GALOIS TEORİSİ

İsmail Naci Cangül

Bursa, 2006

1. Giriş

Galois teorisi, polinomlar, cisimler ve gruplar arasındaki ilişkileri ortaya koyan bir matematik dalıdır.

İkinci dereceden bir polinomun köklerini veren meşhur formüller Babilliler zamanında biliniyordu. 16. yüzyılın ortalarında da, üçüncü ve dördüncü dereceden denklemlerin çözümleri ile ilgili formüller ortaya çıkmıştı. Yaklaşık üç yüz yıl sonra, 1824 de Abel; Lagrange ve Cauchy'nin fikirlerinden faydalanarak, beşinci dereceden bir denklem verildiğinde sadece denklemin katsayılarına bazı cebirsel işlemler uygulanarak denklemin köklerini bulmanın mümkün olmadığını ispatladı. Aslında 1799 da Ruffini, aynı sonucu ispatlamıştı. Ancak ispattaki bazı eksiklikler nedeniyle bu ispat geçerlilik kazanamamıştı.

1829 da Abel, herhangi dereceden bir polinomun köklerini veren böyle bir formülün varlığı için yeterli şartları vermişti. Bu sebeple değişmeli gruplara abelyen gruplar da denilmektedir. Bundan kısa bir süre sonra, 1831 de Galois, herhangi bir polinoma karşılık bir grup tanımladı ve bu grubun özelliklerini kullanarak karşılık gelen polinomun köklerinin varlığı için gerekli ve yeterli şartları belirledi. Böylece, herhangi bir polinomun köklerinin varlığı problemi tamamen çözümlenmiş oldu. Aşağıda bu sonuçları inceleyeceğiz.

2. Evariste Galois (25.10.1811-31.05.1832)

Fransız matematikçisi Galois, 1811 de Paris yakınlarında Bourg la Reine'de doğmuştur. Abel'in çağdaşı olan bu matematikçinin doğum ve ölüm tarihlerine bakarsanız 21 yıllık bir ömür sürdüğünü görür ve bu işte bir yanlışlık olduğunu düşünebilirsiniz. Hiçbir yanlışlık yok. Galois'nın hayatı şanssızlıklarla sürüp gitmiş ve 21 yılda tükenmiştir. Daha 16 yaşında iken pek çok matematik klasiğini okumuş olmasına rağmen üniversiteye kabul edilmemiştir. Kendisini gösterebilmek için 17 yaşında zamanın tanınmış matematikçilerinden Cauchy'ye verdiği makalesini Cauchy kaybetmiştir! (bazıları yeni isimlerden pek de hoşlanmaz.) 18 yaşındayken bir yarışmaya soktuğu bir diğer makalesi de, yarışmanın hakemi Fourier ölünce kaybolmuştur... Zorla girebildiği öğretmen okulundan, okul yönetimini eleştirdiği için kovulmuştur. Bir dergiye sunduğu bir başka makalesi, hakem ispatların içinden çıkamadığı için reddedilmiştir. Siyasi nedenlerle de iki kez hapse girip çıkmıştır. Hem Cumhuriyetçi ve hem de miyoptu.

Ve nihayet, ertesi sabah düello edeceği, Paris'in o soğuk mayıs gecesi gelip çatar. Galois henüz 21 yaşındadır. Tüm hayatı siyasi fikirler ve matematik teorileriyle geçmiş bir genç elbette insan öldürme 'sanatı' üzerine bilgisizdir. Öldürüleceğini anlar. Oysa daha kafasındaki matematik fikirlerini olgunlaştıracak zamanı olmamıştır. Bu genç adam insanoğlunun ölümsüzler listesine adını yazdırmak için son kez hamle yapar. Son gecesinde arkadaşı Chavelier'e bir mektup yazar. Bu mektupta Gauss'un kullandığı bazı teknikleri genelleştirerek, derecesi dörtten büyük olan her polinom için işe yarayacak bir 'kök bulma yöntemi' bulmanın neden imkânsız olduğunu anlatır. İçinde kökleri aradığımız sayı sistemleri "cisimler" ile kökleri kendi arasında döndüren permütasyon "grupları" arasında daha önce gözlemlenmemiş ilişkiler bulur. Bu ilişkiler yumağına bugün genel olarak Galois teorisi denir.

Denklemin katsayılarını içine alan sayı sistemine denklemin tüm köklerini teker teker katarak sistemi büyüttüğümüzü düşünelim. Öte yandan tüm kökleri kendi arasında dönüştüren permütasyon grubu ve bu grubun, bazı kökleri sabit bırakan alt gruplarını düşünelim. Galois bu iki dünya arasında köprü kurar ve bir taraftaki kök bulma problemini, öbür tarafta bir grubun yapısını inceleme problemine dönüştürür. Görür ki, eğer bu tarafta kök bulunabiliyorsa öbür tarafta da grubun özel bir yapısı olması gerekir. Oysa bu özel yapının, derecesi dörtten büyük denklemelere karşılık gelen gruplarda, her zaman olmadığını tespit eder.

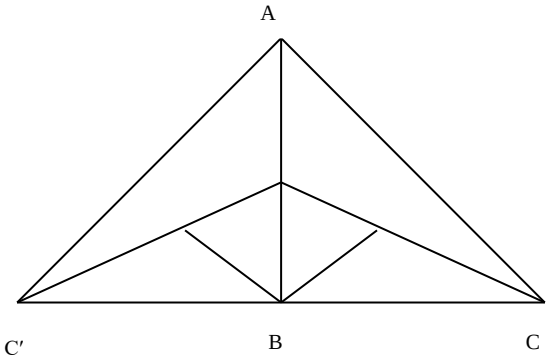
Sonuç olarak insanlığın iki bin yıldır aradığı köklerin, basit cebirsel yöntemlerle bulunamayacağı ortaya konulmaktadır.

Galois'nın mektubu aşağıdaki ifade ile biter: "Bütün bu karmaşık hesapları açmakta kendisine yarar görecek birilerinin çıkacağını umarım." Ertesi gün düelloda vurulur. Hastanede bir gün can çekiştikten sonra ölür. Arkadaşı bu mektubu üç ay sonra yayınlarsa da mektup ilgi görmez. Ancak ölümünden 24 yıl sonra bu genç yaşta ölen adama ilgi duyan bazı matematikçiler onun son mektubunun içindeki karmaşayı çözmekte yarar görürler.

3. Simetriler

Galois, grupları polinomları incelemek amacıyla tanımlamış olsa da günümüzde grupların simetrileri tanımlamanın en net yolu olduğu bilinmektedir. Simetri kelimesinin Yunanca kökü, aynı anda ölçme şeklindedir. Genelde simetri kelimesi, bir bütünün parçalarının birbirlerine ve bütüne göre bir şekilde dengede olması anlamına gelmektedir. Bir anlamda simetri, yapılan düzenlemeye uyum ve estetik kazandırmaktadır. Matematiğin dışında, sanat dallarında da simetri önemli bir yer tutmaktadır.

Simetrinin net bir tanımını vermeden önce, yansıma görüntülerden bahsedelim.



Şekil 1

F ile Şekil 1 deki figürü gösterelim. AB doğrusunu bir ayna gibi düşünürsek, sol tarafın, sağ tarafın bir yansıması olduğunu söyleyebiliriz. Yani sağdaki her bir noktaya karşılık sol tarafta bir tek nokta vardır. C ye karşılık C', D ye karşılık D' noktaları gibi. Bu simetriyi farklı olarak şöyle de canlandırabiliriz. F figürünü harfleri olmadan saydam bir R^2 düzlemine çizelim. Bu düzlemi AB ekseni etrafında döndürdüğümüzü düşünelim. Döndürmeden önce şekli görüp gözlerini kapayan bir kişinin gözlerini tekrar açtığında şeklin çevrildiğini anlaması kesinlikle mümkün değildir. Gerçekten de, F figürünü AB doğrusu y ekseninde, CC' doğrusu da, x ekseninde kalacak şekilde düzleme yerleştirirsek,

$$r : R^2 \to R^2$$
$$(x,y) \to (-x,y)$$

lineer dönüşümü bir yansımadır ve figürü kendisine resmeder. Yani

$$r(F) = F$$

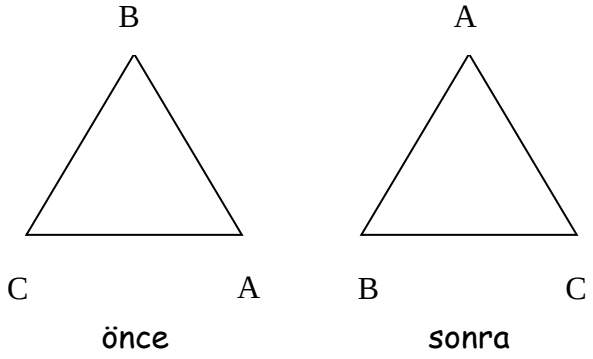
dir.

Diğer yandan, eğer T, merkezi orijinde olan bir çeşitkenar üçgense, T de öyle P noktaları vardır ki P' = r(P) yansıyan görüntüleri T de kalmaz. Yani

$$r(T) \neq T$$

dir.

Bir başka simetri türü de dönmelerdir. Bir Δ eşkenar üçgenini merkezi orijine gelecek şekilde düzleme yerleştirelim. Saat yönünün tersi yönde 120° lik bir ρ dönmesi, Δ üçgenini kendisi üzerine resmedecektir. Yine gözleri kapalı olan birisi üçgenin hareket ettiğini anlayamayacaktır (Şekil 2).



Şekil 2

Eğer düzlemi C kompleks sayılar kümesi ile birebir eşlersek $\rho : C \rightarrow C$ dönme dönüşümü,

$$\rho : re^{i\theta} \rightarrow re^{i(\theta+2\pi/3)}$$

olarak ifade edilebilir. Ayrıca

$$\rho(\Delta) = \Delta$$

dır.

3.1. Tanım. Eğer bir

$$\sigma : R^2 \rightarrow R^2$$

lineer dönüşümü uzaklıkları koruyorsa; yani U ve V noktaları arasındaki uzaklık |U-V| ile gösterilmek üzere

$$|\sigma(U)- \sigma(V)| = |U-V|$$

oluyorsa, σ ya *ortogonal dönüşüm* denilir.

Lineer olmayıp uzaklığı koruyan dönüşümler de mevcuttur. Örneğin, a ve b sabit sayılar olmak üzere

$$(x,y) \rightarrow (x+a,y+b)$$

ötelemesi böyle bir dönüşümdür. Geometrik olarak bu dönüşüm herhangi bir (x,y) vektörünü (x,y) + (a,b) vektörüne taşımaktadır. (aslında her uzaklık koruyan fonksiyonun, yansıma, dönme ve ötelemelerin; ek olarak orijini sabit bırakması durumunda da sadece yansıma ve dönmelerin bir bileşkesi şeklinde olduğu bilinen bir teoremdir).

Her bir σ ortogonal dönüşümünün birebir ve örten olduğu kolayca gösterilebilir. Dolayısıyla σ^{-1} dönüşümü de mevcuttur. Ayrıca σ^{-1} dönüşümünün de ortogonal olduğu kolayca gösterilebilir. Tüm ortogonal dönüşümlerin kümesini $O(2,R)$ ile gösterelim. $O(2,R)$ bileşke işlemine göre bir grup oluşturur. Bu gruba *reel ortogonal grup* adı verilir.

3.2. Lemma. Her bir ortogonal σ dönüşümü açıları korur. Yani, A, V ve B noktaları için A' = σ(A), V' = σ(V) ve B' = σ(B) olmak üzere

$$m(A\hat{V}B) = m(A'\hat{V}'B')$$

şeklindedir.

İspat: İlk olarak V noktasının orijinde olduğu özel durumu ispatlayalım. Bir X vektörünü O da başlayıp X noktasında biten bir vektör gibi düşünelim. Uzunluklar ile noktasal çarpımlar arasındaki

$$|X|^2 = (X,X)$$

bağıntısı hatırlanırsa

$$|A-B|^2 = (A-B,A-B)$$

$$= |A|^2 - 2(A,B) + |B|^2$$

bulunur. A' ve B' için de benzer formüller bulunmaktadır. Ayrıca $|A'-B'| = |A-B|$, $|A'| = |A|$ ve $|B'| = |B|$ olduğundan $(A',B') = (A,B)$ bulunur. Ancak $\theta = m(A\hat{O}B)$ olmak üzere

$$(A,B) = |A||B|\cos\theta$$

olduğu da bilinmektedir. Böylece $m(A\hat{O}B) = m(A'\hat{O}B')$ elde edilir. Fakat σ bir lineer dönüşüm olduğundan

$$O' = \sigma(O) = O$$

olacaktır ve böylece $m(A'\hat{O}B') = m(A'\hat{O}'B')$ elde edilir. Bu da istenilen sonuçtur.

Şimdi de V noktasının orijinde olmaması durumunda AVB açısının değerini belirleyelim. Eğer

$$\tau : W \to W\text{-}V,$$

V noktasını orijine taşıyan öteleme dönüşümü ve

$$\tau' : W \to W + \sigma(V)$$

de orijini $\sigma(V) = V'$ noktasına taşıyan öteleme dönüşümü ise, $\tau'\sigma\tau$ dönüşümü W noktasına uygulanırsa

$$\begin{aligned} \tau'\sigma\tau(W) &= \tau'\sigma(W\text{-}V) \\ &= \tau'(\sigma(W)\text{-}\sigma(V)) \\ &= \sigma(W) - \sigma(V) + \sigma(V) \\ &= \sigma(W) \end{aligned}$$

bulunur. Yani tüm W noktaları için $\sigma(W) = \tau'\sigma\tau(W)$ olduğu ve böylece de $\sigma = \tau'\sigma\tau$ olduğu görülür. τ ve τ' ötelemeleri açıları koruduğundan, bileşke dönüşümü AVB açısını koruyacaktır.

Aşağıdaki tanımda yansıma ve dönme dönüşümlerinin bir genelleştirmesini göreceğiz.

3.3. Tanım. F düzlemde bir figür olsun.

$$\sigma(F) = F$$

olacak şekildeki tüm $\sigma : R^2 \to R^2$ ortogonal dönüşümlerinin ailesi $\Sigma(F)$ ile gösterilir ve *F nin simetri grubu* adını alır. $\Sigma(F)$ in her bir elemanına *F nin bir simetrisi* denilir.

Simetri gruplarının, ortogonal grubun bir altgrubu olduğunu ve böylece de kendi başlarına bir grup olduklarını göstermek kolaydır.

Galois, her bir *f(x)* polinomuna, özellikleri yardımıyla *f(x)* in davranışını anlayabileceğimiz bir grup karşılık getirme fikrini ortaya atmıştı. Bu gruba günümüzde *Galois grup* adı verilmektedir. Bu bölümdeki amacımız, bir çokgenin simetri grubu ile bir polinomun Galois grubu arasındaki benzerliği ortaya çıkarmaktır.

Esas ilgi alanımız Galois grubu olduğundan, burada sadece şu gerçeği hatırlatmak gereklidir. σ bir ortogonal dönüşümse ve U ve V keyfi noktalar ise, U' = σ(U) ve V' = σ(V) olmak üzere UV doğru parçasının görüntüsü yine bir doğru parçası olan U'V' dür. (İspat, W, UV doğrusu üzerinde bir nokta iken

$$|UW| + |WV| = |UV|,$$

ve W, UV üzerinde olmayan bir nokta iken de

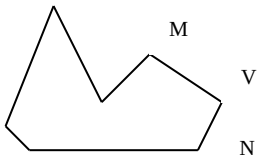
$$|UW| + |WV| > |UV|$$

olduğu şeklindeki, üçgen eşitsizliğinin özel haline dayanmaktadır).

3.4. Lemma. P bir poligon olsun. *Vert(P)* ile P nin köşelerinin kümesini gösterelim. Her bir $\sigma \in \Sigma(P)$ dönüşümü, *Vert(P)* kümesinin bir permütasyonudur.

İspat: V, P nin bir köşesi olsun. Eğer M, V ve N, ardışık köşeler ise, $m(M\hat{V}N) \neq 180^\circ$ dir. Eğer V' = σ(V) denirse V', P nin ya çevresi üzerinde, ya da içinde kalır.

İlk durumda, yani V', P nin çevresi üzerindeyse, Lemma 1 gereği, $m(M\hat{V}N) = m(M'\hat{V}'N')$ olur. Ancak V' bir köşe değilse $m(M'\hat{V}'N') = 180^\circ$ olur ve bu da bir çelişkidir. O halde V', bu durumda bir köşe olmalıdır.



Şekil 3

İkinci durumda ise, yani V' noktası P nin içinde kalıyorsa, merkezi V' noktası olan 2 boyutlu bir D diski, tamamen P çokgeninin içinde kalacak şekilde bulunabilir. σ(P) = P olduğundan D deki her nokta, σ nın görüntüsünde kalır. σ^{-1} de bir ortogonal dönüşümdür ve σ^{-1}(V') = V dir. D diskindeki 0° ile 360° arasındaki her bir açı, bu diskteki belli J ve K noktaları için bir $J\hat{V}'K$ açısı olarak ifade edilebilir. Burada, P deki belli J' ve K' noktaları için $\sigma^{-1}(J\hat{V}'K) = J'\hat{V}K'$ dür. Fakat bu özellikteki açılar

$$0 \leq m(J'\hat{V}K') \leq m(M\hat{V}K)$$

özelliğini sağlar. Yani σ^{-1} ortogonal dönüşümünün korumadığı açılar vardır. Bu ise bir çelişkidir.

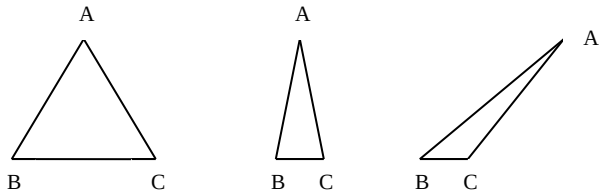
Son olarak her bir V köşesi için $\sigma(V)$ de bir köşedir. Yani σ nın σ_1 kısıtlaması Vert(P) kümesini kendisine resmeder. σ birebir olduğundan σ_1 kısıtlaması da birebirdir. Vert(P) kümesi sonlu olduğundan σ_1 aslında birebir ve örten bir dönüşümdür. Böylece eğer $Vert(P) = \{V_1, V_2, \dots, V_n\}$ ise

$$\{V_1, V_2, \dots, V_n\} = \{\sigma(V_1), \sigma(V_2), \dots, \sigma(V_n)\}$$

$$= \{\sigma_1(V_1), \sigma_1(V_2), \dots, \sigma_1(V_n)\}$$

yazılabileceğinden σ_1 da Vert(P) kümesinin bir permütasyonudur.

3.5. Teorem. P, n köşeli bir çokgen ve $Vert(P) = \{V_1, V_2, \dots, V_n\}$ olsun. Bu durumda $\Sigma(P)$, S_n simetrik grubunun bir altgrubuna izomorfiktir.



Şekil 4

İspat: $\sigma \in \Sigma(P)$ ise, σ nın Vert(P) kümesine kısıtlamasını σ_1 ile gösterelim. Lemma gereği σ_1, Vert(P) kümesinin bir permütasyonudur. Bir başka deyişle, $\sigma_1 \in S_{Vert(P)}$ dir. Bu yüzden σ yı σ_1 e dönüştüren

$$f : \Sigma(P) \rightarrow S_{Vert(P)}$$

dönüşümü, iyi tanımlı bir fonksiyondur.

f in bir homomorfizm olduğunu görmek için $\sigma, \tau \in \Sigma(P)$ alalım. $V \in Vert(P)$ ise, $(\sigma\tau)_1$ ve $\sigma_1\tau_1$ dönüşümlerinin ikisi de V noktasında aynı değeri alırlar. Bu değer de $\sigma(\tau(V))$ dir. Böylece $(\sigma\tau)_1 = \sigma_1\tau_1$ dir ve f bir homomorfizm olur. Yani

$$f(\sigma\tau) = f(\sigma)f(\tau)$$

dur.

Son olarak f birebirdir. Yani Ker f = 1 dir. Çünkü eğer

$$f(\sigma) = \sigma_1 = 1$$

ise o zaman σ her bir $V \in Vert(P)$ köşesini sabit bırakır. Fakat köşeleri R^2 de vektörler olarak düşünürsek, lineer bağımsız olan iki vektör mevcuttur. Bu iki vektör R^2 nin bir tabanını oluşturur. Bu yüzden f, $\Sigma(P)$ ile $S_{Vert(P)} \cong S_n$ in bir altgrubu arasında bir izomorfizmdir.

3.6. Sonuç: Δ, köşeleri A, B ve C olan bir üçgen olsun. Eğer Δ eşkenar bir üçgen ise, $\Sigma(\Delta) \cong S_3$ tür. Eğer Δ sadece bir ikizkenar üçgen ise, $\Sigma(\Delta) \cong Z_2$ dir. Eğer Δ çeşitkenar bir üçgen ise, $\Sigma(\Delta)$ grubunun mertebesi 1 dir.

İspat: Teorem gereği $\Sigma(\Delta)$, S_3 ün bir altgrubuna izomorftur. Eğer Δ eşkenar bir üçgen ise, tam 6 adet simetrisi vardır. Bunlar 3 yükseklik etrafındaki yansımalar ve 0^o, 120^o ve 240^o lik dönme dönüşümleridir. $|S_3| = 6$ olduğundan, $\Sigma(\Delta) \cong S_3$ olduğu görülür. İkinci olarak, Δ bir ikizkenar üçgen olsun. $|AC| = |AB|$ olduğunu kabul edelim. A köşesinden geçen yükseklik etrafındaki yansıma $\Sigma(\Delta)$ da kalmaktadır. Bu özdeşlikten farklı olan tek simetridir. Çünkü her bir σ simetrisi, A açısı B ve C açılarından farklı olduğu için A yı sabit bırakmak zorundadır. Böylece $\Sigma(\Delta) \cong Z_2$ dir. Son olarak, Δ çeşitkenar bir üçgen ise, herhangi bir simetri tüm köşeleri sabit bırakacaktır. Çünkü köşelerdeki açıların hepsi farklıdır. Bu yüzden böyle bir simetri özdeşlik olacaktır.

İleride n tane farklı kökü olan bir polinomun Galois grubunun da S_n in bir altgrubuna izomorf olduğunu göreceğiz. Ayrıca köşelerin simetrilerden kaynaklanmayan permütasyonları olduğu gibi, köklerin de Galois grubundan kaynaklanmayan permütasyonları olabilir. Örneğin, 2.6. Sonuçta bir ikizkenar üçgenin köşelerinin 6 adet permütasyonundan sadece 2 tanesinin simetrilerden kaynaklandığını gördük.

Alıştırmalar

1. F bir kare ise, D_4, 8 mertebeli dihedral grup olmak üzere $\Sigma(F) \cong D_4$ olduğunu gösteriniz.

2. F bir dikdörtgense, $\Sigma(F)$ in Klein-4 grubuna izomorfik olduğunu gösteriniz.

3. $\Sigma(Q) \cong Z_2$ ve $\Sigma(Q') \cong \{e\}$ özelliğinde iki dörtgen bulunuz.

4. Her bir köşesindeki açılar birbirine eşit olan bir çokgene *düzgün çokgen* denilmektedir. Bir P çokgeninin düzgün olması için gerek ve yeter şartın $\Sigma(P)$ nin Vert(P) kümesi üzerinde geçişmeli olarak hareket etmesi olduğunu gösteriniz.

5. P_n ile n köşeli bir düzgün çokgeni gösterelim. $\Sigma(P_n) \cong D_{2n}$ olduğunu gösteriniz.

6. F bir dairesel bölge ise, $\Sigma(F)$ in sonsuz olduğunu gösteriniz.

4. Halkalar

Cisimler ve polinomlar arasındaki ilişkiyi kuran cebirsel yapılar birimli halkalardır. Burada grup, halka, homomorfizm gibi kavramların bilindiğini varsayacağız.

4.1. Tanım. Boş olmayan bir R kümesi üzerinde toplama

$$(r,r') \to r+r'$$

ve çarpma

$$(r,r') \to r.r'$$

işlemleri tanımlı olsun. Eğer

(i) R toplamaya göre değişmeli bir grup;
(ii) Çarpma işlemi birleşmeli ve değişmeli;
(iii) Her $r \in R$ için

$$1.r = r$$

olacak şekilde sıfır elemanından farklı bir $1 \in R$ var;

ve

(iv) Dağılma özelliği: her $r, s, t \in R$ için

$$r(s+t) = rs+rt$$

sağlanıyorsa, R ye *birimli ve değişmeli halka* denilir.

R deki çarpma işlemi göz önüne alınmadığında, R nin *toplamsal grubu* elde edilir.

Bundan sonraki kısımda halka dediğimizde, birimli ve değişmeli bir halkayı anlayacağız.

4.2. Örnek. Bildiğimiz alışılmış toplama ve çarpma işlemleri ile birlikte $\mathbb{Z}$, Q, R ve C kümeleri birer halkadır.

4.3. Örnek. Belirli bir n pozitif tamsayısı için *n modundaki tamsayıların* $\mathbb{Z}_n$ halkasını tanımlayacağız. $\mathbb{Z}_n$ in elemanları, $a \in \mathbb{Z}$ olmak üzere $\mathbb{Z}$ nin

$$[a] = \{ m \in \mathbb{Z} : m \equiv a \ mod \ n \}$$

$$= \{ m \in \mathbb{Z} : m = a + kn, \text{ belli } k \in \mathbb{Z} \}$$

şeklindeki altkümeleridir. [a] kümesine n modunda a nın *denklik sınıfı* denilir. $\mathbb{Z}_n$ deki toplama ve çarpma işlemleri

$$[a] + [b] = [a + b] \quad \text{ve} \quad [a][b] = [ab]$$

ile tanımlanmaktadır ve birim eleman [1] dir. Toplama ve çarpmanın iyi tanımlı olduğu kolayca kontrol edilebilir. $\mathbb{Z}_n$ bu işlemler ile birlikte bir halka oluşturur.

a bir tamsayı ise bölme algoritması gereği, q bir tamsayı ve $0 \leq r < n$ olmak üzere

$$a = qn + r$$

yazılabilir. Yani $a \equiv r \ mod \ n$ dir ve bu durumda [a] = [r] olacağından $\mathbb{Z}_n$ de tam olarak n tane eleman mevcuttur:

$$\mathbb{Z}_n = \{[0], [1], \dots , [n-1] \}.$$

Bu n tane kalan sınıfının ayrık olduğu da kolayca görülebilir.

$\mathbb{Z}_n$ de çalışırken elemanların parantezlerini ihmal etmek bir alışkanlık haline gelmiştir. Dolayısıyla, örneğin $\mathbb{Z}_3$ te $2 + 2 = 1$ yazmak doğru olacaktır.

4.4. Örnek. R bir halka ise *katsayıları R de olan bir f(x) polinomu*nu (kısaca, R üzerinde bir polinomu) tüm i ler için c_i ler R halkasının elemanları ve tüm $i > n$ için $c_i = 0$ olmak üzere bir

$$f(x) = (c_0, c_1, \dots , c_n, 0, 0, \dots)$$

dizisi olarak tanımlıyoruz. Eğer $g(x) = (d_0, d_1, \dots)$, R üzerinde bir başka polinom ise, $f(x) = g(x)$ olması için gerek ve yeter şartın her bir i için $c_i = d_i$ olması olduğu görülür. Bu şekildeki tüm polinomların kümesini R[x] ile gösterelim. R[x] üzerinde toplama ve çarpma işlemlerini aşağıdaki şekilde tanımlayalım:

$$(c_0, c_1, \dots) + (d_0, d_1, \dots) = (c_0+d_0, c_1+d_1, \dots)$$

$$(c_0, c_1, \dots)(d_0, d_1, \dots) = (e_0, e_1, \dots).$$

Burada $e_0 = c_0d_0$, $e_1 = c_0d_1 + c_1d_0$, ve genelde, toplam $i+j = k$ olacak şekildeki tüm i, j ler üzerinden alınmak üzere $e_k = \Sigma\, c_id_j$ şeklindedir.

*Sıfır polinomu*nu **0** ile göstereceğiz ve $(0, 0, \dots)$ olarak tanımlayacağız. Benzer olarak $(1, 0, 0, \dots)$ polinomunu da **1** ile göstereceğiz. R[x] in bir halka olduğunu göstermek rutin fakat uzun bir işlem gerektirmektedir. Bu halkaya *R üzerindeki polinom halkası* denilir.

f(x) gösteriminde x harfinin önemi nedir? x ile R[x] in $x = (0,1,0,0, \dots)$ elemanını gösterelim. $x^2 = (0,0,1,0,0, \dots)$ olduğunu ve tümevarımla x^i elemanının sadece i-inci bileşeni 1, diğer tüm bileşenleri 0 olan bir dizi olduğunu gösterebiliriz. Buradan standart gösterime geçmek te mümkündür:

$$f(x) = (c_0, c_1, \dots, c_n, 0, 0, \dots)$$

$$= (c_0,0,0, \dots)+(0,c_1,0, \dots)+(0,0,c_2,0, \dots)+ \dots$$

$$=c_0(1,0,0, \dots)+c_1(0,1,0, \dots)+c_2(0,0,1,0, \dots)+ \dots$$

$$= c_0 + c_1x + c_2x^2 + \dots + c_nx^n$$

$$= \Sigma\, c_ix^i.$$

Burada x henüz bir değişken değil, halkanın bir elemanı durumundadır. İleride polinom fonksiyonları incelerken x in bir de değişken olarak üstlendiği görevi ele alacağız.

Şimdi $f(x) = c_0 + c_1x + c_2x^2 + \dots + c_nx^n$ yazılımında geçen bazı kavramları hatırlayalım. Eğer f(x) sıfır polinomundan farklı ise, n, $c_n \neq 0$ özelliğindeki en büyük tamsayı olmak üzere, c_n katsayısına *başkatsayı* denilir. n sayısına da *f in derecesi* denilir ve $\partial(f)$ ile gösterilir. Başkatsayısı 1 olan bir polinoma *birim katsayılı polinom* denilir. 0 = (0, 0, ….) sıfır polinomunun başkatsayısı olmadığından dolayı derecesi de mevcut değildir. f(x) in *sabit terimi* c_0 dır. 0 polinomuna veya derecesi 0 olan bir polinoma *sabit (polinom)* denilir. Derecesi 1, 2, 3, 4 ve 5 olan polinomlara sırasıyla *lineer, kuadratik, kübik, kuartik ve kuintik polinomlar* denilir.

4.5. Tanım. $f(x) = \Sigma\, c_ix^i$, bir R halkası üzerinde bir polinom olsun.

$$c_0 + c_1\alpha + \dots + c_n\alpha^n = 0$$

özelliğindeki bir $\alpha \in R$ elemanına *f(x) in R deki bir kökü* denilir.

4.6. Uyarı. $f(x) = x^2-2$, **Q** üzerinde bir polinomdur. Ancak, $\sqrt{2}$ irrasyonel olmasına rağmen $\sqrt{2}$ ye $f(x)$ in bir kökü denilmektedir. Bu sebeple bir $f(x)$ polinomunun bir R halkasındaki köklerinin tanımını, köklerin R den daha büyük bir halkada kalmasına müsaade edecek şekilde genişleteceğiz.

Lineer cebirden biliyoruz ki, bir cisim üzerindeki n bilinmeyenli r tane denklemden oluşan bir lineer denklem sisteminin, $r < n$ iken aşikar olmayan bir çözümü mevcuttur. $r = n$ iken bir determinantın hesaplanması gereklidir. Eğer

$$f(x) = (x-\alpha_1) \dots (x-\alpha_n) = \Sigma\, c_i x^i$$

şeklinde ise n sayısına tümevarım uygulayarak

$$c_{n-1} = -\sum_i \alpha_i$$

$$c_{n-2} = -\sum_{i<j} \alpha_i\alpha_j$$

$$c_{n-3} = -\sum_{i<j<k} \alpha_i\alpha_j\alpha_k$$

$$\vdots$$

$$c_0 = (-1)^n \alpha_1 \dots \alpha_n$$

elde edilir. Böylece $f(x)$ polinomunun $\alpha_1, \dots, \alpha_n$ köklerini $c_1, \dots, c_n$ katsayılarından elde etme problemi, n bilinmeyenli n denklemden oluşan lineer olmayan bir sistemin çözülmesi problemine dönüşür. $n \geq 5$ iken bu problemin "köklerle çözümü"nün olmadığını göstereceğiz.

4.7. Teorem. R bir halka olsun.

(i) R halkasındaki birim tektir.
(ii) Her $r \in R$ için $0.r = 0$ dır.
(iii) Eğer $-r$, $r \in R$ nin toplamsal tersi, yani $-r + r = 0$ ise

$$-r = (-1)r$$

dir.
(iv) Her $r \in R$ için

$$(-1)(-r) = r$$

dir. Özel olarak $(-1)(-1) = 1$ dir.

İspat. **(i)** Varsayalım ki $e \in R$, her $r \in R$ için $er = r$ özelliğinde olsun. Özel olarak $r = 1$ iken $e1 = 1$ olur. Fakat 1 in tanımı gereği $e1 = e$ dir. Bu iki eşitlikten $e = 1$ bulunur.

(ii) Dağılma özelliği gereği

$$0.r = (0+0).r = 0.r + 0.r$$

ve iki taraftan $0.r$ yi çıkararak $0.r = 0$ elde ederiz.

(iii) $$0 = 0.r = (-1+1).r = (-1).r + r$$

eşitliğinde iki tarafa $-r$ ekleyerek istenilen sonucu elde ederiz.

(iv) $$0 = 0.(-r) = (-1+1)(-r) = (-1)(-r) - r$$

eşitliğinde iki tarafa r eklenirse sonuç görülür.

Farz edelim ki, halka tanımındaki $1 \neq 0$ şartında ısrar etmeyelim. Yani R "halka"sında $1 = 0$ olsun. Eğer $r \in R$ ise

$$r = 1.r = 0.r = 0$$

olacağından R sadece bir tek elemandan oluşur. Bu cebirsel sistem ilginç olmadığından bir halka olarak ele alınmayabilir.

Şimdi de bir halkada sıfırla bölmenin neden yasak olduğunu görebiliriz. Eğer $a, b \in R$ ise, a/b elemanı, şayet mevcut olsaydı, R nin

$$b(a/b) = a$$

olacak şekildeki bir elemanı olurdu. Ayrıca b ile bölme işlemi, b ile çarpmanın ters işlemidir. Özel olarak eğer $1/0$ mevcut olsaydı, bu eleman $0.(1/0) = 1$ olacak şekilde bir eleman olurdu. Fakat Teorem 4.7 (i) gereği, $0.(1/0) = 0$ da olduğunu biliyoruz. Böylece $1 = 0$ elde edilir ki bu bir çelişkidir.

4.8. **Tanım**. Bir R halkası ve bir S altkümesi verilsin. Eğer S kümesi çıkarma ve çarpmaya göre kapalı ise ve 1 elemanını bulunduruyorsa, S ye R nin bir *alt halkası* denilir.

Örneğin, $\mathbb{Z}$, $\mathbf{Q}$ nun; $\mathbf{Q}$, $\mathbf{R}$ nin; $\mathbf{R}$ de $\boldsymbol{C}$ nin bir alt halkasıdır. R bir halka ise, $R' = \{(r, 0, 0, \ldots) : r \in R\}$ kümesinin $R[x]$ in bir alt halkası olduğunu kolayca gösterebiliriz. R' genelde R ile özdeşlenir ve bu sayede yukarda verilen alt halka zinciri biraz daha uzatılabilir. Yani $\boldsymbol{C}$ de $\boldsymbol{C}[x]$ in bir alt halkasıdır.

Alıştırmalar

1) Bir R halkasının alt halkalarının herhangi sayıdaki kesişiminin de bir alt halka olduğunu gösteriniz.

2) Herhangi bir R halkasında Binom açılımının geçerli olduğunu ispatlayınız: $n \geq 1$ ise $\binom{n}{i}$ = n!/i!(n-i)! Binom katsayısı olmak üzere

$$(a + b)^n = \Sigma \binom{n}{i} a^i b^{n-i}$$

dir. (Yol gösterme: $\binom{n-1}{i-1} + \binom{n-1}{i} = \binom{n}{i}$ olduğunu kullanınız).

3) p asalsa $i \neq 0$ ve $i \neq p$ için p nin $\binom{p}{i}$ sayısını böldüğünü gösteriniz.

4) R bir halka ve $f(x) \in R[x]$ olsun.

$$f(x) = r_0 + r_1x + ... + r_nx^n$$

şeklindeyse f in **türevi**

$$f'(x) = r_1 + 2r_2x + ... + nr_nx^{n-1}$$

olarak tanımlanır.

$$[f(x) + g(x)]' = f'(x) + g'(x)$$

ve

$$[f(x)g(x)]' = f'(x)g(x) + f(x)g'(x)$$

olduğunu gösteriniz.

5) R bir halka ve S herhangi bir küme olsun. R^S ile S den R ye tüm fonksiyonların kümesini gösterelim. R^S kümesinde aşağıdaki şekilde noktasal toplama ve çarpmayı tanımlayalım:

$$f + g : s \to f(s) + g(s)$$

ve

$$fg : s \to f(s)g(s)$$

olsun. Bu işlemler ile birlikte R^S kümesinin bir halka olduğunu gösteriniz.

5. Tamlık Bölgeleri ve Cisimler

İki tip halka oldukça önemlidir. Bunlar tamlık bölgeleri ve cisimlerdir.

5.1. Tanım. Bir R halkasında sıfırdan farklı herhangi iki elemanın çarpımı da sıfırdan farklı oluyorsa R ye bir *tamlık bölgesi* denilir.

5.2. Örnek. $\mathbb{Z}_6$ bir tamlık bölgesi değildir. Çünkü $[2] \neq 0$ ve $[3] \neq 0$ olmasına rağmen $[2][3] = [6] = 0$ dır.

5.3. Teorem. Bir R halkasının bir tamlık bölgesi olması için gerek ve yeter şart *sadeleştirme kuralının* gerçeklenmesidir. Yani, eğer $ra = rb$ ve $r \neq 0$ ise $a = b$ dir.

İspat. R bir tamlık bölgesi olsun. $ra = rb$ ve $r \neq 0$ olsun. Bu durumda $r(a-b) = 0$ dır. R bir tamlık bölgesi olduğundan $a-b = 0$ olmalıdır. Yani $a = b$ olur.

Tersine R de sadeleştirme kuralı geçerli olsun. R de sıfırdan farklı r ve a elemanlarının $r.a = 0$ olacak şekilde bulunduğunu varsayalım. Bu durumda

$$r.a = 0 = r.0$$

eşitliğinden $a = 0$ bulunur ki bu bir çelişkidir.

5.2. Örneği genelleştirebiliriz:

5.4. Teorem. $\mathbb{Z}_n$ in bir tamlık bölgesi olması için gerek ve yeter şart n nin asal olmasıdır.

İspat: Eğer n asal değilse birleşik bir sayıdır ve dolayısıyla $1 < a, b < n$ olmak üzere $n = ab$ şeklinde yazılabilir. Buradan [a] ve [b] sıfırdan farklı olmak üzere

$$[a][b] = [ab] = [n] = 0$$

elde ederiz ki bu $\mathbb{Z}_n$ in bir tamlık bölgesi olmadığını gösterir.

Tersine, p asal iken $\mathbb{Z}_p$ nin bir tamlık bölgesi olduğunu göstermek istiyoruz. Eğer $\mathbb{Z}_p$ de $[a][b] = 0$ ise bu $ab \equiv 0$ (p) anlamına gelir. Yani p, ab nin bir bölenidir. O

halde p, ya a nın ya da b nin bir bölenidir. Başka bir deyişle [a] = 0 veya [b] = 0 dır.

Bir halkada çarpımsal terse sahip olan elemanlar önemlidir:

5.5. Tanım. u, R halkasının bir elemanı olsun. Eğer uv = 1 olacak şekilde bir $v \in R$ elemanı varsa u ya R de bir *birim* denilir.

2, $\mathbb{Z}$ de bir birim değildir. Çünkü $2.\frac{1}{2} = 1$ olmakla beraber $\frac{1}{2} \notin \mathbb{Z}$ dir. Bununla beraber 2, $\mathbb{Q}$ da bir birimdir.

Şimdi sıfırdan farklı her eleman ile bölme yapabileceğimiz bir halka sınıfını tanımlayacağız. s ile bölmenin aslında s nin s^{-1} tersi ile çarpma anlamına geldiğine dikkat edelim. Yani $r \div s = rs^{-1}$ dir. O halde birimlerle bölme her zaman mümkündür.

5.6. Tanım. Sıfırdan farklı her $r \in R$ elemanının bir birim olduğu bir R halkasına *cisim* denilir.

$\mathbb{Z}$ deki birimler 1 ve -1 dir. Bu yüzden $\mathbb{Z}$ bir cisim değildir. Ancak $\mathbb{Q}$, $\mathbb{R}$ ve $\mathbb{C}$ birer cisimdir.

5.7. Teorem. p asal ise $\mathbb{Z}_p$ bir cisimdir.

İspat. $[a] \in \mathbb{Z}_p$ olsun. Eğer $[a] \neq 0$ ise a tamsayısı p ile bölünemez. (a,p) = 1 olduğunu göstermek istiyoruz. p asal olduğundan pozitif bölenleri sadece 1 ve p dir. O halde aranan obeb ya 1 ya da p dir. p, a yı bölmediğinden (a,p) = 1 olmalıdır. Böylece 1 sayısını a ve p nin bir lineer toplamı şeklinde ifade edebiliriz. Yani

$$1 = sa + tp$$

olacak şekilde s ve t tamsayıları vardır. Buradan $sa - 1 = -tp$ yazabiliriz ve bu da $sa \equiv 1 \ (p)$ anlamına gelir. Denk olarak

$$[1] = [sa] = [s][a]$$

olduğundan [a] nın çarpmaya göre tersi [s] dir. Yani $\mathbb{Z}_p$ bir cisimdir.

Her bir cismin bir tamlık bölgesi olduğu açıktır. Gerçekten de ra = rb ve r sıfırdan farklı ise, r nin tersi r^{-1} mevcut olacağından

$$r^{-1}ra = r^{-1}rb$$

ve böylece de a = b buluruz. Bu iddianın tersi ise yanlıştır. Yani her tamlık bölgesi bir cisim olmayabilir. Örneğin $\mathbb{Z}$ bir tamlık bölgesi olmasına rağmen bir cisim değildir.

Bir F cisminin her bir R alt halkası bir tamlık bölgesidir. Ayrıca, r ve s, R nin elemanları ise, aynı zamanda F nin de elemanlarıdır. Eğer $r \neq 0$, $s \neq 0$ iken $rs = 0$ olsaydı bu durumda az önce ispatlamış olduğumuz, her cismin bir tamlık bölgesi olduğu gerçeği ile çelişiriz.

Şimdi her bir tamlık bölgesinin, bir cismin alt halkası olarak düşünülebileceğini göstereceğiz.

5.8. Teorem. Her bir R tamlık bölgesi için R yi bir alt halka olarak bulunduran bir $Frac(R)$ cismi mevcuttur. Ayrıca, her bir $q \in Frac(R)$ elemanı, $a, b \in R$ ve $b \neq 0$ olmak üzere

$$q = ab^{-1}$$

şeklinde yazılabilir.

İspat. $Frac(R)$ cismini R den, $\mathbb{Q}$ yu $\mathbb{Z}$ den elde ettiğimiz gibi elde edeceğiz. İlk olarak X ile $b \neq 0$ olacak şekildeki tüm $(a,b) \in R \times R$ sıralı ikililerinin kümesini gösterelim. X üzerinde bir "içler dışlar çarpımı" bağıntısını

$$ad = bc \text{ ise } (a,b) \sim (c,d)$$

şeklinde tanımlayalım. Bu bir denklik bağıntısıdır. (a,b) elemanının denklik sınıfını a/b ile gösterelim. $\{a/b : a, b \in R \text{ ve } b \neq 0\}$ kümesini de $Frac(R)$ ile gösterelim.

$Frac(R)$ üzerinde toplama ve çarpma işlemlerini aşağıdaki şekilde tanımlayalım:

$$a/b + c/d = (ad + bc)/bd \quad \text{ve} \quad (a/b)(c/d) = ac/bd.$$

Burada R bir tamlık bölgesi olduğundan $bd \neq 0$ dır. Bu işlemlerin iyi tanımlı olduklarını kontrol etmek zor değildir. Gerçekten de $a'/b' = a/b$ ve $c'/d' = c/d$ ise $a'/b' + c'/d' = a/b + c/d$ ve $(a'/b')(c'/d') = (a/b)(c/d)$ dir. $Frac(R)$ kümesinin bir cisim olduğu da kolayca gösterilebilir. Özel olarak a ve b, R nin sıfırdan farklı elemanları iken a/b nin tersinin b/a olduğunu göstermek de zor değildir.

Bir $a \in R$ elemanını $a/1$ "kesiri" ile özdeşlersek, R yi $Frac(R)$ nin bir alt halkası olarak düşünebiliriz.

Son olarak, eğer $q \in Frac(R)$ ise $q = a/b = a(1/b) = ab^{-1}$ elde ederiz ki bu istenilen sonuçtur.

5.9. Tanım. R bir tamlık bölgesi ise $Frac(R)$ kümesine *R nin kesir cismi* denilir.

$\mathbb{Q} = \text{Frac}(\mathbb{Z})$ olduğu açıktır. K bir cisim ise Frac(K[x]) kümesine *K üzerindeki rasyonel fonksiyonların cismi* denilir ve

$$\text{Frac}(K[x]) = K(x)$$

ile gösterilir. K(x) in elemanları, f(x) ve g(x), K[x] te kalmak ve $g(x) \neq 0$ olmak üzere f(x)/g(x) şeklindedir.

Alıştırmalar

1) (i) R bir halka olsun. R deki tüm birimlerden oluşan U(R) kümesinin çarpmaya göre bir grup olduğunu gösteriniz. U(R) ye bazen *R deki birimlerin kümesi* denilir.

(ii) Bir R halkasının bir cisim olması için gerek ve yeter şartın $R^* = R - \{0\}$ kümesinin çarpmaya göre bir grup olması olduğunu gösteriniz. (Burada $R^* = U(R)$ olduğuna dikkat ediniz)

2) $a \in \mathbb{Z}$ ise, [a] nın $\mathbb{Z}_n$ de bir birim olması için gerek ve yeter şartın (a,n) = 1 olması olduğunu gösteriniz. Birimlerin $U(\mathbb{Z}_n)$ grubunun mertebesinin $\varphi(n)$ olduğu sonucunu elde ediniz.

3) $f(x), g(x) \in R[x]$ olsun. f(x).g(x) in sabit teriminin f(x) ve g(x) polinomlarının sabit terimlerinin çarpımı olduğunu gösteriniz.

4) (i) R bir tamlık bölgesi ise bu taktirde f(x).g(x) in baş katsayısının f(x) ve g(x) polinomlarının baş katsayılarının çarpımı olduğunu ispatlayınız. R bir tamlık bölgesi iken f(x) ve g(x) polinomları R[x] de sıfırdan farklı ise bu taktirde

$$\partial(fg) = \partial(f) + \partial(g)$$

olduğunu gösteriniz.

(ii) R bir tamlık bölgesi ise bu taktirde R[x] in de bir tamlık bölgesi olduğunu ispatlayınız.

(iii) $R = \mathbb{Z}_4[x]$ ise $(2x+1)^2 = 1$ olduğunu gösteriniz. R bir tamlık bölgesi değilken

$$\partial(fg) = \partial(f) + \partial(g)$$

formülünün, R[x] de yanlış olabileceğini gösteriniz.

(iv) f(x) ya da g(x) sabit olmamak üzere, $R = \mathbb{Z}_4[x]$ de $x = f(x)g(x)$ şeklinde bir çarpanlara ayırmanın mümkün olduğunu gösteriniz.

5) $A = R[x]$ olmak üzere $A[y]$ kümesini, R üzerinde iki değişkenli polinomların halkası olarak tanımlayalım ve $R[x,y]$ ile gösterelim. Tümevarım yöntemiyle R üzerinde ikiden fazla değişkene sahip polinomları tanımlayabiliriz. R bir tamlık bölgesi ise, $R[x_1, \ldots, x_n]$ in de bir tamlık bölgesi olduğunu gösteriniz. (F bir cisim iken $Frac(F[x_1, \ldots, x_n])$ kümesi $F(x_1, \ldots, x_n)$ ile de gösterilir)

6) R bir tamlık bölgesi ve $f, g \in R$; $u, v \in R$ için

$$f = ug \quad \text{ve} \quad g = vf$$

şartını sağlayan sıfırdan farklı elemanlar olsun. $uv = 1$ olduğunu ve u ve v nin birimler olduğunu ispatlayınız.

7) **(i)** F bir cisim ise, $F[x]$ deki birimlerin sıfırdan farklı sabitler olduğunu ispatlayınız.

(ii) $\mathbb{Z}_2[x]$ in tam bir tane birime sahip olan sonsuz bir halka olduğunu gösteriniz.

(iii) $\mathbb{Z}_4[x]$ de birim olan fakat sabit olmayan bir polinom örneği veriniz.

8) (i) Polinomlar için bölme algoritmasını ispatlayınız: R bir halka, $f(x), g(x) \in R[x]$ ise ve $g(x)$ in baş katsayısı bir birim ise bu taktirde $R[x]$ de

$$f(x) = q(x)g(x) + r(x)$$

olacak şekilde $q(x)$ ve $r(x)$ polinomları vardır ve ayrıca $r(x) = 0$ ya da $\partial(r) < \partial(g)$ dir.

(ii) R bir tamlık bölgesi ise, bölme algoritmasında ortaya çıkan bölüm ve kalanın tek olduğunu ispatlayınız (bu özellikleri sağlamayan **R** ya da $\mathbb{Z}_4$ gibi halkalar vardır).

9) Bir R halkasının bir F alt cismi, R nin cisim olan bir alt halkasıdır. R halkasının bir X altkümesinin bir alt cisim olması için gerek ve yeter şartın, X in 1 i bulundurması ve X in çıkarma, çarpmaya göre kapalı olması ve tersleri bulundurması olduğunu gösteriniz.

10) Alt cisimlerin herhangi bir ailesinin kesişiminin de bir alt cisim olduğunu gösteriniz (bu kesişimin en azından 1 i bulundurması sebebiyle $\{0\}$ olmadığına dikkat ediniz).

11) (i) $\mathbb{Z}_p[x]$ in $\mathbb{Z}_p$ yi alt cisim olarak bulunduran bir sonsuz tamlık bölgesi olduğunu gösteriniz.

(ii) $\mathbb{Z}_p$ yi bir alt cisim olarak bulunduran bir sonsuz cisim bulunduğunu gösteriniz.

12) $R[x]$ in hiç bir zaman bir cisim olamayacağını gösteriniz.

13) $\mathbb{Z}_n$ in bir cisim olması için gerek ve yeter şartın n nin asal olması olduğunu gösteriniz.

6. Homomorfizm ve İdealler

Bir halkadan diğerine olan dönüşümleri çalışmak bazen oldukça kullanışlıdır.

6.1.Tanım. R ve S herhangi iki halka olsun. Her $r, r' \in R$ için bir

$$\varphi : R \to S$$

fonksiyonu

$$\varphi(r + r') = \varphi(r) + \varphi(r');$$
$$\varphi(r.r') = \varphi(r).\varphi(r');$$
$$\varphi(1) = 1$$

şartlarını sağlıyorsa φ ye bir *halka homomorfizmi* (ya da *halka dönüşümü*) denilir.

Bir $\varphi : R \to S$ halka homomorfizmi birebir ve örten ise *izomorfizm* adını alır. Bu durumda, R ve S ye *izomorfik* denir ve $R \cong S$ şeklinde yazılır.

Sıradaki iki örnek, daha önce verdiğimiz bazı özdeşlemelerin izomorfizmler ile daha kolay anlaşılabileceğini gösterir.

6.2.Örnek. R bir halka ise bu taktirde $R' = \{(r,0,0, ...) : r \in R\}$, R[x] in bir alt halkasıdır ve

$$\varphi : r \mapsto (r, 0, 0, ...)$$

ile tanımlı $\varphi : R \to R'$ fonksiyonu R den R′ ye bir izomorfizmdir.

6.3.Örnek. R, F = Frac(R) kesir cismine sahip bir tamlık bölgesi olsun. Buna göre $R'' = \{r/1 \in F: r \in R\}$ nin F nin bir althalkası olduğunu görmek kolaydır ve

$$\varphi : r \mapsto r/1$$

dönüşümü R den R″ ye bir izomorfizmdir.

6.4.Örnek. $\pi : a \mapsto [a]$ ile tanımlı $\pi : \mathbb{Z} \to \mathbb{Z}_n$ dönüşümü örten bir halka dönüşümüdür.

6.5.Tanım. $\varphi : R \to S$ bir halka dönüşümü ise bu taktirde φ nin *çekirdeği* (*kernel*)

$$\ker \varphi = \{r \in R: \varphi(r) = 0\}$$

şeklinde tanımlanır. φ nin *görüntüsü*

$$\text{im } \varphi = \{s \in S: \text{bir } r \in R \text{ için } s = \varphi(r)\}$$

olarak tanımlanır.

$\varphi : R \to S$ bir halka homomorfizmi ise, $\ker \varphi$ nin R nin toplamaya göre bir alt grubu olduğunu ve çarpmaya göre kapalı olduğunu görmek kolaydır (1 i bulundurmadığı için bir alt halka değildir). Ancak $\text{im } \varphi$, S nin bir alt halkasıdır. Grup teorisinde bir homomorfizmin çekirdeği yalnızca bir alt grup değil, aynı zamanda bir normal alt gruptur. Benzer şekilde halka teorisinde de çekirdeklerin bazı ek özellikleri mevcuttur.

6.6.Tanım. R halkasının bir *ideali*

(i) $a, b \in I$ ise $a - b \in I$
(ii) $a \in I$ ve $r \in R$ ise $ra \in I$

olacak şekilde, sıfırı da bulunduran bir alt kümedir.

R halkasında $I \neq R$ ise I ya bir *has ideal* denilir. Her R halkası, R ve $\{0\}$ ideallerini bulundurur.

6.7.Teorem. $\varphi : R \to S$ bir halka homomorfizmi ise bu taktirde $\ker \varphi$, R de bir has idealdir. Üstelik φ nin birebir olması için gerek ve yeter şart $\ker \varphi = \{0\}$ olmasıdır.

İspat: R ve S halkalarındaki çarpma işlemi dikkate alınmaz ve sadece bunların toplamaya göre değişmeli gruplar olduğu hatırlanırsa bu taktirde φ bir grup homomorfizmi olarak düşünülebilir ve böylece $\ker \varphi$, R grubunun toplamaya göre bir alt grubudur. Eğer $a \in I$ ve $r \in R$ ise, bu taktirde

$$\varphi(ra) = \varphi(r).\varphi(a) = \varphi(r).0 = 0$$

olur. Buna göre, $ra \in \ker \varphi$ ve böylece $\ker \varphi$, R de bir idealdir. $\varphi(1) = 1 \neq 0$ olduğundan $\ker \varphi \neq R$ olduğunu görürüz ve bu durumda $\ker \varphi$ bir has idealdir.

φ birebir ise bu taktirde farklı noktalar farklı görüntülere sahiptir. Keyfi bir $r \neq 0$ elemanı alınırsa bu taktirde $\varphi(r) \neq \varphi(0) = 0$ dır. O halde $r \notin \ker \varphi$ ve $\ker \varphi = \{0\}$ olur. Tersine, $\ker \varphi = \{0\}$ olduğunu kabul edelim. $\varphi(r) = \varphi(r')$ ise bu taktirde

$$0 = \varphi(r) - \varphi(r') = \varphi(r-r');$$

olur. Yani $r-r' \in \ker \varphi = \{0\}$ ve böylece $r = r'$ bulunur. Dolayısıyla φ birebirdir.

Alıştırmalar

1) R bir cisim ise $a \mapsto a/1$ ile verilen $R \to Frac(R)$ dönüşümünün bir izomorfizm olduğunu ispatlayınız. Tersine, R bir tamlık bölgesi ve $a \mapsto a/1$ dönüşümü bir izomorfizm ise bu taktirde R nin bir cisim olduğunu gösteriniz.

2) $\varphi : R \to S$ tamlık bölgeleri arasında bir izomorfizm ise $a/b \mapsto \varphi(a)/\varphi(b)$ ile tanımlı $Frac(R) \to Frac(S)$ şeklinde bir izomorfizm olduğunu gösteriniz.

3) R, F cisminin bir alt halkası olsun ve K, F nin R yi bulunduran bütün alt cisimlerinin kesişimi olsun. $K \cong Frac(R)$ olduğunu ispatlayınız.

4) (i) $\varphi : R \to S$ bir izomorfizm ise bu taktirde $\varphi^{-1} : S \to R$ de bir izomorfizmdir. Gösteriniz.

(ii) $\varphi : R \to S$ ve $\psi : S \to T$ halka homomorfizmleri ise bu taktirde onların bileşkesi olan $\psi\varphi : R \to T$ dönüşümü de bir homomorfizmdir.

5) $a \in R$, R de bir birim ise ve $\varphi : R \to S$ bir halka dönüşümü ise, $\varphi(a)$ nın da S de bir birim olduğunu gösteriniz.

6) (i) R bir halka ise, f(x) in sabit terimi c_0 olmak üzere

$$\varphi : f(x) \mapsto c_0$$

şeklindeki $\varphi : R[x] \to R$ dönüşümünün bir halka dönüşümü olduğunu gösteriniz.

(ii) ker φ yi hesaplayınız.

7) (i) $\sigma : R \to S$ bir halka dönüşümü ise

$$\sum r_i x^i \mapsto \sum \sigma(r_i) x^i$$

ile tanımlı olan $\sigma^* : R[x] \to S[x]$ dönüşümünün de bir halka dönüşümü olduğunu gösteriniz.

(ii) $\tau : S \to T$ bir halka dönüşümü ise, $(\tau\sigma)^* : R[x] \to T[x]$ dönüşümünün $\tau^*\sigma^*$ dönüşümüne eşit olduğunu gösteriniz.

(iii) σ bir izomorfizm ise σ^* ın da bir izomorfizm olduğunu gösteriniz.

8) (i) R deki ideallerin herhangi bir ailesinin kesişimi de R de bir idealdir. X, bir R halkasının herhangi bir altkümesi ise, (X) ile gösterilen ve X i içeren bir en küçük idealin var olduğunu gösteriniz. (X) idealine *X in ürettiği ideal,* yani R de *X i bulunduran tüm ideallerin kesişimi* denir.

(ii) "(X), X i bulunduran bir ideal ise ve eğer J, R de X i bulunduran bir ideal ise bu taktirde $(X) \subset J$ dir" ifadesini ispatlayarak (X) in, X i bulunduran en küçük ideal olduğunu gösteriniz.

9) (i) $a \in R$ ise, $\{ra: r \in R\}$ kümesinin a ile üretilmiş bir ideal olduğunu gösteriniz (Bu ideale *a ile üretilen temel ideal* denilir ve (a) ile gösterilir).

(ii) $a_1, ..., a_n,$ bir R halkasının elemanları ise

$$I = \{r_1a_1 + ... + r_na_n: \ r_i \in R, i = 1, ..., n\}$$

şeklindeki tüm lineer toplamların kümesinin $\{a_1, ..., a_n\}$ tarafından üretilen ideal olan $(a_1, ..., a_n)$ e eşit olduğunu gösteriniz.

10) u, R halkasında bir birim olsun.

(i) Bir I ideali u yu bulunduruyorsa I = R olduğunu gösteriniz.

(ii) $r \in R$ ise bu taktirde (ur) = (r) dir. Özellikle F bir cisim iken R = F[x] deki sıfırdan farklı her (f(x)) temel ideali, baş katsayısı 1 olan bir polinom ile üretilebilir. Gösteriniz.

(iii) R bir tamlık bölgesi ve $r, s \in R$ ise, (r) = (s) olması için gerek ve yeter şartın R deki bir u birimi için s = ur olması olduğunu gösteriniz.

11) R halkasının bir cisim olması için gerek ve yeter şartın R nin tek has idealinin {0} olması olduğunu ispatlayınız.

12) (i) $\mathbb{Z}[x]$ halkasındaki çift sabit terime sahip tüm f(x) dönüşümlerinin I kümesi, $\mathbb{Z}[x]$ de bir idealdir. Bu ideal, x ve 2 nin tüm lineer kombinasyonlarından oluşur; yani I = (x,2) dir. Gösteriniz.

(ii) (x,2) nin $\mathbb{Z}[x]$ de bir temel ideal olmadığını gösteriniz.

13) F bir cisim ve S bir halka ise, bu taktirde her $\varphi : F \to S$ halka dönüşümü birebir olmalıdır ve im φ, S nin F ye izomorfik bir alt cismidir.

7. Bölüm Halkaları

I, R de bir ideal olsun. Bir an için çarpma işlemini göz ardı edelim. I, R toplam grubunun bir altgrubudur. Üstelik R nin değişmeli olması I nın bir normal altgrup olduğunu, ve böylece R/I bölüm grubunun varolduğunu gösterir. R/I bölüm grubunun elemanları, $r \in R$ olmak üzere r+I kosetleridir ve toplama işlemi

$$(r+I) + (r'+I) = (r+r') + I$$

şeklinde verilir. Özel olarak, sıfır elemanı 0+I = I dır. Ayrıca, r+I = r'+I olması için gerek ve yeter şartın $r - r' \in I$ olması olduğunu hatırlayalım. Sonuçta $\pi : R \to R/I$ doğal dönüşümü, $r \mapsto r + I$ ile tanımlanan bir örten grup homomorfizmidir.

7.1.Teorem. I, R halkasında bir has ideal olsun. Bu taktirde R/I toplamsal değişmeli grubuna çarpma işlemi eklenerek, bir halka haline getirilir ve

$$\pi : R \to R/I$$

doğal dönüşümü, örten bir halka homomorfizmi olur.

İspat : R/I üzerindeki çarpmayı

$$(r+I)(r'+I) = rr' + I$$

ile tanımlayalım. Bu işlemin iyi tanımlı olduğunu görmek için $r + I = s + I$ ve $r' + I = s' + I$ olduğunu kabul edelim. $rr' + I = ss' + I$ olduğunu, yani $rr' - ss' \in I$ olduğunu göstermeliyiz. Ancak

$$\begin{aligned} rr' - ss' &= (rr' - rs') + (rs' - ss') \\ &= r(r' - s') + (r - s)s' \end{aligned}$$

dir. Şimdi hipotez gereği $r' - s' \in I$ ve $r - s \in I$ dır. Böylece, I bir ideal olduğundan, $r(r' - s') \in I$ ve $(r - s)s' \in I$ dır. Son olarak, I nın iki elemanının toplamı yine I dadır ve istenildiği gibi $rr' - ss' \in I$ ve $rr' + I = ss' + I$ dır.

R/I değişmeli grubunun bu çarpma işlemiyle birlikte bir halka olduğunu ve özel olarak birim elemanının 1+I olduğunu görmek sıradan bir işlemdir. I bir has ideal

olduğundan $1 \notin I$ ve böylece $1+I \neq 0+I=0$ dır. $(r+I)(r'+I)=rr'+I$ formülü, $\pi : r \to r+I$ doğal dönüşüm iken $\pi(r)\pi(r')=\pi(rr')$ olduğunu ifade eder. Bu sonuçta, π nin bir örten halka homomorfizmi olduğunu ifade eder.

7.2.Tanım. I, R halkasında bir ideal ise, R/I ya *I modunda R nin bölüm halkası* denir.

Aşağıdaki 1. alıştırmada, R = $\mathbb{Z}$ ve I = (n), n ile üretilen temel ideal, olmak üzere, $\mathbb{Z}_n$ in R/I bölüm halkasına eşit olduğunu göreceğiz.

7.3.Örnek. R = F[x], F cismi üzerindeki polinom halkası olsun. I ideali,

$$I = \{f(x)p(x): f(x) \in F[x]\}$$

olacak şekilde derecesi n olan özel bir p(x) polinomu ile üretilen bir esas ideal olsun. $g(x) \in F[x]$ ise Bu taktirde bölme algoritmasından, r(x) ve q(x) polinomları F[x] de, r = 0 veya $\partial(r) < n$ olacak şekilde kalmak üzere

$$g(x) = q(x)p(x) + r(x)$$

yazılır. g(x) + I = r(x) + I olduğuna dikkat edilirse, I nın kendisi hariç her bir kosetin, derecesi n den küçük bir temsilciye sahip olduğu kabul edilebilir. Gerçekten, her bir koset, derecesi n den küçük olan bir tek r(x) temsilcisine sahiptir: eğer aynı özellikte ikinci bir r′(x) olsaydı, bu taktirde $r - r' \in I = (p)$ olurdu. Böylece, $p \mid (r - r')$ dir ve belli bir $f(x) \in F[x]$ için $r - r' = pf$ olur. Ancak, $r - r'$ nün derecesi $n = \partial(p)$ den küçüktür ve bu $\partial(pf) \geq \partial(p)$ oluşu ile bir çelişkidir. R/I daki çarpma işlemi, r(x), f(x)g(x) in p(x) ile bölümünden kalan olmak üzere

$$(f(x)+I)(g(x)+I) = f(x)g(x) + I = r(x) + I$$

şeklinde basitleştirilebilir.

7.4.Örnek. Bir önceki örnekteki F = **R** ve $p(x) = x^2+1$ olması durumunu ele alalım. I = (x^2+1) olmak üzere, **R**[x]/I daki her bir eleman, x^2+1 in derecesi 2 olduğundan, a, b $\in$ **R** için a+bx+I formundadır. Ayrıca

$$(a+bx+I)(c+dx+I) = (a+bx)(c+dx)+I$$

$$= ac+(bc+ad)x+bdx^2+I$$

dır. $x^2 \equiv -1$ (p(x)) olduğundan

$$x^2+I = -1+I$$

şeklindedir. Bu ise

$$(a+bx+I)(c+dx+I) = ac-bd+(bc+ad)x+I$$

olduğunu gösterir.

Artık **R**[x]/I gerçekten bir cisimdir. a ve b, sıfırdan farklı olmak üzere, a+bx+I nın çarpmaya göre tersinin $c = \frac{a}{\left(a^2+b^2\right)}$ ve $d = \frac{-b}{\left(a^2+b^2\right)}$ için c+dx+I şeklinde olduğunu göstermek kolaydır. $a+bx+I \mapsto a+bi$ ile tanımlanmış $\varphi: R[x]/I \to C$ dönüşümünün bir cisim homomorfizmi olduğunu göstermek zor değildir. Özel olarak, $i^2 = -1$ özelliğindeki sanal i sayısı x+I kosetine eşittir.

7.5.Teorem. (Birinci İzomorfizm Teoremi): φ : R $\to$ S dönüşümü, ker φ = I özelliğinde bir halka homomorfizmi ise bu taktirde r + I $\mapsto \varphi(r)$ ile verilen R/I $\to$ im φ şeklinde bir izomorfizm vardır.

İspat : R ve S deki alışılmış çarpmayı bir an için göz ardı edersek, bu taktirde gruplar için birinci izomorfizm teoremi, ϕ : r+I $\mapsto \varphi(r)$ ile tanımlı ϕ : R/I $\to$ im φ fonksiyonunun toplam grupları arasında bir izomorfizm olduğunu belirtir. $\phi(1+I) = \varphi(1) = 1$ olduğundan, ϕ nin çarpma işlemini koruduğu ispatlanırsa ispat tamamlanacaktır. Şimdi r, r′ $\in$ R ise bu taktirde φ bir halka dönüşümü olduğundan

$$\phi((r+I)(r'+I)) = \phi(rr'+I) = \varphi(rr') = \varphi(r)\varphi(r')$$

dür. $\phi(r+I)\phi(r'+I) = \varphi(r)\varphi(r')$ olduğundan

$$\phi((r+I)(r'+I)) = \phi(r+I)\ \phi(r'+I)$$

elde edilir.

Grup teoride olduğu gibi burada da bir karşılık getirme teoremi vardır. Ayrıca, halkalar için ikinci ve üçüncü izomorfizm teoremleri de vardır. Ancak bu teoremler, grup teorisindeki benzerlerinden daha az ilginçtir.

Alıştırmalar

1) n bir pozitif tamsayı ve I = (n), Z de n ile üretilen temel ideal olsun. Bu taktirde Z/I bölüm halkasının Z_n e eşit olduğunu gösteriniz.

2) R bir halka ve I = (x), R[x] te x ile üretilen temel ideal ise R[x]/I $\cong$ R olduğunu gösteriniz.

3) Halkalar için karşılık gelme teoremini ispatlayınız: "I, bir R halkasında bir ideal ise, I $\subset$ J $\subset$ R olacak şekildeki J ideallerinin kümesi ile R/I daki tüm ideallerin ailesi arasında π : R $\to$ R/I doğal dönüşüm olmak üzere

$$J \to \pi(J) = J/I = \{a+I : a \in J\}$$

şeklinde bir birebir örten dönüşüm bulunur." Ayrıca $J \subset J'$ ise $\pi(J) \subset \pi(J')$ dür.

4) I, R halkasında bir ideal; J, S halkasında bir ideal ve $\varphi : R \to S$, $\varphi(I) = J$ özelliğinde bir halka izomorfizmi olsun. $\varphi' : r+I \to \varphi(r)+J$ fonksiyonunun R/I dan S/J ye bir izomorfizm olduğunu gösteriniz.

8. Cisimler Üzerinde Polinom Halkaları

8.1. Teorem. F bir cisim ise F[x] teki her bir ideal bir temel idealdir.

İspat. I, F[x] te bir ideal olsun. $I = \{0\}$ ise $I = (0)$ dır. Yani 0 ile üretilen temel idealdir. Eğer $I \neq \{0\}$ ise, I da derecesi en küçük olan bir m(x) polinomu seçelim. $I = (m(x))$ olduğunu göstermek istiyoruz.

$(m(x)) \subset I$ olduğu açıktır. Tersine I da bir f(x) elemanı alalım. Bölme algoritması gereği, $r(x) = 0$ veya $\partial(r) < \partial(m)$ olmak üzere

$$f(x) = q(x)m(x) + r(x)$$

olacak şekilde q(x) ve r(x) polinomları vardır. $r(x) = f(x) - q(x)m(x) \in I$ dır. $r(x) \neq 0$ ise, bu durumda m(x) in I daki en küçük dereceli polinom oluşu ile çelişiriz. O halde $r(x) = 0$ dır ve $f(x) = q(x)m(x) \in (m(x))$ elde ederiz.

F bir cisim olduğundan buradaki m(x) polinomunu baş katsayısı 1 olan bir polinom olarak seçebiliriz.

8.2. Tanım. R bir halka olsun. Eğer R, her ideali bir temel ideal olan bir bölge ise, R ye bir *temel ideal bölgesi* denilir.

Örneğin Z bir temel ideal bölgesidir. 8.1. Teoreme göre, F bir cisim iken F[x] de bir temel ideal bölgesi olur. Ancak Z[x] bir temel ideal bölgesi değildir (gerçekten de, 7. bölümün sonundaki 12. problemde Z[x] te sabit terimi çift olan tüm polinomlardan oluşan I idealinin bir temel ideal olamayacağını belirtmiştik).

8.3. Tanım. R bir halka ve r ile s, R de iki eleman olsun. Eğer $rr' = s$ olacak şekilde bir $r' \in R$ mevcutsa, *r, s yi böler* veya *s, r nin bir katıdır* denilir. Bu durumda $r|s$ yazılır.

$r|s$ olması için gerek ve yeter şartın s nin r ile üretilen temel ideale yani (r) ye ait olması olduğuna dikkat ediniz. Her $r \in R$ için örülür $r|r$ ve $r|0$ olduğu, fakat $0|r$ olması için gerek ve yeter şartın $r = 0$ olması olduğu, ve son olarak r nin bir birim olması için gerek ve yeter şartın $r|1$ olduğu tanımdan görülür.

8.4. Tanım. R bir tamlık bölgesi ve $f(x), g(x) \in R[x]$ olsun. $f(x)$ ve $g(x)$ in *en büyük ortak böleni (obeb),*

- $d(x)$, $f(x)$ ve $g(x)$ in bir ortak böleni, yani, $d|f$ ve $d|g$;
- $c(x)$, $f(x)$ ve $g(x)$ in bir başka ortak böleni iken $c|d$,

ve

- $d(x)$ in başkatsayısı 1

özelliklerine sahip bir $d(x) \in R[x]$ polinomudur.

$d(x)$ genelde (f,g) ile de gösterilir. $(f,g) = 1$ ise *f(x) ile g(x) aralarında asaldır* denilir.

f ile g nin d ile gösterilen obebi, eğer mevcutsa, bir tektir. Gerçekten de, d' bir başka obeb ise, d' nün sadece bir ortak bölen olduğu kullanılarak $d'|d$; d nin bir ortak bölen olduğu kullanılarak da $d|d'$ elde edilir. O halde sıfırdan farklı belli bir u sabiti için $d' = ud$ yazılabilir. Ancak d ve d' birim başkatsayılı polinomlar olduğundan $u = 1$ ve $d = d'$ bulunur.

Eğer f ve g polinomlarının bir lineer toplamı 1 ise (bu toplam a(x) ve b(x) iki polinom olmak üzere $1 = a(x)f(x) + b(x)g(x)$ şeklinde olsun) bu durumda f ve g aralarında asal olmalıdır. Gerçekten de f ve g yi bölen bir ortak c(x) böleninin 1 i de bölmesi gerekeceğinden c bir birim olacaktır. Şimdi, F bir cisim iken F[x] te obebin her zaman bir lineer toplam şeklinde olduğunu göreceğiz.

8.5. Teorem. F bir cisim ve $f(x)$ ve $g(x)$ $(\neq 0)$, F[x] te iki eleman olsun. Bu durumda $d(x) = (f(x),g(x))$ obebi mevcuttur ve $f(x)$ ile $g(x)$ in bir lineer kombinasyonudur. Yani,

$$d(x) = a(x)f(x) + b(x)g(x)$$

olacak şekilde $a(x)$ ve $b(x)$ polinomları mevcuttur.

İspat. $I = \{ a(x)f(x) + b(x)g(x) : a(x), b(x) \in F[x]\}$

kümesinin F[x] te hem $f(x)$ hem de $g(x)$ i bulunduran bir ideal olduğunu 9. alıştırmada gördük. F bir cisim olduğundan F[x] bir temel ideal bölgesidir ve I bir temel idealdir. 10. alıştırma gereği $I = (d(x))$ olacak şekilde başkatsayısı 1 olan bir $d(x)$ polinomu mevcuttur. I nın her bir elemanı gibi, d de f ve g nin bir lineer toplamı şeklindedir. $f, g \in I = (d)$ olduğundan d, f ile g nin bir ortak bölenidir. Son olarak, eğer c bir ortak bölen ise, $c|f$ ve $c|g$ dir. Yani $f = cc'$ ve $g = cc''$ şeklindedir. Böylece

$$d = af + bg = acc' + bcc'' = c(ac' + bc'')$$

yazılabilir ve bunun da anlamı $c|d$ dir. Sonuç olarak, $d(x)$ obebdir.

8.6. Örnek. F bir cisim ve I, belli bir $p(x)$ polinomu tarafından üretilen temel ideal olmak üzere $R = F[x]/I$ olsun. $f(x)$ ile $p(x)$ aralarında asal ise,

$$s(x)f(x) + t(x)p(x) = 1$$

olacak şekilde $s(x), t(x) \in F[x]$ polinomları mevcuttur. Bu eşitlik R de

$$s(x)f(x) + I = 1 + I$$

haline dönüşür. Böylece $f(x) + I$, R de, tersi $s(x) + I$ olan bir birimdir.

Ters ifade de doğrudur. Gerçekten de, eğer $f(x) + I$, R de bir birim ise, bu durumda $1 + I = (f(x) + I)(g(x) + I) = f(x)g(x) + I$ olacak şekilde $g(x) \in F[x]$ mevcuttur. Buradan, belli bir $h(x) \in F[x]$ için

$$f(x)g(x) - 1 = h(x)p(x)$$

yazabiliriz. Yani $f(x)$ ile $g(x)$ aralarında asaldır.

8.7. Sonuç (Euclid Lemması). F bir cisim olsun. Eğer $p(x) \in F[x]$ indirgenemezse ve $p(x)$, $q_1(x). \ldots . q_n(x)$ çarpımını bölüyorsa, bu durumda $p(x)$, belli bir j için $q_j(x)$ i de böler.

İspat. $n > 1$ e tümevarım uygulayacağız. $(f(x),g(x)) = 1$ iken $f(x)$, $g(x)h(x)$ çarpımını bölüyorsa, bu durumda $f(x)$ in $h(x)$ i böldüğünü göstereceğiz. $1 = af + bg$ olacak şekilde $a(x)$ ve $b(x)$ polinomlarının olduğunu biliyoruz. Böylece $h = afh + bgh$ olur. Varsayım gereği, belli bir k polinomu için $gh = fk$ yazılabileceğinden $h = afh + bfk = f(ah + bk)$ olup $f|h$ elde ederiz.

Teorem 8.5 in ispatı göz önüne alınırsa aşağıdaki sonuç elde edilir. Bu aynı zamanda, obebin neden (f,g) şeklinde gösterildiğini de açıklayacaktır.

8.8. Sonuç. F bir cisim ve $f(x), g(x) \in F[x]$ olsun. Eğer $f(x)$ ve $g(x)$ ile üretilen ideal $I = (f(x),g(x))$ ise, $f(x)$ ile $g(x)$ in obebi $d(x)$ olmak üzere $I = (d(x))$ dir.

Euclid lemmasının ispatı, Z deki Euclid lemmasının çok benzeridir. Bu durum, şimdi ispatlayacağımız Euclid algoritması için de geçerlidir: Verilen $f(x)$ ve $g(x)$ polinomlarının obebi nasıl bulunur? Bu obeb, lineer toplam olarak nasıl ifade edilebilir?

8.9. Teorem (Euclid algoritması). Obebi hesaplamaya yarayan ve onu bir lineer toplam olarak ifade etmeyi sağlayan algoritmalar mevcuttur.

İspat. Fikir tamamen bölme algoritmasının ardarda uygulanmasından ibarettir. Aşağıdaki eşitlikleri ele alalım.

$$
\begin{aligned}
f &= q_1 g + r_1 && \partial(r_1) < \partial(g)\\
g &= q_2 r_1 + r_2 && \partial(r_2) < \partial(r_1)\\
r_1 &= q_3 r_2 + r_3 && \partial(r_3) < \partial(r_2)\\
&\ldots && \ldots\\
r_{n-2} &= q_n r_{n-1} + r_n && \partial(r_n) < \partial(r_{n-1})\\
r_{n-1} &= q_{n+1} r_n + r_{n+1} && \partial(r_{n+1}) < \partial(r_n)\\
r_n &= q_{n+2} r_{n+1}
\end{aligned}
$$

Burada q_i ve r_i lerin bölme algoritmasıyla açıkça bilindiğine dikkat ediniz. İddia ediyoruz ki $d = r_{n+1}$ dir. İlk olarak, bu ardışık bölmelerin belli bir adımda sona ereceğini gözlemleyelim. Bunun sebebi kalanların derecelerinin her bir adımda küçülmesidir. Dolayısıyla $\partial(g)$ adımdan daha az adımda bu iterasyonlar sona erecektir. İkinci olarak, d bir ortak bölendir. Çünkü, $d = r_{n+1}$, r_n i böler ve böylece $(n+1)$-inci eşitlikten, yani $r_{n-1} = q_{n+1} r_n + r_{n+1}$ eşitliğinden, $d | r_{n-1}$ buluruz. Eşitliklerde bu şekilde sondan başa ilerleyerek $d|g$ ve $d|f$ olduğunu elde ederiz. Üçüncü olarak, c bir ortak bölen ise, bu sefer listenin tepesinden başlayarak ve aşağıya doğru ilerleyerek $c|f$ ve $c|g$ den ilk olarak $c|r_1$ olduğunu; $c|g$ ve $c|r_1$ den $c|r_2$ olduğunu ve belli bir adımdan sonra $c|r_{n+1}$ olduğunu elde ederiz. Yani d, aranan obebdir.

Sonuçta a ve b, sondan başa gidilerek bulunabilir. Böylece d, $d = r_{n+1} = r_{n-1} - q_{n+1} r_n$ şeklinde r_{n-1} ile r_n in bir lineer toplamıdır. $r_{n-2} = q_n r_{n-1} + r_n$ oluşu kullanılarak d yi bu sefer r_{n-2} ile r_{n-1} in bir lineer toplamı olarak

$$d = r_{n-1} - q_{n+1}(r_{n-2} - q_n r_{n-1})$$

$$= (1+q_n q_{n+1}) r_{n-1} - q_{n+1} r_{n-2}$$

elde ederiz. Bu işleme d yi f ile g nin bir lineer toplamı şekline getirene kadar devam edilir.

Uygulamada, Euclid algoritması çok kullanışlı olmayabilir. Ancak özellikle f ile p aralarında asal iken $F[x]/(p(x))$ te $f(x)$ in çarpımsal tersini hesaplamada yararlı olabilir (8.6. Örnek). Aşağıdaki sonuç, Euclid algoritmasının bir diğer uygulama alanıdır.

8.10. Sonuç. $k \subset K$ iki cisim ve $f(x), g(x) \in k[x] \subset K[x]$ olsun. f ile g nin $K[x]$ deki obebi, f ile g nin $k[x]$ deki obebi ile aynıdır.

İspat. $K[x]$ deki bölme algoritmasıyla $Q(x), R(x) \in K[x]$ ve $\partial(R) < \partial(g)$ olmak üzere

$$f(x) = Q(x)g(x) + R(x)$$

yazabiliriz. Ayrıca aynı zamanda $f(x), g(x) \in k[x]$ olduğundan bu sefer $k[x]$ deki bölme algoritması kullanılarak $q(x), r(x) \in k[x]$ ve $\partial(r) < \partial(g)$ olmak üzere

$$f(x) = q(x)g(x) + r(x)$$

yazabiliriz. Ancak bu son eşitlik $k[x] \subset K[x]$ olduğu için aynı zamanda $K[x]$ de de gerçeklendiğinden, $K[x]$ deki bölme algoritmasında bölüm ve kalanın tekliğinden $Q(x) = q(x)$ ve $R(x) = r(x)$ elde ederiz. Bu sebeple $K[x]$ deki Euclid algoritmasındaki denklem listesi ile $k[x]$ deki Euclid algoritmasındaki denklemler listesi aynıdır. Bu yüzden de her iki polinom halkasında da aynı obeb elde edilecektir.

8.11. Tanım. F bir cisim ve $f(x), g(x) \in F[x]$ olsun. $f(x)$ ile $g(x)$ in *okek*i aşağıdaki şartları sağlayan bir $m(x) \in F[x]$ polinomudur:

(i) $m(x)$, $f(x)$ ile $g(x)$ in bir ortak katıdır. Yani $f|m$ ve $g|m$ dir;

(ii) $c(x)$, $f(x)$ ile $g(x)$ in herhangi bir ortak katı iken $m|c$ dir.

(iii) $m(x)$ birim başkatsayılıdır.

Sıradaki sonuç, 8.8. Sonuç ile karşılaştırılmalıdır.

8.12. Teorem. F bir cisim ve $f(x), g(x) \in F[x]$ olsun. Bu taktirde f ile g nin okeki $(f) \cap (g)$ nin birim başkatsayılı üretecidir.

İspat. $F[x]$ bir temel ideal bölgesi olduğundan, birim başkatsayılı bir $m(x) \in F[x]$ polinomu için $(f) \cap (g) = (m)$ dir. $m \in (f)$ oluşu belli bir $r(x) \in F[x]$ için $m(x) = f(x)r(x)$ oluşunu; $m \in (g)$ oluşu da belli bir $s(x) \in F[x]$ için $m(x) = g(x)s(x)$ oluşunu gerektirir. O halde $m(x)$, hem f hem de g nin bir ortak katıdır. Son olarak, eğer $h(x)$, f ile g nin bir başka ortak katı ise, $h(x) = f(x)r'(x) = g(x)s'(x)$ yazabiliriz. Bu da $h \in (f) \cap (g) = (m)$ anlamına geleceğinden $m|h$ demektir.

Çarpanlara ayırma ve kökler arasında aşağıdaki ilişki vardır.

8.13. Teorem. $f(x) \in F[x]$ ve $a \in F$ olsun. Bu durumda

$$f(x) = q(x)(x-a) + f(a)$$

olacak şekilde bir $q(x) \in F[x]$ vardır.

İspat. Bölme algoritmasına göre $F[x]$ de, ya $r(x) = 0$ ya da $\partial(r) < 1 = \partial(x-a)$, yani $r(x)$ bir sabit olacak şekilde bir fonksiyon olmak üzere

$$f(x) = q(x)(x-a) + r(x)$$

eşitliği mevcuttur. Bu sabiti a noktasında hesaplarsak, $r = f(a)$ bulunur. Bu değer yerine konulursa iddia görülür.

8.14. Sonuç. $f(x) \in F[x]$ olsun. $a \in F$ nin $f(x)$ in bir kökü olması için gerek ve yeter şart $x-a$ nın $f(x)$ i bölmesidir.

İspat. a, $f(x)$ in bir kökü ise $f(a) = 0$ demektir. Bu durumda teorem gereği, $f(x) = (x-a)q(x)$ yazılabilir. Tersine, eğer $f(x) = (x-a)q(x)$ ise, a noktasında hesaplama yaparak $f(a) = 0$ olduğu kolayca görülür. Yani a, $f(x)$ in bir köküdür.

8.15. Teorem. F bir cisim ve $f(x) \in F[x]$ in derecesi $n \geq 0$ ise, F, $f(x)$ in en çok n kökünü bulundurur.

İspat. F in, $f(x)$ in $n+1$ tane kökünü bulundurduğunu varsayalım. Bu köklere $a_1, a_2, \ldots, a_{n+1}$ diyelim. Sonuç gereği belli bir $g_1(x) \in F[x]$ için $f(x) = (x-a_1)g_1(x)$ yazılabilir. Bu durumda $x-a_2$ farkı, $(x-a_1)g_1(x)$ çarpımını böler. $a_1 \neq a_2$ olduğundan $x-a_1$ ve $x-a_2$ polinomları aralarında asal polinomlardır. Böylece Euclid lemmasına göre $x-a_2$, $g_1(x)$ i bölmelidir. Bu durumda

$$f(x) = (x-a_1)(x-a_2)g_2(x)$$

yazılabilir. Aşağıdaki 3. probleme göre, i ye göre tümevarım uygulayarak

$$f(x) = (x-a_1)(x-a_2) \ldots (x-a_i)g_i(x)$$

ve böylece

$$f(x) = (x-a_1)(x-a_2) \ldots (x-a_{n+1})g_{n+1}(x)$$

yazabiliriz. Ancak bu, sol taraftaki $f(x)$ in derecesinin n, sağ taraftaki çarpımın derecesinin ise n den büyük oluşu sebebiyle mümkün değildir.

Bu son teorem, keyfi bir R halkasında doğru olmayacaktır. Örneğin, x^2-1 in $\mathbf{Z_8}$ de [1], [3], [5] ve [7] olmak üzere dört kökü vardır.

8.16. Örnek. $a \in R$ olsun. $e_a : R[x] \to R$ dönüşümünü

$$f(x) = \sum r_i x^i \to \sum r_i a^i$$

şeklinde tanımlayalım. $e_a(f) = \sum r_i a^i \in R$ elemanını $f(a)$ ile gösterelim. e_a nın bir halka dönüşümü olduğunu gösteriniz. Bu dönüşüme *a noktasındaki hesaplama dönüşümü* denilir. Böylece her bir $f(x) \in R[x]$ polinomu, $f: a \to f(a) = e_a(f)$ şeklinde bir $f: R \to R$ *polinom fonksiyonu* tanımlar. Bu sayede, x değişkenini artık R deki değerleri alacak bir değişken olarak düşünebiliriz.

Alıştırmalar

1) İki elemanının obebi bulunamayacak şekilde bir R bölgesinin var olduğunu gösteriniz. (Yol Gösterme: F bir cisim ve R, $F[x]$ in birinci dereceden terime sahip olmayan tüm polinomlarından oluşan althalkası olsun. Yani $f(x) \in R$ olması için gerek ve yeter şart $f(x) = a_0 + a_2x^2 + a_3x^3 + \ldots$ şeklindedir. x^5 ve x^6 yı göz önüne alınız. Bu iki elemanın birim katsayılı ortak bölenlerinin $1, x^2, x^3$ olduğunu belirleyip bunlardan hiçbirinin diğer ikisine bölünmediğini gösteriniz).

2) **(i)** $a_1, a_2, \ldots, a_n$ tamsayılarının obebini her bir i için $d|a_i$ olacak ve diğer ortak bölenlere bölünebilecek şekildeki bir d pozitif ortak tamsayı böleni olarak tanımlayınız. d nin varlığını ve d nin $a_1, a_2, \ldots, a_n$ tamsayılarının bir lineer birleşimi olduğunu ispatlayınız. (Yol gösterme: d, $\boldsymbol{Z}$ de $a_1, a_2, \ldots, a_n$ ile üretilen idealin pozitif üreteci olsun.)

(ii) F bir cisim olmak üzere $f_1, f_2, \ldots, f_n \in F[x]$ polinomlarının obebini her bir i için $d|f_i$ olacak ve diğer ortak bölenlere bölünebilecek şekildeki bir d birim katsayılı polinomu olarak tanımlayınız. d nin varlığını ve d nin $f_1, f_2, \ldots, f_n$ tamsayılarının bir lineer birleşimi olduğunu ispatlayınız.

3) $a_1, a_2, \ldots, a_n$ bir F cismindeki farklı elemanlar olsun. Bu durumda tüm i ler için $x-a_{i+1}$ ve $(x-a_1)(x-a_2)\ldots(x-a_i)$ polinomlarının aralarında asal olduğunu gösteriniz.

4) $R = Z[x]$ halkasında x ve 2 polinomlarının aralarında asal olduğunu; bununla birlikte

$$1 = x.f(x) + 2.g(x)$$

olacak şekilde $f(x)$ ve $g(x) \in \boldsymbol{Z}[x]$ polinomlarının bulunamayacağını gösteriniz.

5) F bir cisim ve her bir i için $a_i \in F$ olsun. $f(x) = \prod(x-a_i) \in F[x]$ alalım. $f(x)$ in katlı köklerinin bulunmadığını gösteriniz (yani hiçbir $a \in F$ için $f(x)$ in $(x-a)^2$ ile bölünemediğini gösteriniz).

6) $x^3 - 2x^2 + 1$ ve $x^2 - x - 3$ polinomlarının $Q[x]$ deki obebini hesaplayınız ve lineer toplam olarak ifade ediniz.

7) $p(x) = x^3 + x + 1 \in Z_2[x]$ ve $I = (p(x))$ olsun. $Z_2[x]/I$ nın bir cisim olduğunu gösteriniz.

8) R bir halka, $a \in R$ ve $e_a : R[x] \to R$, a noktasındaki değerlendirme fonksiyonu olsun. $\ker e_a$ nın R de a yı kök kabul eden tüm polinomlardan oluştuğunu ve $x-a$

ile üretilen temel ideal $(x-a)$ ile gösterilmek üzere $\ker e_a = (x-a)$ olduğunu gösteriniz.

9) F bir cisim, $f(x), g(x) \in F[x]$ olsun. Eğer $\partial(f) \leq \partial(g) = n$ ise ve ayrıca $n+1$ tane $a \in F$ elemanı için $f(a) = g(a)$ oluyorsa $f(x) = g(x)$ olduğunu gösteriniz.

9. Asal ve Maksimal İdealler

Asal sayı kavramı polinomlara da genelleştirilebilir.

9.1. Tanım. F bir cisim olsun. Sıfırdan farklı bir $p(x) \in F[x]$ polinomu için $\partial(p) \geq 1$ ise ve $F[x]$ te $\partial(f) < \partial(p)$ ve $\partial(g) < \partial(p)$ olmak üzere $p(x) = f(x)g(x)$ şeklinde bir çarpanlara ayırma söz konusu değilse, *$p(x)$ polinomu F üzerinde indirgenemezdir* denilir.

Dikkat edilirse indirgenemezlik F katsayı cismine bağlı bir kavramdır. Örneğin, x^2+1 polinomu $\mathbf{R}$ de indirgenemezken $\mathbf{C}$ de indirgenebilirdir. (derecesi 1 olan) lineer polinomların tanım gereği her cisim üzerinde indirgenemez oldukları açıktır. 8.14. Sonuç gereği bir F cismi üzerinde derecesi en az 2 olan polinomların F de kökü yoktur. Bu ifadenin tersi doğru değildir. Örneğin, $f(x) = x^4 + 2x^2 + 1 = (x^2 + 1)^2$ polinomu $\mathbf{R}$ üzerinde çarpanlarına ayrılabilmesine rağmen hiçbir reel köke sahip değildir.

F bir cisim olmak üzere $p(x), f(x) \in F[x]$ olsun. Eğer $p(x)$ birim katsayılı indirgenemeyen bir polinom ise birim katsayılı çarpanları sadece 1 ve $p(x)$ tir. Böylece (p,f) obeb değeri de ya 1 ya da $p(x)$ olacaktır. O halde $p(x)$, $f(x)$ polinomunu bölmüyorsa $p(x)$ ve $f(x)$ aralarında asaldır.

9.2. Tanım. I, R halkasında bir has ideal olsun. Eğer $ab \in I$ olması $a \in I$ veya $b \in I$ olmasını gerektiriyorsa I ya bir *asal ideal* denilir.

9.3. Örnek. $p \geq 2$ ise $\mathbf{Z}$ deki bir (p) idealinin bir asal ideal olması için gerek ve yeter şartın p nin asal sayı olması olduğunu iddia ediyoruz.

Eğer p asal ise ve $ab \in (p)$ ise $p|ab$ olacağından Euclid Lemması gereği $p|a$ veya $p|b$ elde edilir. Yani $a \in (p)$ veya $b \in (p)$ dir. Böylelikle (p) bir asal idealdir.

Tersine p asal değilse, $a<p$ ve $b<p$ olmak üzere $p = ab$ şeklinde çarpanlarına ayrılabiliyor demektir. Bu durumda ne a ne de b, (p) nin elemanı değildir. Bu da (p) nin asal ideal olmadığı anlamına gelir ki bir çelişkidir.

9.4. Teorem. F bir cisim ise sıfırdan farklı bir $p(x) \in F[x]$ polinomunun indirgenemez olması için gerek ve yeter şart $(p(x))$ in bir asal ideal olmasıdır.

İspat. $p(x)$ indirgenemez olsun. Tanım gereği (p) nin asal ideal olduğunu göstermek için bir has ideal olduğunu ve ayrıca $ab \in (p)$ iken $a \in (p)$ veya $b \in (p)$ olması gerektiğini göstermeliyiz.

Eğer $ab \in (p)$ ise $p|ab$ olacağından Euclid Lemması gereği $p|a$ veya $p|b$ elde edilir. Yani $a \in (p)$ veya $b \in (p)$ dir. Son olarak (p) bir has idealdir. Çünkü aksi taktirde $1 \in R = (p)$ olurdu ki bu da $1 = p(x).f(x)$ olacak şekilde bir $f(x)$ polinomunun varlığını gerektirirdi. Ama 1 sabit olup derecesi sıfırdır ve

$$0 = \partial(pf) = \partial(p) + \partial(f) \geq \partial(p) > 1$$

çelişkisi elde edilir. Dolayısıyla (p) bir asal idealdir.

Tersine, $p(x)$ in indirgenemez olmadığını varsayalım. Bu durumda $\partial(a) < \partial(p)$ ve $\partial(b) < \partial(p)$ olmak üzere p polinomu

$$p(x) = a(x).b(x)$$

şeklinde çarpanlarına ayrılabilir. (p) deki sıfırdan farklı her polinomun derecesi $\partial(p)$ den büyük ya da eşit olduğundan ne a nın ne de b nin (p) de kalmadığı görülür. Yani (p) bir asal ideal değildir.

9.5. Teorem. R deki bir I has idealinin asal ideal olması için gerek ve yeter şart R/I nın bir bölge olmasıdır.

İspat: I bir asal ideal olsun. Eğer $0 = (a+I)(b+I) = ab+I$ ise, $ab \in I$ dır. I bir asal ideal olduğundan $a \in I$ veya $b \in I$ dır. Yani ya $a+I = 0$ ya da $b+I = 0$ dır. Böylece R/I bir bölgedir. Tersi de benzer şekilde ispatlanabilir.

9.6. Tanım. Bir R halkasında bir I has ideali alalım. Eğer R de, I yı bir has ideal olarak bulunduran bir J has ideali bulunamıyorsa I ya bir *maksimal ideal* denir.

9.7. Teorem. Bir R halkasındaki bir I has idealinin bir maksimal ideal olması için gerek ve yeter şart R/I nın bir cisim olmasıdır.

İspat: 7. Bölümün sonundaki 3. alıştırmaya göre I nın bir maksimal ideal olması için gerek ve yeter şart R/I nın $\{0\}$ ve kendisi dışında hiçbir idealinin olmamasıdır. 6. Bölümün sonundaki 11. alıştırmaya göre bu şartın sağlanması için gerek ve yeter şart R/I nın bir cisim olmasıdır.

9.8. Sonuç. Bir R halkasındaki her maksimal I ideali bir asal idealdir.

İspat: I bir maksimal ideal ise R/I bir cisimdir. Her cisim bir bölge olduğundan R/I da bir bölgedir. O halde I bir asal idealdir.

Bu sonucun tersi doğru değildir. Örneğin, $\boldsymbol{Z}[x]$ de (x) temel ideali asal ideal olmasına rağmen maksimal değildir. 7. Bölümün sonundaki 2. alıştırmaya göre

$$\boldsymbol{Z}[x]/(x) \cong \boldsymbol{Z}$$

dir ve $\boldsymbol{Z}$ bir bölge olmasına rağmen bir cisim değildir.

9.9. Teorem. R bir temel ideal bölgesi ise, sıfırdan farklı her bir asal I ideali bir maksimal idealdir.

İspat: $I \subset J \subset R$ olmak üzere I dan farklı bir J idealinin var olduğunu varsayalım. R bir temel ideal bölgesi olduğundan $a, b \in R$ olmak üzere $I = (a)$ ve $J = (b)$ dir. Eğer $a \in J$ ise bir $r \in R$ için $a = rb$ yazılabilir ve böylece $rb \in I$ dır. I asal olduğundan ya $r \in I$ dır ya da $b \in I$ dır. Eğer $b \in I$ ise $J \subset I$ çelişkisi elde edilir. Eğer $r \in I$ ise belli bir $s \in R$ için $r = sa$ yazabiliriz ve böylece $a = rb = sab$ elde ederiz. Buradan da $1 = sb$ elde ederiz ve 6. Bölümün sonundaki 10. alıştırmanın (i) şıkkı gereği $J = (b) = R$ buluruz. Böylece I maksimaldir.

9.10. Sonuç. F bir cisim olsun. $p(x) \in F[x]$ indirgenemezse $F[x]/(p(x))$ bölüm halkası F yi ve $p(x)$ in bir kökünü bulunduran bir cisimdir.

İspat: $p(x)$ indirgenemediğinden $I = (p(x))$ temel ideali sıfırdan farklı bir asal idealdir. $F[x]$ bir temel ideal bölgesi olduğundan I bir maksimal idealdir. Bu yüzden $E = F[x]/I$ bir cisimdir. $a \to a+I$ dönüşümü F den $F' = \{a+I : a \in F\} \subset E$ ye bir izomorfizmdir. (Bu yüzden bazen F ile F' özdeş kabul edilir.)

$\theta = x+I \in E$ olsun. θ nın $p(x)$ in bir kökü olduğunu iddia ediyoruz. $a_i \in F$ olmak üzere $p(x) = a_0+a_1x+ \ldots +a_nx^n$ yazalım. $I = (p(x))$ olduğundan E de

$$\begin{aligned} p(\theta) &= (a_0+I) + (a_1+I)\theta + \ldots + (a_n+I)\theta^n \\ &= (a_0+I) + (a_1+I)(x+I) + \ldots + (a_n+I)(x+I)^n \\ &= (a_0+I) + (a_1x+I) + \ldots + (a_nx^n+I) \\ &= a_0+a_1x+ \ldots +a_nx^n+I \\ &= p(x)+I \\ &= I \end{aligned}$$

dir. Ancak $I = 0+I$, $F[x]/I$ nın sıfır elemanı olduğundan θ, $p(x)$ in bir köküdür.

Örneğin x^2+1, $\boldsymbol{R}[x]$ de indirgenemeyen bir polinomdur ve $\boldsymbol{R}[x]/(x^2+1)$ bölüm halkası $\boldsymbol{R}$ yi ve $i^2 = -1$ olacak şekildeki bir $i = x+I$ elemanını bulunduran bir cisimdir. 7.4. Örnekte $\boldsymbol{R}[x]/(x^2+1)$, $\boldsymbol{C}$ kompleks sayılar cismine izomorfiktir.

9.11. Tanım. $f(x) \in F[x]$ bir polinom olsun. Eğer f, $F[x]$ te lineer çarpanlarına ayrılabiliyorsa f ye F *üzerinde dağılabilirdir* denilir.

Tabii ki $f(x)$ in F üzerinde dağılabilir olması için gerek ve yeter şartın F nin $f(x)$ in tüm köklerini bulundurması olduğu açıktır.

9.12. Teorem (Kronecker). F bir cisim olmak üzere $f(x) \in F[x]$ olsun. Bu taktirde F yi içeren ve üzerinde $f(x)$ in dağılabildiği bir E cismi mevcuttur.

İspat: İspatı $\partial(f)$ e tümevarım uygulayıp yapacağız. $\partial(f) = 1$ ise $f(x)$ lineerdir ve $E = F$ seçebiliriz. Eğer $\partial(f) > 1$ ise $p(x)$ indirgenemeyen bir polinom olmak üzere $f(x) = p(x)g(x)$ yazabiliriz. 9.10. Sonuca göre F yi ve $p(x)$ in bir θ kökünü bulunduran bir B cismi mevcuttur. O halde $B[x]$ te $p(x) = (x-\theta)h(x)$ yazabiliriz. Tümevarımla B yi de içeren ve üzerinde $h(x)g(x)$ in ve dolayısıyla $f(x)$ dağılabildiği bir E cismi mevcuttur.

Şimdi bir $f(x) \in F[x]$ polinomu için köklerin F den daha geniş bir cisimde kalmasını sağlamak amacıyla katlı kök tanımını yeni bir şekle sokacağız.

9.13. Tanım. F bir cisim ve $f(x) \in F[x]$ olsun. Eğer $E[x]$ te

$$f(x) = (x-a)^2 h(x)$$

olacak şekilde F yi de içeren bir E cismi mevcutsa *f nin katlı kökleri mevcuttur* denilir.

8. Bölümün sonundaki 5. alıştırmayı ve Sonuç 8.10 u kullanılarak $f(x)$ in katlı köklerinin olmaması için gerek ve yeter şartın f', f in türevini göstermek üzere $(f,f') = 1$ olması olduğu görülebilir.

Kronecker Teoremi $\boldsymbol{Z}_p$ dışında kalan sonlu cisimler oluşturmada kullanılabilir. Önce cisimlerin önemli bir özelliğini görelim.

9.14. Tanım. F bir cisim olsun. F nin tüm altcisimlerinin kesişimine F nin *asal cismi* denilir.

5. Bölümün sonundaki 10. alıştırmaya göre F nin asal cismi de bir altcisimdir.

9.15. Teorem. F bir cisim olsun. F nin asal cismi ya $\boldsymbol{Q}$ ya, ya da p asal olmak üzere $\boldsymbol{Z}_p$ ye izomorftur.

İspat: 1, F cisminin birimi olsun. $\chi : \boldsymbol{Z} \to F$ dönüşümünü $n \mapsto n.1$ şeklinde tanımlayalım. χ bir halka dönüşümüdür. $I = Ker\ \chi$ denilirse $\boldsymbol{Z}/I$ bir bölgedir. Çünkü F nin bir althalkasına izomorftur. Böylece I bir asal idealdir ve $I = (0)$ ya da p asal olmak üzere $I = (p)$ dir. Eğer $I = (0)$ ise χ, $\boldsymbol{Z}$ yi F ye gömer. 6. Bölümün sonundaki 3. alıştırmaya göre bu durumda asal cisim $\boldsymbol{Q}$ ya izomorftur. $I = (p)$ ise birinci izomorfizm teoremine göre $Im\ \chi \cong \boldsymbol{Z}/(p) \cong \boldsymbol{Z}_p$ dir ve bu da bir cisimdir. Böylece $Im\ \chi$, F nin asal cismidir.

9.16. Tanım. Asal cismi $\boldsymbol{Q}$ ya izomorfik olan bir cismin *karakteristiği 0* dır denilir. Asal cismi $\boldsymbol{Z}_p$ ye izomorf olan bir cisme de *karakteristiği p* dir denilir.

9.17. Lemma. F, karakteristiği $p > 0$ olan bir cisim olsun.

(i) Her $a \in F$ için $pa = 0$ dır.

(ii) Her $a, b \in F$ için $(a+b)^p = a^p+b^p$ dir.
(iii) Her $a, b \in F$ ve her $k \geq 1$ için

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}$$

dır.

İspat: (i) F deki birim elemanı şu an için e ile gösterelim. O halde

$$pa = a + \dots + a = (e + \dots + e)p$$

yazabiliriz. Bununla birlikte $\boldsymbol{Z}_p$ de her biri $[1]$ olan p tane terimin toplamı sıfırdır. F nin karakteristiği p olduğundan $e + \dots + e = 0$ dır. Yani F de $pa = 0$ dır.

(ii) Binom teoreminden

$$(a+b)^p = a^p+\sum_{i=1}^{p-1}\binom{p}{i}a^i b^{p-i} +b^p$$

yazabiliriz. 4. Bölümün sonundaki 3. alıştırma gereği $\boldsymbol{Z}_p$ de tüm $1 \leq i \leq p-1$ için $\binom{p}{i} = 0$ dır.

(iii) İspat k ya tümevarım uygulayarak yapılır. $k = 1$ durumunu (ii) de gördük. Tümevarım gereği

$$\begin{aligned}(a+b)^{p^{k+1}} &= \left[\ (a+b)^{p^k}\ \right]^p \\ &= \left[a^{p^k} + b^{p^k}\right]^p \\ &= a^{p^{k+1}} + b^{p^{k+1}}\end{aligned}$$

elde edilir.

Bu Lemma bize, F karakteristiği p olan bir cisim ve $q = p^k$ iken $a \mapsto a^q$ fonksiyonunun F den F ye bir halka homomofizmi olduğunu gösterir.

F, bir E cisminin altcismi ise E nin toplamsal grubuna F üzerinde bir vektör uzayı gözüyle bakabiliriz. $c \in F$ ve $\alpha \in E$ olmak üzere $c\alpha$ skaler çarpımını c ve α nın E deki çarpımı olarak tanımlayalım. Sonlu bir E cismi bu sebeple $\boldsymbol{Z}_p$ üzerinde bir vektör uzayı olarak düşünülebilir. Eğer $\{\alpha_1, \dots , \alpha_n\}$, E nin bir sıralı tabanı ise E nin her bir a elemanı, c_i ler $\boldsymbol{Z}_p$ de kalmak üzere $(c_1, \dots , c_n)$ şeklindedir. Bu sebeple herbir sonlu cisim p asal ve n bir pozitif tamsayı olmak üzere p^n elemana sahiptir.

9.18. Teorem (Galois). Her p asalı ve her n pozitif tamsayısı için tam olarak p^n tane elemana sahip bir cisim mevcuttur.

İspat: Eğer $p^n = q$ elemana sahip bir K cismi mevcut olsaydı $K^* = K-\{0\}$ $q-1$ mertebeli bir çarpım grubu olurdu. Lagrange teoremi gereği her $a \in K^*$ için $a^{q-1} = 1$ elde edilir. Böylece K nın herbir elemanının

$$g(x) = x^q - x$$

polinomunun bir kökü olduğu görülür.

Kronecker Teoremi gereği $\boldsymbol{Z}_p$ yi bulunduran ve üzerinde $g(x)$ in dağıldığı bir E cismi mevcuttur. $F = \{\alpha \in E : g(\alpha) = 0\}$ tanımlayalım. Yani F, $g(x)$ in tüm köklerinin kümesi olsun. $q = p^n$ olup E nin de karakteristiği p olduğundan $g'(x) = qx^{q-1} - 1 = -1$ dir. 9.17. Lemma gereği $(g,g') = 1$ olur ve $g(x)$ in katlı kökü yoktur. Yani F in mertebesi $q = p^n$ dir.

Şimdi F in cisim olduğunu göstereceğiz. Eğer a ve b F cismindeyse, $a^q = a$ ve $b^q = b$ dir. $(ab)^q = a^q b^q = ab$ olup ab de F nin elemanıdır. b yerine $-b$ alınırsa $(a-b)^q = a^q - b^q = a - b$ elde edilir ki $a - b$ de F dedir. Son olarak a sıfırdan farklı ise $a^{q-1} = 1$ dır ve $a^{-1} = a^{q-2}$ de F dedir.

Alıştırmalar

1) Derecesi 2 ya da 3 olan bir $p(x) \in F[x]$ polinomunun F üzerinde indirgenebilir olması için gerek ve yeter şartın $p(x)$ in hiç bir kökünün F de kalmaması olduğunu gösteriniz. (Bu sonuç derecenin 4 olması durumunda doğru değildir. Gerçekten de $(x^2+1)^2$ polinomu $\mathbf{R}[x]$ te çarpanlarına ayrılabilse de hiç bir köke sahip değildir).

2) $p(x) \in F[x]$ polinomu indirgenemez olsun. $g(x) \in F[x]$ sabit olmayan bir polinom ise, ya $(p(x),g(x)) = 1$ ya da $p(x)|g(x)$ olduğunu gösteriniz.

3) **(i)** a sıfırdan farklı bir sabit ve $p_i(x)$ polinomları farklı olmaları gerekmeyen birim başkatsayılı indirgenemeyen polinomlar olmak üzere $F[x]$ deki sıfırdan farklı herbir $f(x)$ polinomu için

$$f(x) = a\, p_1(x). \ldots .p_t(x)$$

yazılabilir.

(ii) Bu çarpanlara ayırmada çarpanlar ve katlılıkları bir tek şekilde belirlidir.

4) a ve b sıfırdan farklı sabitler, $k_i,\ n_i \geq 0$ ve $p_i(x)$ birbirinden farklı birim başkatsayılı indirgenemeyen polinomlar olmak üzere $f(x) = a\, p_1(x)^{k_1}. \ldots .p_t(x)^{k_t}$ ve $g(x) = b\, p_1(x)^{n_1}. \ldots .p_t(x)^{n_t}$ olsun. $m_i = min\{k_i, n_i\}$ ve $M_i = max\{k_i, n_i\}$ olmak üzere

$$(f,g) = p_1(x)^{m_1}. \ldots .p_t(x)^{m_t}$$

ve

$$[f,g] = p_1(x)^{M_1}. \ldots .p_t(x)^{M_t}$$

olduğunu gösteriniz.

5) **(i)** Bir R halkasındaki sıfır idealinin asal ideal olması için gerek ve yeter şartın R nin bir tamlık bölgesi olması olduğunu gösteriniz.

(ii) Bir R halkasındaki sıfır idealinin maksimal ideal olması için gerek ve yeter şartın R nin bir cisim olması olduğunu gösteriniz.

6) $\mathbf{Z}[x]$ de sabit katsayısı çift olan tüm polinomlardan oluşan I idealinin maksimal ideal olduğunu gösteriniz.

7) $f(x),\ g(x) \in F[x]$ olsun. $(f,g) \neq 1$ olması için gerek ve yeter şartın hem F yi hem de $f(x)$ ve $g(x)$ in bir ortak kökünü bulunduran bir E cisminin var olması olduğunu gösteriniz.

8) **(i)** $f(x) \in \mathbf{Z}_p[x]$ ise $(f(x))^p = f(x^p)$ olduğunu gösteriniz. (Yol Gösterme: Fermat'ın küçük teoreminden faydalanınız)

(ii) $\mathbf{Z}_p[x]$ yerine karakteristiği p olan sonsuz bir cisim alınırsa üstteki iddianın doğru olmayabileceğini gösteriniz. (5. Bölümün sonundaki 11. alıştırmadan faydalanınız)

9) F bir cisim ise $F[x]$ ten F ye herbir değerlendirme dönüşümünün çekirdeğinin bir maksimal ideal olduğunu gösteriniz.

10) F karakteristiği sıfır olan bir cisimse ve $p(x) \in F[x]$ indirgenemezse $p(x)$ in katlı köklerinin bulunmadığını gösteriniz. (Yol Gösterme: $(p(x),p'(x))$ obebini gözönüne alınız).

11) Kronecker teoreminden faydalanarak $\mathbf{Z}_2$ ye x^4-x polinomunun uygun bir kökünü katıp dört elemanlı bir cisim elde ediniz.

12) Sekiz elemanlı bir cisim için toplama ve çarpma tablolarını hazırlayınız. (Yol Gösterme: $\mathbf{Z}_2$ üzerinde x^8-x polinomunu çarpanlarına ayırınız).

13) Dört elemanlı bir cismin sekiz elemanlı bir cismin bir altcismine izomorf olamayacağını gösteriniz.

10. İndirgenemez Polinomlar

Burada polinomların indirgenemezliği ile ilgili bir kural bulmaya çalışacağız. Bu oldukça güç ve genelde çözümsüz bir durumdur.

Eğer $\sigma : R \to S$ bir halka dönüşümü ise $\sigma^* : \sum r_i x^i \mapsto \sum \sigma(r_i) x^i$ ile tanımlı $\sigma^* : R[x] \to S[x]$ dönüşümü de bir halka dönüşümüdür. Bundan faydalanarak aşağıdaki sonucu verebiliriz:

10.1. Teorem. R bir tamlık bölgesi, F bir cisim, olsun. $\sigma : R \to F$ bir halka dönüşümü ve $p(x) \in R[x]$ olsun. Eğer $\partial(\sigma^*(p)) = \partial(p)$ ise $\sigma^*(p(x))$, $F[x]$ de indirgenemezse $p(x)$, $R[x]$ de dereceleri p nin derecesinden küçük olan iki polinomun çarpımı olarak yazılamaz.

Uyarı: $p(x)$ birim başkatsayılı ise derece şartının sağlanacağına dikkat ediniz.

İspat. $\partial(f) < \partial(p)$ ve $\partial(g) < \partial(p)$ olmak üzere $R[x]$ de $p(x) = f(x)g(x)$ olduğunu varsayalım. $F[x]$ de

$$\sigma^*(p) = \sigma^*(f)\,\sigma^*(g)$$

dir. $\sigma^*(p)$ indirgenemediğinden $\partial(\sigma^*(f)) = 0$ olduğunu varsayabiliriz. Ancak

$$\begin{aligned} \partial(p) &= \partial(\sigma^*(p)) \\ &= \partial(\sigma^*(f)) + \partial(\sigma^*(g)) \\ &= \partial(\sigma^*(g)) \\ &\leq \partial(g) \\ &< \partial(p) \end{aligned}$$

çelişkisi elde edilir.

10.2. Örnek. $Z[x]$ teki $f(x) = 8x^3-6x-1$ polinomunu ele alalım. $\sigma : Z \to Z_p$ dönüşümünü kanonik dönüşüm olarak alıp p asalını da uygun şekilde seçerek üstteki teoremden faydalanacağız. Böylece σ^* dönüşümü $f(x)$ in katsayılarını p modunda indirgeyen bir dönüşüm olacaktır. $p = 2$ seçersek derece şartı yerine getirilemez. Çünkü $\sigma^*(f)$ nin derecesi sıfır olur. $p = 3$ seçilirse $\sigma^*(f)$ indirgenemez değildir, çünkü

$$\sigma^*(f) = -x^3-1 = -(x+1)(x^2-x+1)$$

dir. Eğer $p = 5$ seçilirse

$$\sigma^*(f) = 3x^3-x-1$$

bulunur ki bu da 9. Bölümün sonundaki 1. alıştırma gereği $\mathbf{Z}_5$ te hiç kökü olmadığından indirgenemezdir. Teorem 10.1 gereği $f(x)$ $\mathbf{Z}[x]$ te daha küçük dereceli polinomların çarpımı olarak yazılamaz.

Teorem 10.1 her zaman uygulanamaz. Bu bölümün sonundaki 5. alıştırmada $f(x) = x^4-10x^2+1$ polinomunun $\mathbf{Q}[x]$ de indirgenemediğini göreceğiz. Ayrıca ileride bu $f(x)$ fonksiyonunun her p asal değeri için mod p de çarpanlarına ayrılabileceğini göstereceğiz.

Şimdi $\mathbf{Z}[x]$ te bazı fonksiyonların daha küçük dereceli polinomların çarpımı olarak yazılıp yazılamayacağını belirlemeye yarayan bir yöntem göreceğiz. Bununla birlikte esas amacımız polinomların $\mathbf{Q}[x]$ de indirgenip indirgenemediğini anlamaya çalışmaktır. Gauss'un bir sonucu bu tür problemleri kolaylıkla çözebilir.

10.3. Tanım. $\mathbf{Z}[x]$ de bir $f(x) = a_0 + a_1x + ... + a_nx^n$ polinomunu alalım. Eğer katsayıların obebi 1 ise f polinomuna *ilkel*dir denilir.

Eğer $f(x)$ in katsayılarının obebi d ise $(1/d)f(x)$ ilkel bir polinomdur.

$f(x)$ ilkel değilse bu durumda tüm katsayılarını bölen bir p asalı mevcuttur. Eğer katsayıların obebi d ise p, d nin herhangi bir böleni olarak alınabilir.

10.4. Lemma (Gauss Lemması). $f(x)$ ve $g(x)$ ilkel polinomlar ise çarpımları da ilkel polinomdur.

İspat: $f(x)g(x)$ çarpımının ilkel olmadığını varsayalım. Bu demektir ki bu çarpımın tüm katsayılarını bölen bir p asalı mevcuttur. $\sigma : \mathbf{Z} \to \mathbf{Z}_p$ doğal dönüşüm olsun. tüm katsayıları p modunda indirgeyen $\sigma^* : \mathbf{Z}[x] \to \mathbf{Z}_p[x]$ halka dönüşümünü gözönüne alalım.

$$\sigma^*(fg) = \sigma^*(f)\sigma^*(g)$$

dir. Ancak $\mathbf{Z}_p[x]$ de $\sigma^*(f) \neq 0$ ve $\sigma^*(g) \neq 0$ olmasına rağmen $\sigma^*(fg) = 0$ dır. Bu da $\mathbf{Z}_p[x]$ in bir tamlık bölgesi oluşuyla çelişir.

10.5. Lemma. Sıfırdan farklı herbir $f(x) \in \mathbf{Q}[x]$ fonksiyonu, $c(f) \in \mathbf{Q}$ pozitif ve $f^*(x) \in \mathbf{Z}[x]$ ilkel olmak üzere

$$f(x) = c(f).\ f^*(x)$$

şeklinde bir tek biçimde çarpanlarına ayrılabilir.

Uyarı: Bu yazılımdaki pozitif $c(f)$ rasyonel sayısına f nin içeriği denilir.

İspat: $f(x) = (a_0/b_0) + (a_1/b_1)x + ... + (a_n/b_n)x^n \in \mathbf{Q}[x]$ olsun. $B = b_0. ... .b_n$ tanımlayalım. Bu durumda $g(x) = Bf(x) \in \mathbf{Z}[x]$ olacaktır. d, $g(x)$ fonksiyonunun katsayılarının obebi olmak üzere $D = \pm d$ tanımlayalım. Burada işaret D/B yi pozitif yapacak şekilde seçilecektir. $(B/D)f(x) = (1/D)g(x)$ fonksiyonu $\mathbf{Z}[x]$ te kalacaktır ve bir ilkel polinomdur. $c(f) = D/B$ ve $f^*(x) = (B/D)f(x)$ olarak tanımlanırsa $f(x) = c(f).f^*(x)$ ayrışımı istenen çarpanlara ayırmadır.

Şimdi tekliği gösterelim. Bunun için e pozitif bir rasyonel sayı ve $h(x) \in \mathbf{Z}[x]$ ilkel olmak üzere $f(x) = e.h(x)$ in ikinci bir çarpanlara ayrışım olduğunu varsayalım. Şimdi $c(f).f^*(x) = f(x) = e.h(x)$ dir ve dolayısıyla $f^*(x) = [e/c(f)]h(x)$ olur. $e/c(f)$ i sadeleştirip en sade haline getirelim. Yani u ve v aralarında asal pozitif tamsayılar olmak üzere $e/c(f) = u/v$ olsun. $vf^*(x) = uh(x)$ denklemi $\mathbf{Z}[x]$ de sağlanır. Denk katsayıları eşitleyerek v nin $uh(x)$ in herbir katsayısının bir ortak böleni olduğu sonucu bulunur. $(u,v) = 1$ olduğundan $\mathbf{Z}$ deki Euclid Lemması v nin, $h(x)$ fonksiyonunun tüm katsayılarının (pozitif) bir ortak böleni olduğunu gösterir. $h(x)$ ilkel olduğundan $v = 1$ olmalıdır. Benzer bir düşünceyle $u = 1$ olduğu da gösterilir. Böylece $e/c(f) = u/v = 1$ bulunur. Yani $d = c(f)$ dir ve sonuç olarak $f^*(x) = h(x)$ elde edilir.

10.6. Sonuç. $f(x) \in \mathbf{Z}[x]$ ise $c(f) \in \mathbf{Z}$ dir.

İspat. d, $f(x)$ in katsayılarının obebi olsun. O halde $(1/d)f(x) \in \mathbf{Z}[x]$ fonksiyonu ilkel bir fonksiyondur. $f(x) = d.[(1/d)f(x)]$ olarak bir d pozitif rasyonel sayısı (hatta bir tamsayı) ile ilkel bir polinomun çarpımı olarak yazılabileceğinden ve lemma gereği içerik dediğimiz bu sayı bir tek olduğundan $c(f) = d \in \mathbf{Z}$ dir.

10.7. Sonuç. $f(x) \in \mathbf{Q}[x]$ fonksiyonu $\mathbf{Q}[x]$ de $f(x) = g(x)h(x)$ olarak çarpanlarına ayrılabiliyorsa

$$c(f) = c(g)c(h) \quad \text{ve} \quad f^*(x) = g^*(x)h^*(x)$$

dir.

İspat.

$$f(x) = g(x)h(x)$$

$$= [c(g)\, g^*(x)][\, c(h)\, h^*(x)]$$

$$= c(g)c(h)\, g^*(x)h^*(x)$$

yazabileceğimiz açıktır. $c(g)c(h)$ sayısı pozitif bir rasyonel sayı olduğundan ve ayrıca iki ilkel fonksiyonun çarpımının da ilkel olduğunu bildiğimizden önceki lemmadaki çarpanlara ayırmanın tekliği gereği $c(f) = c(g)c(h)$ ve $f^*(x) = g^*(x)h^*(x)$ elde edilir.

10.8. Teorem (Gauss). Eğer $p(x) \in \mathbf{Z}[x]$ fonksiyonu $\mathbf{Z}[x]$ de dereceleri p nin derecesinden küçük olan iki polinomun çarpımı şeklinde yazılamıyorsa, $p(x)$, $\mathbf{Q}[x]$ de indirgenemezdir.

İspat. Eğer $\mathbf{Q}[x]$ de $p(x) = g(x)h(x)$ yazılabiliyorsa yine $\mathbf{Q}[x]$ de g^* ve h^* ilkel polinomlar olmak üzere

$$p(x) = c(g)c(h)\, g^*(x)h^*(x)$$

yazılabilir. Ancak Sonuç 10.6 gereği $c(g)c(h) = c(p) \in \mathbf{Z}$ olduğunu biliyoruz. O halde $p(x) = [c(p)\, g^*(x)]\, h^*(x)$, $\mathbf{Z}[x]$ de bir çarpanlara ayırmadır.

Uyarı: Bu son teoremin ispatı genelleştirilebilir: $\mathbf{Z}$ ve $\mathbf{Q}$ yu sırasıyla bir tamlık bölgesi ve bu bölgenin kesir cismi ile değiştirelim. Bu fikir, R tek şekilde çarpanlara ayırma bölgesi iken $R[x]$ inde tek şekilde çarpanlara ayırma bölgesi olduğunun ispatında kullanılan temel fikirdir. Buradan F bir cisim iken, $F[x_1, \ldots, x_n]$ in tek şekilde çarpanlara ayırma bölgesi olduğu sonucu çıkar.

10.9. Teorem (Eisenstein Kuralı). $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbf{Z}[x]$ olsun. Tüm $i < n$ için a_i leri bölen fakat a_n i bölmeyen ve karesi a_0 ı bölmeyen bir p asalı bulunabiliyorsa $f(x)$ fonksiyonu $\mathbf{Q}[x]$ de indirgenemezdir.

Yani bir $f(x)$ polinomunun $\mathbf{Q}[x]$ de indirgenemez olduğunu göstermek için bir p asal sayısını

$$\begin{aligned} &p \mid a_0, \\ &p \mid a_1, \\ &\quad\vdots \\ &p \mid a_{n-1}, \end{aligned}$$

olacak ancak p, a_n i, p^2 de a_0 ı bölmeyecek şekilde seçebilmeliyiz.

İspat. $g(x) = b_0 + b_1x + \ldots + b_mx^m$ polinomunun derecesi olan m ve $h(x) = c_0 + c_1x + \ldots + c_kx^k$ polinomunun derecesi olan k, n den küçük olmak üzere $\mathbf{Z}[x]$ de $f(x) = g(x)h(x)$ olsun. Katsayıları mod p de indirgeyen $\sigma^* : \mathbf{Z}[x] \to \mathbf{Z}_p[x]$ halka dönüşümünü gözönüne alalım. $\mathbf{Z}_p[x]$ de $\sigma^*(f) = a_nx^n$ dir. Fakat $\sigma^*(f) = \sigma^*(g)\, \sigma^*(h)$ dir ve çarpanlara ayırmanın tekliği gereği $\sigma^*(g)$ ve $\sigma^*(h)$ benzer şekilde çarpanlarına ayrılabilir. Böylece $\sigma^*(g) = b_mx^m$ dir ve tüm $i < m$ ler için $p \mid b_i$ dir. Benzer olarak, $\sigma^*(h) = b_kx^k$ dir ve tüm $j < k$ için $p \mid c_j$ dir. Özel olarak $p \mid b_0$ ve $p \mid c_0$ dır ve bu yüzden $p^2 \mid b_0c_0 = a_0$ olur ki bu bir çelişkidir.

10.10. Örnek. Eisenstein kuralı gereği $x^5 - 4x + 2$ polinomu $\mathbf{Q}$ üzerinde indirgenemezdir. Gerçekten de $p = 2$ asalı alınırsa, ilk terim hariç diğer tüm terimlerin

katsayıları *(-4* ve *2) 2* ile bölünürken, *2* baş katsayı olan *1* i bölmez ve $2^2 = 4$ te sabit terim olan *2* yi bölmez. Yani Eisenstein kuralındaki tüm ön şartlar sağlanmaktadır ve dolayısıyla polinom indirgenemezdir.

10.11. Örnek. $x^3 - 6x^2 + 9x - 15$ polinomu **Q** üzerinde indirgenemezdir. Gerçekten de $p = 3$ asalı alınırsa, ilk terim hariç diğer tüm terimlerin katsayıları *(-6, 9* ve *15) 3* ile bölünürken, *3* baş katsayı olan *1* i bölmez ve $3^2 = 9$ da sabit terim olan *-15* i bölmez. Yani Eisenstein kuralındaki tüm ön şartlar sağlanmaktadırve dolayısıyla polinom indirgenemezdir.

10.12. Örnek. Eisenstein kuralını kullanarak $x^3 - 6x^2 + 9x - 18$ polinomunun **Q** üzerinde indirgenemez olduğunu söyleyemeyiz. Çünkü p asalını *-6, 9* ve *-18* i bölecek şekilde seçmeliyiz ve bu da ancak $p = 3$ olmasıyla mümkün olabilir. Ancak *3, -6, 9* ve *-18* i bölmesine ve başkatsayı olan *1* i de bölmemesine rağmen $3^2 = 9$, sabit terim olan *-18* i bölmemesi gerektiği halde bölmektedir. Dolayısıyla Eisenstein kuralı bu polinomun **Q** üzerinde indirgenemez olduğunu söylemek için yeterli değildir.

10.13. Örnek. $4x^3 - 7x^2 + 21x - 42$ polinomu **Q** üzerinde indirgenemezdir. Gerçekten de $p = 7$ asalı alınırsa, ilk terim hariç diğer tüm terimlerin katsayıları *(-7, 21* ve *-42) 7* ile bölünürken, *7* baş katsayı olan *4* ü bölmez ve $7^2 = 49$ da sabit terim olan *-42* yi bölmez. Yani Eisenstein kuralındaki tüm ön şartlar sağlanmaktadır ve dolayısıyla polinom indirgenemezdir.

10.14. Örnek. $x^2 - 2$ polinomu $p = 2$ için Eisenstein kuralına göre indirgenemezdir.

Şimdi, Eisenstein kuralını kullanamadığımız durumlarda faydalanabileceğimiz ve *mod n de indirgeme* adını vereceğimiz bir yöntem göreceğiz:

$p(x) \in \mathbf{Z}[x]$ polinomu sıfırdan farklı indirgenebilen bir polinom olsun.

$$p(x) = q(x)r(x)$$

diyelim. $\mathbf{Z} \to \mathbf{Z}_n$ dönüşümü yardımıyla elde edilen ve katsayıları mod n de indirgeyen $\mathbf{Z}[x] \to \mathbf{Z}_n[x]$ homomorfizmini düşünelim. Bu dönüşüm altında fonksiyonların görüntülerini altlarını çizerek gösterelim. Bu durumda $\underline{p} = \underline{q}.\underline{r}$ dir. Eğer $\partial\underline{p} = \partial p$ ise $\partial\underline{q} = \partial q$ ve $\partial\underline{r} = \partial r$ olduğu açıktır. Bu yüzden indirgenebilir p polinomunun mod n deki indirgeme dönüşümü altındaki görüntüsü de indirgenebilirdir. Bu da aşağıdaki sonucu gerektirir:

10.15. Teorem. Eğer $p(x) \in \mathbf{Z}[x]$ ise ve $p(x)$ in görüntüsü olan $\underline{p}(x) \in \mathbf{Z}_n[x]$ polinomu indirgenemezse ve bu iki polinomun dereceleri eşitse p polinomu $\mathbf{Z}_n[x]$ in bir elemanı olarak indirgenemezdir.

Uygulamada, gerekli olmasa da, n yi asal alırız. Mod n de indirgeme yapmamızın altında yatan neden, $\mathbf{Z}_n$ sonlu olduğundan, $\underline{p}$ nin sadece sonlu tane mümkün olan çarpanının olmasıdır.

10.16. Örnek. $x^5 - x + 1$ polinomu hiç bir p asalı için Eisenstein kuralındaki şartları sağlamayacaktır. Bunun yerine mod 5 teki indirgemeyi göz önüne alacağız. 0, 1, 2, 3 ve 4 ten hiçbiri kök olmadığından bu polinomun lineer bir çarpanı yoktur. O halde eğer varsa çarpanlar ikinci ve üçüncü derecedendir. Yani a, b, c, d ve e; mod 5 teki 0, 1, 2, 3 veya 4 değerlerini almak üzere

$$x^5 - x + 1 = (x^2 + ax + b)(x^3 + cx^2 + dx + e)$$

şeklinde olmalıdır. Katsayıların eşitlenmesiyle bir denklem sistemi elde edilir:

$$a + c = 0,$$

$$b + ac + d = 0,$$

$$bc + ad + e = 0,$$

$$ae + bd = -1,$$

$$be = 1.$$

Bu denklem sisteminin çözümünün olmadığı açıktır. Dolayısıyla bu polinom mod 5 te indirgenemezdir ve dolayısıyla $\boldsymbol{Z}$ de indirgenemezdir.

Bu örnekte 5 modu yerine daha küçük olan 2 veya 3 modu seçilemez miydi? Bunun için belli bir kural yoktur. Ancak bu örnekte 2 modunda $a = b = c = e = 1$ ve $d = 0$ değerlerinin bir çözüm olduğu kolayca görülebilir. Yani bu polinom mod 2 de

$$x^5 - x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$$

şeklinde çarpanlarına ayrılabilir. Bu yüzden 2 modu bize aradığımız sonucu vermeyecektir. Acaba mod 3 te bu yapılabilir mi?

10.17. Örnek. $x^6 - 2x^3 - 5x^2 - 12$ polinomunun $\boldsymbol{Q}[x]$ de indirgenebilirliğini inceleyiniz.

Eisenstein kuralını uygulayabilmemiz için ilk olarak 2, 5 ve 12 yi aynı anda bölen bir p asalı bulabilmeliyiz. Bu da mümkün değildir. O halde mod n de indirgemeyi kullanarak bu polinomun indirgenebilirliğini araştırmalıyız.

Mod 2 de 0 bir çözüm olduğundan lineer çarpan vardır.

Mod 3 ü deneyelim. 0 yine bir çözümdür ve bir lineer çarpan mevcuttur.

Mod 5 de 0, 1, 2, 3 veya 4 ün çözüm olmadığı kolayca hesaplanabilir. O halde lineer bir çarpan yoktur. Yani iki durum söz konusu olabilir. İlki biri ikinci, diğeri dördüncü

derece olan iki çarpan; ikincisi de her biri üçüncü dereceden olan iki çarpan olabilir. İlk durumda

$$x^6 - 2x^3 - 5x^2 - 12 = (x^2 + ax + b)(x^4 + cx^3 + dx^2 + ex + f)$$

yazalım. Katsayıları eşitlediğimizde

$$a + c = 0,$$

$$ac + b + d = 0,$$

$$ad + bc + e = -2,$$

$$ae + bd + f = -5,$$

$$af + be = 0,$$

$$bf = -12$$

denklemleri elde edilir. Uzun hesaplamalardan sonra bu sistemin bir çözümünün olmadığı görülür. O halde son ihtimal üçüncü dereceden iki çarpandır.

$$x^6 - 2x^3 - 5x^2 - 12 = (x^3 + ax^2 + bx + c)(x^3 + dx^2 + ex + f)$$

yazalım. Buradan elde edilecek

$$a + d = 0,$$

$$ad + b + e = 0,$$

$$ae + bd + c + f = 3,$$

$$af + be + cd = 0,$$

$$bf + ce = 0,$$

$$cf = 3$$

denklemlerinin mod 5 te çözümü olmadığı görülebilir. Yani $x^6 - 2x^3 - 5x^2 - 12$ polinomu 5 modunda indirgenemezdir. O halde $\mathbf{Q}[x]$ de de indirgenemezdir.

10.18. Örnek. $x^4 + 5x^3 - 10x^2 + 4x - 6$ polinomunun indirgenebilirliğini inceleyiniz.

Eisenstein kuralını uygulayabilmemiz için *5, 10, 4* ve *6* sayılarını bölen bir asal sayı bulunması gerekir ki bu mümkün değildir. Bu sebeple mod *n* deki indirgemeyi kullanmalıyız.

2 modunda *0* bir köktür. O halde bir lineer çarpan mevcuttur.

3 modunda *0* yine bir köktür. O halde bir lineer çarpan mevcuttur.

5 modunda *0, 1, 2, 3* ve *4* ün kök olmadığı görülebilir. O halde lineer çarpan yoktur. O halde tek ihtimal ikinci dereceden iki çarpanın varlığıdır. Bunu görmek için

$$x^4 + 5x^3 - 10x^2 + 4x - 6 = (x^2 + ax + b)(x^2 + cx + d)$$

yazalım. Katsayılar eşitlendiğinde

$$a + c = 5,$$

$$ac + b + d = -10,$$

$$ad + bc = 4,$$

$$bd = -6$$

denklemleri elde edilir.

2 modunda $a = b = d = 0$ ve $c = 1$ çözümünün varlığını görmek zor değildir. Yani

$$x^4 + 5x^3 - 10x^2 + 4x - 6 = x^2(x^2 + x)$$

şeklinde çarpanlarına ayrılabilir.

3 modunda $a = d = 0$ ve $b = c = 2$ nin çözüm olduğu açıktır.

5 modunda ise bu denklemlerin çözümü yoktur. Yani *5* modunda $x^4 + 5x^3 - 10x^2 + 4x - 6$ polinomu indirgenemezdir. O halde bu polinom, $\mathbf{Q}[x]$ de de indirgenemezdir.

10.19. Tanım. *p* asal iken

$$\phi_p(x) = (x^p-1)/(x-1) = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$$

polinomuna *p-inci cyclotomic (döngüsel) polinom* adı verilir.

10.20. Teorem. *R* bir halka ve $c \in R$ olsun. $f(x) \mapsto f(x+c)$ dönüşümü $R[x]$ halkasından kendisine bir halka izomorfizmidir.

10.21. Sonuç. *R* bir cisim, $p(x) \in R[x]$ ve $c \in R$ olsun. $p(x)$ in indirgenemez olması için gerek ve yeter şart $p(x+c)$ nin indirgenemez olmasıdır.

10.22. Teorem. Her *p* asalı için *p*-inci döngüsel polinom $\mathbf{Q}[x]$ de indirgenemezdir.

İspat. Üstteki sonuç gereği

$$\phi_p(x) = (x^p-1)/(x-1)$$

polinomunun indirgenemez olması için gerek ve yeter şart

$$\phi_p(x+1) = ((x+1)^p-1)/x$$

polinomunun indirgenemez olmasıdır. Bu son polinom açıldığında $\binom{p}{i}$ Binom katsayısı olmak üzere

$$\phi_p(x+1) = ((x+1)^p-1)/x = x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \ldots + p$$

elde edilir. *p* asal olduğundan ve *p*, tüm $\binom{p}{i}$ katsayılarını böldüğünden Eisenstein kuralı kullanılabilir ve $\phi_p(x)$ indirgenemezdir.

Eğer *n* asal değilse $x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1$ polinomu $\mathbf{Q}[x]$ de çarpanlarına ayrılabilir. Örneğin $n = 4$ için

$$x^3 + x^2 + x + 1 = (x+1)(x^2+1)$$

şeklinde çarpanlarına ayrılabilir.

10.23. Sonuç. Bir *a* tamsayısı bir tamkare değilse, her $n \geq 2$ için $x^n - a$ polinomu $\mathbf{Q}[x]$ de indirgenemezdir.

İspat. $a \neq \pm 1$ olduğundan *a* yı bölen bir *p* asalı mevcuttur. Bu *p* için Eisenstein kuralının uygulanabileceği açıktır.

Bu son sonuç bize **Q** üzerinde herhangi bir *n*-inci dereceden indirgenemeyen polinomların varlığını belirtmektedir.

Alıştırmalar

1) $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbf{Z}[x]$ olsun. Eğer r/s, $(r,s) = 1$ olmak üzere, $f(x)$ in bir rasyonel kökü ise $r \mid a_0$ ve $s \mid a_n$ dir. Bundan faydalanarak $\mathbf{Z}[x]$ teki birim başkatsayılı bir polinomun bir rasyonel kökünün aslında bir tamsayı olması gerektiğini gösteriniz.

2) Aşağıdaki polinomların $\mathbf{Q}[x]$ de çarpanlarına ayrılıp ayrılamadığını araştırınız.

a. $3x^2 - 7x - 5$,
b. $6x^3 - 3x - 18$,
c. $x^3 - 7x + 1$,
d. $x^3 - 9x - 9$.

3) F bir cisim olsun. $a_0 + a_1x + \ldots + a_nx^n \in F[x]$ indirgenemezse, $a_n + a_{n-1}x + \ldots + a_0x^n$ polinomu da indirgenemezdir.

4) $f(x) = x^4 - 10x^2 + 1$ polinomunun $\mathbf{Q}[x]$ de indirgenemez olduğunu gösteriniz. (Yol gösterme: Birinci alıştırmayı kullanarak $f(x)$ in rasyonel kökleri olmadığını gösteriniz. Sonra da

$$x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 - ax + c)$$

olacak şekilde a, b ve c rasyonel sayılarının bulunmadığını gösteriniz.

11. İkinci, Üçüncü ve Dördüncü Dereceden Denklemlerin Genel Çözüm Metodları

Bu bölümde ikinci, üçüncü ve dördüncü dereceden denklemlerin sadece katsayılarından faydalanarak nasıl çözülebileceğine dair yöntemler göreceğiz. Galois'nın göstermiş olduğu temel sonuçlardan biri de hatırlanacağı gibi beş ve daha yüksek dereceden denklemler için bu tür metodların var olmadığı idi.

11.1. Tanım. *n*-inci dereceden bir *f(x)* polinomunda x^{n-1} li terim bulunmuyorsa *f(x)* polinomuna *düşürülmüş polinom* diyeceğiz. Yani böyle bir polinom

$$f(x) = r_n x^n + r_{n-2} x^{n-2} + r_{n-3} x^{n-3} + \ldots$$

şeklindedir.

11.2. Lemma. Eğer $f(X) = a_n X^n + a_{n-1} X^{n-1} + a_{n-2} X^{n-2} + \ldots$ şeklindeyse X yerine $x - a_{n-1}/na_n$ yazılarak

$$f^*(x) = f(x - a_{n-1}/na_n)$$

düşürülmüş polinomu elde edilebilir. Yani her polinom uygun bir dönüşüm yardımıyla düşürülmüş bir polinom haline getirilebilir. Ayrıca, eğer u, $f^*(x)$ in bir kökü ise $u - a_{n-1}/na_n$ de *f(X)* in bir köküdür.

İspat. İlk iddia basit birkaç işlemle gösterilebilir. İkinci ise $0 = f^*(u) = f(u - a_{n-1}/na_n)$ oluşundan görülür.

İkinci dereceden denklemler için kökleri veren formüller genelde verilen ifadeyi tam kare yapmakla elde edilmiştir. Biz burada daha yüksek derecelere de (3 ve 4) genelleştirebileceğimiz bir yöntem kullanacağız.

$$X^2 + bX + c$$

ikinci derece ifadesini ele alalım. X yerine $x - b/2$ yazılmakla

$$x^2 + c - b^2/4$$

düşürülmüş ikinci derece denklemi elde edilir. Bu denklemin aşikâr köklerinin u = $\pm\frac{1}{2}\sqrt{b^2-4ac}$ olduğu kolayca görülmektedir. Lemma 11.2 gereği

$$X = u - a_{n-1}/na_n = -\frac{b}{2}\pm\frac{1}{2}\sqrt{b^2-4ac}$$

değerleri de başlangıçta verilen orjinal ikinci derece denkleminin kökleridir.

Daha yüksek dereceden bir f(x) polinomunun köklerini veren formüllerin arayışına geçmeden önce f(x) $\in$ **Z**[x] olduğunda 10. bölümün ilk alıştırmasını kullanarak verilen ifadenin rasyonel köklerinin olup olmadığına bakılması gerektiğini belirtmeliyiz. Eğer u, örneğin bir f(x) üçüncü derece denkleminin bir kökü ise, f(x) in diğer kökleri f(x)/(x-u) ikinci derece denkleminin kökleri olacaktır.

$X^3 + aX^2 + bX + c$ üçüncü derece denkleminin düşürülmesiyle elde edilen polinom

$$g(x) = x^3 + qx + r$$

formundadır. Lemma 11.2 gereği g(x) in köklerini veren bir formül, orjinal denklemin kökleri için bir formül verecektir. Aşağıda göreceğimiz formül Scipio del Ferro (1515) tarafından verilmiştir. Aynı dönemde benzer bir formül Tartaglia tarafından bulunmuştu. İki formül de yazılı olarak ilk defa Cardan (1545) tarafından yazılan kitapta yer almıştır.

u, g(x) in bir kökü olsun. u = y + z olacak şekilde y ve z sayılarını seçelim. Bu durumda

$$u^3 = (y + z)^3 = y^3 + z^3 + 3(y^2z + yz^2) = y^3 + z^3 + 3uyz$$

yazılabilir. Böylece

$$y^3 + z^3 + (3yz + q)u + r = 0 \qquad (1)$$

elde edilir. Şu ana kadar y ve z ye sadece bir kısıt koyduk. Bu da u = y + z dir. 11. bölümün ilk alıştırması gereği ikinci bir kısıt daha koyabiliriz:

$$yz = -q/3. \qquad (2)$$

O halde (1) denkleminde u ya bağlı olan lineer terim ortadan kalkacaktır. Bu durumda

$$y^3 + z^3 = -r$$

ve

$$y^3z^3 = -q^3/27$$

denklemleri elde edilir. Bu iki denklem y^3 ve z^3 değişkenlerine göre çözülebilir. İkinci denklemden z^3 çekilip diğer denklemde yerine konulduğunda

$$y^3 - q^3/27y^3 = -r$$

ve buradan da

$$y^6 + ry^3 - q^3/27 = 0$$

elde edilir. Bu son formül y^3 değişkenine göre ikinci dereceden bir formüldür ve çözüldüğünde

$$y^3 = \frac{1}{2}(-r + \sqrt{r^2+4q^3/27}) \qquad (3)$$

kökü bulunur. Ayrıca (2) denkleminden $z = -q/3y$ elde edilir. Böylece $g(x)$ in bir $u = y + z$ kökünü bulmuş oluruz. Bu üçüncü derece denklemin diğer iki kökü ise $g(x)/(x-u)$ denkleminin kökleridir.

Şimdi bu iki kökü açık olarak veren bir formül vereceğiz. Eğer $w = e^{2\pi i/3}$ birimin üçüncü dereceden bir kökü ise y nin üç değeri mevcuttur: Birinci değer (3) denklemiyle verilir. Diğer iki kök ise wy ve w^2y dir. Bunlara karşılık gelen değerler de

$$-q/3wy = (1/w)z = w^2z$$

ve

$$-q/3w^2y = (1/w^2)z = wz$$

şeklindedir.

Sonuç olarak üçüncü derece denkleminin köklerini veren kübik formüller

$$R = r^2 + 4q^3/27$$

ve

$$y^3 = \frac{1}{2}(-r + \sqrt{R})$$

olmak üzere

$$y + z; \qquad wy + w^2z; \qquad w^2y + wz$$

şeklinde bulunur.

11.3. Örnek. Eğer $f(x) = x^3 - 15x - 126$ şeklindeyse $f(x)$ zaten düşürülmüş bir polinom olarak verilmiş demektir (aksi halde $x \mapsto x - b/3$ dönüşümü kullanılarak düşürülmüş hale getirilmeliydi). Burada $q = -15$, $r = -126$, $R = 15376$ ve $\sqrt{R} = 124$ tür. Böylece

$$y^3 = \frac{1}{2}(-(-126) + 124) = 125$$

ve böylece de $y = 5$ bulunur. Ayrıca $z = -q/3y = 15/15 = 1$ olduğundan ilk kök

$$u = y + z = 5 + 1 = 6$$

olarak bulunur. Diğer iki kökü bulmak için bölme yaparak

$$(x^3 - 15x - 126)/(x-6) = x^2 + 6x + 21$$

denkleminin köklerine bakılır. Bunlarsa $-3 \pm 2\sqrt{3}\,i$ dir. Bu iki kökü bulmanın yukarıda da belirttiğimiz ikinci bir yolu da kübik formülü kullanmaktır. Bu durumda da kökler $5w + w^2$ ve $5w^2 + w$ şeklindedir. w yerine $e^{2\pi i/3} = \cos(2\pi i/3) + i\sin(2\pi i/3) = -\frac{1}{2} + \frac{\sqrt{3}}{2}$ değeri yazıldığında bu iki kökün yukarıda da bulunduğu gibi

$$5w + w^2 = 5(-\frac{1}{2} + \frac{\sqrt{3}}{2}) + (-\frac{1}{2} + \frac{\sqrt{3}}{2})^2 = -3 + 2\sqrt{3}\,i$$

ve

$$5w^2 + w = 5(-\frac{1}{2} + \frac{\sqrt{3}}{2})^2 + (-\frac{1}{2} + \frac{\sqrt{3}}{2}) = -3 - 2\sqrt{3}\,i$$

olduğu hesaplanabilir.

Aşağıdaki örnek bazen kökleri kolayca bulunabilen üçüncü dereceden bir denklemin kübik formülle çözümünün kolay olmayabileceğini göstermektedir.

11.4. Örnek. $f(x) = x^3 - 7x + 6$ polinomunu göz önüne alalım. Bu polinomun köklerinin 1, 2 ve -3 olduğu deneme yoluyla kolayca hesaplanabilir. Ancak kübik formülden

$$y^3 = \frac{1}{2}(-6 + \sqrt{\frac{-400}{27}})$$

ve böylece de ilk kökün

$$\sqrt[3]{\frac{1}{2}\left(-6+\sqrt{\frac{-400}{27}}\right)} + \sqrt[3]{\frac{1}{2}\left(-6-\sqrt{\frac{-400}{27}}\right)}$$

olduğu bulunur. O halde bu ifade 1, 2 ya da -3 e eşittir. Ama bu ifadenin tamsayı olmanın ötesinde reel ya da rasyonel olup olmadığı bile net değildir.

$R = r^2 + 4q^3/27$ ifadesi negatif oldukça bu durumla karşılaşılacağı açıktır. Çünkü biz her üçüncü derece denklemin en az bir reel kökü olduğunu biliyoruz. Ancak kübik formüldeki kökler $\sqrt{R}$ ifadesini içermektedir.

Benzer şekilde $x^3 - 15x - 4 = 0$ denkleminin kökleri de

$$x = \sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}$$

formülü ile verilmekteyse de aslında bu kökün x = 4 olduğunu görmek çok zor değildir.

16. yüzyılda matematikçiler, bu son örnekte karşılaşılan durumla karşılaştıklarında oldukça şaşırmış ve tabii ki çaresiz kalmışlardı. Bu dönemde ikinci derece denklemlerin sanal kökleri (hatta negatif kökleri bile) yok sayılıyordu. Örneğin alanı A ve çevresi Ç olan bir dikdörtgenin a ve b ile gösterilen kenar uzunluklarını bulmak için

$$A = ab$$

$$Ç = 2a + 2b$$

denklemlerinin çözülmesi gereklidir. Bunu yaparken de b = A/a değeri ikinci denklemde yerine konularak

$$Ç = 2a + 2A/a$$

ve

$$2a^2 - Ça + 2A = 0$$

denklemi elde edilir ki bunun kökleri

$$a = \frac{1}{4}\left(p \pm \sqrt{p^2 - 16A}\right)$$

şeklindedir. $p^2 - 16A$ değeri negatifse verilen çevre ve alana sahip bir dikdörtgenin var olmadığını açıkça söyleyebiliriz. Ancak bu son örnekte karşımıza çıkan kompleks sayılara olan ihtiyacı 16. yüzyılda nasıl açıklayabiliriz? Bazı örneklerde çok ta kullanışlı olmayan

kübik formülün matematik tarihindeki rolü sanıldığından da önemlidir. Çünkü bu denklem yüzünden bazı örneklerde duyulan çaresizlik, atalarımızı kompleks sayılara yöneltmişti.

11.5. Uyarı. $f(x) = x^3 + qx + r$ **üç**üncü derece denklemin köklerini işe yarar bir şekilde veren ve Viete tarafından verilmiş olan trigonometrik bir formül de mevcuttur:

Eğer f(x) in tüm kökleri reel ise bunlar, $t = \sqrt{-4q/3}$ ve $\cos(\alpha) = -4r/t^3$ olmak üzere (q burada negatif olmalıdır)

$$t\cos(\alpha/3), \quad t\cos(\alpha/3 + 2\pi/3), \quad t\cos(\alpha/3 + 4\pi/3)$$

şeklindedir.

Eğer f(x) in kompleks kökleri varsa bu durumda -4q/3 ün işaretine bağlı olarak iki ihtimal söz konusudur. Eğer $-4q/3 \geq 0$ ise f(x) in reel kökü $\cosh(\beta) = -4r/t^3$ olmak üzere

$$t\cosh(\beta/3)$$

tür. Eğer $-4q/3 < 0$ ise f(x) in reel kökü, $\sinh(\gamma) = -4r/t^3$ olmak üzere

$$t\sinh(\gamma/3)$$

dir.

Şimdi dördüncü derece denklemlerin çözümünü ele alalım. Bu denklemler için ilk formüller yaklaşık 1545 yılında Luigi Ferrari tarafından bulunmuştur. Ancak burada 1637 de Descartes tarafından verilen metodu ele alacağız. Dördüncü dereceden

$$X^4 + aX^3 + bX^2 + cX + d$$

polinomunu alalım. $X = x - a/4$ dönüşümü yapılarak

$$h(x) = x^4 + qx^2 + rx + s$$

düşürülmüş polinomu elde edilir. Lemma 11.2 gereği h(x) in köklerini veren bir formül bize aynı zamanda orjinal denklemin köklerini veren bir formül de verecektir.

$$x^4 + qx^2 + rx + s = (x^2 + kx + l)(x^2 - kx + m)$$

yazalım. Eğer k, l ve m değerlerini bulursak problem ikinci dereceden denklemlerin çözümüne dönüşmüş olur. Sağ taraftaki çarpmalar yapılır ve polinom eşitliği kullanılırsa

$$l + m - k^2 = q,$$

$$k(m - l) = r,$$

$$lm = s$$

eşitlikleri elde edilir. İlk iki denklemden

$$2m = k^2 + q + r/k$$

$$2l = k^2 + q - r/k$$

elde edilir. Buradaki m ve l değerleri yukardaki denklemde yerine konulduğunda

$$k^6 + 2qk^4 + (q^2 - 4s)k^2 - r^2 = 0$$

denklemi elde edilir ki bu k^2 ye göre bir üçüncü dereceden denklemdir. Dolayısıyla yukarıda gördüğümüz yöntemlerden biriyle çözülebilir. Bulunan k değeri yerine konulduğunda l ve m de bulunabilir ve böylece elde edilecek ikinci dereceden iki denklemin çözümleri bize orjinal denklemin dört çözümünü verecektir.

11.6. Örnek. Kökleri, yapılacak tüm bu işlemlerden sonra tanınabilir şekilde elde edilecek olan bir dördüncü derece denklemini yazmak kolay değildir. Bu örnekteki 4. dereceden polinom 19. yüzyılda yazılmış olan bir ders kitabından alınmıştır. Eğer

$$f(x) = x^4 - 2x^2 + 8x - 3$$

ise polinom düşürülmüş bir polinomdur. Bu yüzden iki tane ikinci dereceden ifadenin çarpımı olarak yazılmaya hazırdır.

$$x^4 - 2x^2 + 8x - 3 = (x^2 + kx + l)(x^2 - kx + m)$$

yazalım. Sağ taraf çarpılıp karşılıklı terimlerin katsayıları eşitlenirse

$$l + m - k^2 = -2,$$

$$k(m - l) = 8,$$

$$lm = -3$$

eşitlikleri elde edilir. İlk iki denklemden

$$2m = k^2 - 2 + 8/k$$

$$2l = k^2 - 2 - 8/k$$

elde edilir. Buradaki m ve l değerleri yukardaki denklemde yerine konulduğunda

$$k^6 - 4k^4 + 16k^2 - 64 = 0$$

denklemi elde edilir ki bu k^2 ye göre bir üçüncü dereceden denklemdir. $t = k^2$ dönüşümü yapılırsa

$$t^3 - 4t^2 + 16t - 64 = 0$$

kübik denklemi elde edilir. Bu da

$$t^3 - 2^2t^2 + 2^4t - 2^6 = 0$$

şeklinde düzenlendiğinde aslında

$$(t - 2^2)^3 = 0 \quad \text{yani} \quad (k^2 - 2^2)^3 = 0$$

denklemi elde edilmiş olur. Bu son denklemin aşikar çözümleri de $k = \pm 2$ dir. $k = 2$ alırsak

$$2m = 4 - 2 + 4 = 6$$

$$2l = 4 - 2 - 4 = -2$$

ve böylece $m = 3$ ve $l = -1$ bulunur. Benzer şekilde $k = -2$ alındığında da $m = -1$ ve $l = 3$ bulunacaktır. Böylece

$$x^4 - 2x^2 + 8x - 3 = (x^2 + 2x - 1)(x^2 - 2x + 3)$$

ve

$$x^4 - 2x^2 + 8x - 3 = (x^2 - 2x + 3)(x^2 + 2x - 1)$$

ayrışımları elde edilir. Bu iki ayrışım da aynı olduğundan aranan dört kökün

$$-1 + i\sqrt{2}\,,\ -1 - i\sqrt{2}\,,\ 1 + i\sqrt{2} \quad \text{ve} \quad 1 - i\sqrt{2}$$

olduğu görülebilir.

Alıştırmalar

1) u ve v sayıları verildiğinde

$$y + z = u \text{ ve } yz = v$$

olacak şekilde (kompleks de olabilecek) y ve z sayılarının var olduğunu gösteriniz.

2) $x^3 + x^2 - 36$ ifadesini $\mathbf{Q}[x]$ de çarpanlarına ayırınız.

3) $g(x) = x^3 + qx + r$ olsun ve $R = r^2 + 4q^3/27$ sayısını tanımlayalım. u, g(x) in bir kökü olsun ve $y^3 = \frac{1}{2}(-r + \sqrt{R})$ olmak üzere $u = y + z$ diyelim.

$$z^3 = \frac{1}{2}(-r - \sqrt{R})$$

olması gerektiğini gösteriniz.

4) Aşağıda verilen $f(x) \in \mathbf{R}[x]$ polinomlarının köklerini bulunuz.

a) $f(x) = x^3 - 3x + 1$
b) $f(x) = x^3 - 9x + 28$
c) $f(x) = x^3 - 24x^2 - 24x - 25$
d) $f(x) = x^3 - 15x - 4$
e) $f(x) = x^3 - 6x + 4$
f) $f(x) = x^4 - 15x^2 - 20x - 6$.

12. Cisim Genişlemeleri ve Sonlu Cisimler

Bu bölümde cisimlerin nasıl daha büyük cisimler elde etmede kullanıldığını ve bunun nasıl yapıldığını göreceğiz. Eğer $f(x) \in F[x]$ ise $f(x)$ in köklerinin F katsayı cisminde kalmayabileceği bilinmektedir. Örneğin $x^2+1 \in \mathbf{R}[x]$ olmakla beraber bu polinomun kökleri olan $\pm i$ sayıları $\mathbf{R}$ da kalmamaktadır. Bu iki kök daha geniş bir cisim olan $\mathbf{C}$ kompleks sayılar cisminde kalmaktadır. Yani bir polinomun kökleri katsayılarının alındığı cisimde kalmak zorunda değildir. Bu şekilde yeterli olmayan bir cismin bazı elemanlar katılarak yeterli bir cisim haline getirilmesine cisim genişlemesi denilmektedir.

Çeşitli cisim genişlemeleri mevcut olsa da biz bunlardan en yaygını olan basit genişlemelerle ilgileneceğiz.

12.1. Tanım. F cismi bir E cisminin altcismi ise E ye F *nin bir genişlemesi* denilir.

Örneğin $\mathbf{R}$, $\mathbf{Q}$ nun; $\mathbf{C}$ de hem $\mathbf{R}$ nin hem de $\mathbf{Q}$ nun bir genişlemesidir. Benzer olarak $F[x]$ ve $F[y]$, F cisminin; $F[x,y]$ de tüm bunların bir genişlemesidir.

Aşağıdaki teorem cisim genişlemelerinin varlığıyla ilgilidir.

12.2. Teorem (Kronecker). F bir cisim, $f(x)$ te $F[x]$ polinom halkasında sabit olmayan bir polinom olsun. Bu durumda F nin bir E genişlemesi ve $f(\alpha) = 0$ olacak şekilde bir $\alpha \in E$ sayısı mevcuttur.

12.3. Örnek. $F = \mathbf{R}$ ve $f(x) = x^2+1$ olsun. $\langle x^2+1\rangle$, $\mathbf{R}[x]$ de bir maksimal idealdir. O halde $\mathbf{R}[x]/\langle x^2+1\rangle$ bir cisimdir. Her bir $r \in \mathbf{R}$ sayısına $\mathbf{R}[x]/\langle x^2+1\rangle$ cisminde bir $r+\langle x^2+1\rangle$ elemanı karşılık getirilerek $\mathbf{R}$ ye $E = \mathbf{R}[x]/\langle x^2+1\rangle$ nin bir alt cismi olarak bakabiliriz.

$$\alpha = x + \langle x^2+1\rangle$$

denilirse $\mathbf{R}[x]/\langle x^2+1\rangle$ de

$$\alpha^2 + 1 = (x + \langle x^2+1\rangle)^2 + (1+ \langle x^2+1\rangle)$$

$$= (x^2 + 1) + \langle x^2+1\rangle = 0$$

dır. O halde α, $x^2 + 1$ polinomunun bir köküdür. $\mathbf{R}[x]/\langle x^2+1\rangle$ ile $\mathbf{C}$ özdeşlenebilir.

12.4. Tanım. *F* bir cisim ve α, *F* nin bir *E* genişlemesinde kalan bir eleman olsun. Eğer sıfırdan farklı bir $f(x) \in F[x]$ fonksiyonu için $f(\alpha) = 0$ oluyorsa α, *F üzerinde cebirseldir* denir. Aksi taktirde α *ya F üzerinde transandanttır* denilir.

12.5. Örnek. ***C***, ***Q*** nun bir genişlemesidir. $\sqrt{2}$, $x^2 - 2 = 0$ polinomunun bir kökü olduğundan $\sqrt{2}$, ***Q*** üzerinde cebirseldir. Ayrıca *i*, $x^2 + 1$ polinomunun bir kökü olarak ***Q*** üzerinde cebirseldir. π ve *e* sayıları ise ***Q*** üzerinde transandanttır.

Nasıl bir polinomun indirgenemez olması yerine bu polinomun bir cisim üzerinde indirgenemez olmasından bahsediyorsak, benzer şekilde bir sayının cebirsel oluşundan değil bir cisim üzerinde cebirsel oluşundan bahsederiz. Bunun sebebi de aşağıdaki örnektir:

12.6. Örnek. π reel sayısı ***Q*** üzerinde transandanttır. Ancak π, ***R*** üzerinde cebirseldir. Çünkü π, reel katsayılı $(x - \pi) \in \mathbf{R}[x]$ polinomunun bir köküdür.

12.7. Örnek. $\sqrt{1+\sqrt{3}}$ sayısı ***Q*** üzerinde cebirseldir. Gerçekten de $\alpha = \sqrt{1+\sqrt{3}}$ denilirse $\alpha^2 = 1 + \sqrt{3}$ veya denk olarak $\alpha^2 - 1 = \sqrt{3}$ elde edilir. İkinci kez kare alınırsa α nın $x^4 - 2x^2 - 2 \in \mathbf{Q}[x]$ polinomunun bir kökü olduğu görülür.

12.8. Tanım. ***C*** nin ***Q*** üzerinde cebirsel olan bir elemanına bir *cebirsel sayı* denilir. Benzer şekilde ***C*** nin ***Q*** üzerinde transandant olan bir elemanına bir *transandant sayı* denilir.

12.9. Teorem. *E*, *F* nin bir genişlemesi olsun ve $\alpha \in E$, *F* üzerinde cebirsel olsun. Bu durumda $p(\alpha) = 0$ olacak şekilde indirgenemeyen bir $p(x) \in F[x]$ polinomu mevcuttur. Bu polinom sabit farkıyla tektir. Eğer $f(x) \in F[x]$, $f(\alpha) = 0$ olacak şekilde indirgenemeyen ve sıfırdan farklı bir başka polinom ise $p(x)$, $f(x)$ i böler.

12.10. Tanım. *E*, *F* nin bir genişlemesi olsun ve $\alpha \in E$, *F* üzerinde cebirsel olsun. 12.9. Teoremde bahsedilen birim başkatsayılı polinoma α *nın F üzerindeki minimal polinomu* denilir. Kısaca $irr(\alpha,F)$ ile gösterilir. $irr(\alpha,F)$ nın derecesi α nın *F* üzerindeki derecesidir ve $deg(\alpha,F)$ ile gösterilir.

12.11. Örnek. $irr(\sqrt{2},\mathbf{Q}) = x^2 - 2$ dir. 12.7. Örnekteki $\alpha = \sqrt{1+\sqrt{3}}$ sayısı için $irr(\alpha,\mathbf{Q}) = x^4 - 2x^2 - 2$ dir.

12.12. Tanım. Belli bir $\alpha \in E$ için $E = F(\alpha)$ ise *E* ye *F cisminin bir basit genişlemesi* denilir.

α, *F* üzerinde cebirsel ise aşağıdaki teorem bize $F(\alpha)$ nın elemanlarının yapısı hakında net bilgi verecektir.

12.13. Teorem. $E = F(\alpha)$, F cisminin bir basit genişlemesi ve α, F üzerinde cebirsel olsun. $irr(\alpha,F)$ polinomunun derecesi $n \geq 1$ olsun. $E = F(\alpha)$ nın her bir β elemanı b_i ler F de kalmak üzere

$$\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$$

olarak bir tek şekilde ifade edilebilir.

Bu teorem bize basit genişlemelerin elemanları hakkında fikir vermektedir. Eğer genişleme n-inci dereceden indirgenemeyen bir polinom ile yapılmışsa genişleme cismindeki elemanlar $n-1$-inci dereceden olacaktır.

12.14. Örnek. $p(x) = x^2 + x + 1$ polinomu $Z_2[x]$ de indirgenemezdir. Çünkü ne 0, ne de 1 bu polinomun bir köküdür. O halde Z_2 nin $x^2 + x + 1$ polinomunun bir α kökünü de içeren bir E genişlemesi mevcuttur. 12.13. Teorem gereği $Z_2(\alpha)$ nın elemanları $0 + 0\alpha$, $1 + 0\alpha$, $0 + 1\alpha$ ve $1 + 1\alpha$ dır. Yani, 0, 1, α ve $1 + \alpha$ dır. Bu da dört elemanlı bir sonlu cisimdir.

12.15. Tanım. Bir F cisminin bir E genişlemesini ele alalım. Eğer E nin her bir elemanı F de cebirsel ise E ye F *nin bir cebirsel genişlemesi* denilir.

12.16. Tanım. $F[x]$ deki sabit olmayan her polinomun F de bir kökü varsa F ye *cebirsel kapalı cisim* denilir.

Reel sayılar cismi cebirsel kapalı değildir. Çünkü reel katsayılı $x^2 + 1$ polinomunun kökleri reel değildir. Rasyonel sayılar cismi de cebirsel kapalı değildir. Ancak kompleks sayılar cismi cebirsel kapalıdır. Sayı cisimleri içinde cebirsel kapalı olan tek cisim de kompleks sayılardır.

12.17. Teorem. Bir F cisminin cebirsel kapalı olması için gerek ve yeter şart $F[x]$ deki sabit olmayan her polinomun $F[x]$ de lineer çarpanlarına ayrılabilmesidir.

İspat. F cebirsel kapalı olsun ve $F[x]$ de sabit olmayan bir $f(x)$ polinomu alalım. O halde $f(x)$ in bir $a \in F$ kökü vardır. Dolayısıyla $x-a$, $f(x)$ in bir çarpanıdır. Yani

$$f(x) = (x-a)g(x)$$

yazılabilir. Burada $g(x)$ sabit değilse bir $b \in F$ kökü vardır. Sonuçta

$$f(x) = (x-a)(x-b)h(x)$$

yazabiliriz. Bu şekilde devam edilerek $f(x)$, $F[x]$ de lineer çarpanlarına ayrılabilir.

Tersine, $F[x]$ deki sabit olmayan her bir $f(x)$ polinomunun lineer çarpanlarına ayrılabildiğini varsayalım. Eğer $ax-b$, $f(x)$ in bir lineer çarpanıysa b/a, $f(x)$ in bir köküdür. Bu yüzden F cebirsel kapalıdır.

12.18. Teorem. Her F cisminin bir cebirsel kapanışı vardır.

Şimdi de sonlu cisimlerin yapısını ele alacağız. Daha önceden p asal bir sayı olmak üzere $\mathbf{Z}_p$ nin bir cisim olduğunu; n asal olmadığında da $\mathbf{Z}_n$ in cisim olmayıp sadece bir halka olduğunu görmüştük. Bu bölümde ise $\mathbf{Z}_2$ ye $\mathbf{Z}_2$ de olmayan bir eleman katarak dört elemanlı olan bir cisim elde ettik. Aslında tüm sonlu cisimler $\mathbf{Z}_p$ ye uygun elemanların katılmasıyla elde edilmektedir. İlk olarak Galois tarafından ayrıntılı bir şekilde incelendikleri için bu cisimlere Galois cismi de denilmektedir.

12.19. Teorem. F, eleman sayısı q olan bir cisim olsun. Eğer E, F nin n-inci dereceden bir genişlemesi ise E nin eleman sayısı q^n dir.

İspat. E yi F üzerinde bir vektör uzayı olarak düşünelim. $\{1, \alpha, ..., \alpha^{n-1}\}$ kümesi E için F üzerinde bir taban olsun. E cismindeki her β elemanının $b_i \in F$ olmak üzere bir tek şekilde

$$\beta = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}$$

olarak ifade edilebileceğini görmüştük. Her bir b_i, F deki q elemandan biri olarak seçileceğinden ve n tane b_i bulunduğundan bu şekilde oluşturulabilecek β elemanlarının toplam sayısı q^n'dir.

12.20. Tanım. R, toplamaya göre etkisiz elemanı 0 olan bir halka olsun. Eğer en az bir pozitif n tamsayısını her $r \in R$ için

$$n.r = 0$$

olacak şekilde bulabiliyorsak bu özellikteki en küçük n tamsayısına R halkasının *karakteristiği* denilir. Aksi halde R halkasının karakteristiği 0 olarak alınır. R'nin karakteristiği $Kar(R)$ ile gösterilir.

12.21. Örnek. $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ ve $\mathbf{C}$'nin karakteristiği sıfırdır. $\mathbf{Z}_n$'in karakteristiği ise n dir.

12.22. Sonuç. E, karakteristiği p olan sonlu bir cisim olsun. E cisminin eleman sayısı n pozitif bir tamsayı olmak üzere p^n'dir.

12.23. Teorem. E, $\mathbf{Z}_p$'nin cebirsel kapanışında kalan p^n elemanlı bir cisim olsun. E cisminin elemanları $\mathbf{Z}_p[x]$ halkasında $x^{p^n} - x$ polinomunun kökleridir.

İspat. E cismindeki sıfırdan farklı elemanların kümesi E^* olsun. E^* cisimdeki çarpma işlemine göre p^n-1 mertebeli bir gruptur. Bir grupta her bir elemanın mertebesi grubun

mertebesini böleceğinden her bir $\alpha \in E^*$ için α'nın mertebesi p^n-1 farkını böler. O halde $\alpha^{p^n-1}=1$ ve böylece de $\alpha^{p^n}=\alpha$ elde edilir. Sıfır da $x^{p^n}-x$ polinomunun bir kökü olduğundan her $\alpha \in E$, $x^{p^n}-x$ polinomunun bir köküdür. $x^{p^n}-x$ polinomunun en fazla p^n tane kökü olabileceğinden E cisminin $x^{p^n}-x$ polinomunun Z_p cisminin cebirsel kapanışındaki tüm kökleri bulundurduğu açıktır.

12.24. Teorem. F karakteristiği p olan bir cisim olsun. $x^{p^n}-x$ polinomunun F nin cebirsel kapanışında tam p^n tane farklı kökü vardır.

İspat. $x^{p^n}-x$ polinomunun tüm köklerinin katlılıklarının 1 olduğunu, yani hiçbir kökün katlılığının 2 olamayacağını göstermeliyiz.

Sıfırın tek katlı bir kök olduğu açıktır.

α, $x^{p^n}-x$ in sıfırdan farklı bir kökü olsun. O halde α, $x^{p^n-1}-1$ in de bir köküdür. $f(x) = x^{p^n-1}-1$ diyelim. Eğer $x-\alpha$, $f(x)$ in bir çarpanı ise

$$g(x) = \frac{f(x)}{x-\alpha} = x^{p^n-2}+\alpha x^{p^n-3}+\alpha^2 x^{p^n-4}+\ldots+\alpha^{p^n-3}x+\alpha^{p^n-2}$$

yazabiliriz. Göstermeye çalıştığımız $f(x)$ in $x-\alpha$ ile iki kez bölünmeyeceği, yani $g(x)$ in $x-\alpha$ ile bölünmeyeceğidir. Dikkat edilirse $g(x)$ te p^n-1 tane terim vardır ve $g(\alpha)$ hesaplanmaya kalkıldığında bu terimlerin hepsi α^{p^n-2} ye eşit olacaktır. O halde

$$g(\alpha) = (p^n-1)\,\alpha^{p^n-2}$$

$$= (p^n-1)\,\alpha^{p^n-1}.\frac{1}{\alpha}$$

elde edilir. $\alpha^{p^n-1} = 1$ olduğundan karakteristiğin de p olduğu gözönüne alındığında

$$g(\alpha) = (p^n-1).\frac{1}{\alpha}$$

$$= -\frac{1}{\alpha}$$

elde edilir. Yani $g(\alpha)$ sıfırdan farklıdır.

12.25. Sonuç. Her bir p^n asal kuvveti için p^n elemanlı bir sonlu cisim mevcuttur.

Böylece her sonlu cismin eleman sayısının ancak p^n olabileceğini ve tersine her bir p^n asal kuvveti için sonlu bir cismin mevcut olduğunu göstermiş olduk. Bu cisim p^n

elemanlı Galois cismi (Galois Field) olarak adlandırılır ve kısaca $GF(p^n)$ ile ya da bazen F_{p^n} ile gösterilir.

12.26. Sonuç. F herhangi bir sonlu cisim olsun. Her pozitif n tamsayısı için $F[x]$ de n-inci dereceden indirgenemeyen bir polinom mevcuttur.

12.27. Örnek. i) GF(9) cismini elde edelim.

GF(9), GF(3)={0,1,2} cisminin 2. dereceden bir genişlemesidir. $Z_3[x]$ de x^2+x+2 indirgenemez polinomunun bir kökü α olsun.

$$\Rightarrow GF(9) = \{\alpha + b\alpha | a, b \in GF(3)\}$$
$$= \{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$$

Tersleri: $\alpha^2+\alpha+2=0 \Rightarrow \alpha^2+\alpha=1$

Buna göre;

$$1^{-1}=1$$
$$2^{-1}=\frac{1}{2}=\frac{4}{2}=2$$
$$\alpha^{-1}=\frac{1}{\alpha}=\frac{\alpha^2+\alpha}{\alpha}=\alpha+1$$
$$(\alpha+2)^{-1}=\frac{1}{\alpha+2}=\frac{\alpha^2+\alpha}{\alpha+2}=\frac{\alpha^2+\alpha+\overbrace{\alpha^2+\alpha+2}^{0}+\overbrace{3\alpha}^{0}}{\alpha+2}=\frac{\alpha^2+5\alpha+2}{\alpha+2}=\frac{(\alpha+2)(\alpha+1)}{\alpha+2}=2\alpha+1$$
$$(2\alpha)^{-1}=\frac{1}{2\alpha}=\frac{\alpha^2+\alpha}{2\alpha}=\frac{\alpha+1}{2}=\frac{\alpha+1}{-1}=-\alpha-1=2\alpha+2$$

elde edilir.

ii) İkinci olarak GF(16) cisminin elemanlarını bularak terslerini araştıralım. 16 elemanlı cisim GF(16) = GF(2^4) olup GF(2) = {0,1} cisminin 4. dereceden bir genişlemesi olarak elde edilebilir. O halde 4. dereceden birim başkatsayılı indirgenemeyen bir polinom bulmalıyız. Bu polinoma $f(x) = x^4 + ax^3 + bx^2 + cx + d$ dersek a, b, c ve d; 0 veya 1 olduğunda elde edilecek 16 polinomdan indirgenemez olanlar $x^4 + x + 1$, $x^4 + x^2 + 1$, $x^4 + x^3 + 1$ şeklindedir. Bunlardan örneğin ilkini seçersek ve bunun bir köküne α dersek $f(\alpha) = \alpha^4 + \alpha + 1 = 0$ olacaktır.

GF(2^4) = {$a + b\alpha + c\alpha^2 + d\alpha^3$: a, b, c, d $\in$ GF(2)} şeklindedir. O halde GF(2^4) = {0, 1, α, $1 + \alpha$, α^2, $1 + \alpha^2$, $1 + \alpha + \alpha^2$, α^3, $1 + \alpha^3$, $1 + \alpha + \alpha^3$, $1 + \alpha^2 + \alpha^3$, $1 + \alpha + \alpha^2 + \alpha^3$, $\alpha + \alpha^3$, $\alpha^2 + \alpha^3$, $\alpha + \alpha^2 + \alpha^3$, $\alpha + \alpha^2$} olur.

Şimdi de elemanların terslerini bulalım: $\alpha^4+\alpha+1=0\Rightarrow\alpha^4+\alpha=-1=1$

Buna göre;

$*1^{-1}=1$

$*\alpha^{-1}=\frac{1}{\alpha}=\frac{\alpha^4+\alpha}{\alpha}=\alpha^3+1$

$*(\alpha+1)^{-1}=\frac{1}{\alpha+1}=\frac{\alpha^4+\alpha}{\alpha+1}=\frac{\alpha(\alpha+1)\left(\alpha^2-\alpha+1\right)}{\alpha+1}=\alpha\left(\alpha^2-\alpha+1\right)=\alpha\left(\alpha^2+\alpha+1\right)=\alpha^3+\alpha^2+\alpha$

$*\left(\alpha^2\right)^{-1}=\frac{1}{\alpha^2}=\frac{\alpha^4+\alpha}{\alpha^2}=\frac{\alpha^3+1}{\alpha}=\frac{\alpha^3+\alpha^4+\alpha}{\alpha}=\alpha^3+\alpha^2+1$

$*\left(\alpha^2+1\right)^{-1}=\frac{1}{\alpha^2+1}=\frac{\alpha^4+\alpha}{\alpha^2+1}=\frac{\alpha^4-\alpha}{\alpha^2-1}=\frac{\alpha(\alpha-1)\left(\alpha^2+\alpha+\right)}{(\alpha-1)(\alpha+1)}=\frac{\alpha\left(\alpha^2+\alpha+1\right)}{\alpha+1}$

$=\frac{\alpha\left(\alpha^2+\alpha+\alpha^4+\alpha\right)}{\alpha+1}=\frac{\alpha\left(\alpha^4+\alpha^2\right)}{\alpha+1}=\frac{\alpha^3\left(\alpha^2+1\right)}{\alpha+1}=\frac{\alpha^3\left(\alpha^2-1\right)}{\alpha+1}=\frac{\alpha^3(\alpha-1)(\alpha+1)}{\alpha+1}$

$=\alpha^3(\alpha-1)=\alpha^4-\alpha^3=\alpha+1+\alpha^3=\alpha^3+\alpha+1$

$*\left(\alpha^2+\alpha\right)^{-1}=\frac{1}{\alpha^2+\alpha}=\frac{\alpha^4+\alpha}{\alpha^2+\alpha}=\frac{\alpha(\alpha+1)\left(\alpha^2-\alpha+1\right)}{\alpha(\alpha+1)}=\alpha^2-\alpha+1$

$*\left(\alpha^3\right)^{-1}=\frac{1}{\alpha^3}=\frac{\alpha^4+\alpha}{\alpha^3}=\frac{\alpha^3+1}{\alpha^2}=\frac{\alpha^3+\alpha^4+1}{\alpha^2}=\frac{\alpha^2+\alpha^3+1}{\alpha}=\frac{\alpha^2+\alpha^3+\alpha^4+\alpha}{\alpha}$

$=\alpha^3+\alpha^2+\alpha+1$

$*\left(\alpha^3+\alpha\right)^{-1}=\frac{1}{\alpha^3+\alpha}=\frac{\alpha^4+\alpha}{\alpha^3+\alpha}=\frac{\alpha^3+1}{\alpha^2+1}=\frac{\alpha^3-1}{\alpha^2-1}=\frac{(\alpha-1)\left(\alpha^2+\alpha+1\right)}{(\alpha-1)(\alpha+1)}=\frac{\alpha^2+\alpha+1}{\alpha+1}$

$=\frac{\alpha^2+\alpha+\alpha^4+\alpha}{\alpha+1}=\frac{\alpha^4+\alpha^2}{\alpha+1}=\frac{\alpha^2\left(\alpha^2+1\right)}{\alpha+1}=\frac{\alpha^2\left(\alpha^2-1\right)}{\alpha+1}=\alpha^2(\alpha-1)=\alpha^3-\alpha^2=\alpha^3+\alpha^2$

elde edilir.