hoca nasıl biri en ufak fikrim yoktu. Ben de isimleri birbirine

¹ Editör Notu: Bölümde Python, C++, Matlab, R, Java programlarının işlendiği seçmeli dersler mevcut!

uyumlu olsun diye sırasıyla Fazilet Hoca, Adnan Hoca ve Nazife Hoca'dan dersleri seçtim. Analiz dersinin ilk haftasında lise matematiğinin tamamı 6 ders saatinde bitmişti. Sonrasında derslerin gerçek yüzünü görmeye başladım. Analiz ve Analitik Geometri bir nebze anlaşılabilir oluyordu. Ama Soyut Matematik gerçekten de kafa karıştırıcıydı. Gerçi Soyut Matematik'teki konuları da mezun olduğum sene "Heeee böyle miymiş yaa" diyerek anladım. Neyse şimdi sorsanız hiçbir şey hatırlamıyorum orası ayrı.

İlk senenin ikinci dönemi Soyut Matematik'te bir çılgınlık yapıp Adnan Hoca'dan Nuri Hoca'ya geçiş yaptık. Tabii o dönem Nuri Hoca da şaşırdı. Şubesi bir anda kalabalıklaştı. Nuri Hoca'nın dersleri o kadar güzel ilerliyordu ki vize dönemi gelene kadar derslerin nasıl geçtiğini anlamadık bile. Yıllarca test çözmeye, soru bankası bitirmeye alışmışız, fakat bu derse nasıl çalışacağız bir türlü anlayamıyoruz. Meşhur mavi kapaklı Soyut Matematik kitabımız dışında pek de ek materyalimiz yoktu. Vizelere, finallere girdik ve çok güzel bir şekilde dersten kaldık. Yanlış hatırlamıyorsam 1 kişi falan geçti. O dönem anladım ki matematiğe çalışmayı öğrenmek farklı bir şey. Dersteyken anladığımı sanıyordum daha sonra yurda döndüğümde o gün anlatılan konuyu bile hatırlamıyordum. Çok büyümlü bir dersti benim için. Derken ilk dönem bitti.

İkinci sınıf başladı. Artık tecrübeliydim ve akademik anlamda ilerlemeyeceğimin bilincine varmışım. O dönem Oğuz Hoca ile Uygulamalı Bilgisayar Cebiri dersinde yollarımız kesişti. Hem yazılım hem de matematik bir aradaydı. Ders ilgimi çok çekmişti. Tabii bazı şeyleri yazılım sektörüne girince daha iyi anladım. O dönem SageMath üzerinden bu dersi işlemiştik. Oğuz Hoca, Cloud / Open Source gibi kavramları alttan alttan bize işlemiş aslında. Dersin işleneceği platformun bulut tabanlı olması sayesinde, hiç bilgisayarı olmayanlar dahi kütüphane gibi ortamlardan bağlanıp dersine çalışabili. Daha sonra ilerleyen dönemlerde seçmeli olarak aldığımız Matematiksel Yazma Becerileri dersini de Bülent Hoca ile Overleaf üzerinden işlemiştik. Bunu bu denli ayrıntılı anlatmamın sebebi, bölümdeki hocalarımızın güncel teknolojileri ve ekosistemleri yakından izleyip bizi onlarla tanıştırmaları sayesinde edindiğim bakış açısını vurgulamak.

Birinci sınıfın sonunda akademik anlamda ilerlemeyeceğimi ve bana göre olmadığını fark edince kendime bir yol haritası çizmem gerektiğini biliyordum. Bilgisayar ve elektronik ile ilkokuldan beri çok sıkı fikiydim. Format atar, crack yapar, bilgisayarına virüs bulaştırırdım. Kasayı söküp temizleyip geri toplardım. Havya ile lehim yapıp analog devreler oluşturdum. Yani bunlara ilgim olduğu için teknoloji alanında güncel olarak yönelebileceğim alanlardan ilki yazılım oldu. Bölümde yazılımla alakalı doğrudan sektöre yönelik dolu dolu bir müfredat yok. Zaten bölümün amacı Matematikçi yetiştirmek. Haliyle bölümdeki seçmeli yazılım derslerinin çoğu matematik problemlerini modelleyerek işleniyordu. Transkriptimde gözüksün belki ileride yazılım geliştiren bir şirkete başvururum düşüncesi ile son sınıfta JAVA dersini almıştım. (Arkadaşlar bu bir şehir efsanesi. Emin olun bunun işe alımda en ufak bir faydası yok.) Bölümde yazılımla ilgilenen arkadaşlarımın sayısı 3-4 kişiden fazla değildi. Onlar da şimdi çok iyi yerlerde ekip lideri, yönetici vb. pozisyonlara geldiler. Nereden veya nasıl başlayacağımı da pek bilmiyordum. Ama Python, Matematiksel Yazma Becerileri'nde dersi işlerken kullandığımız dilin alt yapısında vardı. O yüzden Python öğreneyim dedim. Derken Facebook'ta bulduğum yazılım gruplarına katıldım ve kütüphaneden aldığım farklı diller ile ilgili kitapları incelemeye başladım. Öğrenmesi en kolay görünen PHP oldu. Uzun bir süre PHP ile projeler yaptım. En azından bir yazılım dilini iyi kötü biliyordum. Web arayüz kısmında HTML-CSS-JS üçlüsünü doğru düzgün yazmayı beceremiyordum. Ama hazır şablonlarla entegrasyon yapıyordum. Buradan elde ettiğim sonuç "Ortaya bir ürün çıkartabilmek" oldu. Bu da özgüvenimi artırdı.

Bu arada not olarak belirtmek isterim. İlkokuldan beri var olan bilgisayar kasamı üniversite 3. sınıfa kadar kullandım. Emektar bilgisayarım o dönem bazı high level dillerin IDE'lerini açabilecek ve projeyi derleyebilecek güce sahip değildi. Ben de onu yormayacak dilleri bulmaya çalıştım. Ekonomik olarak gücünüz yok veya bilgisayarınız yeterli performansa sahip değilse bile pes etmeyin lütfen.

Cebirsel Kodlama Teorisi ve Matematiksel Yazma Becerileri derslerinde Bülent Hoca ile tanıştım. Bülent Hoca'yı mühendislik bölümlerinde servis dersleri için giderken görüyordum. Elinde tableti oluyordu hep. Teknoloji ile arasının iyi olduğunu düşündüm. Bu dersler yazılıma olan ilgimi daha da artırmıştı. Çünkü dersi işleyen hoca da teknoloji ile iç içeydi. Aynı dönem Oğuz Hoca ile Kriptoloji dersimde vardı. Orada da blok zincir alanında bir ilerleme sağlamıştık. O dönem gerçekten en verimli zamanlarımda olduğumu anlamıştım. Öğrenci ve öğretmen bire bir çalıştığı tek kotalı dersler vardı. Çalışma Metotları, Bilgisayar Destekli Matematik Projeleri gibi. Bu derslerde dönem başı ödevi alıp dönem sonu teslim etmek yerine haftada 2'şer saat yüz yüze matematik ve yazılım iç içe olacak şekilde çalışmalar yaptık. Web

tabanlı uygulama geliştirdik, Arduino’da programladık, teorik matematik konularına da çalıştık. Siz siz olun bölümdeki hocalarla iletişiminizi kopartmayın. Onların size gelmesini beklemeyin. Siz onlara gidin. Hocalarımızdan öğreneceğimiz çok fazla hayat tecrübesi var.

Günler günleri, aylar ayları, yıllar yılları kovaladı. Derken mezun olamadığımı fark ettim. Çünkü dönemde en fazla 5-6 ders alıyordum. 9-10 ders alıp 4-5’inden kalmaktansa 5-6 ders alıp hepsinden geçmek en doğrusuydu bana göre. Baktım ki eksik derslerim var. Yarım dönem daha uzadı okul. Sonrasında da mezun oldum. Adını anmadığım birçok hocam var her birinin yeri ayrı benim için. Pınar Hocam ile yaptığımız müzikleri, İpek Hocam ile içtiğimiz kahveleri, Ahmet Hocam ile ondan hiç ders alamama rağmen sohbetlerimizi, Talha Hocam, İsmail Hocam, Oğulcan Hocam ile kapı önü sohbetlerimizi, akademik danışmanım Mesut Hoca’mı hiç unutmuyorum. Hepiniz iyi ki varsınız ve hayatıma dokundunuz.

Şimdi soru cevap şekilde bazı konulara değinmek istiyorum. Bölüm benim için çok ama çok dolu geçti. Anlatacak bir sürü anı ve deneyim biriktirdim.

1. Bölümdeki aldığım derslerin mesleğime etkisi oldu mu?

İşin aslı şu ders burada faydalı oldu, bu ders burada faydalı oldu gibi somut örnek veremem. Çünkü bölüm bana bakış açısı kazandırdı. Zaten 1. sınıftan sonra da istediğim şey buydu. Bölümde elbette katma değeri yüksek bir çok ders işleniyor. Ama şimdi bana sorsanız hiçbirini hatırlamam. Ama o dersleri öğrenirken harcadığım zaman ve çalışma disiplininin mesleğime dolaylı yoldan fayda sağladığını söyleyebilirim.

2. Tekrardan üniversite okuyacak olsam Matematik Bölümü’nü tercih eder miyim?

Evet kesinlikle!

3. Bölümde okurken ek işlerde çalıştım mı?

Evet çalıştım. Matematik özel dersi de verdim. Sadece 1 hafta dershanede de çalıştım. Benim matematik özel dersi verdiğim hiçbir öğrenci başarılı olmadı. Çünkü benim öğretebilme kabiliyetim düşüktü. Zaten matematik özel dersini de matematiği zayıf olan öğrenciler alıyor. İyice yorucuydu benim için. Tahammül edemiyordum. Ama matematik özel dersinden daha çok enstrüman özel dersi verdim. Kesinlikle daha keyifliydi. Kafelerde canlı müzik yapıyordum. Yazılım bilgisi olarak ilerledikten süre sonra geliştirdiğim yazılımları da satmaya başlamıştım. Özel ders kadar olmasa da ek bir gelir elde ediyordum.

Hem okuyup hem çalışmak ekonomik olarak size katkı sağlayabilir. Ama bölümünüzdeki derslerden uzaklaşmayın. Farkında olmadan anlamsız bir döngüye giriyorsunuz. Üniversiteyi kazanmak için yıllarca çalışıp bölümü kazanıyorsunuz. Ardından bölümde derslere katılmak yerine dershanelerde öğretmen olarak çalışıyorsunuz. Sizin gibi üniversite kazanmak isteyen derslane öğrencilerine, üniversite öğrencisi olarak öğretmenlik yapıp başladığınız yere geri dönüyorsunuz.

Üniversite yıllarınız kolay kolay geri gelmeyecek. Mümkün olduğunca derslerden ve okuldan uzaklaşmayın. Özel ders vermeyin veya dershanede çalışmayın demiyorum ama bu okulunuzu etkilemesin. Bölümümüzdeki akademik kadro ile kuracağınız bilgi ve tecrübe alışverişinin kıymeti mezun olunca belli oluyor.

4. Bölümde okurken katıldığım topluluklar oldu mu?

Matematik Düşünme ve Araştırma Topluluğu’nda kısa bir süre bulundum. O dönem topluluk yeni kuruluyordu. Sonrasında Robot Topluluğu’na katılmıştım. En son Endüstri ve Sistem Topluluğu’na katıldım. ACM, IEEE gibi topluluklarda vardı. Fakat o dönem bilgisayar mühendisleri tarafından dışlandığımı hissettim ve katılmaya çekindim. Şimdiki aklım olsa o topluluklara da katılırdım. Belki de yazılım öğrenme sürecimde daha çok katkı sağlardı.

5. Staj ve iş bulma sürecim nasıl ilerledi?

Staj ve yarı zamanlı iş başvurularım hep reddedildi. CV’im yazılım sektörü için tüm ihtiyaçları karşılamıyordu. Tabii o dönem bunun farkında değildim. Zor bir şekilde elektronik devre kartı ve donanım geliştiren bir firmada staj yapma şansını buldum. Staj kapsamında Arduino Uno için

Radio Shield PCB (Baskı devre kartı) tasarımı yaptım. Ardından bu kartı Çin’de bastırıp ürün haline getirdim.

İş başvurularımın hepsi reddedildi. Ben de mezun olmaya yakın özel okullarda öğretmenlik, enstrüman eğitmeni, robotik kodlama eğitmeni gibi alanlara başvurdum. Formasyonum olmadığı için okullara kabul edilmem zordu. Ama Ankara’da tek başıma yaşayıp kiramı ödeyebilmek ve geçimimi sağlayabilmek için çalışmak zorundaydım. Mutlaka bir gün yazılım alanına yönelebileceğime inanıyordum. Umudum olmadan bir iş görüşmesine gittim. “1-2 hafta deneme süresi yapalım” dediler. 3. gün işe alındım.

Son olarak, üniversite eğitimi ve çalışma hayatımı göz önüne alarak bölümdeki öğrenci arkadaşlarıma sunları öneririm:

- En az bir tane üniversite topluluğuna katılın.
- İmkânınız varsa Nesin Matematik Köyü’ne bir kez olsun gidin derim. Ben yaz ayında iki dönem gitmiştim.
- Çalıştaylar, paneller, proje yarışmaları vb. etkinliklere katılım sağlayın. Özellikle akademik ağınızın gelişmesinde büyük fayda sağlayacak.
- Kişisel gelişimden uzak kalmayın ve hobi edinin müzik, görsel sanatlar, tiyatro gibi.
- Hata yapmaktan korkmayın.
- Güzel dostluklar kurun, sizin zamanınızı boşa harcayan kişilerden uzak durun. Hayatta geri getiremeyeceğiniz şeylerden bir tanesi de zaman.
- Sporla iç içe olun. Ben bunu biraz geç fark ettim. Sonra bilgisayar başında bir sürü kilo aldım. Verene kadar çok zorluklar çektim.
- Bölümün girişinin solunda bir erik veya elma ağacı vardı. Hâlâ duruyorsa oradan meyve yiyin derim.

■ ZEYNEP BAŞER 20’ – Kilis 7 Aralık Üniversitesi, Araştırma Görevlisi



✉ Zeynep.baser@kilis.edu.tr

Hacettepe Üniversitesi yalnız akademik anlamda değil, aynı zamanda sosyal olarak da zengin bir ortama sahip. Beytepe Kampüsü ise sakin ve yeşil bir kampüs, her şeyden önce böyle bir ortamda öğrenim görmek, ağaçların arasındaki kütüphanede ders çalışmak insanı inanılmaz motive ediyor. Bölümümüze gelecek olursak; akademik kadrosu her alanda zengin bir bölümde okumanın faydasını zaman geçtikçe daha da iyi anlıyorum.

Hem lisans hem de yüksek lisans eğitimimi Hacettepe Üniversitesi’nde yapmış olmak çoğu zaman zorlayıcı, stresli olsa da bu süreç hayatımdaki çoğu konuda inanılmaz gelişme göstermemi, her konuda sabır, merak ve eleştirel bir bakış açısı kazanmamı sağladı. Şu an araştırma görevlisi olarak sürdürdüğüm kariyerimde bunların büyük faydasını görüyorum. İlk iki sene üniversiteye ve derslere alışmanın telaşında zorlu geçti fakat lisans bittikten sonra genelde herkes üniversite ortamından uzaklaşmak istese de üçüncü ve dördüncü sınıfta sevdiğim alanın derslerine yönelerek bu derslerde aldığım keyif ile eğitim hayatıma devam etmek istedim. Bu yüzden cebir alanında yüksek lisansa başladım. Her dersin katkısı farklı derecelerde önemli olsa da lisansüstü eğitime yönelmemde uygulamalı soyut cebir, kriptoloji, oyun teorisi, elementer sayılar teorisi gibi derslerden aldığım keyif çok etkili oldu. Farklı alanlarda çalışan ve alanlarında iyi olan hocalarımızın olması çok büyük avantaj. Şu an akademide olan biri olarak bunun akademik olarak ilerlemek isteyen öğrenciler için büyük bir avantaj olduğunu görüyorum.

Akademiye ilerlemek istediğime karar verdikten sonra lisans eğitimim bitmeden yabancı dil sınavı ve diğer gerekli sınavlara girdim. Ortalamamın düşüklüğü beni zorlarsa da diğer puanlarımı yüksekte tutmak araştırma görevlisi olmamda etkili oldu. Akademide ilerlemek isteyen öğrenciler için benim tavsiyem

kesinlikle lisans sürecindeyken ilgi duydukları alanın dersleri için temellerini iyi oluşturmaları. Bu ileride işleri çok kolaylaştıracaktır. Ayrıca, gerekli ALES ve yabancı dil puanlarını lisans sürecinde alıp ve gerekirse bu sınavlara tekrar tekrar girerek puanlarını yükseltip bu konuda rahat etmeleri çok iyi olur.

Bölümümüzde düzenlenen çeşitli etkinlikler bölüme karşı ilgi ve motiveyi artırırken farklı üniversitelerden gelen akademisyenlerin seminerlerini dinlemek matematiksel olarak güncel kalmamızı sağladı. Son zamanlarda teknolojinin de gelişmesiyle gelişen programlama, AI, kodlama gibi alanların temeli olan bölümümüz artık daha da kıymetli. Mezuniyet sonrası iş imkânımız artık daha da fazla.

Fen bilimlerinde öğrenci olmak çok zor gibi düşünülüyor. Aslında çok çok zor olduğu zamanlar var. Psikolojik olarak da fiziksel olarak da çok zorlayıcı olabiliyor. Ama en sonunda bir teoremi ispatlamak hatta ispata giden ufacık bir adım atmak bütün her şeye değişiyor. İnsanın sevdiği işi yapması her şeyden önemli, ancak işi en iyi bilenlerden öğrenmek büyük bir şans. Bu süreçte kurulan dostluklar da üniversite hayatına ayrı bir güzellik katıyor.

Üniversite deneyimi, hayatımızın en önemli zamanlarından biri. Eğer gerçekten matematik sevmiyorsak bu 4 sene (belki daha fazlası) zulüm gibi gelecektir. Fakat seven birisi için derslerden kalsa da zorlansa da matematik okumanın vereceği keyif her şeye geçecektir. Bu yüzden “matematik” okumak isteyenler için Hacettepe Üniversitesi Matematik Bölümü gerçekten olabilecek en iyi tercihlerden birisi bence.

■ TUĞÇE ALTUNDAĞ ÇAKIRCA 20' – *Anadolu Hayat Emeklilik, Aktüerya Birimi, Kıdemli Uzman Yrd.*



in tuğçe-altundağ-çakırca

Hacettepe Üniversitesi Matematik Bölümü'nde geçirdiğim yıllar, hem kişisel hem de akademik olarak beni en çok dönüştüren dönemlerdi. Matematik her zaman zor ama bir o kadar da tatmin edici bir alandı. Özellikle uygulamalı matematik derslerinde çok keyif aldım; hatta bu süreçte Mustafa Hoca ile birlikte bir makale yazma fırsatı da yakaladım. Bu deneyim, hem araştırma disiplini öğrenmemi sağladı hem de akademik yazım becerilerimi geliştirdi.

Matematik Bölümünde öğrenim görürken, aynı zamanda Aktüerya Bilimleri Bölümünde çift ana dal yaptım. 2020 yılında Matematik Bölümünden, 2021 yılında ise Aktüerya Bilimleri Bölümünden mezun oldum. Matematik altyapım sayesinde Aktüerya ve sonrasında başladığım İstatistik yüksek lisans eğitimimde kendimi çok daha hazırlıklı hissettim. Analitik düşünme becerisi, soyut kavramları somut modellere dönüştürme yeteneği ve sistemli çalışma alışkanlığı, tüm bu süreçte bana güçlü bir temel oluşturdu. Bu sayede farklı disiplinlere daha kolay adapte olabildim ve karşılaştığım karmaşık problemleri daha bütüncül bir yaklaşımla ele alabildim.

2022 yılında Ernst & Young bünyesinde Aktüerya ekibine katıldım. Denetim ve danışmanlık tarafında çalıştım. Aslında matematik mezunları için de açık olan bu alana, bölümde edindiğim altyapı sayesinde rahatlıkla adım atabildim. Temmuz 2025 itibarıyla Ernst & Young'dan ayrılarak Anadolu Hayat Emeklilik Sigorta Şirketindeki yeni görevime geçtim.

Öğrencilere tavsiyem, üniversite hayatlarını sadece derslerle sınırlı tutmamalarıdır. İlgi duydukları farklı alanlara yönelmeleri, çift ana dal ve yan dal olanaklarını araştırarak bu fırsatları değerlendirmeleri, kendilerine hem akademik hem kişisel açıdan çok şey katacaktır. Ayrıca merak duydukları konularda akademisyenlerle iletişim kurmaktan çekinmemelerini, fikir danışmalarını, hatta mümkünse araştırma projelerinde yer alarak deneyim kazanmalarını da önemle tavsiye ederim. Üniversite yılları, hem kendini tanımak hem de ilgi alanlarını keşfetmek için eşsiz bir fırsattır. Bölüm olarak, uygulamalı projelere ve sektörel bağlantılara daha çok yer verilmesinin öğrencilerin mezuniyet sonrası yolculuğuna büyük katkı sağlayacağını düşünüyorum.

Hacettepe Matematik, bana sadece bir diploma değil; analitik düşünmeyi, sabırlı çalışmayı, çok boyutlu bakış açısını ve farklı alanlara geçiş esnekliğini kazandırdı. Bu nedenle her zaman minnettar olacağım. Sorusu olan ya da kariyer yolculuğumla ilgili daha fazla bilgi almak isteyen öğrenciler, LinkedIn üzerinden benimle diledikleri zaman iletişime geçebilirler.

■ ALİ EMİR ERCAN '24 – DefineX, Yazılım Geliştirme Uzmanı



 aliemirercan

Hacettepe Üniversitesi Matematik Bölümü'nden 2024 yılında mezun oldum. Şu anda bir yazılım geliştirici olarak fintech alanında çalışıyorum. Lisans eğitimim boyunca yalnızca matematiğin teorik yönlerine değil, aynı zamanda bilgisayar bilimiyle kesişen alanlara da ilgi duydum. Bu yazıda, Hacettepe'de geçirdiğim yılların kariyerime nasıl yön verdiğini anlatmak ve aynı zamanda mezuniyet sonrası deneyimlerimi paylaşmak istiyorum.

Lisans eğitimime başladığımda yazılım sektörüne dair doğrudan bir kariyer planım yoktu. Bilgisayarlarla her zaman iyi anlaşırdım fakat bunu meslek olarak değerlendirecek kadar önemsememiştim. Temel bilimlerle uğraşmak, bana çok daha anlamlı ve “önemli” bir şeyle meşgul olduğum hissini veriyordu; bu yüzden gelecekteki kariyerimin de bu doğrultuda şekilleneceğini düşünüyordum.

Ancak pandemiyle birlikte herkesin vaktini farklı uğraşlarla doldurmaya çalıştığı o dönemde, ben de bilgisayar bilimlerine yöneldim. O zamana kadar bölümde bazı programlama dersleri almıştım fakat bu derslere pek ciddiyetle yaklaşmamıştım. Pandemi sürecinde ise bu alana, tıpkı matematikteki bir lisans dersi gibi düzenli ve disiplinli şekilde çalışmaya başladığımda, konunun sandığımdan çok daha

derinlikli olduğunu fark ettim. Bilgisayar bilimi yalnızca monitöre bakıp kod yazmaktan ibaret değildi; temel bilimlerle doğrudan ilişkili, kuramsal arka planı güçlü bir alandı. Üstelik diğer temel bilimlerden farklı olarak, öğrendiğiniz kuramsal bilgiyi pratiğe dökme ve sonuçlarını kısa sürede gözlemleme imkânı sunuyordu. Sanırım beni bu alana asıl çeken de tam olarak buydu: teoriden uygulamaya doğrudan geçiş yapabilmenin verdiği tatmin duygusu.

Pandemi sürecinde vaktimi yazılımın birçok alanını keşfetmeye çalışarak geçirdim. Bir yandan temel bilgisayar bilimi konularına odaklanmaya devam ediyordum; çünkü hangi alanda çalışılırsa çalışılsın, bazı temel kavramların mutlaka bilinmesi gerektiğini fark etmiştim. Bu ortak zemini oluşturmak önceliğimdi. Bunun yanı sıra, oldukça dağınık ama öğretici bir merak süreci yaşadım. Bir gün mobil uygulama geliştirmeye ilgi duyup Android Studio indiriyor, birkaç buton yerleştirdikten sonra ilgimi kaybediyordum. Ertesi gün kendimi gömülü sistem programlamasıyla ilgili videolar izlerken buluyordum. Bu çabaların hiçbiri düzenli veya derinlikli değildi elbette; daha çok neye ilgi duyduğumu anlamaya çalıştığım, içgüdüsel bir keşif süreciydi. Geriye dönüp baktığımda, bu deneyimsiz ama samimi denemelerin oldukça faydalı olduğunu söyleyebilirim. Yazılıma yeni başlayan herkese önerebileceğim bir şey varsa, o da şudur: Farklı alanlara temas ederek her konudan biraz fikir sahibi olmak, ilgi alanlarını belirlemede ve ilerleyen dönemlerde daha bilinçli tercihler yapmada büyük katkı sağlıyor.

Bu dönemden sonra ilğim büyük ölçüde web programlamaya kaydı. Zaten o zamanların en popüler konusu da buydu — o dönemlerde büyük dil modelleri henüz yalnızca basit sohbet botlarıydı ve yapay zekâ henüz web teknolojilerinin önündeki tahtı devralmamıştı. Fakat beni web programlamaya çeken esas neden, bu alanın popülerliğinden çok sunduğu esneklikti. Web geliştirme, diğer birçok yazılım alanına kıyasla çok daha az sayıda “genel geçer kural” içerir. Her uygulama ve her kullanım durumu kendi bağlamı içinde değerlendirilir ve bu bağlam zamanla değişebilir. Bu yüzden alınan kararların, yalnızca teknik açıdan değil, uzun vadeli etkileri de düşünülerek verilmesi gerekir.

Aynı işlevi yerine getirecek iki farklı uygulama bile; kullanıcı sayısı, kullanıcıların coğrafi dağılımı, uygulamanın büyüme potansiyeli, zaman ve kaynak kısıtları gibi faktörler doğrultusunda tamamen farklı biçimlerde tasarlanabilir. Genelde tek bir doğru yoktur; bunun yerine birden fazla “yanlış” vardır ve bizim görevimiz bağlama en uygun, en az sorun çıkaracak çözümü bulmaktır. Bu da aslında, matematik bölümü hakkında sıkça söylenen “analitik düşünme yeteneği kazandırır” söyleminin somut karşılığıdır. Web geliştirme süreçlerinde verilen her karar, bu analitik süzgeçten geçirilmiş ve gerekçelendirilmiş olmalıdır ki hem mevcut kaynakları etkili kullanabilelim hem de geleceğe yönelik teknik borcu en aza indirebilelim.

Tüm bu öğrenme sürecinin ardından, yüz yüze eğitime geri döndüğümüzde profesyonel anlamda

ilk işimi yapmak için staj arayışına başladım. O dönemde bölümün düzenlediği bir etkinlikte tanıştığım, mezunlarımızdan birinin referansı ile yaz döneminde ilk stajıma başladım. Staj yaptığım şirket, temel olarak ses ve görüntü sistemlerine odaklanan; hem donanım hem de yazılım geliştiren küçük bir teknoloji firmasıydı. Ekibin küçüklüğü, herkesin birçok farklı işle ilgilenme fırsatı bulduğu oldukça öğretici bir ortam yaratıyordu. Bir gün web uygulaması geliştirirken, ertesi gün masaüstü uygulamalarıyla veya Windows API'leriyle uğraşabiliyordunuz. Bu yönüyle, pandemi dönemindeki keşif sürecimi adeta profesyonel bir bağlamda tekrar yaşıyor gibiydim — ancak bu kez sıkılıp bırakma gibi bir seçeneğim olmadığı için deneyim çok daha derin ve öğreticiydi. Stajımın ardından ekiple çalışmaya devam etme fırsatı buldum ve burada yaklaşık dokuz ay kadar çalıştım.

Daha sonrasında, Türkiye'nin en büyük yazılım danışmanlığı şirketlerinden birine başvurdum ve burada yeni kurulan bir ekipte back-end geliştirici olarak çalışmaya başladım. Bu kez çok daha büyük bir ekibin parçasıydım; ancak önceki işime kıyasla çok daha dar bir alanda, çok daha derinlemesine çalışma imkânı buldum. Geliştirdiğimiz uygulamaların geniş kullanıcı kitlelerine sorunsuz bir şekilde ulaşması gerekiyordu. Bu da, daha önce bahsettiğim "en az yanlış bulma" yaklaşımını, çok daha fazla olasılık arasından dikkatle uygulamamı gerektiriyordu. Bu süreçte, finansal teknolojiler alanında daha önce denenmemiş birçok çözümün parçası olma fırsatı yakaladım ve hâlâ da bu tür yenilikçi çalışmaların içinde yer almaya devam ediyorum. Yaklaşık bir buçuk yıldır bu şirkette çalışmayı sürdürüyorum.

Tüm bu deneyimlerime dayanarak, şu anda bölümde eğitimine devam eden arkadaşların da aklını kurcaladığını düşündüğüm bazı sorulara yanıt vermek isterim. Bunlardan ilki, benim de lisans yıllarında sıkça düşündüğüm şu soruydu: "Temel bilimlerde okumak, yazılım sektöründe bana bir dezavantaj yaratır mı?" Bugünden baktığımda bu soruya gönül rahatlığıyla "hayır" diyebiliyorum.

Temel bilimlerden mezun olmak, yazılım sektöründe ilerlemek için bir engel değil. Elbette bazı kurumsal yapılar (özellikle savunma sanayii gibi belirli alanlar) mühendislik diplomasını şart koşabiliyor. Ancak bunun dışındaki pek çok sektörde, özellikle özel yazılım şirketlerinde ve girişimlerde bu tür bir ayrımın pratikte bir karşılığı yok. Ne kendi kariyerimde ne de benzer yollardan geçmiş çevremde böyle bir engelle karşılaştım. Aksine, yazının başında da değindiğim gibi, matematik eğitiminin kazandırdığı soyut düşünme becerisi, problem çözme disiplini ve analitik yaklaşım yazılım alanında çok sağlam bir temel oluşturuyor.

Ancak bu temel, tek başına yeterli değil. Bilgisayar bilimlerinin kuramsal yönlerine de hâkim olmak büyük önem taşıyor. Bölümümüzde bu altyapıyı destekleyecek 'Veri Yapıları ve Algoritmalar' ve 'Nesneye Yönelik Programlama' gibi dersler açılıyor; bu dersleri mutlaka almanızı tavsiye ederim. Fakat bu dersler başlangıç için iyi bir temel sunsa da, sektöre hazırlık açısından yeterli olmayabilir. Yazılımın yanı sıra donanım, haberleşme, işletim sistemleri ve iş geliştirme gibi bilgisayar mühendisliğine ait temel alanlarda da okuma yapmanız ve genel bir kavrayış geliştirmeniz, sektöre adım atma sürecinizi çok daha kolay ve sağlıklı hâle getirecektir. Aksi takdirde, bu geçiş süreci daha zorlayıcı olabilir.

Bir diğer sıkça sorulan soru ise özellikle son zamanlarda yalnızca temel bilimler öğrencilerinde değil, yazılım sektörüne ilgi duyan pek çok kişide ortaklaşa ortaya çıkıyor: Yapay zekâ devrimiyle birlikte yazılım sektöründe istihdam azalıyor mu? Hâlâ bu alana yatırım yapmak ve kendini bu yönde geliştirmek mantıklı mı? Bu soruya dair farklı kesimlerden çok sayıda görüş ve tahmin duyuyoruz. Ancak ben, bu yorumların büyük çoğunluğunun varsayımdan öteye geçmediğini düşünüyorum.

Kişisel kanaatim, şu an yaşadığımız istihdam sorunlarının yapay zekâ teknolojilerinin gelişimiyle doğrudan ilişkili olmadığı yönünde. Özellikle pandemi döneminde hızlı ve kontrolsüz şekilde büyüyen teknoloji şirketleri, sonrasında gelen ekonomik daralma sürecine uyum sağlamakta zorlandı. Bu durum, doğal olarak işe alımlarda yavaşlamaya ve bazı şirketlerde işten çıkarmalara yol açtı. Öte yandan, mevcut yapay zekâ araçlarının bu sürecin ana nedeniymiş gibi sunulmasının, çoğu zaman bu teknolojileri geliştiren şirketlerin kendi başarılarını pazarlama çabasıyla da ilişkili olduğunu düşünüyorum.

Gerçekte bugün elimizdeki yapay zekâ sistemleri, henüz bağımsız olarak bir kod tabanını emanet edebileceğimiz, uçtan uca sistem geliştirebilecek seviyede değil. Daha çok bir asistan gibi iş görüyor, üretkenliği artıran ama karar verme ve tasarım süreçlerinde hâlâ insan girdisine ihtiyaç duyan araçlar olarak işlev görüyorlar. İleride bu durum değişir mi? Evet, mümkün. Ama öyle bir noktaya gelirse, yalnızca yazılım sektörü değil; ekonomi, üretim, hukuk, eğitim gibi pek çok alan köklü bir dönüşüm geçirecektir. Bu da bizi çok daha kapsamlı, yeni bir toplumsal ve ekonomik yapı tartışmasına götürür.

Bu nedenle, yazılım sektöründe çalışan ve kendine sağlam bir altyapı kazandırmış bir bireyin, hangi koşulda olursa olsun işsiz kalacağına inanmıyorum. Yazılım, hâlâ yatırım yapılması son derece mantıklı bir alan. Üstelik bu alanda başarılı olmanın yolu, yazının başından beri vurguladığım gibi, matematiksel düşünme becerilerini geliştirmekten ve bilgisayar bilimlerinin temelini sağlam atmaktan geçiyor. Günümüzde bu becerilerin önemi azalmıyor, aksine her geçen gün daha da artıyor.

Sonuç olarak, bu yolculuk boyunca edindiğim her deneyim bana şunu gösterdi: Ne geçmişteki tercihleriniz ne de mezun olduğunuz bölüm, tek başına sizi tanımlar. Önemli olan, neye ilgi duyduğunuzu keşfetmek, bu ilginin peşinden istikrarlı bir şekilde gitmek ve değişen koşullara uyum sağlayacak donanımı zamanla inşa edebilmek. Hacettepe Matematik'te kazandığım disiplinli düşünme alışkanlığı, bana yalnızca soyut problemleri değil, gerçek dünya sorunlarını da çözmeyi öğretti. Umarım bu satırlar, kendi yolculuğunuzda hem içinizi rahatlatır hem de size ilham verir.

Sorularınız olursa ya da yalnızca sohbet etmek isterseniz bana her zaman ulaşabilirsiniz.

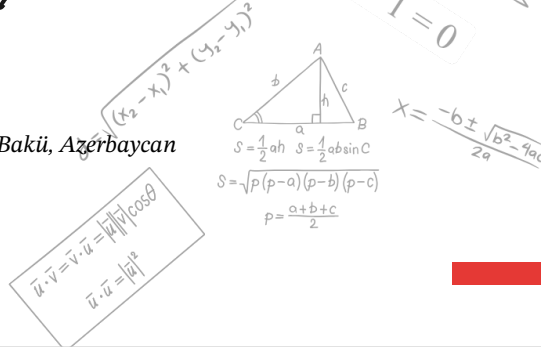
Başarılı ve merak dolu bir yolculuk diliyorum.

Meraklısına Problemler

REFAİL ALİZADE

ADA Üniversitesi Matematik Bölümü, Bakü, Azərbaycan

✉ refailalizade@yahoo.com



Problem 1.

a, b, c sayıları $a^3 + b^3 = 2^c$ eşitliğini sağlayan pozitif tam sayılar olsun. Bu durumda $a = b$ olduğunu kanıtlayınız.

Problem 2.

ABC üçgeni, A köşesinde dik açılı bir üçgen olsun ve $|AB| > |AC|$ koşulu sağlansın. ABC üçgeninin çevrel çemberine A noktasında teğet olan doğru, BC doğrusu ile P noktasında kesişmektedir. P noktası BD doğru parçasının orta noktası olacak şekilde bir D noktası tanımlansın. D noktasından geçen ve AP doğrusu ile paralel olan doğru, ACD üçgeninin çevrel çemberini A dışındaki bir E noktasında tekrar kesmektedir.

Bu durumda A noktasının EBP üçgeninin iç teğet çemberinin merkezi olduğunu gösteriniz.

Problem 3.

Her bir birim karesinde pozitif bir tam sayı bulunan 2016×2016 boyutlarında bir ızgara verilmiştir. Bu ızgara üzerinde aşağıdaki iki tür hamlenin yapılabildiği bir oyun düşünün:

- Bir satır seçip o satırdaki tüm sayıları 2 ile çarpabilirsiniz.
- Bir pozitif tam sayı ve bir sütun seçip, seçtiğiniz sayıyı o sütundaki tüm sayılardan çıkarabilirsiniz.

Bütün sayılar sıfır olduğunda oyunu kazanmış oluyorsunuz. Bu kurallara göre, sonlu sayıda hamleyle oyunu her zaman kazanmak (yani tüm sayıları sıfırlamak) mümkün müdür?

Problem 4.

Aşağıdaki şekilde tanımlanan $a_1, a_2, a_3, \dots$ dizisini ele alalım: $a_1 = 1$ ve $n \geq 2$ için

$$a_n = n - \left\lfloor \sqrt{a_{n-1}} \right\rfloor.$$

Buna göre dizinin a_{800} terimini bulunuz. (Not. Burada $\lfloor x \rfloor$ ile x 'ten küçük ya da eşit en büyük tam sayı gösterilmektedir).

Problem 5.

Altı ardışık tam sayıdan oluşan herhangi bir dizide

$$(x^2 + 1)(x^4 + 1)(x^6 - 1)$$

ifadesi 2016'nın bir tam katı olacak şekilde en az bir x tam sayısı bulunduğunu kanıtlayınız.



HACETTEPE ÜNİVERSİTESİ
FEN FAKÜLTESİ
MATEMATİK BÖLÜMÜ



www.mat.hacettepe.edu.tr



[hacettepe_matematik_resmi](https://www.instagram.com/hacettepe_matematik_resmi)