İSTANBUL KÜLTÜR ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

CİSİM GENİŞLEMELERİ HAKKINDA

YÜKSEK LİSANS TEZİ

Mehmet Fatih UÇAR

Anabilim Dalı : Matematik-Bilgisayar

Programı : Matematik-Bilgisayar

HAZİRAN 2007

İSTANBUL KÜLTÜR ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

CİSİM GENİŞLEMELERİ HAKKINDA

YÜKSEK LİSANS TEZİ
Mehmet Fatih UÇAR
0509040001

Tezin Enstitüye Verildiği Tarih : 21 Haziran 2007
Tezin Savunulduğu Tarih : 16 Temmuz 2007

Tez Danışmanı : Prof. Dr. Hülya ŞENKON
Diğer Jüri Üyeleri : Prof. Dr. Ahmet FEYZİOĞLU
Doç. Dr. Çiğdem GENCER

HAZİRAN 2007

ÖNSÖZ

Yüksek Lisans tezi olarak hazırlanan bu çalışma tarihçe, temel kavramlar ve cisim genişlemeleri bölümlerinden oluşmaktadır. Bu çalışmanın amacı cisim genişlemeleri teorisini inceleyerek Galois Teorisine bir giriş yapmaktır.

Bu çalışmanın hazırlanmasında emeği geçen herkese teşekkürü borç bilirim. Eksik yanları ve gözden kaçmış olabilecek yanlışlar konusunda hocalarımın hoşgörüsüne sığınırım.

İstanbul, Haziran 2007 Mehmet Fatih UÇAR

İÇİNDEKİLER

Üniversitesi : **İstanbul Kültür Üniversitesi**
Enstitüsü : **Fen Bilimleri**
Anabilim Dalı : **Matematik-Bilgisayar**
Programı : **Matematik-Bilgisayar**
Tez Danışmanı : **Prof. Dr. Hülya Şenkon**
Tez Türü ve Tarihi : **Yüksek Lisans – Haziran 2007**

ÖZET

CİSİM GENİŞLEMELERİ

Mehmet Fatih UÇAR

Bu çalışmada amaç, Galois Teorisinin temellerini oluşturan, cisim genişlemeleri teorisini ayrıntılı bir şekilde vermek ve Galois Teorisine bir giriş yapmaktır. Bu amaç doğrultusunda I. Bölümde, cisim teorisinin tarihsel gelişiminde matematikçilerin yaptığı çalışmalar ve katkıları yer almaktadır. II. Bölümde ise cisim genişlemeleri teorisinde kullanılacak temel kavramlar verilmektedir. III. Bölümde cisim genişlemeleri teorisi, ayrıntılı bir şekilde ele alınmaktadır. Bu bölümün 1. paragrafında cisim genişlemeleri ile ilgili genel bilgiler verilmekte, 2. paragrafta cisim genişlemelerinin önemli bir sınıfını oluşturan cebirsel genişlemeler incelenmekte, 3. paragrafta Kronecker Teoremi verilmekte, 4. paragrafta elemanter sayılar teorisinden önemli sonuçların da katkısıyla, sonlu cisimler teorisi ele alınmakta, 5. paragrafta parçalanış cisimleri incelenmekte, 6. ve son paragrafta ise Galois Teorisine giriş yapılmaktadır.

Anahtar Kelimeler : **Cisim genişlemesi, Galois genişlemesi, Cisim izomorfisi**

University	**:**	**İstanbul Kültür University**
Institute	**:**	**Institute of Science**
Science Programme	**:**	**Mathematics-Computer**
Programme	**:**	**Mathematics-Computer**
Supervisor	**:**	**Prof. Dr.Hülya Şenkon**
Degree Awarded and Date	**:**	**MS – June 2007**

SUMMARY

FIELD EXTENSIONS

Mehmet Fatih UÇAR

The object of this thesis is to give the theory of field extensions which gives the exposition to Galois Theory. For this purpose, in Chapter I a historical introduction is given, in Chapter II some fundamental concepts which are necessary in the teory of field extensions are given. Chapter III which is the last chapter of the thesis, consists of six paragraphs. In the first paragraph the generalconcepts about field extensions are given, in the second paragraph the algebraic extensions are studied, in the third paragraph Kronecker's Theorem is proved, in the fourth paragraph the theory of finite fieldes is considered, in the fifth paragraph the splitting fields are studied and in the last paragraph an introduction to Galois Theory is given

Keywords : Field extension, Galois extension, Field isomorphism

BÖLÜM I. TARİHÇE

Matematik tarihinde uzun bir süre cebir, polinomların kökleri üzerinde çalışma olarak anlaşıldı. Bu tabii ki, verilen özel bir polinomun köklerinin nümerik hesabından açıkça ayırdedilmelidir. Newton metodu, polinomların köklerinin hesaplanmasında en iyi bilinen yöntemdir. Köklerin gerçek değerini hesaplama işi, ikinci derecede önemli amaçtı. Cebirin asıl amacı, köklerin yapısını anlamaktı: "Kökler katsayılara nasıl bağlıdır?", "Kökler bir formülle verilebilir mi?" gibi.

Tabii ki, polinomların köklerinin varlığıyla ilgili olarak da benzer bir soru söz konusudur: "Her polinomun bir kökü var mı?" Burada üstü kapalı olarak, polinomların katsayılarının reel sayılar olduğu anlaşılırdı. A. Girard (1595 – 1632), herhangi bir ispat yöntemi vermeksizin, her polinomun (mutlaka kompleks sayılar kümesi olması gerekmeyen) uygun bir sayı kümesi içinde bir kökünün bulunduğunu ifade etti. R. Descartes (1596 – 1650), c bir polinomun bir kökü ise $x-c$ nin bu polinomun bir böleni olduğunu ileri sürdü ve özel bir aralığın içindeki reel köklerin sayısını belirlemek için bir kural verdi. L. Euler (1707 – 1783), her polinomun kompleks bir köke sahip olduğunu açıkladı. Bu sonuç, kendisine hiç uygun olmayan bir isimle, "cebirin esas teoremi" olarak adlandırıldı. Euler, bu teoremi derecesi ≤ 6 olan polinomlar için ispatladı. J.R. D'Alembert (1717 – 1783), J.L. Lagrange (1736 – 1813) ve P.S. Laplace (1749 – 1827) ise bunu ispatlamak için girişimlerde bulundular. Gauss'un eleştirdiği gibi, onların ispatları aslında uygun bir sayı kümesinde bir kökün varlığını kabul edip, o kökün de olduğunu göstermektedir. Gauss kendisi çeşitli ispatlar verdi ki, bunlardan hiçbiri modern standartlarda tamamen kabul görmedi. Bununla beraber, Gauss, cebirin esas teoreminin geçerli sayılan ilk ispatını sunmuş olmak gibi bir öneme sahiptir. Kronecker (1823 – 1891) in 1882 yılında ispatlamış olduğu, herhangi bir polinomun uygun bir "sayı" kümesinde bir kökünün bulunduğuna ilişkin teorem, şu an geçerli olan esas teoremdir.

Bu teorem, köklerin varlığını mümkün kılar, fakat köklerin yapısı hakkında bir açıklama yapamaz.

2. dereceden denklemlerin çözümü, çok eski uygarlıklar zamanında bilinmekteydi. 3. ve 4. dereceden polinomlar, İtalyan matematikçiler tarafından incelendi. Scipione del Ferro (1465 – 1526), 1515 yılında $x^3 + ax = b$ şeklindeki 3. dereceden denklemi köklü ifadelerle çözmeyi başardı. 1535'te ise Tartaglia (1499/1500 – 1557), $x^3 + ax^2 = b$ biçimindeki 3. dereceden denklemi çözdü. G. Cardano (1501 – 1576), 3. dereceden genel $x^3 + bx^2 + cx + d$ polinomunda x yerine $x-(b/3)$ koyarak, bu polinomu, içinde x^2'li terim bulunmayan bir polinoma dönüştürdü. Böylece, genelliği bozmaksızın, 3. derece denklemini $x^3 + px + q = 0$ şeklinde varsayarak, kökler için

$$\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$$

formülünü buldu. Bu formül, her ne kadar Cardano formülü olarak biliniyorsa da, aslında Tartaglia'ya aittir. Tartaglia bu formülü buldu, gizlilik içinde Cardano ile paylaştı, fakat Cardano sözünü tutmayarak, formülü 1545 yılında Ars Magna isimli kitabında yayınladı. Cardano'yu bu çalışmada özgün kılan ise, genel 3. derece denklemini "indirgenemeyen biçim" denilen $x^3 + px + q = 0$ şekline dönüştürmesi, 3. dereceden bir polimonun en fazla üç farklı kökünün bulunabileceğini belirtmesi ve simetrik polinomlara bir giriş yapmış olmasıdır.

Cardano'nun kitabı, 1540' larda öğrencisi L.Ferrari (1522 – 1565) 'nin bulduğu, 4. dereceden polinomların köklerinin bulunması ile ilgili bir metod içermektedir. Bu kitap, cebirin gelişimine büyük katkı sağladı. Cardano, tasavvur edilemez gibi görülen karmaşık sayılarla bile işlem yaptı. Ondan önceki matematikçiler, karmaşık sayılara gereksinim duymamışlar, $x^2 = -1$ biçimindeki denklemleri basitçe çözülemez olarak kabul etmişlerdi. Bununla beraber, Cardano'nun formülünde, bütün kökler reel olsa bile, negatif bir sayının karekökünün alınması gerekiyordu.

Sonuç olarak, 16. yüzyılın ilk yarısında cebir konusunda önemli ilerlemeler sağlandı. 1494 e kadar Fra Luca Pacioli (1445–1514 veya 1517), 3. dereceden bir polinomun kök işaretleri ile çözülemeyeceğini iddia ederken, 1540 larda hem 3. hem de 4. dereceden denklem, kök işaretleriyle çözüldü. Bir sonraki aşama ise 5. dereceden veya daha genel olarak, n. dereceden bir polinomun kökleri için bir formül bulmak olacaktı.

Derecesi ≤ 4 olan denklemlerin başka çözümleri, daha sonra Descartes, Walter von Tschirnhaus (1651-1708) ve Euler tarafından da verilmişti. Adı geçen matematikçiler, 5. dereceden bir polinomun kökleri için bir formül bulmaya çalıştılar, fakat başarılı olamadılar. Bunun üzerine matematikçiler, 5. dereceden bir denklemin kök işaretleriyle çözülebilmesi konusunda şüpheye düştüler.

Lagrange $1770 - 1771$ de, o zamana dek bilinen bütün polinom çözümü yöntemlerini irdelediği "Réflexions sur la résolution algébrique des équations" isimli uzun çalışmasını yayınladı. Amacı, polinom köklerinin bulunması ile ilgili, bilinen bu yöntemlerden genel bir çözüm türetmekti. 2., 3. ve 4. dereceden polinomları inceleyerek, bu yöntemleri genel bir prensip altında toplamayı başardı. Bir polinomun kökleri, *rezolvent* adı verilen bir *t* büyüklüğü cinsinden ifade edilmektedir ve *t* nin kendisi, aynı zamanda *rezolvent polinomu* denilen yardımcı bir polinomun köküdür. Verilen polinomun derecesi *n* ise, rezolvent polinomun x^n ye göre derecesi $(n-1)!$ dir. O halde $n \leq 4$ için yardımcı denklemin derecesi, verilen polinomun derecesinden daha küçüktür ve bu denklem, tümevarımla cebirsel olarak çözülebilir. Fakat $n \geq 5$ için yardımcı denklemi çözmek, asıl denklemi çözmekten daha kolay değildir.

Rezolvent, köklerin bir fonksiyonu olup, bu köklerin uygun permütasyonları ile sabit kalır. Örneğin derece 4 ise, $r_1r_2 + r_3r_4$ fonksiyonu r_1, r_2 ve r_3, r_4 kökleri, aralarında yer değiştirdiği takdirde değişmez. Lagrange böylece, uygun bir söyleyiş ve gösterim kullanmaksızın, köklerin permütasyonları ile uğraşmış, bugünkü dille, n. dereceden simetrik grupta çalışmıştır.

Lagrange, $n \leq 4$ durumlarında rezolvent polinomunun, r_i ler verilen polinomun kökleri, α ise $x^n - 1$ 'in bir kökü olmak üzere, $r_1 + \alpha r_2 + \cdots + \alpha^{n-1} r_n$ şeklinde olacağını belirtti. Bu şekildeki bir rezolvent, *n*=5 için geçerli değildi, fakat farklı biçimdeki ifadeler rezolvent olabilirdi. Lagrange, ne tür ifadelerin rezolvent olabileceği konusunda çalışmalar yaptı.

1799 da P.Ruffini (1765 – 1822), 5. dereceden genel denklemin cebirsel olarak çözümünün mümkün olmadığına ilişkin, çok tartışmaya yol açan bir ispat öne sürdü. 1826 yılında Abel, bu imkansızlık teoreminin ilk tam ispatını verdi. Bu ispat, iki kısımdan oluşmaktadır. İlk kısımda, rezolventlerin genel yapısının 3. ve 4. derece için Lagrange'ın önerdiği biçimde olması gerektiği, ikinci kısımda ise, 5. dereceden bir polinomun bir köke sahip olamayacağı gösterilmektedir. Ayrıca, ispatsız olarak, derecenin 5 ten büyük olması durumunda genel denklemin cebirsel olarak çözülemeyeceği eklenmiştir. Abel, hangi özel denklemlerin kök işaretleriyle çözülebileceğini de araştırdı. Bugünkü dille, bir denklemin kök işaretleriyle çözülebilmesi için bu denklemin Galois grubunun komütatif olması gerektiğini ifade eden bir teorem ispatladı. Bu yüzdendir ki, komütatif gruplar aynı zamanda "abel grubu" olarak da anılmaktadır.

Abel son olarak, genel denklemin kök işaretleriyle çözülemeyeceğini ispatladı. "Genel polinom", katsayıları bağımsız değişkenler olan, yani bilinmeyenler olan polinomdur. Abel'in teoremi, katsayıları karmaşık sayılar olan polinomlar için birşey ifade etmemektedir. Fakat, derecesi 5 veya 5 ten büyük olan, sabit katsayılı bazı polinom denklemleri, kök işaretleriyle çözülebilmektedir. Bir denklemin kök işaretleriyle çözülebilmesi için gerekli kriter nedir? Bu sorunun yanıtı, Fransız matematikçi Evariste Galois (1811 – 1832) tarafından verildi. Galois ile birlikte cebirin esas konusu, artık polinom denklemleri oldu. Galois, cebirsel yapıların (gruplar, halkalar, vektör uzayları, cisimler, vb) araştırılması anlamına gelen modern cebirin başlangıcına damgasını vurmuş oldu.

Galois, kısa ve dramatik bir yaşam sürdü. Makale yayımlamaya lise öğrencisi iken başladı (1828). Olağanüstü bir yeteneğe sahipti. "Ecole Plytéchnique" e girmek istiyordu, fakat iki defa girdiği giriş sınavlarını kazanamadı. Daha sonra söylediğine göre, başarısızlığının nedeni, soruları çok basit olması nedeniyle cevaplamamasıydı. Daha sonra "Ecole Normale" e girdi (1829), fakat oradan da öğrenci gazetesinde yayımlanan bir yazı yüzünden atıldı. Adı gitgide kötüye çıkmıştı. Bir taraftan matematik dersleri vererek hayatını kazanmaya çalışan Galois, bir taraftan da siyasete bulaşmıştı. 1830 Devrimi'ne Cumhuriyetçi olarak katıldı. Siyasi nedenlerle de iki kez hapse girip çıkan Galois, gizemli bir düello sonucu öldü.

Galois, Fransız Akademisi'ne birçok makale göndermiş, fakat bu makaleler, anlaşılamaz bulunarak geri çevrilmişti. Galois isminin tüm dünyada duyulmaya başlaması ve onun gelmiş geçmiş en iyi matematikçilerden biri olduğunun anlaşılması, J.Liouvelle (1809 – 1882) in 1846 da Galois'nın yaşam öyküsünü yayımlaması ile gerçekleşti.

Galois, her bir rezolvent denklemini, verilen polinomun katsayılarının ait olduğu cisim ile köklerinin ait olduğu cisim arasında yer alan bir ara cisim ile ilişkilendirdi. Galois'nın dahiyane fikri, verilen polinom ve ara cisimler ile bir dizi

grubu ilişkilendirmek ve cisimler hakkındaki bilgileri, gruplar teorisindeki ifadelere çevirmekti. Böylece gruplar teorisi, Galois tarafından inşa edilmiş oldu. Galois, bir polinom denkleminin kök işaretleriyle çözülebilmesi için gerek ve yeter koşulun, grup serisinde her grubun normal ve bir sonraki grup içinde asal indeksli olması olduğunu ispat etti.

Galois'nın verdiği kriter, bir polinomun kök işaretleriyle çözülüp çözülemeyeceğini anlamak için efektif bir yol değildir. O zamanki diğer matematikçiler, varolan çözülebilirliğin, verilen denklemin katsayılarının incelenmesi ya da bu denklemle ilgili daha düşük dereceli denklemlerin çözülmesi gibi daha somut yollarla gerçekleşmesini umuyorlardı. Galois bir yazısında: "Bana kök işaretleriyle çözülüp çözülmeyeceğini merak ettiğiniz bir polinom denklemi verirseniz ben size sadece cevabı veririm, bunun çok da pratik olmayan ispatını herhangi bir şekilde sizinle ya da bir başkasıyla paylaşmak istemem" açıklamasını yapmıştı. Galois'nın başardığı ve çağdaşlarının kıymetini bilmeyi başaramadığı şey, grup ve cisim yapıları arasındaki büyüleyici paralelliktir.

Galois'nın çalışmaları, önceleri sayı ve şekil bilimi olan cebir ve matematikte önemli bir değişime yol açtı. Gauss ve Galois'dan itibaren matematik artık yapılar bilimi olmuştu. Galois teorisi, matematik tarihinde cisim ve grup gibi iki farklı yapıyı karşılaştıran ilk teoridir. Bu gelişmeye ayak uydurmak kolay değildi. Galois'dan sonraki matematikçiler bile Galois teorisini, denklemler teorisinde belli soruları yanıtlamakta bir araç olarak kullandılar. Galois teorisi ve uygulamaları hakkında ilk kitabı Heinrich Weber (1842 – 1913) yazdı. Weber, cebirle ilgili ünlü kitabında (1894) bir bölümü bu teoriye, bir bölümü de ilgili uygulamalarına ayırmıştı.

Galois teorisine değinen ilk yazar ise E.Betti (1823 – 1892) dir. Betti, Galois'nın çizgisini takip ettiği "Sulla risoluzione delle equazioni algebriche" isimli bir makale yayımladı (1852) ki, bu makale orijinal bir açıklamadan çok, bir yorum niteliği taşımaktaydı. Bu teori hakkında diğer bir yorum da J.A.Serret (1819 – 1885) tarafından yapıldı.

Camile Jordan (1838 – 1922), Galois teorisine, Galois'nın çizgisini izlemeksizin yorum getiren ilk kişi oldu. Jordan ile birlikte önem, polinomlardan gruplara geçmişti. Jordan, birçok önemli ve özgün katkı yaptı: asal polinomlar ile tranzitif gruplar arasındaki ilişkiyi açıkladı, tranzitif gruplar teorisini geliştirdi, bölüm gruplarını yardımcı denklemin grubu olarak tanımladı, çözülebilir bir grubun herhangi iki kompozisyon serisindeki bölüm gruplarının birbirine izomorf olduğunu ispatladı. Grup kavramı belli başlı uğraş haline gelse de, polinom denklemlerinin çözümü hala en büyük ilgiye sahipti.

Aynı dönemde, iki Alman matematikçi, L. Kronecker (1823 – 1891) ve R. Dedekind (1831 – 1916), cisim teorisine çok önemli katkılar yaptılar.

Dedekind, Galois teorisi ile ilgili dersler vermekteydi. Görünen odur ki, Galois grubunun bir permütasyon grubundan çok, bir cismin otomorfi grubu olarak görülmesi gerektiğini ilk farkeden, Dedekind'tir. Dedekind aslında, "permütasyon" terimini bugün kullandığımız cisim otomorfisinin yerine kullanmaktadır. Buradan Dedekind'in Galois teorisini, çok doğru olarak, polinomlara ilişkin bir teori olarak

değil, cisimlere ilişkin bir teori olarak algıladığı anlaşılmaktadır. Dedekind, taban cismi üzerindeki bir genişleme cisminin elemanlarının bağımlılığı/bağımsızlığı kavramını ortaya çıkardı.

Kronecker, "katma" kavramını ayrıntılı olarak inceledi; bir cisme cebirsel elemanlar gibi, transandant elemanların da katılmasının mümkün olduğunu öne sürdü ve her polinomun uygun bir genişleme cisminde lineer çarpanlara ayrılabileceğine ilişkin, önemli bir teorem ispatladı.

Weber, Kronecker ve Dedekind'in fikirlerini ileri götürdü. Onun katkısı, konu hakkındaki ilk modern yaklaşım olarak, sadece ile sınırlı kalmıyor, keyfi bir cismi de kapsıyordu. Weber, teorinin cisim genişlemeleri ve bu genişlemelerin otomorfi grupları ile ilgili olduğunu açık olarak belirtiyordu. Weber, çalışmaları ile bulunduğu çağın biraz ötesinde idi; o zamanki birçok matematikçi, onun yaklaşımlarını çok soyut ve zorlayıcı buluyordu.

Daha sonra Emil Artin (1898 – 1962) geldi ve lineer cebir ve cisim teorisi tekniklerini birleştirdi. Genişlemeler bazen cisimler, bazen de vektör uzayları olarak gözönüne alınırlar. Artin, cisim otomorfilerini inceledi, bir genişlemenin derecesinin o genişlemenin otomorfi grubunun mertebesine eşit olduğunu ispatladı, Galois genişlemesi kavramını ortaya attı ve rezolventin rolünü ortadan kaldırdı. Artin daha sonra, ara cisimler ile otomorfi grubunun alt grupları arasında ilişki kurdu. Bütün hesaplamalar, teoriden çıkarıldı. Önceleri bir yazar, bir parçalanış cismini oluşturmak için adım-adım rezolvent katılımına sayfalar harcarken, Artin sadece "*E, f(x)* in bir parçalanış cismi olsun" diye yazıyordu. Artin ile, Galois teorisi, geçmişle olan bütün bağlantısını koparmıştı.

BÖLÜM II. TEMEL KAVRAMLAR

Tanım 2.1. A ve B gibi iki küme verilmiş olsun. Eğer A nın her a elemanına belirli bir kurala göre B nin bir b elemanı karşılık getirilirse *A kümesini B kümesi içine resmeden bir tasvir tanımlanmıştır* denir. b elemanına *a elemanının bu tasvirdeki resmi (görüntüsü), a* ya da *b nin aynı tasvirdeki bir orijinali* denir. B nin her elemanının A da en az bir orijinali varsa, yani B nin her elemanı, verilen tasvirde bir resim ise bu tasvire *A nın B üzerine bir tasviri* denir. B nin verilen tasvirde resim olan her elemanının A da bir tek orijinali varsa bu tasvire *A nın B içine (1-1) bir tasviri* denir. A nın B içine bir tasvirinde B nin her elemanı bir resim ise ve bu elemanlardan her birinin A da bir tek orijinali varsa bu tasvire *A nın B üzerine (1-1) bir tasviri* denir. Bir A kümesini bir B kümesi içine resmeden bir f tasviri söz konusu olduğu zaman

$$f : A \to B \qquad \text{veya} \qquad A \xrightarrow{f} B$$
$$a \to b = f(a) \qquad\qquad a \to b = f(a)$$

yazılır.

Tanım 2.2. Bir A kümesinin her a elemanına kendisini tekabül ettiren tasvire *A nın kendi üzerine idantik tasviri* denir ve bu tasvir, I_A ile gösterilir.

Tanım 2.3. Bir A kümesini bir B kümesi içine resmeden bir f tasviri ile B yi bir C kümesi içine resmeden bir g tasviri verilmiş olsun. A nın her a elemanına C nin $g(f(a))$ elemanını tekabül ettiren h tasvirine *f ve g tasvirlerinin bileşkesi(* veya *kompozisyonu)* denir ve bu tasvir, genellikle $h=gf$ ile gösterilir.

$$A \xrightarrow{f} B \xrightarrow{g} C \qquad\qquad h : A \to C$$
$$a \to f(a) \to g(f(a)) \qquad\qquad a \to g(f(a))$$

Tanım 2.4. Bir A kümesi ile ondan farklı olması gerekmeyen bir B kümesi gözönüne alalım. $A_1 \subset A$ olmak üzere, A_1 i B içine resmeden bir f_1 tasviri verilmiş olsun. A yı B içine resmeden ve her $a \in A_1$ için $f(a) = f_1(a)$ koşulunu gerçekleyen (yani A_1 kümesi üzerinde f_1 ile aynı etkiyi yapan) bir f tasvirine f_1 *tasvirinin A ya bir uzatılmışı* veya *genişletilmişi* denir.

Tanım 2.5. Bir A kümesi ile ondan farklı olması gerekmeyen bir B kümesi gözönüne alalım. A yı B içine resmeden bir f tasviri ile A nın herhangi bir A_1 alt kümesi verilmiş olsun. A_1 i B içine resmeden ve her $a \in A_1$ için $f_1(a) = f(a)$ koşulunu gerçekleyen f_1 tasvirine *f tasvirinin A_1 e kısıtlanmışı* veya *daraltılmışı* denir ve $f_1 = f_{|A_1}$ yazılır.

Tanım 2.6. Bir A kümesini bir B kümesi üzerine (1-1) olarak resmeden bir f tasviri verilmiş olsun. Her $b \in B$ ye tek türlü belirli olduğunu bildiğimiz $a \in A$ orijinalini tekabül ettirelim. Böylece elde edilen tasvir, aşikar olarak B yi A üzerine (1-1) olarak resmeder ki, buna *f tasvirinin tersi* denir ve bu tasvir, f^{-1} ile gösterilir.

Teorem 2.7 [[1], *S*.23, *Theorem* 3.11]**.** $f : A \to B,\ g : B \to C$ iki tasvir ve $gf : A \to C$ bu tasvirlerin bileşkesi olsun. Bu takdirde

(1) *f* ve *g* üzerine ise *gf* de üzerinedir,

(2) *f* ve *g* (1-1) ise *gf* de (1-1) dir.

Teorem 2.8 [[1], *S*.26, *Theorem* 3.17]**. (1)** $f : A \to B$ tasviri, üzerine (1-1) olsun. Bu takdirde $f^{-1} : B \to A$ tasviri de üzerine (1-1) dir.

(2) Bir $f : A \to B$ tasviri verildiğine göre, $gf = I_A,\ \ fg = I_B$ olacak şekilde bir $g : B \to A$ tasviri varsa *f* üzerine (1-1) dir (*g*, *f* nin tersidir).

Tanım 2.9. Herhangi bir *M* kümesi verildiğine göre, $M \times M$ yi *M* içine resmeden bir tasvir varsa, yani $a,b \in M$ olmak üzere, her sıralı (*a*,*b*) çiftine tamamen belirli bir $c \in M$ tekabül ettirilebiliyorsa *M de bir ikili işlem tanımlanmıştır* denir. Bir ikili işlem, genellikle "$\circ$" işaretiyle gösterilir ve bu işlem sonucunda (*a,b*) den elde edilen eleman *c* olduğuna göre, $c = a \circ b$ yazılır.

Tanım 2.10. İçinde en az bir tane ikili işlem tanımlanmış bir kümeye bir *cebirsel yapı* denir. Örneğin bir *M* kümesinde "$\circ$" gibi bir ikili işlem tanımlanmış ise bu cebirsel yapıyı $< M, \circ >$ şeklinde göstereceğiz. İçinde bir tane ikili işlem tanımlanmış bir cebirsel yapıya *tek işlemli bir cebirsel yapı* denir. İçinde iki tane ikili işlem tanımlanmış bir cebirsel yapıya *iki işlemli bir cebirsel yapı* denir; verilen küme *M* ve içinde tanımlanmış olan işlemler "$\circ$" ve "$*$" ise söz konusu cebirsel yapı, $< M; \circ, * >$ şeklinde gösterilir.

Tanım 2.11. Bir *G* kümesinde aşağıdaki koşullara uyan bir "$\circ$" ikili işlemi tanımlanmış ise *G* ye "$\circ$" *işlemine göre bir grup* denir:

(1) Her $a,b \in G$ için $a \circ b \in G$ dir.

(2) Her $a,b,c \in G$ için $(a \circ b) \circ c = a \circ (b \circ c)$ dir.

(3) Her $a \in G$ için $e \circ a = a$ olacak şekilde en az bir $e \in G$ vardır.

(4) Her $a \in G$ ye karşılık, $a^* \circ a = e$ olacak şekilde en az bir $a^* \in G$ vardır.

Bu grup, $< G, \circ >$ ile gösterilir. "$\circ$" işlemi komütatif ise bu *G* grubuna *komütatif bir grup* veya *abel grubu* denir.

Tanım 2.12. İki işlemli bir *H* cebirsel yapısı, "+" işaretiyle göstereceğimiz ve *toplama* adını vereceğimiz birinci işleme göre bir abel grubu, "." işaretiyle göstereceğimiz (veya elemanları yan yana yazacağımız) ve *çarpma* adını vereceğimiz ikinci işleme göre de bir yarı grup ise ve bundan başka, çarpma işlemi toplama işlemine göre iki yanlı distribütif ise (yani her $a,b,c \in H$ üçlüsü için $a(b+c) = a \cdot b + a \cdot c$ ve $(b+c)a = b \cdot a + c \cdot a$ ise) *H* ya bir *halka* denir ve bu halka $< H; +, \cdot >$ ile gösterilir. $< H, + >$ grubunun 0_H nötr elemanına *H halkasının sıfırı* denir. Özellikle *H* nın "." işlemine göre de 1_H gibi bir nötr elemanı varsa buna *H halkasının birimi* denir ve bu durumda halkaya *birimli bir halka* denir.

Tanım 2.13. Komütatif bir $< H; +, \cdot >$ halkasında $a \neq 0_H$, $b \neq 0_H$ ve $a \cdot b = 0_H$ olacak şekilde *a, b* elemanları varsa *a* ve *b* ye *H nın birer sıfır-böleni*, (*a*,*b*)

çiftine *H nın bir sıfır-bölen çifti* ve H ya da bir *sıfır-bölenli halka* denir. Hiçbir sıfır-böleni bulunmayan bir halkaya da *sıfır-bölensiz halka* denir.

Tanım 2.14. Bir $< K;+,\cdot >$ halkasında $K-\{0_K\}$ alt kümesi, "." işlemine göre bir grup oluşturuyorsa bu halkaya bir *cisim* denir. Bir $< K;+,\cdot >$ cismi verildiğine göre, $< K-\{0_K\},\cdot >$ grubunu kısaca K^* ile göstereceğiz. Bir halka (cisim) içinde tanımlanmış olan çarpma işlemi komütatif ise o halkaya (cisme) bir *komütatif halka (komütatif cisim)* denir. Komütatif, birimli ve sıfır bölensiz bir halkaya *bir tamlık bölgesi* denir.

Tanım 2.15. Bir *C* cebirsel yapısı verilmiş olsun. *C* nin bir $C' \neq \varnothing$ alt kümesi, *C* deki ikili işlem veya işlemlere göre kendi başına *C* ile aynı türden bir cebirsel yapı oluşturuyorsa C' ye *C nin bir alt cebirsel yapısı* denir. Örneğin *C* bir grup, halka, cisim, tamlık bölgesi ise C' ye sırasıyla *C nin bir alt grubu, alt halkası, alt cismi* diyeceğiz ve kısaca $C' \underset{a.g.}{\subset} C$, $C' \underset{a.h.}{\subset} C$, $C' \underset{a.c.}{\subset} C$ yazacağız.

Teorem 2.16 (Alt Grup Kriteri) [5, *S*.18, *Teorem* 1.2.2]**.** Bir *G* grubunun boş olmayan bir *H* alt kümesinin, *G* nin bir alt grubu olabilmesi için gerek ve yeter koşullar şunlardır:

(1) Her $a,b \in H$ için $a \cdot b \in H$,

(2) Her $a \in H$ için $a^{-1} \in H$.

Teorem 2.17 (Alt Halka Kriteri) [5, *S*.124, *Teorem* 2.2.1]**.** Bir $< H;+,\cdot >$ halkasında boş olmayan bir H' alt kümesinin bir alt halka olabilmesi için gerek ve yeter koşullar şunlardır:

(1) Her $a,b \in H'$ için $a-b \in H'$,

(2) Her $a,b \in H'$ için $a \cdot b \in H'$.

Tanım 2.18. Bir $M = \{a,b,c,...\}$ kümesinde aşağıdaki özelikleri gerçekleyen, "$\square$" işaretiyle göstereceğimiz bir ikili bağıntı tanımlanmış olsun:

(1) $a \square a$ (*refleksiflik* veya *yansıma* özeliği)

(2) $a \square b \Rightarrow b \square a$ (*simetri* özeliği)

(3) $a \square b,\ b \square c \Rightarrow a \square c$ (*transitiflik* veya *geçişme* özeliği).

Bu şekilde tanımlanan "$\square$" bağıntısına *M de bir denklik* (*eşdeğerlik*) *bağıntısı* denir ve $a \square b$, "*a*, *b* ye denktir" şeklinde okunur.

Tanım 2.19. Bir *M* kümesi, ikişer ikişer ayrık bir takım alt kümelerinin birleşimi olarak gösterilebilirse *M, verilen alt kümeler yardımıyla sınıflara ayrılmıştır* denir ve o alt kümelere de *bu ayrılıştaki sınıflar* adı verilir. *M* nin söz konusu sınıflara ayrılışı, *N* bu ayrılıştaki sınıflardan herhangi biri olmak üzere, $M = \bigcup N$ şeklinde gösterilir. N' ve N'', bu sınıflardan herhangi ikisi ise ya $N' = N''$ dür veya $N' \neq N''$ olup, sınıflara ayrılışın tanımı gereğince $N' \cap N'' = \varnothing$ tur.

Teorem 2.20 [4, *S*.28, *Teorem* 1.3.8]**.** Bir *M* kümesinde tanımlanmış her denklik bağıntısı, *M* nin bir sınıflara ayrılışını belirtir; karşıt olarak, *M* nin her sınıflara ayrılışı, *M* de bir denklik bağıntısı belirtir.

Tanım 2.21. Bir *C* cebirsel yapısında bir "$\square$" denklik bağıntısı verilmiş olsun. Eğer *C* de tanımlanmış herhangi bir "$\circ$" ikili işlemi için

$$a' \square a,\ \ b' \square b \Rightarrow a' \circ b' \square a \circ b$$

koşulu gerçekleniyorsa "$\square$" *denklik bağıntısı,* "$\circ$" *işlemi ile uygunluk halindedir* denir.

Teorem 2.22 [4, *S*.212, *Teorem* 3.4.8]**.** Bir *C* cebirsel yapısının herhangi bir sınıflara ayrılışı verilmiş olsun ve bu ayrılışın belirttiği "$\square$" denklik bağıntısını gözönüne alalım. $\overline{C}$ sınıflar kümesinin $\overline{a},\overline{b},...$ elemanları arasında, *C* deki bir "$\circ$" işlemine paralel bir işlemin

$$\overline{a} \circ \overline{b} = \overline{a \circ b}$$

şeklinde tanımlanabilmesi için gerek ve yeter koşul, "$\square$" denklik bağıntısının "$\circ$" işlemi ile uygunluk halinde olmasıdır.

Tanım 2.23. Bir *C* cebirsel yapısının herhangi bir sınıflara ayrılışı verilmiş olsun. Bu sınıflara ayrılışın belirttiği denklik bağıntısı, *C* deki her işlemle uygunluk halinde ise $\overline{C}$ sınıflar kümesinde *C* deki işlemlerin herbirine paralel birer işlem, yukarıdaki gibi tanımlanabilir. Eğer $\overline{C}$, bu işlemlere göre *C* ile aynı türden bir cebirsel yapı oluşturuyorsa $\overline{C}$ ye *C nin bir bölüm yapısı* denir. Örneğin *C* bir grup veya halka ise $\overline{C}$ ye sırasıyla *C nin bir bölüm grubu* veya *bölüm halkası* denir.

Tanım 2.24. Bir *C* cebirsel yapısında tanımlanmış olan bir "$\square$" denklik bağıntısı, *C* deki her işlemle uygunluk halinde ise "$\square$" bağıntısına bir *kongrüans bağıntısı* denir.

Tanım 2.25. *C* ve C' gibi, her ikisi de tek veya her ikisi de çift işlemli iki cebirsel yapı verilmiş olsun. Eğer *C* yi C' içine resmeden ve işlemlerin sonuçlarını koruyan bir φ tasviri varsa *C cebirsel yapısı* φ *tasviri ile* C' *ye homomorf olarak resmedilmiştir* veya kısaca *C,* C' *ye homomorftur* denir ve $C \square C'$ veya $C \overset{\varphi}{\square} C'$ yazılır. Bu durumda φ ye *C yi* C' *ye resmeden bir homomorfi,* C' ye de *C nin bir homomorf resmi* denir. φ homomorfisi, üstelik üzerine ve (1-1) ise *C,* C' *ye izomorftur* denir ve $C \cong C'$ veya $C \overset{\varphi}{\cong} C'$ yazılır; φ ye *C yi* C' *ye resmeden bir izomorfi,* C' ye de *C nin bir izomorf resmi* denir. Bir *C* cebirsel yapısının kendi üzerine bir izomorfisine *C nin bir otomorfisi* denir. I_C idantik tasviri, aşikar olarak *C* nin bir otomorfisidir ki, buna *C nin idantik otomorfisi* denir.

Şu halde φ, bir $< C, \circ >$ cebirsel yapısını bir $< C', * >$ cebirsel yapısına resmeden bir homomorfi ise

$$\varphi : C \to C'$$
$$a \to \varphi(a)$$
$$b \to \varphi(b)$$
$$\varphi(a \circ b) = \varphi(a) * \varphi(b)$$

dir. İki işlemli cebirsel yapılarda her iki işlemin birden korunması gerekir, yani φ, bir $< C; +, \cdot >$ cebirsel yapısını bir $< C'; \oplus, \square >$ cebirsel yapısına resmeden bir homomorfi ise her $a, b \in C$ için

$$\varphi(a + b) = \varphi(a) \oplus \varphi(b),$$
$$\varphi(a \cdot b) = \varphi(a) \square \varphi(b)$$

dir.

Tanım 2.26. *a*, bir $< G, \cdot >$ grubunun herhangi bir elemanı, *n* de herhangi bir tam sayı olmak üzere, a^n (*a nın n. kuvveti*) şu şekilde tanımlanır:

(1) $n > 0$ ise $a^n = \begin{cases} a \ \ (n = 1 \text{ için}) \\ \underbrace{a \cdot a \cdots a}_{n \text{ tane}} \ \ (n \geq 2 \text{ için}), \end{cases}$

(2) $n = 0$ ise $a^n = 1_G$,

(3) $n < 0$ ve $n = -n' \ (n' > 0)$ ise $a^n = \begin{cases} a^{-1} = a \text{ nın } G \text{ deki tersi } (n' = 1 \text{ için}) \\ a^{-n'} = \left(a^{-1}\right)^{n'} \ (n' \geq 2 \text{ için}). \end{cases}$

Lemma 2.27 (Kuvvetlerin Temel Özelikleri) $\left([4, S.10]\right)$**.**

(1) $(a^{-1})^{-1} = a$

(2) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Genelleştirme. $(a_1 \cdot a_1 \cdots a_k)^{-1} = a_k^{-1} \cdots a_2^{-1} \cdot a_1^{-1} \ (k \geq 2)$.

(3) $a^m \cdot a^n = a^{m+n} \ (m, n \in \square)$

Genelleştirme. $a^{m_1} \cdot a^{m_2} \cdots a^{m_k} = a^{m_1 + m_2 + \ldots + m_k} \ (k \geq 2;\ m_1, m_2, \ldots, m_k \in \square)$.

(4) $(a^m)^n = a^{mn} \ (m, n \in \square)$

(5) $a \cdot b = b \cdot a$ ise her $n \in \square$ için $(a \cdot b)^n = a^n \cdot b^n$ dir.

Tanım 2.28. *a*, bir $< G, + >$ abel grubunun herhangi bir elemanı, *n* de herhangi bir tam sayı olmak üzere, *na* (*a nın n katı*) şöyle tanımlanır:

(1) $n > 0$ ise $na = \begin{cases} a \ \ (n = 1 \text{ için}) \\ \underbrace{a + a + \ldots + a}_{n \text{ tane}} \ \ (n \geq 2 \text{ için}), \end{cases}$

(2) $n = 0$ ise $na = 0_G$,

(3) $n = -n' \ (n' > 0)$ ise $na = \begin{cases} -a = a \text{ nın } G \text{ deki zıddı } (n' = 1 \text{ için}) \\ (-n')a = n'(-a) \ \ (n' \geq 2 \text{ için}). \end{cases}$

Lemma 2.29 (Katların Temel Özelikleri).

(1) $-(-a)=a$

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

Genelleştirme. $-(a_1+a_2+\cdots+a_k)=(-a_k)+\cdots+(-a_2)+(-a_1)$

$=(-a_1)+(-a_2)+\cdots+(-a_k)$ $(k\geq 2)$.

(3) $ma+na=(m+n)a$ $(m,n\in\mathbb{Z})$

Genelleştirme. $m_1a+m_2a+\cdots+m_ka=(m_1+m_2+\cdots+m_k)a$

$(k\geq 2;\ m_1,m_2,...,m_k\in\mathbb{Z})$

(4) $n(ma)=(nm)a$ $(m,n\in\mathbb{Z})$

(5) $<G,+>$ komütatif olduğundan her $a,b\in G$ çifti için $a+b=b+a$ dır. Şu halde her $a,b\in G$ ve her $n\in\mathbb{Z}$ için $n(a+b)=na+nb$ dir.

Tanım 2.30. *G* bir grup ve *M*, *G* nin boş olmayan herhangi bir alt kümesi olsun. *G* nin *M* yi kapsayan bütün alt gruplarının arakesitine (ki, bu arakesit te *G* nin bir alt grubudur) *G nin M tarafından doğurulan alt grubu, M* nin elemanlarına da *bu alt grubun doğurayları* denir ve söz konusu alt grup, *G*(*M*) ile gösterilir.

$$G(M)=\bigcap_{M\subset H\underset{a.g.}{\subset} G} H.$$

$M=\{a\}$ ise *G*(*M*), yani *G*($\{a\}$) yerine kısaca *G*(*a*) yazılır.

Eğer *M* nin doğurduğu alt grup, *G* ile çakışıyorsa, yani *G*(*M*)=*G* ise M nin elemanlarına *G nin doğurayları* adı verilir ve *G grubu, M nin elemanları tarafından doğurulmuştur* denir. Özellikle *M* kümesi sonlu ve *G*(*M*)=*G* ise *G* grubuna *sonlu doğuraylı bir grup* denir.

Tanım 2.31. Bir tek elemanı tarafından doğurulan bir gruba bir *devresel grup* denir. Buna göre, bir *a* elemanı tarafından doğurulan, sonlu bir *G* devresel grubu

$$G=\{1_G,a,a^2,...,a^{n-1}\}\ (a^n=1_G)$$

şeklindedir ki, bu grubu kısaca $<a>$ ile göstereceğiz.

Tanım 2.32. *G* sonlu bir grup ve $a\in G$ olduğuna göre, *a* nın *G* içinde doğurduğu devresel grubun mertebesine, başka bir deyişle, $a^t=1_G$ koşuluna uyan $t\in\mathbb{Z}$ lerin en küçüğüne *a elemanının* (*G grubundaki*) *mertebesi* denir ki, bu mertebeyi $|a|$ ile göstereceğiz.

Tanım 2.33. *a* ve *b*, bir $<G,\cdot>$ grubunun

$$|a|=n\geq 2,\ |b|=2,\ b\cdot a=a^{-1}\cdot b$$

koşullarına uyan iki elemanı olmak üzere,

$$G=\{a^k\cdot b^l \mid k=0,1,...,n-1;\ l=0,1\}$$

ise *G* ye bir "*dihedral grup*" denir.

Teorem 2.34 [[1], *S*.109, *Theorem* 11.8]**.** *G* bir devresel grup ve $H\underset{a.g.}{\subset} G$ olsun. Bu takdirde *H* da bir devresel gruptur. Daha açık bir şekilde ifade etmek gerekirse:

$G =< a >$ olsun. Bu takdirde, $H = \{1_G\}$ ise $H =< 1_G >$ dir; $H \neq \{1_G\}$ ise t, $\{n \in \square \mid a^n \in H\}$ kümesinin en küçük elemanı olmak üzere, $H =< a^t >$ dir.

Tanım 2.35. *G* bir grup, *H* da *G* nin herhangi bir alt grubu olsun. $a, b \in G$ olduğuna göre, $a^{-1} \cdot b \in H$ ise $a \underset{\text{sol}}{\square} b(H)$, $a \cdot b^{-1} \in H$ ise $a \underset{\text{sağ}}{\square} b(H)$ yazacağız. Bu şekilde tanımlanan "$\underset{\text{sol}}{\square}$" ve "$\underset{\text{sağ}}{\square}$" bağıntıları, *G* de birer eşdeğerlik bağıntısıdır. Ayrıca $a \underset{\text{sol}}{\square} b(H)$ ($a \underset{\text{sağ}}{\square} b(H)$) ise *a*, *b* ye *H alt grubuna göre soldan* (*sağdan*) *eşdeğerdir* denir. *G* nin *H* alt grubuna göre "$\underset{\text{sol}}{\square}$" ("$\underset{\text{sağ}}{\square}$") eşdeğerlik bağıntısının *G* de belirttiği sınıflara *G nin H alt grubuna göre sol* (*sağ*) *kalan sınıfları* veya *H nın G içindeki sol* (*sağ*) *kalan sınıfları* denir.

Teorem 2.36 [5, *S*.61, *Teorem* 1.6.5]**.** *G* nin *H* ya göre bir sol (sağ) kalan sınıfı, *a* bu sınıfın herhangi bir elemanı olmak üzere, bir $aH = \{a \cdot h \mid h \in H\}$ $\left(Ha = \{h \cdot a \mid h \in H\}\right)$ alt kümesi ile çakışır.

Teorem 2.37 (Lagrange Teoremi) [5, *S*.63, *Teorem* 1.6.11]**.** Sonlu bir G grubunda her H alt grubunun mertebesi, G nin mertebesini böler, yani $|G| = N$ ve $|H| = n$ ise $n \mid N$ dir.

Tanım 2.38. *G* bir grup, *H* da *G* nin bir alt grubu olsun. Eğer her $a \in G$ için $aH = Ha$ ise *H* ya *G nin bir normal alt grubu* denir ve $H \lhd G$ yazılır.

Teorem 2.39 [5, *S*.78, *Teorem* 1.8.13]**.** Bir *G* grubunun bir *H* normal alt grubuna göre "$\underset{\text{sol}}{\square}$" ve "$\underset{\text{sağ}}{\square}$" eşdeğerlik bağıntıları, birbiriyle çakışır ve *G* de bir kongrüans bağıntısı olur.

Teorem 2.40 [5, *S*.79, *Teorem* 1.8.14]**.** *G* bir grup ve $H \lhd G$ ise yukarıki Teoremdeki kongrüans bağıntısının *G* de belirttiği kalan sınıfları arasında, $aH \circ bH = (a \cdot b)H$ şeklinde bir "$\circ$" işlemi tanımlanabilir ve söz konusu kalan sınıflarından oluşan $\overline{G}$ kümesi, "$\circ$" işlemine göre bir gruptur.

Tanım 2.41. $< \overline{G}, \circ >$ grubuna *G nin H normal alt grubuna göre bölüm grubu* denir ve bu grup, G / H ile gösterilir.

Tanım 2.42. *A* ve *B*, bir $< G, \cdot >$ grubunun boş olmayan iki alt kümesi olsun. $a \in A$, $b \in B$ olmak üzere, mümkün olan bütün $a \cdot b$ çarpımlarını oluşturalım. Bu çarpımlar içinde birbirine eşit olanlar varsa, onlardan birer tane alınarak elde edilen kümeye *A ve B kümelerinin (bu sıradaki) çarpımı* denir ve bu çarpım $A \cdot B$ ile gösterilir.

Teorem 2.43 [5, *S*.80, *Not* 1.8.16]**.** Yukarıda tanımlanan $aH \circ bH$, aynı zamanda aH ve bH kümelerinin çarpımına eşittir, yani $aH \circ bH = aH \cdot bH$ dır.

Tanım 2.44. $\varphi : G \to G_1$ bir grup homomorfisi olsun.

$$\left\{ \varphi(a) \in G_1 \,\middle|\, a \in G \right\} = \left\{ b \in G_1 \,\middle|\, b = \varphi(a) \;\; (a \in G) \right\}$$

kümesine, yani G nin elemanlarının φ deki bütün görüntülerinin kümesine G nin φ *tasvirindeki görüntüsü* denir ve bu küme, $\mathrm{Im}\,\varphi$ veya $\varphi(G)$ ile gösterilir.

Teorem 2.45 [5, *S*.102, *Teorem* 1.10.1] **.** $< G, \cdot >$ bir grup, G' tek işlemli bir cebirsel yapı ve G' , G nin bir φ homomorfisindeki resmi olsun. Bu takdirde $\mathrm{Im}\,\varphi$, G' deki ikili işleme göre bir gruptur ve bundan başka, aşağıdaki özelikler geçerlidir:

(1) G nin, φ deki görüntüleri $1_{G'}$ olan elemanlarının kümesi, G nin N gibi bir normal alt grubudur.

(2) Herhangi bir $a' \in G'$ verildiğine göre, G nin, φ deki görüntüleri a' olan elemanlarının kümesi, N nin G içindeki uygun bir kalan sınıfıdır.

(3) $G / N \cong \mathrm{Im}\,\varphi$ dir.

Tanım 2.46. Yukarıdaki N normal alt grubuna φ *homomorfisinin çekirdeği* denir ve $N = \ker \varphi$ yazılır. Şu halde

$$\ker \varphi = \left\{ a \in G \,\middle|\, \varphi(a) = 1_{G'} \right\}$$

dür.

Teorem 2.47 [1, *S*.211, *Theorem* 20.8]**.** Bir $\varphi : G \to G'$ grup homomorfisinin (1-1) olması için gerek ve yeter koşul, $\ker \varphi = \left\{ 1_G \right\}$ olmasıdır.

Teorem 2.48 (Binom Teoremi) [1, *S*.335, *Theorem* 29.16]**.** $< H; +, \cdot >$ bir halka ve $a, b \in H$ olsun. $a \cdot b = b \cdot a$ ise her $n \in \mathbb{N}$ için $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k$ dır.

Tanım 2.49. Bir H halkasının aşağıdaki koşulları gerçekleyen bir $\mathfrak{I}$ alt kümesine *H nın bir sol (sağ) ideali* denir:

(1) Her $a, b \in \mathfrak{I}$ için $a - b \in \mathfrak{I}$,

(2) Her $h \in H$ ve her $a \in \mathfrak{I}$ için $h \cdot a \in \mathfrak{I}$ $(a \cdot h \in \mathfrak{I})$.

$\mathfrak{I}$, H nın hem bir sol, hem de bir sağ ideali ise $\mathfrak{I}$ ye bir *iki yanlı ideal* veya yalnızca *ideal* denir.

Tanım 2.50. H komütatif bir halka ve $a_1, a_2, ..., a_k \in H$ olmak üzere,

$$\mathfrak{I} = \left\{ h_1 \cdot a_1 + h_2 \cdot a_2 + ... + h_k \cdot a_k + n_1 a_1 + n_2 a_2 + ... + n_k a_k \,\middle|\, h_i \in H,\; n_i \in \mathbb{N} \;\; (i = 1, ..., k) \right\}$$

kümesi, H nın bir idealidir. H birimli ise

$$n_i a_i = n_i (1_H \cdot a_i) = (n_i 1_H) \cdot a_i$$

yazılabilir, yani $s_i := n_i 1_H \in H$ olmak üzere, $n_i a_i = s_i \cdot a_i \quad (i = 1,...,k)$ dir. Buna göre $\tilde{h}_i := h_i + s_i \in H \quad (i = 1,...,k)$ olmak üzere

$$\Im = \left\{ \tilde{h}_1 \cdot a_1 + \tilde{h}_2 \cdot a_2 + ... + \tilde{h}_k \cdot a_k \,\middle|\, \tilde{h}_i \in H \quad (i = 1,...,k) \right\}$$

olur. Bu durumda $\Im$ ye $a_1, a_2, ..., a_k$ *tarafından doğurulmuş ideal* adı verilir ve $\Im = (a_1, a_2, ..., a_k)$ yazılır; $a_1, a_2, ..., a_k$ ya da $\Im$ *idealinin doğurayları* denir.

Tanım 2.51. Bir tek *a* elemanı tarafından doğurulan bir ideale *esas ideal* denir ve bu ideal, (*a*) ile gösterilir. Buna göre

$$(a) = \left\{ h \cdot a \,\middle|\, h \in H \right\}$$

dır. Bir *H* halkasının bütün idealleri esas idealler ise *H* ya bir *esas ideal halkası* denir.

Teorem 2.52 [5, *S*.132, *Teorem* 2.2.31]**.** *H* bir halka, $\Im$ de *H* nın herhangi bir ideali olsun. *H* nın $\Im$ idealine göre kalan sınıfları (yani $< H, + >$ grubunun $< \Im, + >$ alt grubuna göre kalan sınıfları) arasında

$$(a + \Im) + (b + \Im) = (a + b) + \Im, \quad (a + \Im) \cdot (b + \Im) = (a \cdot b) + \Im \quad (a, b \in H)$$

şeklinde bir toplama ve bir de çarpma işlemi tanımlanabilir ve söz konusu kalan sınıflarından oluşan $\bar{H}$ kümesi, bu işlemlere göre bir halkadır.

Tanım 2.53. $< \bar{H}; +, \cdot >$ halkasına *H nın* $\Im$ *idealine göre bölüm halkası* denir ve bu halka $H / \Im$ ile gösterilir.

Teorem 2.54 [5, *S*.144, *Teorem* 2.3.3]**.** Bir *H* halkası ile iki işlemli bir H' cebirsel yapısı verilmiş olsun. Eğer H', *H* nın bir φ homomorfisindeki resmi ise $\mathrm{Im}\,\varphi$, H' deki işlemlere göre bir halkadır ve bundan başka, aşağıdaki özelikler geçerlidir:

(1) *H* nın, φ deki görüntüleri $0_{H'}$ olan elemanlarının kümesi, *H* nın $\Im$ gibi bir idealidir.

(2) Herhangi bir $a' \in H'$ verildiğine göre, *H* nın, φ deki görüntüleri a' olan elemanlarının kümesi, $\Im$ nin *H* içindeki uygun bir kalan sınıfıdır.

(3) $H / \Im \cong \mathrm{Im}\,\varphi$ dir.

Tanım 2.55. Yukarıdaki $\Im$ idealine φ *homomorfisinin çekirdeği* denir ve $\Im = ker\,\varphi$ yazılır. Şu halde

$$ker\,\varphi = \left\{ a \in H \,\middle|\, \varphi(a) = 0_{H'} \right\}$$

dür.

Lemma 2.56 [1, *S*.349, *Lemma* 30.16]**.** $\varphi : H \to H_1$ ve $\psi : H_1 \to H_2$ iki halka izomorfisi olsun. Bu takdirde

(1) $\psi\varphi : H \to H_2$ bir halka izomorfisidir,

(2) $\varphi^{-1} : H_1 \to H$ bir halka izomorfisidir.

Teorem 2.57 [[1], *S*.352, *Theorem* 30.19(7)]. $\varphi : H \to H'$, H nın H' üzerine bir halka homomorfisi olsun. $\Im$, H nın $\ker\varphi$ yi kapsayan bir ideali ise $\Im_1$, $\Im$ nin φ deki görüntüsü olmak üzere, $H/\Im \cong H'/\Im_1$ dir.

Tanım 2.58. $a_0, a_1, ..., a_n, ...$ terimleri bir $< H; +, \cdot >$ halkasından alınan ve en çok sonlu sayıda terimi 0_H dan farklı olan bir dizi, *x* te bir işaret olmak üzere

$$a_0 + a_1x + a_2x^2 + ... + a_nx^n + ... \qquad (2.1)$$

şeklindeki sembolik ifadeleri oluşturalım. Burada *x* e bir *değişken* (*belirsiz* veya *bilinmeyen*) (2.1) sembolüne *H halkası üzerinde tek değişkenli bir polinom*, a_i $(i = 0,1,2,...)$ lere bu polinomun *katsayıları*, a_nx^n ye bu polinomun *genel terimi*, a_n ye de bu polinomun *genel katsayısı* denir. Polinomları *A*(*x*), *B*(*x*), *f*(*x*), *g*(*x*),... ile göstereceğiz.

Şimdi H üzerindeki bütün tek değişkenli polinomlardan oluşan kümeyi $\overline{H[x]}$ ile gösterelim.

Teorem 2.59 [[5], *S*.162, *Yard*.*Teorem* 2.6.3]. $A(x), B(x) \in \overline{H[x]}$ ve

$$A(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n + ..., \qquad (2.2)$$

$$B(x) = b_0 + b_1x + b_2x^2 + ... + b_nx^n + ... \qquad (2.3)$$

ise

$$c_n = a_n + b_n \quad (n = 0,1,...)$$

olmak üzere oluşturulan

$$c_0 + c_1x + c_2x^2 + ... + c_nx^n + ... \qquad (2.4)$$

ifadesi, $\overline{H[x]}$ ye aittir.

Tanım 2.60. (2.4) teki

$$C(x) = c_0 + c_1x + c_2x^2 + ... + c_nx^n + ..., \; c_n = a_n + b_n \quad (n = 0,1,...)$$

polinomuna *A(x) ve B(x) polinomlarının (bu sıradaki) toplamı* denir ve $C(x) = A(x) \oplus B(x)$ yazılır.

Teorem 2.61 [[5], *S*.163, *Yard*.*Teorem* 2.6.5]. $A(x)$ ve $B(x)$ polinomları (2.2) ve (2.3) teki gibi verildiğine göre,

$$d_n = a_0 \cdot b_n + a_1 \cdot b_{n-1} + ... + a_n \cdot b_0 = \sum_{i=0}^{n} a_i \cdot b_{n-i} \quad (n = 0,1,...) \qquad (2.5)$$

olmak üzere oluşturulan

$$d_0 + d_1x + d_2x^2 + ... + d_nx^n + ... \qquad (2.6)$$

ifadesi, $\overline{H[x]}$ ye aittir.

Tanım 2.62. (2.6) daki

$$D(x) = d_0 + d_1 x + d_2 x^2 + ... + d_n x^n + ..., \; d_n = \sum_{i=0}^{n} a_i \cdot b_{n-i} \quad (n = 0,1,...)$$

polinomuna *A(x) ve B(x) polinomlarının (bu sıradaki) çarpımı* denir ve $D(x) = A(x) \square B(x)$ yazılır.

Teorem 2.63 [5, *S*.164,*Teorem* 2.6.7]**.** $\overline{H[x]}$ kümesi, yukarıda tanımlanan "$\oplus$" ve "$\square$" işlemlerine göre bir halkadır.

Teorem 2.64 [5, *S*.166,*Yard*.*Teorem* 2.6.9]**.** $\overline{H[x]}$ halkası, H ya izomorf bir alt halka içerir ki, bu $\overline{H} = \left\{ a_0 + 0_H x + ... + 0_H x^n + ... \middle| \, a_0 \in H \right\}$ dan ibarettir.

Tanım 2.65. $H[x] = \left(\overline{H[x]} - \overline{H} \right) + H$ halkasına *H halkası üzerindeki tek değişkenli polinomlar halkası*, bu halkanın *H* ya ait olan elemanlarına da *sabit polinomlar* denir. Eğer $f(x) \in H[x]$ ise $f(x)$ e *katsayıları H ya ait olan bir polinom* veya *H üzerinde alınmış bir polinom* denir.

H[*x*] polinom halkası için, *H halkasına x değişkeninin katılması ile elde edilmiştir* de denir. Şimdi *H* ya bir x_1 değişkenini katmakla elde edilen $H[x_1]$ halkasına ikinci bir x_2 değişkeni katalım ve bu şekilde devam ederek $x_1, x_2, ..., x_n$ gibi *n* tane değişken kattığımızı düşünelim. Böylece elde edilen $H[x_1][x_2]...[x_n]$ halkasına *H halkası üzerinde n değişkenli polinomlar halkası* denir. $i_1, i_2, ..., i_n$ sayıları 1,2,...,*n* sayılarının herhangi bir permütasyonunu göstermek üzere, $H[x_{i_1}][x_{i_2}]...[x_{i_n}] = H[x_1][x_2]...[x_n]$ olup, söz konusu halka, kısaca $H[x_1, x_2, ..., x_n]$ şeklinde gösterilir. Buna uygun olarak, $H[x_1, x_2, ..., x_n]$ nin herhangi bir elemanı da $A(x_1, x_2, ..., x_n)$ şeklinde gösterilir.

Tanım 2.66. Bir *T* tamlık bölgesinde bütün elemanları bölen bir elemana *T nin bir aritmetik birimi* denir.

Teorem 2.67 [5, *S*.177, *Teorem* 2.7.7]**.** T nin bütün aritmetik birimleri, 1_T nin bölenlerinden ibarettir.

Tanım 2.68. *T* bir tamlık bölgesi ve $a, b \in T$ olsun. ε, *T* nin bir aritmetik birimi olmak üzere, $b = \varepsilon \cdot a$ ise *b*, *a ile ilgilidir* denir ve $b \approx a$ yazılır.

Tanım 2.69. Bir $a \in T$ nin ε ve $\varepsilon \cdot a$ bölenlerine *a nın triviyal bölenleri* denir.

Tanım 2.70. Bir T tamlık bölgesinde aritmetik birimlerden farklı olan ve triviyal bölenlerinden başka hiçbir böleni bulunmayan bir elemana bir *asal eleman* denir.

Tanım 2.71. Bir T tamlık bölgesinin 0_T den ve aritmetik birimlerden farklı her elemanı, T ye ait sonlu sayıda asal elemanın çarpımı olarak gösterilebiliyorsa ve bu gösteriliş, çarpanların sırasından ve aralarında ilgililikten vazgeçildiği takdirde, tek türlü belirli ise T ye *asal çarpanlara ayrılışın tek olduğu bir tamlık bölgesi* denir.

Teorem 2.72 [[1], *S*.383, *Theorem* 32.25]**.** D bir esas ideal halkası ve π, D nin 0_D den ve 1_G den farklı bir elemanı olsun. Bu takdirde π nin asal olması için gerek ve yeter koşul, $D/D\pi$ bölüm halkasının bir cisim olmasıdır.

Lemma 2.73 [[1], *S*.395, *Lemma* 33.7]**.** H ve H' iki halka ve $\varphi : H \to H'$ bir halka homomorfisi olsun. Bu takdirde

$$\hat{\varphi}\left(\sum_{i=0}^{m} a_i x^i\right) = \sum_{i=0}^{m} \varphi(a_i) x^i$$

şeklinde tanımlanan $\hat{\varphi} : H[x] \to H'[x]$ tasviri de bir halka homomorfisidir. Üstelik, $\ker \hat{\varphi} = (\ker \varphi)[x]$ ve $\operatorname{Im} \hat{\varphi} = (\operatorname{Im} \varphi)[x]$ tir.

Lemma 2.74[[1], *S*.419, *Lemma* 35.3]**.** H bir halka, *S, H* yı kapsayan bir halka ve s, S in bir elemanı olsun. S komütatif ise

$$T_s : H[x] \to S$$
$$f \to f(s)$$

tasviri bir halka homomorfisidir ki, bu halka homomorfisine *sübstitüsyon homomorfisi* denir.

Teorem 2.75. H ve H' halkaları birbirine izomorf ise $H[x]$ ve $H'[x]$ polinom halkaları da birbirine izomorftur.

Teorem 2.76 [[5], *S*.165, *Teorem* 2.6.8]**.** T bir tamlık bölgesi ise $T[x]$ de bir tamlık bölgesidir.

Tanım 2.77. T bir tamlık bölgesi olsun. $T[x]$ te bir f polinomu ile sıfır polinomundan (yani bütün katsayıları 0_T olan polinomdan) farklı bir g polinomu verildiğine göre, $f = g \cdot h$ olacak şekilde bir $h \in T[x]$ varsa *f, g ile bölünebilir* denir ve $g \mid f$ yazılır.

Sıfırdan farklı bir $e \in T[x]$ polinomu, uygun bir $h \in T[x]$ için $e \cdot h = 1_T$ koşulunu gerçekliyorsa, veya buna denk olarak, her $f \in T[x]$ için $e \mid f$ ise e ye *T[x] in bir aritmetik birimi* denir.

Teorem 2.78 [[5], *S*.179, *Örnek* 2.7.17]**.** K bir komütatif cisim olmak üzere, $K[x]$ polinom halkasındaki aritmetik birimler, K nın 0_K dan farklı elemanlarından, yani K^* grubunun elemanlarından ibarettir.

Tanım 2.79. $T[x]\setminus\{0_T\}$ ye ait bir f polinomu, $T[x]$ in bir aritmetik birimi değilse ve $T[x]$ te $f = g \cdot h$ şeklinde çarpanlarına ayrıldığında g ve h dan en az biri aritmetik birim oluyorsa, f ye *T üzerinde asal bir polinom* denir.

Teorem 2.80 [[1], *S*.409, *Theorem* 34.5(3)]**.** K bir cisim olsun. Bu takdirde $K[x]$, asal çarpanlara ayrılışın tek olduğu bir tamlık bölgesidir.

Tanım 2.81. T asal çarpanlara ayrılışın tek olduğu bir tamlık bölgesi ve f, $T[x]$ te sıfır polinomundan farklı herhangi bir polinom olsun. f nin katsayılarının bir en büyük ortak bölenine *f nin bir muhtevası* denir ve bu muhteva, $C(f)$ ile gösterilir.

Tanım 2.82. T bir tamlık bölgesi olsun ve T yi kapsayan bir K komütatif cisminin bulunduğunu varsayalım. K nın T yi kapsayan bütün K_i alt cisimlerinin arakesiti de K nın T yi kapsayan bir alt cismidir ki, bu

$$\bigcap_{T\subset K_i \underset{a.c.}{\subset} K} K_i = K' \tag{2.7}$$

cismine *T tamlık bölgesinin K cismi içinde doğurduğu alt cisim* denir.

Tanım 2.83. $a,b \in T$ ve $a \neq 0_T$ olmak üzere, $a \cdot x = b$ nin K cismi içinde tek türlü belirli olan $x = a^{-1} \cdot b = b \cdot a^{-1}$ çözümü, $\frac{b}{a}$ şeklinde gösterilir ve $\frac{b}{a}$ ya *T tamlık bölgesine ilişkin bir kesir* denir.

T nin her a elemanı, T ye ilişkin bir kesir olarak gösterilebilir, çünkü $1_T \cdot a = a$ dır ki, buradan da $a = \frac{a}{1_T}$ sonucu çıkar. Şu halde T ye ilişkin bütün kesirlerden oluşan kümeyi $\overline{K}$ ile gösterirsek,

$$T \subset \overline{K} \subset K$$

dır.

Teorem 2.84 [[5], *S*.155, *Teorem* 2.5.6]**.** $\overline{K}$ kümesi K nın bir alt cismi olup, (2.7) deki K' cismiyle çakışır.

Tanım 2.85. $\overline{K}\,(=K')$ cismine *T tamlık bölgesinin kesirler cismi* denir.

Tanım 2.86. T bir tamlık bölgesi ise Teorem 2.75 e göre $T[x]$ polinom halkası da bir tamlık bölgesidir. $T[x]$ in kesirler cismine *T üzerindeki tek değişkenli rasyonel fonksiyonlar cismi* denir ve bu cisim $T(x)$ ile gösterilir. Şu halde

$$T(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in T[x],\ g(x) \neq 0_T \right\}$$

dir.

Lemma 2.87 [1, *S*.413, *Lemma* 34.11]**.** *T*, asal çarpanlara ayrılışın tek olduğu bir tamlık bölgesi ve *F*, *T* nin kesirler cismi olsun. *f*, *T*[*x*] e ait ve $C(f) \approx 1$ koşulunu sağlayan, sıfırdan farklı bir polinom olsun. Bu takdirde *f* nin *F*[*x*] te asal olması için gerek ve yeter koşul, $f \in T[x]$ olmasıdır.

Teorem 2.88 [1, *S*.421, *Theorem* 35.6]**.** *T* bir tamlık bölgesi ve *f*, *T*[*x*] te keyfi bir polinom olsun. *E*, *T* yi kapsayan bir tamlık bölgesi ve $a \in E$ olsun. Bu takdirde *a* nın *f* nin bir kökü olması için gerek ve yeter koşul, *E*[*x*] te $(x-a) \mid f$ olmasıdır.

Teorem 2.89 [1, *S*.421, *Theorem* 35.7]**.** *T* bir tamlık bölgesi, *f, T*[*x*] te sıfırdan farklı bir polinom ve *E, T* yi kapsayan bir tamlık bölgesi olsun. Bu takdirde *f* nin *E* ye ait birbirinde farklı en fazla $deg\, f$ tane kökü vardır.

Lemma 2.90 [1, *S*.429, *Lemma* 35.16]**.** *H* bir halka ve $f_1, f_2, ..., f_n, f, g \in H[x]$ olsun. Bu takdirde

(1) $(f_1 + f_2 + ... + f_n)' = f_1' + f_2' + ... + f_n'$,

(2) $(f_1 f_2 ... f_n)' = f_1' f_2 ... f_n + f_1 f_2' ... f_n + ... + f_1 f_2 ... f_n'$,

(3) $(g^n)' = n g^{n-1} g'$,

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

tir.

Teorem 2.91 [1, *S*.430, *Theorem* 35.17]**.** *T* bir tamlık bölgesi ve *E*, *T* yi kapsayan bir tamlık bölgesi olsun. $c \in E$ ve *f, T*[*x*] te sıfırdan farklı bir polinom olsun. Bu takdirde *c* nin, *f* nin çokkatlı bir kökü olması için gerek ve yeter koşul, *c* nin *f* polinomu ile f' türevinin bir ortak kökü olmasıdır.

Teorem 2.92 [1, *S*.430, *Theorem* 35.18]**.** *K* bir cisim ve *E*, *K* yı kapsayan bir tamlık bölgesi olsun. *f* ve *g, K*[*x*] te sıfırdan farklı keyfi iki polinom olsun. Bu takdirde

(1) *f* ve *g* aralarında asal ise *f* ve *g* nin *E* de ortak kökü yoktur.

(2) *f* ve f' aralarında asal ise *f* nin *E* de çokkatlı kökü yoktur.

(3) *f, K*[*x*] te asal ise ya *f* ve *g* aralarında asaldır ya da *K*[*x*] te $f \mid g$ dir.

(4) *f*, *K*[*x*] te asal ve $deg\, f > deg\, g$ ise, *f* ve *g* nin *E* de ortak kökü yoktur.

(5) *f*, *K*[*x*] te asal ve $f' \neq 0_K$ ise, *f* nin *E* de çokkatlı kökü yoktur.

(6) *f*, *K*[*x*] te asal ise ve *f* nin *E* ye ait, çokkatlı olmayan bir kökü varsa, bu takdirde $f' \neq 0_K$ dır.

Tanım 2.93. Bir *C* cebirsel yapısına öyle bir *O* kümesi bağlanabilsin ki, $O \times C = \{(\alpha, a) \mid \alpha \in O, a \in C\}$ kümesini *C* içine resmeden, yani her $(\alpha, a) \in O \times C$ ye tamamen belirli bir $c \in C$ tekabül ettiren bir tasvir bulunsun. Bu durumda *C* ye *O*

üzerinde bir operatörlü cebirsel yapı, O ya bir *operatör bölgesi, O* nun elemanlarına da *operatörler* veya *skalerler* denir. (α, a) ya karşı gelen c, genellikle $c = \alpha a$ şeklinde gösterilir ve buna a *nın* α *operatörüyle (skaleriyle) çarpımı* denir. Belirli bir $\alpha \in O$ ve bir $a \in C$ verildiğine göre, αa yı bulmaya da *C nin a elemanına* α *operatörünü uygulamak* veya *a elemanını* α *skaleriyle çarpmak* denir.

Tanım 2.94. $< V, + >$ bir abel grubu, $< K; +, \cdot >$ da bir komütatif cisim olsun ve $K \times V$ yi V içine resmeden bir operatörlü çarpım verilmiş olsun. Bu operatörlü çarpım, aşağıdaki koşulları gerçeklediği takdirde *V* ye *K üzerinde bir vektör uzayı (lineer küme)* veya kısaca bir *K-vektör uzayı* denir (burada $a, b \in V$ ve $\alpha, \beta \in K$ dır):

(1) $\alpha(a+b) = \alpha a + \alpha b$,

(2) $(\alpha + \beta)a = \alpha a + \beta a$,

(3) $\alpha(\beta a) = (\alpha \cdot \beta)a$,

(4) $1_K a = a$.

Tanım 2.95. $v_1, v_2, ..., v_n$ bir *K* cismi üzerinde bir vektör uzayının (birbirinden farklı olması gerekmeyen) sonlu sayıda vektörü olsun. Bu takdirde $\alpha_1, \alpha_2, ..., \alpha_n \in K$ olmak üzere oluşturulan

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n$$

vektörüne $v_1, v_2, ..., v_n$ *vektörlerinin bir K-lineer kombinezonu* denir.

Tanım 2.96. *V* ve *U,* aynı *K* cismi üzerinde iki vektör uzayı olsun. Her $v_1, v_2, v \in V$ ve her $\alpha \in K$ için

$$\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2),\ \varphi(\alpha v) = \alpha\varphi(v)$$

koşullarını sağlayan bir $\varphi : V \to U$ tasvirine bir *vektör uzayı homomorfisi* veya bir *K-lineer transformasyon* veya bir *K-lineer tasvir* denir. φ (1-1) ve üzerine ise φ ye bir *vektör uzayı izomorfisi* denir ve $V \cong U$ yazılır.

Tanım 2.97. *V,* bir *K* cismi üzerinde bir vektör uzayı ve $v_1, v_2, ..., v_n$, *V* ye ait sonlu sayıda vektör olsun. *K* da

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = 0_V$$

olacak şekilde, hepsi birden 0_K ya eşit olmayan $\alpha_1, \alpha_2, ..., \alpha_n$ skalerleri varsa, $v_1, v_2, ..., v_n$ *vektörleri K üzerinde lineer bağımlıdır* denir. Eğer $v_1, v_2, ..., v_n$ vektörleri, *K* üzerinde lineer bağımlı değilse, yani $\alpha_1, \alpha_2, ..., \alpha_n \in K$ olmak üzere,

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = 0_V$$

şeklindeki bir bağıntıdan daima $\alpha_1 = \alpha_2 = ... = \alpha_n = 0_K$ sonucu çıkıyorsa $v_1, v_2, ..., v_n$ *vektörleri K üzerinde lineer bağımsızdır* denir.

Tanım 2.98. *V,* bir *K* cismi üzerinde bir vektör uzayı ve $A = \{v_1, v_2, ..., v_n\}$, *V* nin boş olmayan sonlu bir alt kümesi olsun. Bu takdirde $v_1, v_2, ..., v_n$ vektörlerinin *K* üzerindeki bütün lineer kombinezonlarının

$$W = \left\{ \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n \,\middle|\, \alpha_1, \alpha_2, ..., \alpha_n \in K \right\}$$

kümesi, V nin bir alt uzayıdır. Bu W alt uzayına *V nin A tarafından doğurulan alt uzayı* veya *V nin $v_1, v_2, ..., v_n$ vektörleri tarafından doğurulan alt uzayı* veya *A nın K-span'i* denir ve bu alt uzay $s_K(A)$ ile gösterilir. $A = \{v_1, v_2, ..., v_n\}$ sonlu bir küme ise $s_K(\{v_1, v_2, ..., v_n\})$ yerine $s_K(v_1, v_2, ..., v_n)$ yazılır. $s_K(\varnothing) = \{0_K\}$ dır.

Tanım 2.99. V, bir K cismi üzerinde bir vektör uzayı olsun. V nin boş olmayan bir B alt kümesi, K üzerinde lineer bağımsız ise ve K üzerinde V yi doğuruyorsa (yani $s_K(B) = V$ ise) B ye *K üzerinde V nin bir tabanı* veya *V nin bir K-tabanı* denir.

Lemma 2.100 [2, *S*.496, *Lemma* 41.10]**.** V, U, W bir K cismi üzerinde üç vektör uzayı, $\varphi : V \to U$ ve $\psi : U \to W$ iki vektör uzayı izomorfisi olsun. Bu takdirde

(1) $\psi\varphi : V \to W$ bileşke tasviri, bir vektör uzayı izomorfisidir,

(2) φ nin $\varphi^{-1} : U \to V$ tersi, bir vektör uzayı izomorfisidir.

Teorem 2.101 [2, *S*.508, *Theorem* 42.8]**.** V, bir K cismi üzerinde bir vektör uzayı ve $B = \{v_1, v_2, ..., v_n\}$, V nin boş olmayan bir alt kümesi olsun. Bu takdirde B nin, V nin bir K-tabanı olması için gerek ve yeter koşul, V nin her a elemanının $\alpha_1, \alpha_2, ..., \alpha_n \in K$ skalerleri ile

$$a = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n$$

şeklinde tek türlü yazılabilmesidir.

Teorem 2.102(Steinitz Yer Değiştirme Teoremi)[2, *S*.509, *Theorem* 42.10]**.** V, bir K cismi üzerinde bir vektör uzayı ve $w_1, w_2, ..., w_m$, V ye ait sonlu sayıda vektör olsun. $v_1, v_2, ..., v_n \in V$, $w_1, w_2, ..., w_m$ nin $s_K(w_1, w_2, ..., w_m)$ K-span'inde n tane lineer bağımsız vektör olsun. Bu takdirde $n \le m$ dir. Bundan başka, V ye ait $v_1, v_2, ..., v_n$ gibi, n tane lineer bağımsız vektör verildiğine göre, V de

$$s_K(v_1, v_2, ..., v_n, w_{n+1}, w_{n+2}, ..., w_m) = s_K(w_1, w_2, ..., w_m)$$

olacak şekilde m tane $w_1, w_2, ..., w_m$ vektörü vardır.

Lemma 2.103 [2, *S*.513, *Lemma* 42.13]**.** V, bir K cismi üzerinde bir vektör uzayı, $dim_K V = n \in \mathbb{N}$ ve $v_1, v_2, ..., v_n$, V ye ait n tane vektör olsun. Bu takdirde

(1) $v_1, v_2, ..., v_n$ vektörleri, K üzerinde lineer bağımsız ise $s_K(v_1, v_2, ..., v_n) = V$ dir,

(2) $s_K(v_1, v_2, ..., v_n) = V$ ise $v_1, v_2, ..., v_n$ vektörleri K üzerinde lineer bağımsızdır.

Teorem 2.104 [2, *S*.513, *Theorem* 42.14]**.** *V*, bir *K* cismi üzerinde *m* ($m \geq 1$) boyutlu bir vektör uzayı olsun. $v_1, v_2, ..., v_n$ de V ye ait *n* ($n \geq 1$) tane lineer bağımsız vektör olsun. Bu takdirde *V* nin $\{v_1, v_2, ..., v_n\} \subset B$ olacak şekilde bir *B K*-tabanı vardır.

Tanım 2.105. *V* bir *K* cismi üzerinde bir vektör uzayı olsun. *V* nin sonlu bir *K*-tabanı varsa *V* nin herhangi bir *K*-tabanındaki elamanların sayısına *V* nin *K* üzerindeki boyutu veya *V* nin *K*-boyutu denir ve bu boyut, $dim_K V$ şeklinde gösterilir. *V* nin hiçbir sonlu *K*-tabanı yoksa V nin *K*-boyutu sonsuz olarak tanımlanır ve bu durumda $dim_K V = \infty$ yazılır.

Lemma 2.106 [2, *S*.514, *Lemma* 42.15]**.** *V*, bir *K* cismi üzerinde sonlu boyutlu bir vektör uzayı ve *W*, *V* nin bir alt uzayı olsun. Bu takdirde

(1) *W* sonlu boyutludur ve $dim_K W \leq dim_K V$ dir,

(2) $dim_K W = dim_K V$ olması için gerek ve yeter koşul, $W = V$ olmasıdır.

Teorem 2.107 [2, *S*.519, *Theorem* 42.22]**.** *V* ve *U*, bir *K* cismi üzerinde sonlu boyutlu iki vektör uzayı ve $\varphi : V \to U$ bir *K*-lineer tasvir olsun. *V* ve *U* nun K üzerindeki boyutlarının aynı olduğunu varsayalım. Bu takdirde aşağıdaki ifadeler birbirine denktir:

(1) φ (1-1) dir,

(2) φ üzerinedir,

(3) φ bir vektör uzayı izomorfisidir.

BÖLÜM III. CİSİM GENİŞLEMELERİ

§ 1. Cisim Genişlemeleri İle İlgili Genel Bilgiler

Tanım 3.1.1. $<E;+,.>$ bir cisim ve K, E nin boş olmayan bir alt kümesi olsun. K, E de tanımlanan işlemlere göre kendi başına bir cisim oluşturuyorsa K ya *E nin bir alt cismi* denir. Bu durumda E ye de *K nın bir cisim genişlemesi* veya kısaca *K nın bir genişlemesi* denir.

E nin K nın bir genişlemesi olduğunu göstermek için E/K yazılır ve bu sembol, *E/K cisim genişlemesi* diye okunur. Bu sembolün bir bölüm grubu veya bir bölüm uzayıyla karıştırılması söz konusu değildir. Cisim genişlemeleri için sık sık Hasse diyagramlarını kullanacağız. Örneğin

şekli, K nın E nin bir alt cismi olduğunu gösterecektir.

Alt gruplarda, alt halkalarda ve alt uzaylarda olduğu gibi, alt cisimler için de bir kriter verilebilir:

Lemma 3.1.2 (Alt Cisim Kriteri). E bir cisim ve K, E nin boş olmayan bir alt kümesi olsun. K nın E nin bir alt cismi olabilmesi için gerek ve yeter koşullar şunlardır:

Her $a,\ b \in K$ için
(i) $a+b \in K$,
(ii) $-b \in K$,
(iii) $a \cdot b \in K$,
(iv) $b^{-1} \in$K $(b \neq 0_K$ için).

İspat. E bir cisim olduğuna göre bir halkadır ve E nin 0_E den farklı elemanları, çarpma işlemine göre bir komütatif grup oluştururlar. O halde K nın E nin bir alt cismi olabilmesi için gerek ve yeter koşul, K nın E nin bir alt halkası olması ve K nın 0_E den farklı elemanlarının çarpma işlemine göre bir komütatif grup oluşturmasıdır. Kuşkusuz, $E^* = E - \{0_E\}$ grubunun her alt grubu komütatiftir. Bundan dolayı K nın E nin bir alt cismi olabilmesi için gerek ve yeter koşul, K nın E nin bir alt halkası olması ve $K - \{0_K\}$ nın E^* ın bir alt grubu olmasıdır. Şimdi K nın E nin bir alt halkası olabilmesi için gerek ve yeter koşul, (i), (ii), (iii) ün sağlanmasıdır; $K - \{0_K\}$ nın E^* ın bir alt grubu olması için gerek ve yeter koşul ise

$$(iii)'\ \text{Her}\ a,b \in K - \{0_K\}\ \text{için}\ a \cdot b \in K - \{0_K\}$$

ve (iv) ün sağlanmasıdır. $K \subset E$ ve E cismi sıfır-bölensiz olduğundan $(iii)'$, (iii) ten daha zayıftır. Dolayısıyla, K nın E nin bir alt cismi olabilmesi için gerek ve yeter koşul, (i), (ii), (iii) ve (iv) ün sağlanmasıdır.

Not 3.1.3. Şu andan itibaren, bir K cisminin 0_K dan farklı bir b elemanının tersi için b^{-1} yerine $\frac{1_K}{b}$ (veya $1_K / b$) yazacağız. Benzer şekilde, bir cisimde a herhangi bir eleman, b de cismin sıfırından farklı herhangi bir eleman olmak üzere $a \cdot b^{-1} = b^{-1} \cdot a$ çarpımı yerine $\frac{a}{b}$ (veya a/b) yazacağız.

Lemma 3.1.2 ye göre K, E nin bir alt cismi ise $a, b \in K$ için

$$a+b \ , \ a-b \ , \ a \cdot b \ , \ \frac{a}{b} \in K$$

dır (son durumda $b \neq 0_K$ olduğu varsayılmaktadır). O halde E nin bir alt cismi, E nin toplama, çıkarma, çarpma ve (0_E den farklı elemanlar ile) bölmeye göre kapalı bir alt kümesidir.

Örnek 3.1.4. $\mathbb{C}$, $\mathbb{R}$ nun bir genişlemesi ve $\mathbb{R}$ de $\mathbb{Q}$ nun bir genişlemesidir. $\mathbb{Q}$, aynı zamanda $\mathbb{C}$ nin bir alt cismidir.

Örnek 3.1.5. K herhangi bir cisim, x te K üzerinde bir değişken ise K, $K(x)$ in bir alt cismidir. Gerçekten, K nın bir a elemanını $\frac{a}{1_K}$ rasyonel fonksiyonu ile özdeşleştirebiliriz ki, burada pay ve payda, $K \subset K[x]$ in elemanlarıdır. Benzer şekilde, y K üzerinde başka bir değişken olmak üzere K, $K(x,y)$ nin bir alt cismidir.

Örnek 3.1.6. $\mathbb{Q}(i) := \{x + yi \in \mathbb{C} : x, y \in \mathbb{Q}\} \subset \mathbb{C}$ kümesini gözönüne alalım. Her $a, b \in \mathbb{Q}(i)$ için $a = x + yi$ ve $b = z + ui$ $(x, y, z, u \in \mathbb{Q})$ olup,

(i) $a+b=(x+z)+(y+u)i \in \mathbb{Q}(i)$,

(ii) $-b=(-z)+(-u)i \in \mathbb{Q}(i)$,

(iii) $a \cdot b =(xz-yu)+(xu+yz)i \in \mathbb{Q}(i)$,

(iv) $b^{-1} = \frac{1}{z+ui} = \frac{z}{z^2+u^2} + \frac{-u}{z^2+u^2} i \in \mathbb{Q}(i)$ ($b=z+ui \neq 0+0i = 0_{\mathbb{C}}$ olmak koşuluyla)

dir. Dolayısıyla $\mathbb{Q}(i)$, $\mathbb{C}$ nin bir alt cismidir. $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ Gauss tam sayılar halkasının kesirler cismi olan bu cisim, *Gauss cismi* olarak adlandırılır.

Örnek 3.1.7. $\mathbb{Q}(\sqrt{2}) := \{x + y\sqrt{2} \in \mathbb{C} : x, y \in \mathbb{Q}\}$, $\mathbb{C}$ nin bir alt cismidir. Gerçekten, her $a, b \in \mathbb{Q}(\sqrt{2})$ için $a = x + y\sqrt{2}$, $b = z + u\sqrt{2}$ $(x, y, z, u \in \mathbb{Q})$ olup,

(i) $a + b = (x + z) + (y + u)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$,

(ii) $-b = (-z) + (-u)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$,

$(iii)\ a\cdot b=(xz+2yu)+(xu+yz)\sqrt{2}\in \mathbb{Q}(\sqrt{2}),$

$(iv)\ b^{-1}=\dfrac{z}{z^2-2u^2}+\dfrac{-u}{z^2-2u^2}\sqrt{2}\in \mathbb{Q}(\sqrt{2})$ $(b=z+u\sqrt{2}\neq 0+0\sqrt{2}=0$ olmak koşuluyla)

dir. Burada $\sqrt{2}\in\mathbb{Q}$ nin bir irrasyonel sayı olduğu, dolayısıyla z ve u, en az biri sıfırdan farklı iki rasyonel sayı olmak üzere, $z^2-2u^2\neq 0$ olduğu kullanılmaktadır.

Örnek 3.1.8. $L:=\left\{x+y\sqrt[3]{2}\in\mathbb{Q} : x,y\in\mathbb{Q}\right\}\subset\mathbb{Q}$ kümesini gözönüne alalım. L, $\mathbb{Q}$ nin bir alt cismi değildir, çünkü örneğin $\sqrt[3]{2}\in L$, fakat $\sqrt[3]{2}\cdot\sqrt[3]{2}=\sqrt[3]{4}\notin L$ dir. $\sqrt[3]{4}\in L$ olduğunu varsayalım, yani $x+y\sqrt[3]{2}=\sqrt[3]{4}$ olacak şekilde $x,y\in\mathbb{Q}$ bulunsun.

$$(x+y\sqrt[3]{2})^2=(\sqrt[3]{4})^2\Rightarrow x^2+2\sqrt[3]{2}xy+\sqrt[3]{4}y^2=\sqrt[3]{16}=2\sqrt[3]{2}\,.$$

Son eşitlikte $\sqrt[3]{4}=x+y\sqrt[3]{2}$ yazalım.

$$x^2+2\sqrt[3]{2}xy+(x+y\sqrt[3]{2})y^2=2\sqrt[3]{2}\ ,$$

$$x^2+xy^2=-\sqrt[3]{2}(2xy+y^3-2)\ ,$$

$$\sqrt[3]{2}=-\frac{x^2+xy^2}{y^3+2xy-2}\cdot$$

$x,y\in\mathbb{Q}$ olduğundan $-\dfrac{x^2+xy^2}{y^3+2xy-2}\in\mathbb{Q}$ olur, oysa $\sqrt[3]{2}\notin\mathbb{Q}$ dur [5, S.213].

Bu şekilde bir çelişki elde ettiğimize göre, $x+y\sqrt[3]{2}=\sqrt[3]{4}$ olacak şekilde $x,y\in\mathbb{Q}$ yoktur, yani $\sqrt[3]{4}\notin L$ dir. Diğer taraftan,

$$\mathbb{Q}(\sqrt[3]{2}):=\left\{x+y\sqrt[3]{2}+z\sqrt[3]{4}\in\mathbb{Q} : x,y,z\in\mathbb{Q}\right\}=\left\{x+y\sqrt[3]{2}+z(\sqrt[3]{2})^2\in\mathbb{Q} : x,y,z\in\mathbb{Q}\right\},$$

$\mathbb{Q}$ nin bir alt cismidir. Gerçekten, her $a,b\in\mathbb{Q}(\sqrt[3]{2})$ için $a=x+y\sqrt[3]{2}+z\sqrt[3]{4}$, $b=u+v\sqrt[3]{2}+w\sqrt[3]{4}$ $(x,y,z,u,v,w\in\mathbb{Q})$ olup,

$$(i)\quad a+b=(x+u)+(y+v)\sqrt[3]{2}+(z+w)\sqrt[3]{4}\in\mathbb{Q}(\sqrt[3]{2})\ ,$$

$$(ii)\quad -b=(-u)+(-v)\sqrt[3]{2}+(-w)\sqrt[3]{4}\in\mathbb{Q}(\sqrt[3]{2})\ ,$$

$$(iii)\ a\cdot b=(xu+2yw+2zv)+(xv+yu+2zw)\sqrt[3]{2}+(xw+yv+zu)\sqrt[3]{4}\in\mathbb{Q}(\sqrt[3]{2}),$$

$$(iv)\quad b^{-1}=\frac{1}{u+v\sqrt[3]{2}+w\sqrt[3]{4}}\in\mathbb{Q}(\sqrt[3]{2})$$

dir.

Örnek 3.1.9. K bir cisim ve $K_i\ (i\in I)$ K nın alt cisimlerinin bir ailesi olsun. Bu takdirde $\bigcap_{i\in I}K_i$, K nın bir alt cismidir. Çünkü Lemma 3.1.2 deki kapalılık özelikleri her K_i için geçerli olduğundan $\bigcap_{i\in I}K_i$ için de geçerlidir.

Son örnekten, bir K cisminin bütün alt cisimlerinin kesişiminin K nın bir alt cismi olduğu sonucuna varırız (En azından K nın kendisi, K nın bir alt cismi olduğundan bu kesişim boş değildir).

Tanım 3.1.10. K bir cisim olsun. K nın bütün alt cisimlerinin kesişimine K *nın asal alt cismi* denir.

O halde K nın her alt cismi, K nın asal alt cismini kapsar, yani onun bir genişlemesidir. Şimdi K nın asal alt cismindeki elemanları belirlemeye çalışalım. P, K nın asal alt cismini göstersin. K nın birim elemanıyla $1_{\square} \in \square$ i birbirinden açık bir şekilde ayırt etmek için K nın birim elemanını e ile göstereceğiz. $0_K \in P$, $e \in P$ ve $0_K \neq e$ olduğunu biliyoruz, çünkü P bir cisimdir. P, toplama işlemine göre bir grup olduğundan $e+e=2e$, $2e+e=3e$, $3e+e=4e$, ...P nin elemanlarıdır ve aynı zamanda $-e$, $-2e$, $-3e$, $-4e$,... de P nin elemanlarıdır. Bundan dolayı

$$..., -4e, -3e, -2e, -e, 0_K, e, 2e, 3e, 4e,...$$

elemanlarının hepsi P ye aittir, yani $\{me \in K : m \in \square\} \subset P$ dir. Bundan başka, P (0_K dan farklı elemanlar ile) bölmeye göre de kapalıdır ve bu nedenle $P_0 := \{me/ne \in K : m,n \in \square\}$, P nin bir alt kümesidir. P_0 ın K nın bir alt cismi olduğunu (ve dolayısıyla $P_0 = P$ olduğunu) beklemek gayet doğaldır. Gerçekten, bölüm tanımı ve birimin ve katların özelikleri kullanılarak,

her me/ne, $re/se \in P_0$ $(m,n,r,s \in \square)$ için

(i) $\dfrac{me}{ne} + \dfrac{re}{se} = \dfrac{(ms+rn)e}{(ns)e} \in P_0$,

(ii) $-\dfrac{re}{se} = \dfrac{(-r)e}{se} \in P_0$,

(iii) $\dfrac{me}{ne} \cdot \dfrac{re}{se} = \dfrac{(mr)e}{(ns)e} \in P_0$,

(iv) $\dfrac{1_K}{\frac{re}{se}} = \dfrac{se}{re} \in P_0$ $\quad (\dfrac{re}{se} \neq 0_K$, yani $re \neq 0_K$ olmak koşuluyla)

olduğu gösterilebilir.

Teorem 3.1.11. Herhangi bir K cisminin asal alt cismi, $\square$ ya ya da uygun bir p asal sayısı için $\square_p$ ye izomorftur.

İspat. e, K nın birim elemanı ve P de K nın asal alt cismi olsun. O zaman $1e = e \neq 0_K$ ve $(-1)e = -e \neq 0_K$ dır. Şimdi $ne = 0_K$ koşulunu sağlayan bir $n \neq 0$ tam sayısının varlığı ve yokluğuna göre iki durum ayıracağız.

1. Durum: $ne = 0_K$ olacak şekilde, sıfırdan farklı bir n tam sayısının bulunduğunu varsayalım. Bu takdirde $ke = 0_K$ olacak şekilde k doğal sayıları vardır. Bu k doğal sayılarının en küçüğü p olsun. Şu halde $pe = 0_K$ dır. Şimdi

$$\varphi : \mathbb{Z} \to P$$
$$n \to ne$$

tasvirinin bir halka homomorfisi, *p* nin bir asal sayı olduğunu ve $P \cong \mathbb{Z}_p$ olduğunu iddia ediyoruz.

Her $m, n \in \mathbb{Z}$ için, Lemma 2.29(3) e göre

$$\varphi(m+n) = (m+n)e = me + ne = \varphi(m) + \varphi(n),$$

(4) e göre ise

$$\varphi(mn) = (mn)e = (me)(ne) = \varphi(m) \cdot \varphi(n)$$

dir. Dolayısıyla φ bir halka homomorfisidir.

p bileşik bir sayı olsa $r, s \in \mathbb{Z}$, $1 < r < p$, $1 < s < p$ olmak üzere, *p=rs* olur ve buradan $0_K = pe = (rs)e = (re)(se)$ elde edilir. *K* sıfır-bölensiz olduğundan buradan $re = 0_K$, $se = 0_K$ dan en az birinin doğru olduğu sonucu çıkar. Bu ise *p* nin $pe = 0_K$ koşulunu sağlayan en küçük doğal sayı oluşuyla çelişir. O halde *p* bir asal sayıdır.

$P \cong \mathbb{Z}_p$ olduğunu ispatlamak için $Ker\varphi$ yi bulacağız. $pe = 0_K$ dan $p \in Ker\varphi$ sonucu çıkar ve dolayısıyla her $n \in \mathbb{Z}$ için $pn \in Ker\varphi$ olur (çünkü $Ker\varphi$, $\mathbb{Z}$ nin bir idealidir). O halde

$$p\mathbb{Z} \subset Ker\varphi \tag{3.1}$$

dir. Diğer taraftan $m \in Ker\varphi$ ise *m=qp+r* ve $0 \le r < p$ olacak şekilde $q, r \in \mathbb{Z}$ vardır. Buradan

$0_K = me = (qp + r)e = (qp)e + re = q(pe) + re = q0_K + re = 0_K + re = re$, yani $re = 0_K$ elde edilir. $0 \le r < p$ olduğundan *r*=0 olmak zorundadır. Buradan da *m=qp* , yani $m \in p\mathbb{Z}$ sonucu çıkar. O halde

$$Ker\varphi \subset p\mathbb{Z} \tag{3.2}$$

dir. (3.1) ve (3.2) den $Ker\varphi = p\mathbb{Z}$ sonucu çıkar. Bu nedenle

$\mathbb{Z}_p = \mathbb{Z} / p\mathbb{Z} = \mathbb{Z} / Ker\varphi \cong \mathrm{Im}\,\varphi \subset P$ ve dolayısıyla $\mathbb{Z}_p \cong \mathrm{Im}\,\varphi$ dir. $\mathbb{Z}_p$ bir cisim olduğundan, ona izomorf olan $\mathrm{Im}\,\varphi$ halkası da bir cisimdir. Dolayısıyla $\mathrm{Im}\,\varphi$, *K* nın bir alt cismidir, o halde $P \subset \mathrm{Im}\,\varphi$ dir. Buradan, iddia edildiği üzere, $P = \mathrm{Im}\,\varphi$ ve $P \cong \mathbb{Z}_p$ sonucuna varırız.

2. Durum: $ne = 0_K$ olacak şekilde, sıfırdan farklı hiçbir *n* tam sayısının bulunmadığını varsayalım.

$$\psi : \mathbb{Q} \to P$$
$$m/n \to me/ne$$

tasvirinin bir halka homomorfisi olduğunu ve $P \cong \mathbb{Q}$ olduğunu iddia ediyoruz.

Önce ψ nin iyi tanımlı olduğunu göstereceğiz.

$\frac{m}{n} = \frac{m'}{n'} \in \mathbb{Q}$ $(m, n, m', n' \in \mathbb{Z}, n \neq 0, n' \neq 0)$ ise $mn' = m'n \in \mathbb{Z}$ dir, bu nedenle

$(mn')e=(m'n)e\in P$ ve dolayısıyla $(me)(n'e)=(m'e)(ne)\in P$ dir. Bu eşitliğin her iki tarafını $\frac{1_K}{ne}\cdot\frac{1_K}{n'e}\in P$ ile çarparak $\frac{me}{ne}=\frac{m'e}{n'e}$ elde edilir. Şu halde ψ iyi tanımlıdır.

Şimdi ψ nin bir halka homomorfisi olduğunu gösterelim. Her $\frac{m}{n},\frac{r}{s}\in\mathbb{Q}$ $(m,n,r,s\in\mathbb{Z},n\neq 0,s\neq 0)$ için

$$\psi\left(\frac{m}{n}+\frac{r}{s}\right)=\psi\left(\frac{ms+rn}{ns}\right)=\frac{(ms+rn)e}{(ns)e}=\frac{(ms)e+(rn)e}{(ns)e}$$

$$=\frac{(me)(se)+(re)(ne)}{(ne)(se)}=\frac{me}{ne}+\frac{re}{se}=\psi\left(\frac{m}{n}\right)+\psi\left(\frac{r}{s}\right),$$

$$\psi\left(\frac{m}{n}\cdot\frac{r}{s}\right)=\psi\left(\frac{mr}{ns}\right)=\frac{(mr)e}{(ns)e}=\frac{(me)(re)}{(ne)(se)}=\frac{me}{ne}\cdot\frac{re}{se}=\psi\left(\frac{m}{n}\right)\cdot\psi\left(\frac{r}{s}\right)$$

dir. Şu halde ψ gerçekten bir halka homomorfisidir.

2. durumda her $m\in\mathbb{Z}-\{0\}$ için $me\neq 0_K$ olduğunu varsaydığımızdan dolayı,

$$Ker\psi=\left\{\frac{m}{n}\in\mathbb{Q}:\frac{me}{ne}=0_K\right\}=\left\{\frac{m}{n}\in\mathbb{Q}:me=0_K\right\}=\left\{\frac{m}{n}\in\mathbb{Q}:m=0\right\}=\{0\}$$

dır, bu nedenle $\mathbb{Q}\cong\mathbb{Q}/\{0\}=\mathbb{Q}/Ker\psi\cong\mathrm{Im}\psi\subset P$ ve dolayısıyla $\mathbb{Q}\cong\mathrm{Im}\psi$ dir. $\mathbb{Q}$ bir cisim olduğundan buradan $\mathrm{Im}\psi$ nin de bir cisim olduğu sonucu çıkar. Şu halde $\mathrm{Im}\psi$, K nın bir alt cismidir, bu nedenle $P\subset\mathrm{Im}\psi$ dir ve iddia edildiği üzere, buradan $P=\mathrm{Im}\psi$ ve dolayısıyla $P\cong\mathbb{Q}$ sonucu çıkar.

Tanım 3.1.12. *K* bir cisim ve *e*, *K* nın birim elemanı olsun. $ne=0_K$ olacak şekilde, sıfırdan farklı *n* tam sayıları varsa ve *p* bu koşulu sağlayan en küçük doğal sayı ise, *K* ya *karakteristiği p olan bir cisim, p* ye ise *K nın karakteristiği* denir ve *karK=p* yazılır. $ne=0_K$ olacak şekilde, sıfırdan farklı hiçbir *n* tam sayısı yoksa, K ya *karakteristiği 0 olan bir cisim*, 0 a ise *K nın karakteristiği* denir ve *karK*=0 yazılır.

Buna denk olarak, *K* nın asal alt cisminin $\mathbb{Z}_p$ veya $\mathbb{Q}$ ya izomorf oluşuna göre, *K* nın karakteristiği *p* veya *0* dır. Örneğin $kar\mathbb{Z}_p=p$ ve $kar\mathbb{Q}(i)=kar\mathbb{Q}(\sqrt{2})=kar\mathbb{Q}=kar\mathbb{R}=0$ dır. Genellikle $\mathbb{Z}_p$ veya $\mathbb{Q}$ yu *K* nın asal alt cismi ile aynı kabul edeceğiz. Özellikle *K* nın birimi olarak *e* yerine 1 yazacağız. Böylece *K*, $\mathbb{Z}_p$ veya $\mathbb{Q}$ nun bir genişlemesi olarak düşünülecektir.

K, karakteristiği *p* olan bir cisim ise, her $a\in K$ için $pa=0_K$ olduğuna işaret edelim. Gerçekten,

$$pa = \underbrace{a + a + ... + a}_{p \text{ tane}} = 1 \cdot a + 1 \cdot a + ... + 1 \cdot a = (\underbrace{1 + 1 + ... + 1}_{p \text{ tane}})a = (p1)a = 0_K \cdot a = 0_K$$

dır.

Şimdi iki anlaşma yapacağız: Bundan böyle $\square_p$ yerine F_p yazacağız. Bu her zaman bize F_p nin bir cisim olduğunu anımsatacaktır. İkinci olarak, F_p nin elemanlarını yazarken çizgileri atacağız. Örneğin $\overline{2} \in \mathrm{F}_5$ yerine 2 yazacağız. 2 tam sayısını $\overline{2} \in \mathrm{F}_2$, $\overline{2} \in \mathrm{F}_3$, $\overline{2} \in \mathrm{F}_5$, daha genel olarak $\overline{2} \in \mathrm{F}_p$ (p herhangi bir asal sayı) ile karıştırmamaya dikkat etmeliyiz. "2" den hangi anlamda söz edildiği, metinden anlaşılacaktır.

Şimdi cisim homomorfilerini inceleyeceğiz.

Lemma 3.1.13. *K* bir cisim ise *K* nın yalnızca iki ideali vardır ki, bunlar da *K* ve $\{0_K\}$ dan ibarettir.

İspat. *A*, *K* nın bir ideali ve $A \neq \{0_K\}$ ise $a \neq 0_K$ olacak şekilde bir $a \in A$ vardır. *a* nın *K* da $\frac{1_K}{a}$ gibi bir tersi vardır ve *A* bir ideal olduğundan $\frac{1_K}{a} \cdot a = 1_K \in A$ dır. Buradan her $b \in K$ için $b = b \cdot 1_K \in A$ ve dolayısıyla $K \subset A$ elde edilir; şu halde *A*=*K* dır.

Lemma 3.1.14. K_1 , K_2 iki cisim ve $\varphi : K_1 \to K_2$ bir halka homomorfisi ise, ya her $a \in K_1$ için $\varphi(a) = 0_{K_2}$ dir veya φ (1-1) dir.

İspat. $Ker\varphi, K_1$ in bir ideali olduğundan, Lemma 3.1.13 e göre ya $Ker\varphi = K_1$ ya da $Ker\varphi = \{0_{K_1}\}$ dir. Birinci durumda her $a \in K_1$ için $\varphi(a) = 0_{K_2}$ dir, ikinci durumda ise φ (1-1) dir.

Bir cisimden diğerine halka homomorfilerini incelerken, doğal olarak tanım kümesindeki her elemanı sağ taraftaki cismin sıfır elemanına götüren, ilginç olmayan halka homomorfisini ihmal etmek isteriz. Bunun dışındaki tüm halka homomorfileri, Lemma 3.1.14 e göre (1-1) dir. Bu bizi şu tanıma götürür:

Tanım 3.1.15. K_1 , K_2 iki cisim ve $\varphi : K_1 \to K_2$ tasviri, (1-1) bir halka homomorfisi ise, φ ye bir *cisim homomorfisi* denir. φ tasviri K_1 in K_2 üzerine bir cisim homomorfisi ise φ ye bir *cisim izomorfisi* denir. *K* nın kendi üzerine bir cisim izomorfisine *K* nın bir *(cisim) otomorfisi* denir.

$\varphi : K_1 \to K_2$ bir cisim izomorfisi ise φ , $< K_1, + >$ grubunun $< K_2, + >$ grubuna bir homomorfisidir, o halde $\varphi(0_{K_1}) = 0_{K_2}$ ve aynı zamanda $Ker\varphi = \{0_{K_1}\}$ dir.

Şu halde $\varphi\big|_{K_1-\{0_{K_1}\}} : K_1 - \{0_{K_1}\} \to K_2 - \{0_{K_2}\}$ tasviri, üzerine (1-1) bir tasvirdir. Buna ek olarak, her $a,b \in K_1$ için $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$ olduğundan, her $a,b \in K_1 - \{0_{K_1}\}$ için de $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$ dir ve dolayısıyla $\varphi_{K_1^*} : K_1^* \to K_2^*$ tasviri, K_1^* grubunun K_2^* grubu üzerine (1-1) bir homomorfisidir, yani $K_1^* \cong K_2^*$ dır. Özellikle 1_{K_1} *ve* 1_{K_2}, sırasıyla K_1 ve K_2 cisimlerinin birimleri olmak üzere, $\varphi(1_{K_1})=1_{K_2}$ dir.

Lemma 3.1.16. K_1, K_2, K_3 üç cisim olsun.

(1) $\varphi : K_1 \to K_2$ ve $\psi : K_2 \to K_3$ cisim homomorfileri ise, $\psi\varphi : K_1 \to K_3$ te bir cisim homomorfisidir.

(2) $\varphi : K_1 \to K_2$ ve $\psi : K_2 \to K_3$ cisim izomorfileri ise, $\psi\varphi : K_1 \to K_3$ te bir cisim izomorfisidir.

(3) $\varphi : K_1 \to K_2$ bir cisim izomorfisi ise, $\varphi^{-1} : K_2 \to K_1$ de bir cisim izomorfisidir.

İspat. (1) $\psi\varphi$ tasviri, Lemma 2.56(1) e göre bir halka homomorfisidir, Teorem 2.7(2) ye göre de (1-1) dir. Şu halde $\psi\varphi$ bir cisim homomorfisidir.

(2) $\psi\varphi$ tasviri, (1) den dolayı bir cisim homomorfisidir, Teorem 2.7(1) e göre de üzerinedir. Şu halde $\psi\varphi$ bir cisim izomorfisidir.

(3) $\varphi^{-1} : K_2 \to K_1$ tasviri, Lemma 2.56(2) ye göre bir halka homomorfisidir, Teorem 2.8(1) e göre de (1-1) dir. Şu halde φ^{-1} bir cisim izomorfisidir.

Bir $\varphi : K_1 \to K_2$ cisim homomorfisi (1-1) bir fonksiyon olarak karakterize edilebilir, öyle ki, her $a,b \in K_1$ (bölmede $b \neq 0_{K_1}$) için

$\varphi(a+b)=\varphi(a)+\varphi(b)$, $\varphi(a-b)=\varphi(a)-\varphi(b)$, $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$, $\varphi(\frac{a}{b})=\frac{\varphi(a)}{\varphi(b)}$

dir. Şimdi bazı örnekler verelim.

Örnek 3.1.17.

$$\varphi : \mathbb{C} \to \mathbb{C}$$
$$x \to \overline{x}$$

tasviri, $\mathbb{C}$ nin bir otomorfisidir, çünkü her $x,y \in \mathbb{C}$ için

$$\overline{x+y}=\overline{x}+\overline{y} \quad , \quad \overline{x-y}=\overline{x}-\overline{y} \quad , \quad \overline{x\cdot y}=\overline{x}\cdot\overline{y} \quad , \quad \overline{(x/y)}=\overline{x}/\overline{y}$$

dir.

Örnek 3.1.18.

$$\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$$
$$a+b\sqrt{2} \to a-b\sqrt{2}$$

tasviri, $\mathbb{Q}(\sqrt{2})$ nin bir otomorfisidir, çünkü

her $a+b\sqrt{2}$, $c+d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ $(a,b,c,d \in \mathbb{Q})$ için

$$\varphi((a+b\sqrt{2})+(c+d\sqrt{2})) = \varphi((a+c)+(b+d)\sqrt{2}) = (a+c)-(b+d)\sqrt{2}$$
$$= (a-b\sqrt{2})+(c-d\sqrt{2}) = \varphi(a+b\sqrt{2})+\varphi(c+d\sqrt{2}) \ ,$$
$$\varphi((a+b\sqrt{2})(c+d\sqrt{2})) = \varphi((ac+2bd)+(ad+bc)\sqrt{2}) = (ac+2bd)-(ad+bc)\sqrt{2}$$
$$= (ac+2(-b)(-d))+(a(-d)+(-b)c)\sqrt{2} = (a-b\sqrt{2})(c-d\sqrt{2})$$
$$= \varphi(a+b\sqrt{2})\cdot\varphi(c+d\sqrt{2})$$

dir. Buna göre φ bir cisim homomorfisidir; $\varphi(1) = \varphi(1+0\sqrt{2}) = 1-0\sqrt{2} = 1 \neq 0$ olduğundan $Ker\varphi \neq \mathbb{Q}(\sqrt{2})$ dir ve dolayısıyla φ (1-1) dir.

Örnek 3.1.19. *K* bir cisim ve *x*, *K* üzerinde bir değişken olsun.

$$\varphi : K(x) \to K(x)$$
$$\frac{p(x)}{q(x)} \to \frac{p(x^2)}{q(x^2)}$$

tasviri bir cisim homomorfisidir. $\mathrm{Im}\varphi \subset K(x)$ olduğundan *K*(*x*), kendi has alt kümesi olan $\mathrm{Im}\varphi$ ye izomorftur.

E/K bir cisim genişlemesi olsun. Bu takdirde *E* bir toplamsal gruptur ve her $a,b \in K$ ve her $x,y \in E$ için

$$a(x+y) = a\cdot x + a\cdot y \ , \ (a+b)x = a\cdot x + b\cdot x \ , \ (a\cdot b)x = a(b\cdot x) \ , \ 1_E \cdot x = x$$

tir. O halde *E*, *K* üzerinde bir vektör uzayıdır. *E* nin hem cisim, hem de vektör uzayı yapısı üzerine çalışmak, çok yararlı olacaktır. Özellikle *E* nin *K* üzerindeki boyutu, çok önemli bir rol oynayacaktır.

Tanım 3.1.20. *E/K* bir cisim genişlemesi olsun. *E* nin *K* üzerindeki boyutuna *E nin K üzerindeki derecesi* veya *E/K genişlemesinin derecesi* denir.

E nin *K* üzerindeki derecesi için $dim_K E$ yerine $|E:K|$ yazmak daha uygun olacaktır. $|E:K|$ nın sonlu veya sonsuz oluşuna göre *E* ye *K nın sonlu boyutlu bir genişlemesi* veya *K nın sonsuz boyutlu bir genişlemesi* denir. "Sonlu boyutlu genişleme" yerine bazen kısaca "sonlu genişleme" terimi kullanılır.

Cisim teorisinde önemli bir gerçek şudur: Sonlu boyutlu bir genişlemenin sonlu boyutlu bir genişlemesi, gene sonlu boyutlu bir genişlemedir ve bu arada dereceler çarpılır. Daha açık olarak:

Teorem 3.1.21. *F/E* ve *E/K* cisim genişlemeleri ve $|F:E|$ ve $|E:K|$ dereceleri sonlu olsun. Bu takdirde *F/K* sonlu boyutlu bir genişleme olup,

$$|F:K| = |F:E|.|E:K|$$

dır; ayrıca $\{f_1, f_2, ..., f_r\}$, F nin bir E-tabanı ve $\{e_1, e_2, ..., e_s\}$, E nin bir K-tabanı ise $\{f_i \cdot e_j \ (i = 1, 2, ..., r; j = 1, 2, ..., s)\}$, F nin bir K-tabanıdır.

İspat. $K \underset{a.c.}{\subset} E$ ve $E \underset{a.c.}{\subset} F$ ise $K \underset{a.c.}{\subset} F$ dir; o halde F, K nın bir genişlemesidir. Şimdi dereceyle ilgili iddiaya gelelim. Kısalık için $|F : E| = r$ ve $|E : K| = s$ diyelim. F nin K üzerindeki boyutunun rs olduğunu göstereceğiz.

$\{f_1, f_2, ..., f_r\}$, F nin bir E-tabanı, $\{e_1, e_2, ..., e_s\}$ de E nin bir K-tabanı olsun. F nin rs elemanlı bir K-tabanını bulmalıyız. Bunun için yapılacak en doğal şey, rs tane $f_i \cdot e_j$ çarpımını gözönüne almaktır. $\{f_i \cdot e_j \ (i = 1, 2, ..., r; j = 1, 2, ..., s)\}$ nin F nin bir K-tabanı olduğunu iddia ediyoruz.

Önce $f_i \cdot e_j$ çarpımlarının K üzerinde F yi doğurduklarını gösterelim. f, F nin keyfi bir elemanı olsun. Bu takdirde uygun $b_1, b_2, ..., b_r \in E$ ile

$$f = b_1 \cdot f_1 + b_2 \cdot f_2 + ... + b_r \cdot f_r$$

yazabiliriz, çünkü $\{f_i \ (i = 1, ..., r)\}$ E üzerinde F yi doğurmaktadır. Öte yandan, her i (i=1,...,r) için, uygun $a_{i1}, a_{i2}, ..., a_{is} \in K$ ile

$$b_i = a_{i1} \cdot e_1 + a_{i2} \cdot e_2 + ... + a_{is} \cdot e_s$$

yazabiliriz, çünkü $\{e_j \ (j = 1, ..., s)\}$ K üzerinde E yi doğurmaktadır. Buradan

$$f = \sum_{i=1}^{r} b_i \cdot f_i = \sum_{i=1}^{r} (\sum_{j=1}^{s} a_{ij} \cdot e_j) f_i = \sum_{i=1}^{r} \sum_{j=1}^{s} a_{ij} (e_j \cdot f_i)$$

elde edilir, yani f, $e_j \cdot f_i = f_i \cdot e_j$ lerin K üzerindeki bir lineer kombinezonudur. Şu halde $\{f_i \cdot e_j\}$, K üzerinde F yi doğurur. Bundan başka, $f_i \cdot e_j$ ler K üzerinde lineer bağımsızdır. Gerçekten, c_{ij} ler K nın elemanları olmak üzere,

$$\sum_{i=1}^{r} \sum_{j=1}^{s} c_{ij} \cdot f_i \cdot e_j = 0_F$$

olsa

$$\sum_{i=1}^{r} (\sum_{j=1}^{s} c_{ij} \cdot e_j) f_i = 0_F \qquad (\sum_{j=1}^{s} c_{ij} \cdot e_j \in E \ (i = 1, ..., r))$$

olur. $\{f_i \ (i = 1, ..., r)\}$ E üzerinde lineer bağımsız olduğundan buradan $\sum_{j=1}^{s} c_{ij} \cdot e_j = 0_E \ (i = 1, ..., r)$ sonucu çıkar. $\{e_j \ (j = 1, ..., s)\}$ K üzerinde lineer bağımsız olduğundan buradan da $c_{ij} = 0_K \ (i = 1, ..., r; \ j = 1, ..., s)$ elde edilir. Şu halde $\{f_i \cdot e_j\}$ K üzerinde lineer bağımsızdır. Sonuç olarak $\{f_i \cdot e_j\}$, F nin bir K-tabanıdır ki, buradan da $|F : K| = rs = |F : E| . |E : K|$ sonucu çıkar.

Teorem 3.1.21 den tümevarımla şu sonuca varabiliriz:
$K_n / K_{n-1}, K_{n-1} / K_{n-2}, ..., \ K_2 / K_1$ sonlu boyutlu cisim genişlemeleri ise

$$|K_n : K_1| = |K_n : K_{n-1}| \cdot |K_{n-1} : K_{n-2}| \cdots |K_2 : K_1|$$

dir. Teorem 3.1.21 ve bu genelleştirilmişi, sonsuz boyutlu genişlemeler için de doğrudur, fakat burada ona ihtiyacımız olmayacaktır.

Lemma 3.1.22. *F/E* ve *E/K* iki cisim genişlemesi olsun. $|F:K|$ sonlu ise $|F:E|$ ve $|E:K|$ da sonludur, hatta her ikisi de $|F:K|$ nın bölenleridir ve $|F:K| = |F:E|.|E:K|$ dır.

İspat. $n=|F:K|$ olsun ve $\{f_i \ (i=1,...,n)\}$ F nin K üzerinde bir tabanı olsun. Bu takdirde $\{f_i \ (i=1,...,n)\}$ E üzerinde F yi doğurur ve dolayısıyla Steinitz'in yer değiştirme teoremine göre $|F:E| \le n$ dir. O halde $|F:E|$ sonludur. Şimdi $|E:K|$ nın sonluluğuna bakalım. E, K üzerinde sonsuz boyutlu olsaydı E nin $n+1$ tane K-lineer bağımsız elemanı bulunurdu, böylece F nin $n+1$ tane K-lineer bağımsız elemanı bulunmuş olurdu ki, bu $|F:K|=n$ oluşu ile çelişirdi. O halde $|E:K|$ sonludur.

Teorem 3.1.21 den $n=|F:K| = |F:E|.|E:K|$ elde edilir. Şu halde $|F:E|$ ve $|E:K|$, n yi böler.

Tanım 3.1.23. *E, K* nın bir genişleme cismi olsun. *F* bir cisim ve $K \subset F \subset E$ ise *F* ye *E/K genişlemesinin bir ara cismi* denir.

Tanım 3.1.24. *E/K* bir cisim genişlemesi ve *S*, *E* nin bir alt kümesi olsun. *E* nin $K \cup S$ yi kapsayan bütün alt cisimlerinin kesişimine (ki bu kesişim, Örnek 3.1.9 a göre *E* nin bir alt cismidir) *E nin K üzerinde S tarafından doğurulan alt cismi* denir ve bu cisim *K*(*S*) ile gösterilir.

Bu tanımdan hemen $K \subset K(S) \subset E$ olduğu, yani *K*(*S*) nin *E/K* nın bir ara cismi olduğu sonucu çıkacaktır. *S*, *E* nin sonlu bir alt kümesi ise, yani $S=\{a_1,a_2,...,a_n\}$ ise $K(\{a_1,a_2,...,a_n\})$ yerine $K(a_1,a_2,...,a_n)$ yazılır. Özellikle $a \in E$ ise *K*(*a*), tanım gereği, *E* nin hem *K* yı, hem de *a* yı kapsayan en küçük alt cismidir. S_n deki herhangi bir $\begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}$ permütasyonu için $K(a_1,a_2,...,a_n) = K(a_{i_1},a_{i_2},...,a_{i_n})$ dir.

Tanım 3.1.25. *E/K* bir cisim genişlemesi ve *S*, *E* nin bir alt kümesi olsun. *E* nin $K \cup S$ yi kapsayan bütün alt halkalarının kesişimine (ki bu kesişim, *E* nin bir alt halkasıdır) *E nin K üzerinde S tarafından doğurulan alt halkası* denir ve bu halka, *K*[*S*] ile gösterilir.

E nin $K \cup S$ yi kapsayan her alt cismi, aynı zamanda *E* nin $K \cup S$ yi kapsayan bir alt halkası olduğundan, $K \subset K[S] \subset K(S) \subset E$ dir. *S*, *E* nin sonlu bir alt kümesi, yani $S=\{a_1,a_2,...,a_n\}$ ise $K[\{a_1,a_2,...,a_n\}]$ yerine $K[a_1,a_2,...,a_n]$ yazılır. Özellikle $a \in E$ ise *K*[*a*], tanım gereği, *E* nin hem *K* yı, hem de *a* yı

kapsayan en küçük alt halkasıdır. S_n deki herhangi bir $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ permütasyonu için $K[a_1, a_2, ..., a_n] = K[a_{i_1}, a_{i_2}, ..., a_{i_n}]$ dir.

Örnek 3.1.26. $\mathbb{C}/\mathbb{R}$ genişlemesinde, $\mathbb{C}$ nin $\mathbb{R}$ üzerinde *i* tarafından doğurulan alt cismini bulalım. $\mathbb{C}$ nin hem $\mathbb{R}$ yu, hem de *i* yi kapsayan her alt cismi, $\frac{a+bi}{c+di}$ $(a,b,c,d \in \mathbb{R},\ c+di \neq 0_{\mathbb{R}})$ biçimindeki her kompleks sayıyı içerir. Şimdi $F = \left\{ \frac{a+bi}{c+di} \in \mathbb{C} : a,b,c,d \in \mathbb{R},\ c+di \neq 0_{\mathbb{R}} \right\}$ kümesini gözönüne alalım.

Her $x, y \in F$ için $x = \frac{a+bi}{c+di}$ ve $y = \frac{e+fi}{g+hi}$ $(a,b,c,d,e,f,g,h \in \mathbb{R})$ olup,

(i) $x + y = \frac{(ag+ce-bh-df)+(ah+bg+cf+de)i}{(cg-dh)+(ch+dg)i} \in F$,

(ii) $-y = \frac{(-e)+(-f)i}{g+hi} \in F$,

(iii) $x \cdot y = \frac{(ae-bf)+(af+be)i}{(cg-dh)+(ch+dg)i} \in F$,

(iv) $y^{-1} = \frac{g+hi}{e+fi} \in F$ $(e+fi \neq 0_{\mathbb{R}}$ olmak koşuluyla)

dir. O halde *F*, $\mathbb{C}$ nin $\mathbb{R}$ ve *i* yi kapsayan bir alt cismidir, dolayısıyla *F*, $\mathbb{C}$ nin $\mathbb{R}$ üzerinde *i* tarafından doğurulan alt cismidir.

F nin her elemanı $x + yi$ $(x, y \in \mathbb{R})$ biçiminde yazılabileceğinden $\left\{ x + yi \in \mathbb{C} \mid x, y \in \mathbb{R} \right\} = F$ dir ve *F*, Örnek 3.1.6 da tanımlanan $\mathbb{R}(i)$ cismine eşittir. Şu halde Örnek 3.1.6 daki $x + yi$ gösterimi, Tanım 3.1.24 deki ile tutarlıdır.

Yukarıki örnek, bir alt cisim üzerinde bir alt küme tarafından doğurulan cismin elemanlarının nasıl belirleneceğini göstermesi bakımından önemlidir.

Lemma 3.1.27. *E/K* bir cisim genişlemesi ve $a_1, a_2, ..., a_n \in E$ olsun. Bu durumda

(1) $K[a_1, a_2, ..., a_n] = \left\{ f(a_1, a_2, ..., a_n) \in E : f \in K[x_1, x_2, ..., x_n] \right\}$,

(2) $K(a_1, a_2, ..., a_n) =$

$$\left\{ \frac{f(a_1, a_2, ..., a_n)}{g(a_1, a_2, ..., a_n)} \in E : f, g \in K[x_1, x_2, ..., x_n],\ g(a_1, a_2, ..., a_n) \neq 0_E \right\}$$

dir.

İspat. (1) Eşitliğin sağ tarafındaki kümeye A diyelim. E nin K yı ve $\{a_1, a_2, ..., a_n\}$ kümesini kapsayan her alt halkası, $ka_1^{m_1}a_2^{m_2}...a_n^{m_n}$ $\left(k \in K, m_i \in \mathbb{Z}^+ \cup \{0\}\ (i = 1,2,...,n)\right)$ biçimindeki elemanları, dolayısıyla aynı zamanda

$$\sum k_{m_1 m_2 ... m_n} a_1^{m_1} a_2^{m_2} ... a_n^{m_n} \left(k_{m_1 m_2 ... m_n} \in K, m_i \in \mathbb{Z}^+ \cup \{0\}\ (i = 1,2,...,n)\right) \quad (3.3)$$

biçimindeki elemanları içerecektir. Fakat (3.3) toplamı,

$$f(x_1, x_2, ..., x_n) = \sum k_{m_1 m_2 ... m_n} x_1^{m_1} x_2^{m_2} ... x_n^{m_n} \in K[x_1, x_2, ..., x_n]$$

polinomunun $x_1 = a_1,\ x_2 = a_2, ...,\ x_n = a_n$ için değerinden başka birşey değildir. Dolayısıyla A nın her elemanı, E nin K yı ve $\{a_1, a_2, ..., a_n\}$ kümesini kapsayan her alt halkasına aittir. O halde

$$A \subset K[a_1, a_2, ..., a_n]$$

dir. Bu kapsama bağıntısının tersini ispatlamak için, A nın E nin bir alt halkası olduğunu göstermek yeterlidir, çünkü $K \cup \{a_1, a_2, ..., a_n\} \subset A \subset E$ dir. Herhangi bir $f(a_1, a_2, ..., a_n),\ g(a_1, a_2, ..., a_n) \in A \quad (f, g \in K[x_1, x_2, ..., x_n])$ çifti verildiğine göre,

$$f(a_1, a_2, ..., a_n) + g(a_1, a_2, ..., a_n) = (f + g)(a_1, a_2, ..., a_n) \in A\ ,$$

$$-g(a_1, a_2, ..., a_n) = (-g)(a_1, a_2, ..., a_n) \in A\ ,$$

$$f(a_1, a_2, ..., a_n) \cdot g(a_1, a_2, ..., a_n) = (f \cdot g)(a_1, a_2, ..., a_n) \in A$$

dır. Çünkü $f, g \in K[x_1, x_2, ..., x_n]$ olduğundan $f + g,\ -g,\ f \cdot g \in K[x_1, x_2, ..., x_n]$ dir. Şu halde Teorem 2.17 ye göre A, E nin bir alt halkasıdır. Böylece $K[a_1, a_2, ..., a_n] = A$ olduğu ispatlanmış olur.

(2) Burada da düşünce şekli, (1) dekine benzerdir. (2) eşitliğinin sağ tarafındaki kümeye B diyelim. $A \subset B$ olduğu açıktır.

$B = \left\{\frac{b}{c} \in E : b, c \in A,\ c \neq 0_E\right\} = \left\{b \cdot c^{-1} \in E : b, c \in A,\ c \neq 0_E\right\}$ olduğuna dikkat edelim.

E nin K yı ve $\{a_1, a_2, ..., a_n\}$ kümesini kapsayan her alt cismi $K[a_1, a_2, ..., a_n] = A$ yı da kapsayacaktır ve bir alt cisim, bölmeye göre kapalı olduğundan, aynı zamanda $\frac{b}{c}$ $(b, c \in A,\ c \neq 0_E)$ elemanlarını da kapsayacaktır. Bu, B nin, E nin K yı ve $\{a_1, a_2, ..., a_n\}$ kümesini kapsayan her alt cismin içinde olduğu anlamına gelir. O halde

$$B \subset K\left(a_1, a_2, ..., a_n\right)$$

dir. Bu kapsama bağıntısının tersini ispatlamak için B nin E nin bir alt cismi olduğunu göstermek yeterlidir, çünkü $K \cup \{a_1, a_2, ..., a_n\} \subset B \subset E$ dir. Herhangi bir $\frac{b}{c}, \frac{d}{e}$ $(b, c, d, e \in A;\ c, e \neq 0_E)$ çifti verildiğine göre,

$$\frac{b}{c} + \frac{d}{e} = \frac{b \cdot e + d \cdot c}{c \cdot e} \in B\ ,$$

$$-\frac{d}{e} \in B\ ,$$

$$\frac{b}{c}\cdot\frac{d}{e}=\frac{b\cdot d}{c\cdot e}\in B\ ,$$

$$\frac{1_E}{\frac{d}{e}}=\frac{e}{d}\in B\ \ (d/e\neq 0_E, yani\ d\neq 0_E \text{ olmak koşuluyla})$$

dir, çünkü b,c,d,e A nın elemanları olduğundan $b\cdot e+d\cdot c$, $c\cdot e$, $-d$, $b\cdot d$ ve $c\cdot e$ de A nın elemanlarıdır ve $c\neq 0_E$, $e\neq 0_E$ olduğundan $c\cdot e\neq 0_E$ dir (A, E nin bir alt halkası olduğundan sıfır-bölensizdir). Dolayısıyla Lemma 3.1.2 e göre B, E nin bir alt cismidir. Böylece $K(a_1,a_2,...,a_n)=B$ olduğu ispatlanmış olur.

Şimdi Lemma 3.1.27 nin ışığı altında Örnek 3.1.26 yı yeniden ele alalım. Örnek 3.1.26 daki F cismi tam olarak, $K=\mathbb{Q}$, $n=1$, $a_1=i\in\mathbb{C}$ olmak üzere, Lemma 3.1.27 de tanımlanan cisimdir. Diğer taraftan $\{x+yi\in\mathbb{C}: x,y\in\mathbb{Q}\}$ cismi tam olarak $\mathbb{C}$ nin, $K=\mathbb{Q}$, $n=1$, $a_1=i\in\mathbb{C}$ olmak üzere, Lemma 3.1.27 de tanımlanan alt halkasıdır. Dolayısıyla $\mathbb{Q}(i)=\mathbb{Q}[i]$ dir.

Lemma 3.1.28. *E/K* bir cisim genişlemesi ve $a,b,a_1,a_2,...,a_n\in E$ olsun.

(1) $K(a)=K$ olması için gerek ve yeter koşul, $a\in K$ olmasıdır,

(2) $K(a_1,a_2,...,a_{n-1},a_n)=\big(K(a_1,a_2,...,a_{n-1})\big)(a_n)$ ve

$K[a_1,a_2,...,a_{n-1},a_n]=\big[K[a_1,a_2,...,a_{n-1}]\big][a_n]$ dir,

(3) $K(a,b)=\big(K(a)\big)(b)=\big(K(b)\big)(a)$ ve $K[a,b]=\big[K[a]\big][b]=\big[K[b]\big][a]$

dır.

İspat. (1) *Gereklik.* $K(a)=K$ ise $a\in K$ dır: $K(a)$ nın tanımı gereğince $a\in K(a)$ dır. $K(a)=K$ olduğundan buradan $a\in K$ elde edilir.

Yeterlik. $a\in K$ ise $K(a)=K$ dır: $a\in K$ olduğundan $K=K\cup\{a\}$ dır. K, E nin hem K yı, hem de a yı kapsayan bütün alt cisimlerinin kesişimi olduğundan, buradan $K(a)=K$ sonucu çıkar.

(2) $L=K(a_1,a_2,...,a_{n-1})$ diyelim. L, K yı ve $a_1,a_2,...,a_{n-1}$ i kapsamaktadır. $L(a_n)$, E nin hem L yi, hem de a_n yi kapsayan bir alt cismidir, o halde $L(a_n)$, E nin, K yı, $a_1,a_2,...,a_{n-1}$ i ve a_n yi kapsayan bir alt cismidir. Bu durumda E nin K yı ve $a_1,a_2,...,a_{n-1},a_n$ yi kapsayan bütün alt cisimlerinin kesişimi olan $K(a_1,a_2,...,a_{n-1},a_n)$, $L(a_n)$ nin bir alt cismidir. O halde

$$K(a_1,a_2,...,a_{n-1},a_n)\subset L(a_n) \tag{3.4}$$

dir. Diğer taraftan $K(a_1,a_2,...,a_{n-1},a_n)$, E nin K yı, $a_1,a_2,...,a_{n-1}$ i ve aynı zamanda a_n yi kapsayan bir alt cismidir. O halde $L=K(a_1,a_2,...,a_{n-1})$ in tanımından $L\subset K(a_1,a_2,...,a_{n-1},a_n)$ elde edilir ve $a_n\in K(a_1,a_2,...,a_{n-1},a_n)$ dir. Şu halde

$K(a_1, a_2, ..., a_{n-1}, a_n)$, E nin hem L yi, hem de a_n yi kapsayan bir alt cismidir. $L(a_n)$ nin tanımı gereğince buradan

$$L(a_n) \subset K(a_1, a_2, ..., a_{n-1}, a_n) \tag{3.5}$$

elde edilir. (3.4) ve (3.5) ten $K(a_1, a_2, ..., a_{n-1}, a_n) = L(a_n)$ sonucu çıkar.

Diğer eşitlik de benzer yolla, alt cisim yerine alt halka kullanılarak ispatlanır.

(3) (2) yi iki kez kullanarak $\big(K(a)\big)(b) = K\big(a,b\big) = K\big(b,a\big) = \big(K(b)\big)(a)$ ve benzer şekilde $\big[K[a]\big][b] = K[a,b] = K[b,a] = \big[K[b]\big][a]$ elde edilir.

Şimdi cisim genişlemelerinin çok önemli bir sınıflandırmasını oluşturan cebirsel ve transandant genişlemeleri tanımlayacağız.

Tanım 3.1.29. *E/K* bir cisim genişlemesi olsun. *E* nin bir *a* elemanı verildiğine göre, *a* yı kök kabul eden, yani $f(a) = 0_E$ koşuluna uyan, sıfırdan farklı bir $f \in K[x]$ varsa, *a* elemanına *K üzerinde cebirsel* denir. *a* cebirsel değilse, yani $f(a) = 0_E$ olacak şekilde, sıfırdan farklı hiçbir $f \in K[x]$ yoksa *E* nin bu *a* elemanına *K üzerinde transandant* denir.

E nin bütün elemanları *K* üzerinde cebirsel ise *E* ye *K nın bir cebirsel genişlemesi, E/K* ya da bir *cebirsel genişleme* denir. Bu durumda *E, K üzerinde cebirseldir* denir. *E*, *K* nın bir cebirsel genişlemesi değilse, *E* ye *K nın bir transandant genişlemesi*, *E/K* ya da bir *transandant genişleme* denir. Eğer durum böyle ise, yani *E*, *K* üzerinde cebirsel olmayan en az bir eleman içeriyorsa, *E, K üzerinde transandanttır* denir.

Örnek 3.1.30. *K* herhangi bir cisim olsun. *K* nın her *a* elemanı için $f_a(x) := x - a \in K[x]$ tir ve *a*, f_a nın bir köküdür. O halde *K* nın her elemanı *K* üzerinde cebirseldir ve dolayısıyla *K*, *K* nın bir cebirsel genişlemesidir.

Örnek 3.1.31. $i \in \mathbb{C}$, $x^2 + 1 \in \mathbb{R}[x]$ polinomunun bir köküdür. O halde *i*, $\mathbb{R}$ üzerinde cebirseldir. Ayrıca $\mathbb{R}(i)$ nin her $a + bi$ $(a, b \in \mathbb{R})$ elemanı,

$$[x - (a + bi)][x - (a - bi)] = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$$

polinomunun bir köküdür ve dolayısıyla $\mathbb{R}$ üzerinde cebirseldir. O halde $\mathbb{R}(i)/\mathbb{R}$ bir cebirsel genişlemedir.

Örnek 3.1.32. $\sqrt{2} \in \mathbb{R}$, $x^2 - 2 \in \mathbb{Q}[x]$ polinomunun bir köküdür. O halde $\sqrt{2}$, $\mathbb{Q}$ üzerinde cebirseldir. Ayrıca $\mathbb{Q}(\sqrt{2})$ nin her $a + b\sqrt{2}$ $(a, b \in \mathbb{Q})$ elemanı,

$$[x - (a + b\sqrt{2})][x - (a - b\sqrt{2})] = x^2 - 2ax + (a^2 - 2b^2) \in \mathbb{Q}[x]$$

polinomunun bir köküdür ve dolayısıyla $\mathbb{Q}$ üzerinde cebirseldir. O halde $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ bir cebirsel genişlemedir.

Örnek 3.1.33. Sayılar teorisinden bilindiği üzere, π ve e reel sayıları $\mathbb{Q}$ üzerinde transandanttır. O halde $\mathbb{Q}(\pi)/\mathbb{Q}$ bir transandant genişlemedir, $\mathbb{Q}(\pi)$ ve $\mathbb{Q}(e)$ de $\mathbb{Q}$ nun transandant genişlemeleridir.

Örnek 3.1.34. K bir cisim ve x, K üzerinde bir değişken olmak üzere, $K(x)$, K nın bir genişleme cismidir ve $x \in K(x)$ tir. f, $K[x]$ te sıfırdan farklı herhangi bir polinom ise $f(x) = f \neq 0_K$ dır. O halde x, K üzerinde transandanttır ve $K(x)/K$ bir transandant genişlemedir. Benzer şekilde, $K[x]$ te sıfırdan farklı her f polinomu için $f(x^2) \neq 0_K$ olduğundan x^2, K üzerinde transandanttır. Diğer taraftan y, K üzerinde başka bir değişken ise, x, $y^2 - x^2 \in \left(K(x^2)\right)[y]$ polinomunun bir köküdür, dolayısıyla x, $K(x^2)$ üzerinde cebirseldir. O halde bir eleman, bir cisim üzerinde transandant, başka bir cisim üzerinde cebirsel olabilir.

Tanım 3.1.35. *E/K* bir cisim genişlemesi olsun. *E* de *E=K*(*a*) olacak şekilde bir *a* elemanı varsa *E* ye *K nın bir basit genişlemesi* denir. Bu durumda *E* nin *E=K*(*a*) eşitliğini sağlayan herhangi bir *a* elemanına *E/K genişlemesinin bir primitif elemanı* denir. *E* de $E = K(a_1, a_2, ..., a_n)$ olacak şekilde sonlu sayıda $a_1, a_2, ..., a_n$ elemanı varsa *E* ye *K üzerinde sonlu doğuraylı bir cisim* denir.

Not 3.1.36. Sonlu boyutlu genişlemeler ile sonlu doğuraylı genişlemeler, birbiriyle karıştırılmamalıdır.

Teorem 3.1.37. *E/K* bir cisim genişlemesi ve $a \in E$, K üzerinde transandant olsun. Bu durumda x, K üzerinde bir değişken olmak üzere, $K(a) \cong K(x)$ tir.

İspat. $K(x)$ ten $K(a)$ üzerine bir izomorfi bulmalıyız. Bunun için

$$\varphi : K(x) \to K(a)$$
$$\frac{f}{g} \to \frac{f(a)}{g(a)}$$

tasvirini ele alalım. Bu tasvir, iyi tanımlanmış bir tasvirdir. Gerçekten, verilen herhangi bir $\frac{f}{g} \in K(x)$ $(f, g \in K[x],\ g \neq 0_K)$ için $g(a) \neq 0_K$ dır (çünkü a, K üzerinde transandanttır) ve dolayısıyla $\varphi\left(\frac{f}{g}\right) = \frac{f(a)}{g(a)}$, $K(a)$ nın tamamen belirli bir elemanıdır. Öte yandan $K(x)$ te $f/g = f_1/g_1$ $(f, g, f_1, g_1 \in K[x], g \neq 0_K, g_1 \neq 0_K)$ ise $K[x]$ te $f \cdot g_1 = f_1 \cdot g$ dir ki, buradan Lemma 2.74 e göre E de $f(a) \cdot g_1(a) = f_1(a) \cdot g(a)$ $(g_1(a) \neq 0_K,\ g(a) \neq 0_K)$ eşitliği elde edilir. Bu eşitliğin her iki tarafı $1_K / g_1(a) \cdot g(a)$ ile çarpılarak

$$\varphi\left(\frac{f}{g}\right) = \frac{f(a)}{g(a)} = \frac{f_1(a)}{g_1(a)} = \varphi\left(\frac{f_1}{g_1}\right)$$

bulunur. Bu ise φ nin iyi tanımlı olduğunu gösterir.

φ bir halka homomorfisidir, çünkü Lemma 2.74 e göre her $\frac{f}{g},\frac{h}{k}\in K(x)$ $(f,g,h,k\in K[x],\ g\neq 0_K, k\neq 0_K)$ için

$$\varphi\left(\frac{f}{g}+\frac{h}{k}\right)=\varphi\left(\frac{f\cdot k+h\cdot g}{g\cdot k}\right)=\frac{(f\cdot k+h\cdot g)(a)}{(g\cdot k)(a)}=\frac{f(a)\cdot k(a)+h(a)\cdot g(a)}{g(a)\cdot k(a)}$$
$$=\frac{f(a)}{g(a)}+\frac{h(a)}{k(a)}=\varphi\left(\frac{f}{g}\right)+\varphi\left(\frac{h}{k}\right)$$

ve

$$\varphi\left(\frac{f}{g}\cdot\frac{h}{k}\right)=\varphi\left(\frac{f\cdot h}{g\cdot k}\right)=\frac{(f\cdot h)(a)}{(g\cdot k)(a)}=\frac{f(a)\cdot h(a)}{g(a)\cdot k(a)}$$
$$=\frac{f(a)}{g(a)}\cdot\frac{h(a)}{k(a)}=\varphi\left(\frac{f}{g}\right)\cdot\varphi\left(\frac{h}{k}\right)\qquad (g(a)\neq 0_K,\ k(a)\neq 0_K)$$

dır.

$$\begin{aligned}K\,\text{er}\,\varphi&=\{f/g\in K(x):f,g\in K[x],\ g\neq 0_K,\ f(a)/g(a)=0_K\}\\&=\{f/g\in K(x):f,g\in K[x],\ g\neq 0_K,\ f(a)=0_K\}\\&=\{f/g\in K(x):f,g\in K[x],\ g\neq 0_K, f=0_K\}\\&=\{0_K\}\end{aligned}$$

olduğundan φ (1-1) dir. O halde φ bir cisim homomorfisidir. Lemma 3.1.27(2) ye göre $\varphi:K(x)\to K(a)$ üzerinedir, dolayısıyla φ bir cisim izomorfisidir, yani $K(a)\cong K(x)$ tir.

§ 2. Cebirsel Genişlemeler

E/K bir cisim genişlemesi ve $a \in E$, *K* üzerinde cebirsel olsun. Bu takdirde *K*[*x*] te $f(a) = 0_K$ olacak şekilde, sıfırdan farklı bir f polinomu vardır. Şu halde $A = \{f \in K[x] : f(a) = 0_K\} \subset K[x]$ kümesi, sadece sıfırdan oluşmamaktadır. *A*, *K*[*x*] in bir idealidir, çünkü *A*, $T_a : K[x] \to E$ sübstitüsyon homomorfisinin çekirdeğidir.

O halde *A*, *K*[*x*] in bir idealidir ve $A \neq \{0_K\}$ dır. *K*[*x*] bir esas ideal halkası olduğundan, sıfırdan farklı uygun bir $f_0 \in K[x]$ polinomu için $A = K[x]f_0 = (f_0)$ dır. Herhangi bir $g \in K[x]$ polinomu için $(g) = A = (f_0)$ bağıntısının gerçeklenmesi için gerek ve yeter koşul, f_0 ve *g* nin *K*[*x*] te aralarında ilgili olmaları, yani uygun bir $c \in K^*$ için $g(x) = cf_0(x)$ olmasıdır. $c_0 f_0(x)$ in baş katsayısı 1 e eşit olacak şekilde bir tek $c_0 \in K^*$ vardır. Bu c_0 ile, $g_0(x) = c_0 f_0(x)$ diyelim. O halde g_0, *K*[*x*] te $(g_0) = A = \{f \in K[x] : f(a) = 0_K\}$ olacak şekilde tek monik polinomdur ve bir $f \in K[x]$ için $f(a) = 0_K$ olması için gerek ve yeter koşul, *K*[*x*] te $g_0 \mid f$ olmasıdır. Özellikle, *a* yı kök olarak kabul eden herhangi bir $f \in K[x]$ için $deg\, g_0 \leq deg\, f$ tir.

Bu şekilde, $a \in E$ yi *K*[*x*] te tek türlü belirli bir g_0 monik polinomu ile ilişkilendirmiş oluruz. Bu g_0, *K*[*x*] te *a* yı kök olarak kabul eden en küçük dereceli monik polinomdur.

g_0, *K* üzerinde asaldır. Çünkü $g_0(x) = p(x) \cdot q(x)$, $1 \leq deg\, p(x) < deg\, g_0(x)$ ve $1 \leq deg\, q(x) < deg\, g_0(x)$ olacak şekilde $p(x), q(x) \in K[x]$ polinomları bulunsa, $0_K = g_0(a) = p(a) \cdot q(a)$ eşitliğinden $p(x) \in A$ ve $q(x) \in A$ dan en az birinin doğru olduğu ve dolayısıyla *K*[*x*] te $g_0 \mid p$ ve $g_0 \mid q$ dan en az birinin doğru olduğu sonucu çıkar ki, bu $deg\, p(x) < deg\, g_0(x)$ ve $deg\, q(x) < deg\, g_0(x)$ oluşu ile çelişir.

Böylece aşağıdaki teoremi ispat etmiş olduk:

Teorem 3.2.1. *E/K* bir cisim genişlemesi ve $a \in E$ olsun. *a*, *K* üzerinde cebirsel ise, *K*[*x*] te sıfırdan farklı bir tek *g*(*x*) polinomu vardır, öyle ki, her $f(x) \in K[x]$ için, $f(x) = 0_K$ olması için gerek ve yeter koşul, *K*[*x*] te $g(x) \mid f(x)$ olmasıdır. Özellikle *a*, *g*(*x*) in bir köküdür ve *g*(*x*), *K*[*x*] teki polinomlar arasında *a* yı kök olarak kabul eden en küçük dereceli polinomdur. Üstelik *g*(*x*), *K* üzerinde asaldır.

Tanım 3.2.2. *E/K* bir cisim genişlemesi ve $a \in E$, *K* üzerinde cebirsel olsun. Teorem 3.2.1 deki, tek türlü belirli olan *g*(*x*) polinomuna *a nın K üzerindeki minimal polinomu* denir. *a* nın *K* üzerindeki minimal polinomuna aynı zamanda *a nın K üzerindeki asal polinomu* da denir. *E* nin *K* üzerinde cebirsel olan bir *a* elemanı ve bir $h(x) \in K[x]$ polinomu verildiğine göre, *h*(*x*) in *a* nın *K* üzerindeki minimal polinomu olup olmadığını anlamak için, *a* yı kök olarak kabul eden bütün

$f(x) \in K[x]$ polinomları için $h(x) \mid f(x)$ olup olmadığını kontrol etmemiz gerekir gibi görünüyor. Fakat neyse ki, aşağıdaki teoremde göreceğimiz gibi, minimal polinomların başka bir karakterizasyonu vardır.

Teorem 3.2.3. *E/K* bir cisim genişlemesi ve $a \in E$ olsun. *a* nın *K* üzerinde cebirsel olduğunu varsayalım. *h*(*x*), *K*[*x*] te sıfırdan farklı bir polinom olsun.

(i) *h*(*x*) monik,
(ii) *a*, *h*(*x*) in bir kökü,
(iii) *h*(*x*), *K* üzerinde asal

ise *h*(*x*), *a* nın *K* üzerindeki minimal polinomudur.

İspat. İddiayı ispat etmek için, *h*(*x*) in *a* yı kök olarak kabul eden herhangi bir $f(x) \in K[x]$ polinomunu böldüğünü göstermemiz gerekir. *f*(*x*), *K*[*x*] e ait bir polinom olsun ve *a* nın *f*(*x*) in bir kökü olduğunu varsayalım. *f*(*x*) i *h*(*x*) ile bölersek,uygun $q(x)$, $r(x) \in K[x]$ ile

$$f(x) = q(x) \cdot h(x) + r(x) \qquad r(x) = 0_K \text{ veya } deg\, r(x) < deg\, h(x)$$

elde ederiz. Bu eşitlikte *x* yerine *a* koyarsak

$$0_K = f(a) = q(a) \cdot h(a) + r(a) = q(a) \cdot 0_K + r(a) = r(a) \Rightarrow r(a) = 0_K$$

olur. *r*(*x*), *K*[*x*] te sıfır polinomundan farklı olsaydı, *h*(*x*) asal polinomunun, derecesi onunkinden daha küçük olan *r*(*x*) polinomu ile ortak *a* kökü bulunmuş olurdu ki, Teorem 2.92(4) e göre bu mümkün değildir. O halde $r(x) = 0_K$ ve dolayısıyla $f(x) = q(x) \cdot h(x)$ tir. Böylece *a* yı kök kabul eden her $f(x) \in K[x]$ için $h(x) \mid f(x)$ olduğu ispatlanmış olur.

Örnek 3.2.4. $i \in \mathbb{C}$ nin $\mathbb{R}$ üzerindeki minimal polinomunu bulalım. *i*, monik ve $\mathbb{R}$ üzerinde asal olan $x^2 + 1 \in \mathbb{R}[x]$ polinomunun bir köküdür, o halde Teorem 3.2.3 e göre $x^2 + 1$, *i* nin $\mathbb{R}$ üzerindeki minimal polinomudur. Aynı şekilde, $x^2 + 1 \in \mathbb{Q}[x]$, *i* nin $\mathbb{Q}$ üzerindeki minimal polinomudur. Diğer taraftan $x^2 + 1 \in (\mathbb{R}(i))[x]$, $\mathbb{R}(i)$ üzerinde asal değildir, çünkü $(\mathbb{R}(i))[x]$ te $x^2 + 1 = (x - i)(x + i)$ dir. $i, x - i$ nin bir kökü olup, $x - i$, $(\mathbb{R}(i))[x]$ te bir monik asal polinomdur, dolayısıyla $x - i$, $i \in \mathbb{C}$ nin $\mathbb{R}(i)$ üzerindeki minimal polinomudur.

Örnek 3.2.5. $u = \sqrt{2} + \sqrt{3} \in \mathbb{C}$ nin $\mathbb{Q}$ üzerindeki minimal polinomunu bulalım.

$$\begin{aligned} u &= \sqrt{2} + \sqrt{3} \\ u - \sqrt{2} &= \sqrt{3} \\ u^2 - 2\sqrt{2}u + 2 &= 3 \\ u^2 - 1 &= 2\sqrt{2}u \\ u^4 - 2u^2 + 1 &= 8u^2 \\ u^4 - 10u^2 + 1 &= 0 \end{aligned} \tag{3.6}$$

olduğundan $\sqrt{2}+\sqrt{3}$, $f(x)=x^4-10x^2+1\in\mathbb{Q}[x]$ monik polinomunun bir köküdür. Şimdi $f(x)$ in $\mathbb{Q}$ üzerinde asal olduğunu gösterelim. Sonuçta Teorem 3.2.3 e göre $f(x)$, $\sqrt{2}+\sqrt{3}$ ün $\mathbb{Q}$ üzerindeki minimal polinomu olacaktır.

Lemma 2.87 ye göre, $f(x)$ in $\mathbb{Q}$ üzerinde asal olduğunu göstermek yeter. $\pm1/\pm1=\pm1$ sayıları $f(x)$ in kökleri olmadığından $f(x)$ in $\mathbb{Q}[x]$ te birinci dereceden polinom çarpanı yoktur. $f(x)$, $\mathbb{Q}[x]$ te

$$x^4-10x^2+1=(x^2+ax+b)(x^2+cx+d) \tag{3.7}$$

şeklinde, ikinci dereceden iki polinomun çarpımı biçiminde yazılabilseydi

$$(x^2+ax+b)(x^2+cx+d)=x^4+(a+c)x^3+(d+ac+b)x^2+(ad+bc)x+bd$$
$$=x^4-10x^2+1$$

olurdu ve buradan

$$a+c=0\quad,\quad d+ac+b=-10\quad,\quad ad+bc=0\quad,\quad bd=1$$

elde edilirdi. Son denklemden $b=d=\pm1$ bulunur ve ilk iki denklemden

$$a+c=0\ ,\ ac=-12\qquad\text{veya}\qquad a+c=0\ ,\ ac=-8,$$

yani

$$a^2=12\qquad\text{veya}\qquad a^2=8$$

sonucu çıkardı, oysa karesi 12 veya 8 e eşit olan hiçbir a tam sayısı yoktur. O halde $f(x)$, $\mathbb{Q}[x]$ te asaldır ve dolayısıyla $\sqrt{2}+\sqrt{3}$ ün $\mathbb{Q}$ üzerindeki minimal polinomudur.

Dördüncü dereceden $f(x)$ polinomunun $\mathbb{Q}$ üzerinde asal olduğu, derecesi dörtten daha küçük olan başka bir polinomun, $\mathbb{Q}$ dan daha geniş bir cisim üzerinde asal olduğu gösterilerek ispatlanabilirdi. Şimdi probleme daha derin bir bakış açısı getiren bu yöntemi vereceğiz.

(3.6) eşitliği, $\sqrt{2}+\sqrt{3}$ ün $f_2(x):=x^2-2\sqrt{2}x-1\in(\mathbb{Q}(\sqrt{2}))[x]$ polinomunun bir kökü olduğunu gösterir. $\sqrt{2}+\sqrt{3}$ ün $\mathbb{Q}(\sqrt{2})$ üzerindeki minimal polinomu $g(x)\in(\mathbb{Q}(\sqrt{2}))[x]$ olsun. Bu takdirde $(\mathbb{Q}(\sqrt{2}))[x]$ te $g(x)\,|\,f_2(x)$ tir. Burada $g(x)\neq f_2(x)$ olsa $deg\,g(x)=1$ ve $g(x)=x-(\sqrt{2}+\sqrt{3})$ olurdu, çünkü $x-(\sqrt{2}+\sqrt{3})$ polinomu, $\sqrt{2}+\sqrt{3}$ ü kök kabul eden, birinci dereceden tek monik polinomdur. Fakat $g(x)\in(\mathbb{Q}(\sqrt{2}))[x]$ tir; buradan $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2})$ ve dolayısıyla $\sqrt{3}\in\mathbb{Q}(\sqrt{2})$ sonucu çıkar. O halde uygun $m,n\in\mathbb{Q}$ $(m\neq0,\ n\neq0)$ ile $\sqrt{3}=m+n\sqrt{2}$ olur ve buradan

$$3=m^2+2\sqrt{2}mn+2n^2\Rightarrow\sqrt{2}=\frac{3-m^2-2n^2}{2mn}\in\mathbb{Q}$$

elde edilir ki, bu bir çelişkidir, çünkü $\sqrt{2}\notin\mathbb{Q}$ dur. O halde $f_2(x)=g(x)$ tir ve $f_2(x)$, $\sqrt{2}+\sqrt{3}$ ün $\mathbb{Q}(\sqrt{2})$ üzerindeki minimal polinomudur.

Şimdi $f(x)$ in $\mathbb{Q}$ üzerinde asal olduğu kolayca gösterilebilir. $f(x)$ in $\mathbb{Q}$ [x] te birinci dereceden çarpanı yoktur. $f(x)$, $\mathbb{Q}$ [x] te a,b,c,d rasyonel sayılar (tam sayı

olmaları gerekmez) olmak üzere, (3.7) deki gibi çarpanlara ayrılabilseydi, $\sqrt{2}+\sqrt{3}$, (3.7) deki çarpanlardan birinin, örneğin x^2+ax+b nin bir kökü olurdu. Dolayısıyla $(\square(\sqrt{2}))[x]$ te $\sqrt{2}+\sqrt{3}$ ü kök kabul eden x^2+ax+b polinomu, $(\square(\sqrt{2}))[x]$ te $\sqrt{2}+\sqrt{3}$ ün $\square(\sqrt{2})$ üzerindeki minimal polinomu olan $f_2(x)=x^2-2\sqrt{2}x-1$ ile bölünebilirdi. Buradan dereceler ve baş katsayılar karşılaştırılarak $x^2-2\sqrt{2}x-1=x^2+ax+b$ ve dolayısıyla $a=-2\sqrt{2}$ elde edilirdi ki, bu *a* nın rasyonel oluşuyla çelişir. O halde *f*(*x*), $\square$ üzerinde asaldır.

Aşağıdaki lemma, son örnekte kullandığımız düşünce tarzını belirginleştirir:

Lemma 3.2.6. $K_1\subset K_2\subset E$ üç cisim ve $a\in E$ olsun. *a*, K_1 üzerinde cebirsel ise K_2 üzerinde de cebirseldir. Üstelik f_1 ve f_2, *a* nın sırasıyla K_1 ve K_2 üzerindeki minimal polinomları ise $K_2[x]$ te $f_2\,|\,f_1$ dir.

İspat. *a*, K_1 üzerinde cebirsel ve $f_1(x)$, *a* nın K_1 üzerindeki minimal polinomu ise $f_1(a)=0_K$ dır. $f_1(x)\in K_1[x]\subset K_2[x]$ olduğundan buradan, *a* nın K_2 üzerinde cebirsel olduğu sonucu çıkar. O halde $f_1(a)=0_K$ ve $f_1(x)\in K_2[x]$ ten, *a* nın K_2 üzerindeki $f_2(x)$ minimal polinomunun tanımı gereğince $K_2[x]$ te $f_2(x)\,|\,f_1(x)$ elde edilir.

Şimdi basit cebirsel genişlemeleri tanımlayacağız. Daha önceden bulduğumuz $\square[i]=\square(i)$ eşitliğini anımsayalım. Bu durum, bir cebirsel eleman tarafından doğurulan bir basit genişlemenin gözönüne alındığı her zaman geçerlidir.

Teorem 3.2.7. *E/K* bir cisim genişlemesi ve $a\in E$ olsun. *a* nın *K* üzerinde cebirsel olduğunu varsayalım, *f* de *a* nın *K* üzerindeki minimal polinomu olsun. *K*[*x*] te *f* tarafından doğurulan esas ideali $K[x]f=:(f)$ ile gösterecek olursak,

$$K(a)=K[a]\cong K[x]/(f)$$

tir.

İspat. $T_a:K[x]\to E$ sübstitüsyon homomorfisini gözönüne alalım. Teorem 3.2.1 e göre $KerT_a=\{h\in K[x]:h(a)=0_E\}=(f)$ tir ve Lemma 3.1.27(1) e göre $\operatorname{Im}T_a=K[a]$ dır. O halde $K[x]/(f)=K[x]/KerT_a\cong\operatorname{Im}T_a=K[a]$ dır.

Şimdi $K(a)=K[a]$ eşitliğinin gerçeklendiğini gösterelim. $K[a]\subset K(a)$ olduğundan sadece $K(a)\subset K[a]$ olduğunu göstermeliyiz. Bunun için, Lemma 3.1.27 ye göre, sadece, $g(a)\neq 0_E$ koşuluna uyan her $g(x)\in K[x]$ için $\dfrac{1_K}{g(a)}\in K[a]$ olduğunu göstermemiz gerekir. Gerçekten, $g(x)\in K[x]$ ve $g(a)\neq 0_E$ ise *f*, *g* yi bölemez ve *f*, *K*[*x*] te asal olduğundan *f*(*x*) ve *g*(*x*) polinomları, Teorem 2.92(3) e göre *K*[*x*] te aralarında asaldır. O halde

$$f(x)\cdot r(x)+g(x)\cdot s(x)=1$$

olacak şekilde $r(x),\ s(x) \in K[x]$ vardır. Bu eşitlikte x yerine a koyarsak, $f(a) = 0_E$ olduğundan $g(a) \cdot s(a) = 1_K$ elde ederiz. Buradan $\dfrac{1_K}{g(a)} = s(a) \in K[a]$ sonucu çıkar, dolayısıyla $K(a) \subset K[a]$ dır. O halde $K(a) = K[a]$ dır.

Teorem 3.2.8. *E/K* bir cisim genişlemesi ve $a \in E$ olsun. *a* nın *K* üzerinde cebirsel olduğunu varsayalım ve *f*, *a* nın *K* üzerindeki minimal polinomu olsun. Bu durumda

$$\left|K(a) : K\right| = deg\ f$$

tir, yani *K*(*a*) cisminin *K* üzerindeki derecesi, *a* nın *K*[*x*] teki *f* minimal polinomunun derecesine eşittir. *deg f* =*n* ise $\left\{1, a, a^2, ..., a^{n-1}\right\}$, *K*(*a*) nın bir *K*-tabanıdır ve *K*(*a*) nın her elemanı

$$k_0 + k_1 \cdot a + k_2 \cdot a^2 + ... + k_{n-1} \cdot a^{n-1} \qquad (k_0, k_1, k_2, ..., k_{n-1} \in K)$$

şeklinde tek türlü gösterilebilir.

İspat. $A := \left\{1, a, a^2, ..., a^{n-1}\right\}$ in, *K*(*a*) nın bir *K*-tabanı olduğunu ispatlayacağız. Önce *A* nın *K* üzerinde *K*(*a*) yı doğurduğunu gösterelim. Teorem 3.2.7 den $K(a) = K[a]$, Lemma 3.1.27(1) den de $K[a] = \left\{g(a) \in E : g \in K[x]\right\}$ olduğunu biliyoruz. O halde *K*(*a*) nın her *u* elemanı, *g*(*x*), *K*[*x*] te uygun bir polinom olmak üzere, *g*(*a*) şeklinde yazılabilir. Bu *g*(*x*) polinomunu, derecesi *n* olan bir *f*(*x*) polinomu ile bölersek, uygun *q*(*x*), $r(x) \in K[x]$ ile

$$g(x) = q(x) \cdot f(x) + r(x) \qquad (r(x) = 0_E \text{ veya } deg\ r(x) \le n-1)$$

elde ederiz. Bu eşitlikte *x* yerine *a* koyarsak,

$$u = g(a) = q(a) \cdot f(a) + r(a) = q(a) \cdot 0_E + r(a) = r(a)$$

buluruz. O halde $r(x) = k_0 + k_1 x + k_2 x^2 + ... + k_{n-1} x^{n-1} \qquad (k_i \in K; i = 0, 1, ..., n-1)$ dersek,

$$u = k_0 + k_1 \cdot a + k_2 \cdot a^2 + ... + k_{n-1} \cdot a^{n-1}$$

olur ve dolayısıyla *A*, *K* üzerinde *K*(*a*) yı doğurur.

Şimdi *A* nın *K* üzerinde lineer bağımsız olduğunu gösterelim.

$$k_0 + k_1 \cdot a + k_2 \cdot a^2 + ... + k_{n-1} \cdot a^{n-1} = 0_E \qquad (k_0, k_1, k_2, ..., k_{n-1} \in K)$$

ise *a*, $h(x) = k_0 + k_1 x + k_2 x^2 + ... + k_{n-1} x^{n-1} \in K[x]$ polinomunun bir köküdür, dolayısıyla Teorem 3.1.37 ye göre $f(x) \mid h(x)$ tir. Burada $h(x) = 0_E$ olmalıdır, çünkü aksi halde $h(x) \neq 0_E$ olurdu ki, bu $n = deg\ f \le deg\ h \le n-1$ oluşu ile çelişirdi. $h(x) = 0_E$ olması ise $k_0 = k_1 = k_2 = \cdots = k_{n-1} = 0_E$ olması demektir. O halde *A*, *K* üzerinde lineer bağımsızdır.

Böylece *A* nın *K*(*a*) nın bir *K*-tabanı olduğunu ispatlamış olduk. Buradan

$$\left|K(a) : K\right| = dim_K K(a) = \left|\left\{1, a, a^2, ..., a^{n-1}\right\}\right| = n = deg\ f(x)$$

sonucu çıkar ve Teorem 2.101 e göre *K*(*a*) nın her elemanı

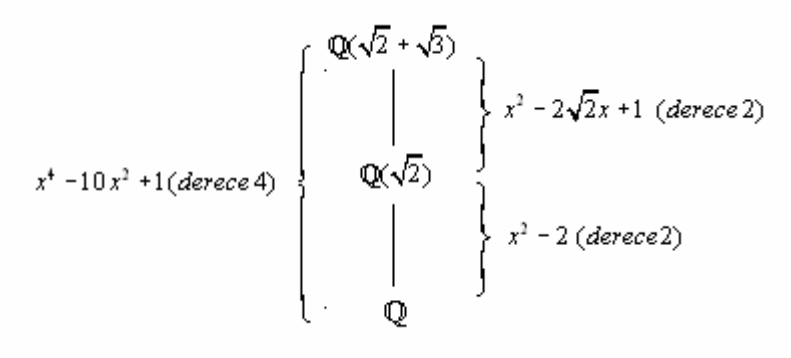
$$k_0 + k_1 \cdot a + k_2 \cdot a^2 + ... + k_{n-1} \cdot a^{n-1}$$

şeklinde tek türlü gösterilebilir.

Tanım 3.2.9. *E/K* bir cisim genişlemesi ve $a \in E$ olsun. *a* nın *K* üzerinde cebirsel olduğunu varsayalım. *a* nın *K* üzerindeki minimal polinomunun derecesine (ki, bu aynı zamanda *K*(*a*) nın *K* üzerindeki derecesidir) *a nın K üzerindeki derecesi* denir.

Örnek 3.2.10. $i \in \mathbb{C}$ nin $\mathbb{R}$ üzerindeki minimal polinomu, Örnek 3.2.4 e göre $x^2+1 \in \mathbb{R}[x]$ tir ve x^2+1 in derecesi 2 dir. O halde $i \in \mathbb{C}$, $\mathbb{R}$ üzerinde cebirsel olup, $\mathbb{R}$ üzerindeki derecesi 2 dir. Benzer şekilde, $i \in \mathbb{C}$ nin $\mathbb{Q}$ üzerindeki minimal polinomu $x^2+1 \in \mathbb{Q}[x]$ tir ve *i* nin $\mathbb{Q}$ üzerindeki derecesi 2 dir.

Örnek 3.2.11. Örnek 3.2.5 te $\sqrt{2}+\sqrt{3} \in \mathbb{C}$ nin $\mathbb{Q}$ üzerindeki minimal polinomunu $x^4-10x^2+1 \in \mathbb{Q}[x]$ olarak bulmuştuk. Şu halde $\sqrt{2}+\sqrt{3}$ ün $\mathbb{Q}$ üzerindeki derecesi 4 tür. Bu sonuç aynı zamanda Teorem 3.2.8 den de çıkarılır. Gerçekten, 1 ve $\sqrt{2}$ sayıları $\mathbb{Q}(\sqrt{2})$ cisminin bir $\mathbb{Q}$ -tabanını oluştururlar, dolayısıyla $\left|\mathbb{Q}(\sqrt{2}):\mathbb{Q}\right|=2$ dir. Şimdi aşağıdaki şemaya dikkat edelim:



$\sqrt{2}=-\frac{9}{2}(\sqrt{2}+\sqrt{3})+\frac{1}{2}(\sqrt{2}+\sqrt{3})^3$ yazılabileceğinden $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ ve dolayısıyla $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$ tür. O halde $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$ genişlemesinin bir ara cismidir. Buna göre Teorem 3.1.21 den

$$4=\left|\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}\right|=\left|\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}(\sqrt{2})\right|\cdot\left|\mathbb{Q}(\sqrt{2}):\mathbb{Q}\right|=2\left|\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}(\sqrt{2})\right|$$

ve dolayısıyla

$$\left|\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}(\sqrt{2})\right|=2$$

elde edilir, o halde $\sqrt{2}+\sqrt{3}$ ün $\mathbb{Q}(\sqrt{2})$ üzerindeki derecesi 2 dir.

Örnek 3.2.12. $i \in \mathbb{C}$ nin $\mathbb{R}$ üzerindeki minimal polinomu $x^2+1 \in \mathbb{R}[x]$ olduğundan, Teorem 3.2.7 ye göre $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}(i)$ dir. $\mathbb{R}[x]/(x^2+1)$ halkasında $x^2+\mathbb{R}[x](x^2+1)=-1+\mathbb{R}[x](x^2+1)$ eşitliği geçerlidir. Burada işlemler $\mathbb{R}[x]$ halkasındaki gibi yapılmakta, fakat $[x+\mathbb{R}[x](x^2+1)]^2=x^2+\mathbb{R}[x](x^2+1)$ yerine $-1+\mathbb{R}[x](x^2+1)$ konmaktadır. Aynı şekilde $\mathbb{R}(i)=\mathbb{C}$ de işlemler, $i \in \mathbb{C}$ üzerinde bir

değişkenmiş gibi yapılmakta ve i^2 yerine -1 yazılmaktadır. Böylece $\mathbb{Q}[x]/(x^2+1) \cong \mathbb{Q}(i) = \mathbb{C}$ olduğu ispatlanmış olur.

Örnek 3.2.13. Benzer şekilde, *E/K* bir cisim genişlemesi ve $a \in E$, K üzerinde minimal polinomu $x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + ... + c_1 x + c_0$ olan cebirsel bir eleman ise, yani

$$a^n = -c_{n-1} \cdot a^{n-1} - c_{n-2} \cdot a^{n-2} - ... - c_1 \cdot a - c_0$$

ise $K(a)$ cismi

$$k_0 + k_1 \cdot a + k_2 \cdot a^2 + ... + k_{n-1} \cdot a^{n-1} \qquad (k_0, k_1, k_2, ..., k_{n-1} \in K)$$

elemanlarından oluşur. $K(a)$ da hesaplamalar, a K üzerinde bir değişkenmiş gibi düşünülerek ve a^n yerine $-c_{n-1} \cdot a^{n-1} - c_{n-2} \cdot a^{n-2} - ... - c_1 \cdot a - c_0$ yazılarak yapılır.

Örneğin, $\sqrt{2} + \sqrt{3} \in \mathbb{C}$ yerine a yazılırsa, $\mathbb{Q}(a)$ da $a^4 = 10a^2 - 1$ elde edilir. $t = 2 + a - a^2 + 3a^3 \in \mathbb{Q}(a)$ *ve* $u = a + a^2 + 2a^3 \in \mathbb{Q}(a)$ ise

$t + u = 2 + 2a + 5a^3 \in \mathbb{Q}(a)$,

$$\begin{aligned} tu &= (2 + a - a^2 + 3a^3)(a + a^2 + 2a^3) \\ &= 2a + 2a^2 + 4a^3 + a^2 + a^3 + 2a^4 - a^3 - a^4 - 2a^5 + 3a^4 + 3a^5 + 6a^6 \\ &= 2a + 3a^2 + 4a^3 + 4a^4 + a^5 + 6a^6 \\ &= 2a + 3a^2 + 4a^3 + 4(10a^2 - 1) + a(10a^2 - 1) + 6a^2(10a^2 - 1) \\ &= 2a + 3a^2 + 4a^3 + 40a^2 - 4 + 10a^3 - a + 60(10a^2 - 1) - 6a^2 \\ &= -64 + a + 637a^2 + 14a^3 \in \mathbb{Q}(a) \end{aligned}$$

dır.

Şimdi $a^2 + a + 1$ in tersini bulalım. Teorem 3.2.7 ye göre $\mathbb{Q}[x]$ te

$$(x^4 - 10x^2 + 1)r(x) + (x^2 + x + 1)s(x) = 1$$

olacak şekilde $r(x)$, $s(x)$ polinomları bulmalıyız. Bunu Öklid algoritmesiyle yapalım.

$$x^4 - 10x^2 + 1 = (x^2 - x - 10)(x^2 + x + 1) + (11x + 11)$$

$$x^2 + x + 1 = \left(\frac{1}{11}x\right)(11x + 11) + 1$$

olup, buradan

$$\begin{aligned} 1 &= \left(x^2 + x + 1\right) - \left(\frac{1}{11}x\right)(11x + 11) \\ &= \left(x^2 + x + 1\right) - \left(\frac{1}{11}x\right)\left[\left(x^4 - 10x^2 + 1\right) - \left(x^2 - x - 10\right)\left(x^2 + x + 1\right)\right] \\ &= \left(x^2 + x + 1\right)\left[1 + \left(\frac{1}{11}x\right)\left(x^2 - x - 10\right)\right] - \left(\frac{1}{11}x\right)\left(x^4 - 10x^2 + 1\right) , \end{aligned}$$

yani

$$1 = \left(x^2 + x + 1\right)\left(\frac{1}{11}x^3 - \frac{1}{11}x^2 - \frac{10}{11}x + 1\right) - \left(\frac{1}{11}x\right)\left(x^4 - 10x^2 + 1\right)$$

elde edilir. Bu eşitlikte x yerine a yazılarak

$$1=\left(a^2+a+1\right)\left(\frac{1}{11}a^3-\frac{1}{11}a^2-\frac{10}{11}a+1\right)$$

ve dolayısıyla

$$1/\left(a^2+a+1\right)=\frac{1}{11}a^3-\frac{1}{11}a^2-\frac{10}{11}a+1$$

bulunur.

Dikkat edilirse, *a* burada yalnızca $a^4-10a^2+1=0$ bağıntısını sağlayan bir semboldür. *a* nın sayısal değeri olan $\sqrt{2}+\sqrt{3}=3,14626337...$ bir reel sayı olarak dikkate alınmamıştır. Bu, müthiş bir esneklik sağlar: *a* yı $\mathbb{Q}$ nun, x^4-10x^2+1 polinomunun bir kökünü içeren herhangi bir *E* genişleme cisminin bir elemanı olarak düşünebiliriz. Bu fikir, aşağıda ele alınacaktır.

Teorem 3.2.14. *E/K* sonlu boyutlu bir genişleme olsun. Bu durumda *E, K* üzerinde cebirseldir ve aynı zamanda sonlu doğuraylıdır.

İspat. $\left|E:K\right|=n\in\mathbb{N}$ olsun. *E* nin *K* üzerinde cebirsel olduğunu ispatlamak için, *E* nin her elemanının *K*[*x*] te sıfırdan farklı bir polinomun kökü olduğunu göstermeliyiz. *u*, *E* nin keyfi bir elemanı ise, Steinitz yer değiştirme teoremine göre *E* nin *n+1* tane $1,u,u^2,...,u^{n-1},u^n$ elemanı, *K* üzerinde lineer bağımsız olamaz. O halde

$$k_0+k_1\cdot u+k_2\cdot u^2+...+k_{n-1}\cdot u^{n-1}+k_n\cdot u^n=0_E$$

olacak şekilde, hepsi birden sıfır olmayan $k_0,k_1,k_2,...,k_{n-1},k_n\in K$ vardır. Şu halde $g(x)=k_0+k_1x+k_2x^2+...+k_{n-1}x^{n-1}+k_nx^n$, *K*[*x*] te derecesi $\le n$ olan, sıfırdan farklı bir polinomdur ve *u*, *g*(*x*) in bir köküdür. O halde *u*, *K* üzerinde cebirseldir. *u*, *E* nin keyfi bir elemanı olduğundan, buradan *E* nin *K* üzerinde cebirsel olduğu sonucu çıkar.

İkinci olarak, $\{b_1,b_2,...,b_n\}\subset E$, *E* nin bir *K*-tabanı ise,

$$\begin{aligned}E=s_K(b_1,b_2,...,b_n)&=\left\{k_1'\cdot b_1+k_2'\cdot b_2+...+k_n'\cdot b_n:k_1',k_2',...,k_n'\in K\right\}\\&\subset\left\{f(b_1,b_2,...,b_n)\in E:f\in K[x_1,x_2,...,x_n]\right\}\\&=K(b_1,b_2,...,b_n)\\&\subset E\end{aligned}$$

ve dolayısıyla $E=K(b_1,b_2,...,b_n)$ dir, yani *E*, *K* üzerinde sonlu doğuraylıdır.

Yukarıki ispatta *g*(*x*) polinomunun derecesinin $\le n$ olduğu gerçeğini ayrı bir lemma olarak ifade edelim:

Lemma 3.2.15. *E/K*, derecesi $\left|E:K\right|=n\in\mathbb{N}$ olan bir cisim genişlemesi olsun. Bu durumda *E* nin her elemanı *K* üzerinde cebirseldir ve bu elemanın *K* üzerindeki derecesi, en fazla *n* ye eşittir.

Şimdi, cebirsel elemanlar tarafından doğurulan bir genişlemenin cebirsel olduğunu göstereceğiz.

Teorem 3.2.16. *E/K* bir cisim genişlemesi ve $a_1, a_2, ..., a_{n-1}, a_n$ *E* nin sonlu sayıda elemanı olsun. $a_1, a_2, ..., a_{n-1}, a_n$ nin *K* üzerinde cebirsel olduğunu varsayalım. Bu durumda $K(a_1, a_2, ..., a_{n-1}, a_n)$, *K* nın bir cebirsel genişlemesidir. Aslında, $K(a_1, a_2, ..., a_{n-1}, a_n)$ *K* nın sonlu boyutlu bir genişlemesidir ve

$$\left|K(a_1, a_2, ..., a_{n-1}, a_n) : K\right| \leq \left|K(a_1) : K\right| \cdot \left|K(a_2) : K\right| \cdots \left|K(a_n) : K\right|$$

dır.

İspat. $r_1 = \left|K(a_1) : K\right|$ olsun. *i*=2,...,*n*-1,*n* için a_i elemanı *K* üzerinde cebirseldir, dolayısıyla Lemma 3.2.6 ya göre aynı zamanda $K(a_1, ..., a_{i-1})$ üzerinde cebirseldir. Buna ek olarak, a_i nin $K(a_1, ..., a_{i-1})$ cismi üzerindeki minimal polinomu, a_i nin *K* üzerindeki minimal polinomunun bir bölenidir; bu minimal polinomların dereceleri karşılaştırılıp, Teorem 3.2.8 kullanılarak

$$r_i := \left|(K(a_1, ..., a_{i-1}))(a_i) : K(a_1, ..., a_{i-1})\right| \leq \left|K(a_i) : K\right| \qquad (i=2,...,n\text{-}1,n)$$

elde edilir.

$$K \subset K(a_1) \subset K(a_1, a_2) \subset ... \subset K(a_1, a_2, ..., a_{n-1}) \subset K(a_1, a_2, ..., a_{n-1}, a_n)$$

ve Lemma 3.1.28(2) ye göre

$$K(a_1, ..., a_{i-1}, a_i) = (K(a_1, ..., a_{i-1}))(a_i) \qquad (i=2,...,n\text{-}1,n)$$

olduğundan, Teorem 3.1.21 e göre

$$\begin{aligned}\left|K(a_1, a_2, ..., a_{n-1}, a_n) : K\right| &= r_n r_{n-1} ... r_2 r_1 \\ &\leq \left|K(a_n) : K\right| \cdot \left|K(a_{n-1}) : K\right| \cdots \left|K(a_2) : K\right| \cdot \left|K(a_1) : K\right|\end{aligned}$$

elde edilir. O halde $K(a_1, a_2, ..., a_{n-1}, a_n)$, *K* nın sonlu boyutlu bir genişlemesidir ve Teorem 3.2.14 e göre *K* nın bir cebirsel genişlemesidir.

Lemma 3.2.17. *E/K* bir cisim genişlemesi ve $a, b \in E$ olsun. *a* ve *b*, *K* üzerinde cebirsel ise, $a+b$, $a-b$, $a \cdot b$ ve a/b ($b \neq 0_E$ olduğu durumda) *K* üzerinde cebirseldir.

İspat. *a* ve *b, K* üzerinde cebirsel ise, Teorem 3.2.16 ya göre *K*(*a,b*), *K* nın bir cebirsel genişlemesidir, yani *K*(*a,b*) nin her elemanı *K* üzerinde cebirseldir. $a+b$, $a-b$, $a \cdot b$, a/b de *K*(*a,b*) nin elemanları olduğundan, onlar da *K* üzerinde cebirseldir.

Teorem 3.2.18. *E/K* bir cisim genişlemesi, *A* da *E* nin *K* üzerinde cebirsel olan bütün elemanlarının kümesi olsun. Bu durumda *A*, *E* nin bir alt cismidir (ve dolayısıyla *E/K* genişlemesinin bir ara cismidir).

İspat. $a, b \in E$ ise *a* ve *b*, *K* üzerinde cebirseldir, o halde $a+b$, $a-b$, $a \cdot b$ ve $1_E/b$ ($b \neq 0_E$ olduğu durumda), Lemma 3.2.17 ye göre *K* üzerinde cebirseldir, dolayısıyla Lemma 3.1.2 ye göre *A*, *E* nin bir alt cismidir. *K* nın her elemanı Örnek 3.1.30 a göre *K* üzerinde cebirsel olduğundan, $K \subset A$ dır. O halde *A*, *E/K* genişlemesinin bir ara cismidir.

Tanım 3.2.19. *E/K* bir cisim genişlemesi, *A* da *E* nin *K* üzerinde cebirsel olan bütün elemanlarından oluşan alt cismi olsun. Bu durumda *A* ya *K nın E deki cebirsel kapanışı* denir.

A, şüphesiz *K* nın bir cebirsel genişlemesidir. Gerçekten, $a \in E$ ise, *a* nın *K* üzerinde cebirsel olması için gerek ve yeter koşul, $a \in A$ olmasıdır ve *F, E/K* nın bir ara cismi ise, *F* nin *K* üzerinde cebirsel olması için gerek ve yeter koşul, $F \subset A$ olmasıdır.

Bu bölümün son teoremi, bir cebirsel genişlemenin bir cebirsel genişlemesinin gene bir cebirsel genişleme olduğunu ifade etmektedir (cebirsel genişlemenin transitifliği).

Teorem 3.2.20. *F, E, K* üç cisim olsun. *F, E* nin bir cebirsel genişlemesi, *E* de *K* nın bir cebirsel genişlemesi ise *F, K* nın bir cebirsel genişlemesidir.

İspat. *F* nin her elemanının *K* üzerinde cebirsel olduğunu göstermeliyiz. $u \in F$ alalım. *F, E* üzerinde cebirsel olduğundan *u* da *E* üzerinde cebirseldir, o halde $f(u) = 0_E$ olacak şekilde bir

$$f(x) = e_0 + e_1 x + ... + e_n x^n \in E[x]$$

vardır. $L = K(e_0, e_1, ..., e_n)$ diyelim. $f(x) \in L[x]$ olduğu açıktır. *E*, *K* üzerinde cebirsel olduğundan $e_0, e_1, ..., e_n$ lerin herbiri *K* üzerinde cebirseldir ve Teorem 3.2.16 ya göre *L/K* sonlu boyutludur. Ayrıca, $f(u) = 0_E$ ve $f(x) \in L[x]$ olduğundan, *u* nun *L* üzerinde cebirsel olduğu sonucu çıkar ve Teorem 3.2.8 e göre *L*(*u*)/*L* sonlu boyutludur. O halde $|L(u) : K| = |L(u) : L| \cdot |L : K|$ sonlu bir sayıdır, yani *L*(*u*), *K* nın sonlu boyutlu bir genişlemesidir. Teorem 3.2.14 e göre *L*(*u*), *K* nın bir cebirsel genişlemesidir. O halde *L*(*u*) nun her elemanı *K* üzerinde cebirseldir. Özellikle $u \in L(u)$ olduğundan, *u* nun *K* üzerinde cebirsel olduğu görülür. *u*, *F* nin keyfi bir elemanı olduğundan, buradan *F* nin *K* nın bir cebirsel genişlemesi olduğu sonucu çıkar.

Tanım 3.2.21. *K* ve *L,* bir *E* cisminin iki alt cismi olsun. *P*, *E* nin asal alt cismi olmak üzere, *E* nin *P* üzerinde $K \cup L$ tarafından doğurulan alt cismine *K ve L nin kompozitumu* denir ve bu cisim, *KL* ile gösterilir.

O halde bu tanıma göre $KL = P(K \cup L) = P(L \cup K) = LK$, yani *KL*=*LK* dır. *KL* kompozitumu, *E* nin, *K* ve *L* nin ikisini birden kapsayan en küçük alt cismidir ki, buradan da *KL*=*K*(*L*)=*L*(*K*) sonucu çıkar.

K ve *L* gibi iki cismin kompozitumunu tanımlamak için, bunların daha geniş bir cisim içinde bulunmaları zorunludur. *K* ve *L*, ortak bir cismin alt cisimleri değilse *KL* kompozitumu tanımlanamaz.

E/K bir cisim genişlemesi ve $a, b \in E$ ise *K*(*a*) ve *K*(*b*) nin *K*(*a*)*K*(*b*) kompozitumu, $K(P \cup \{a, b\}) = K(a, b)$ dir.

§ 3. Kronecker Teoremi

Bu paragrafta L. Kronecker'in, bir cisim üzerindeki herhangi bir polinomun uygun bir genişleme cisminde bir kökünün bulunduğunu ifade eden önemli bir teoremini ispatlayacağız. Bu teorem, cisim genişlemelerinin esas teoremi olarak kabul edilebilir. Kronecker'in felsefi bakış açısından beklenebileceği üzere, ispat konstrüktif bir ispattır, yani sadece bir genişlemenin varlığı ispatlanmakla kalmayıp, aslında elemanlarının neler olduğu ve onların nasıl toplandığı, çarpıldığı ve terslerinin alındığı gösterilmektedir.

Polinomların kökleriyle ilgili tartışmalarımızda
(1) bir K cisminin,
(2) $K[x]$ te bir $f(x)$ polinomunun,
(3) K nın bir E genişleme cisminin,
(4) E nin, $f(x)$ in kökü olan bir a elemanının
verildiğini varsaydık. Fakat birçok durumda sadece bir K cismi ve $K[x]$ te bir $f(x)$ polinomu verildi, problem de, $f(x)$ in bir kökünü bulmaktı. Daha ayrıntılı olarak problem, K nın bir E genişlemesini ve E nin $f(a)=0_E$ olacak şekilde bir a elemanını bulmaktır. Sadece a yı bulmakla kalmayıp, aynı zamanda başta verilmeyen E yi de bulmamız gerekir. Kronecker teoremi, bunu nasıl yapacağımızı anlatır.

Şimdi, 18. ve 19. yüzyılda kompleks sayıların matematikte ortaya çıktığı şu tarihi örneği gözönüne alalım: Matematikçiler, $\mathbb{R}$ reel sayılar cismini ve $x^2+1\in\mathbb{R}[x]$ polinomunu biliyordu. Bu polinomun $\mathbb{R}$ de kökü yoktur, çünkü karesi -1 e eşit olan hiçbir reel sayı yoktur. Fakat 3. dereceden bir polinomun köklerini veren, Cardano formülleri gibi öyle güçlü gösterimler vardı ki, $x^2+1\in\mathbb{R}[x]$ polinomunun bir kökü için de böyle birşey bulunabilirdi. Sonra ne yaptı matematikçiler? Bir reel sayı olmadığını çok iyi bildikleri $\sqrt{-1}$ sembolünü türettiler ve $a+b\sqrt{-1}$ $(a,b\in\mathbb{R})$ ifadelerini gözönüne aldılar. Bu tipteki ifadelere "*kompleks sayılar"* denildi. $a+b\sqrt{-1}$ ve $c+d\sqrt{-1}$ gibi iki kompleks sayının eşit kabul edilmesi için gerek ve yeter koşul, $a=c$ ve $b=d$ olmasıdır. İki kompleks sayının toplamı

$$(a+b\sqrt{-1})+(c+d\sqrt{-1})=(a+c)+(b+d)\sqrt{-1},$$

çarpımı ise, $(\sqrt{-1})^2$ sembolü -1 reel sayısına eşit olarak yorumlanmak üzere,

$$\begin{aligned}(a+b\sqrt{-1})(c+d\sqrt{-1}) &= ac+ad\sqrt{-1}+b\sqrt{-1}c+b\sqrt{-1}d\sqrt{-1}\\ &= ac+bd(\sqrt{-1})^2+(ad+bc)\sqrt{-1}\\ &= (ac-bd)+(ad+bc)\sqrt{-1}\end{aligned}$$

şeklinde tanımlandı. Dolayısıyla $\sqrt{-1}$, hesaplanabilen bir nesne haline geldi. Kompleks sayılar, $\mathbb{R}$ nin cisim özelikleri kullanılarak ve $(\sqrt{-1})^2$ yerine -1 konularak çarpıldı. Kompleks sayıların sıralı reel sayı ikilileri olarak inşası, 19. yüzyılın ortalarında W.R. Hamilton tarafından verildi. Kompleks sayıların daha önceki matematikçiler tarafından kullanılan tanımında temel olarak hiçbir hata yoktu. $\mathbb{C}$ cismi, $\mathbb{R}$ nin $x^2+1\in\mathbb{R}[x]$ polinomunun bir kökünü içeren $\mathbb{R}(i)$

genişleme cismi olarak bu şekilde inşa edildi. Daha ayrıntılı bir şekilde belirtmek gerekirse, $0+1\sqrt{-1}$ kompleks sayısı x^2+1 in bir köküdür.

Başka bir örnek verelim: $\square$ cismi ve $x^4-10x^2+1\in\square[x]$ polinomu verilsin. Bu polinomun bir kökünü bulmak isteyelim. Örnek 3.2.13 te olduğu gibi, burada da $a^4-10a^2+1=0$ koşuluna uyan bir *a* sembolü türetiriz ve $c_0,c_1,c_2,c_3\in\square$ üzerinde birbirinden bağımsız olarak dolaşmak üzere, bütün $c_0+c_1a+c_2a^2+c_3a^3$ ifadelerini gözönüne alırız. Bu ifadeler yeni "*sayılar*"dır. Bu yeni "*sayılar*", $\square$ cisminin temel özelikleri kullanılarak ve a^4-10a^2+1 yerine 0 yazılarak veya buna denk olarak, a^4 yerine $10a^2-1$ yazılarak çarpılır. $\square$ (*a*) cismi, $\square$ ve *a* dan, $\square$ nun, $x^4-10x^2+1\in\square[x]$ polinomunun bir kökünü içeren bir genişleme cismi olarak inşa edilmiştir. Daha ayrıntılı olarak, $0+1a+0a^2+0a^3$ "*sayısı*", x^4-10x^2+1 in bir köküdür.

Genel durumda ne yapılacağı şimdi daha açıktır. Bir *K* cismi ve *K*[*x*] te asal olan bir *f*(*x*) polinomu verildiğine göre, *f*(*x*) in bir kökünü bulmak için, $f(u)=0_K$ koşuluna uyan bir *u* sembolü türetiriz ve $n=deg\,f(x)$ ve $1,u,u^2,...,u^{n-1}$ ler hesaplanabilen nesneler olmak üzere, *K*-tabanı $1,u,u^2,...,u^{n-1}$ olan *K*-vektör uzayını gözönüne alırız. Bu *K*-vektör uzayının elemanlarını, *u* yu *K* üzerinde bir değişken olarak kabul edip, *f*(*u*) yerine 0_K yazarak çarparız. Bunu yapmanın en mantıklı yolu, Teorem 3.2.7 de de önerildiği gibi, $K[x]/(f)$ bölüm halkasını gözönüne almaktır.

Teorem 3.3.1 (Kronecker Teoremi). *K* bir cisim ve *f*(*x*), *K*[*x*] te asal bir polinom olsun. Bu takdirde *K* nın, *f*(*x*) in bir kökünü içeren bir *E* genişleme cismi vardır.

İspat. *K*[*x*] in *f*(*x*) tarafından doğurulan esas ideale göre bölüm halkası $E=K[x]/(f)$ olsun. *K*[*x*] bir esas ideal halkası ve *f*(*x*), *K*[*x*] te asal olduğundan, Teorem 2.72 ye göre $E=K[x]/(f)$ bölüm halkası, bir cisimdir.

$$\varphi: K\to E$$
$$k\to k+(f)$$

tasviri bir halka homomorfisidir, çünkü her $k_1,k_2\in K$ için

$$\varphi(k_1+k_2)=(k_1+k_2)+(f)=(k_1+(f))+(k_2+(f))=\varphi(k_1)+\varphi(k_2),$$
$$\varphi(k_1\cdot k_2)=k_1\cdot k_2+(f)=(k_1+(f))\cdot(k_2+(f))=\varphi(k_1)\cdot\varphi(k_2)$$

dir. *f*(*x*), *K*[*x*] te asal olduğundan, *K*[*x*] te bir aritmetik birim değildir, dolayısıyla $\varphi(1_K)=1_K+(f)\neq 0_K+(f)$ tir ve Lemma 3.1.14 e göre φ (1-1) dir. Şu halde φ bir cisim homomorfisidir. *K* yı *E* deki $\varphi(K)$ görüntüsüyle özdeşleştirelim ve $k\in K$ olmak üzere, $k+(f)$ yerine *k* yazalım. Bu şekilde, *K* yı *E* nin bir alt cismi, *E* yi de *K* nın bir genişlemesi olarak elde etmiş oluruz.

Kısalık açısından $u=x+(f)\in E$ yazalım. *u* nun, *f*(*x*) in bir kökü olduğunu iddia ediyoruz. Gerçekten,

$$f(x) = b_0 + b_1x + b_2x^2 + ... + b_nx^n \in K[x] \quad (b_n \neq 0_K)$$

ise

$$f(u) = b_0 + b_1 \cdot u + b_2 \cdot u^2 + ... + b_n \cdot u^n$$

$$= (b_0 + (f)) + (b_1 + (f))(x + (f)) + (b_2 + (f))(x + (f))^2 + ... + (b_n + (f))(x + (f))^n$$

$$= (b_0 + (f)) + (b_1 + (f))(x + (f)) + (b_2 + (f))(x^2 + (f)) + ... + (b_n + (f))(x^n + (f))$$

$$= b_0 + b_1x + b_2x^2 + ... + b_nx^n + (f)$$

$$= f + (f)$$

$$= 0_K + (f)$$

$$= 0_E \in E$$

dir ve dolayısıyla $u \in E$, $f(x)$ in bir köküdür. Böylece E, K nın, $f(x)$ in bir kökünü içeren bir genişleme cismidir (K yı $\varphi(K) \subset E$ ile özdeşleştirdiğimizden dolayı, $k \in K$ olmak üzere, $k + 0_K \cdot u + 0_K \cdot u^2 + ... + 0_K \cdot u^n \in E$ yerine k yazabiliriz).

Yukarıki ispattaki gösterimi aynen koruyalım. $K(u) \subset E$ olduğu açıktır. Aynı zamanda, E nin her elemanı $c_0 + c_1x + c_2x^2 + ... + c_mx^m + (f)$ biçiminde olup,

$$c_0 + c_1x + c_2x^2 + ... + c_mx^m + (f) = c_0 + c_1(x + (f)) + c_2(x + (f))^2 + ... + c_m(x + (f))^m$$

$$= c_0 + c_1 \cdot u + c_2 \cdot u^2 + ... + c_m \cdot u^m$$

yazılabilir ve dolayısıyla $K(u)$ ya aittir; o halde $E \subset K(u)$ dur. Bu ise, $E = K(u)$ demektir, yani $E = K(u)$, K nın bir basit genişlemesidir.

Şimdi $F = K(t)$, K nın, $f(x) \in K[x]$ in bir $t \in F$ kökü tarafından doğurulan başka bir basit genişlemesi olsun. Teorem 3.2.7 ye göre

$$T_u : K[x] \to K(u) \qquad T_t : K[x] \to K(t)$$
$$g(x) \to g(u) \qquad g(x) \to g(t)$$

sübstitüsyon homomorfilerinden hareketle

$$\alpha : K[x]/(f) \to K(u) \qquad \beta : K[x]/(f) \to K(t)$$
$$g(x) + (f) \to g(u) \qquad g(x) + (f) \to g(t)$$

cisim izomorfileri elde edilir. Dolayısıyla

$$\beta\alpha^{-1} : K(u) \to K(t)$$
$$g(u) \to g(t)$$

bir cisim izomorfisidir, yani $K(u) \cong K(t)$ dir. Üstelik, her $k \in K$ için $\alpha(k) = \alpha(k + (f)) = T_u(k) = k$ ve benzer şekilde her $k \in K$ için $\beta(k) = k$ olduğundan $\beta\alpha^{-1}$ in $K \subset K(u)$ ya kısıtlanmışı, K nın idantik tasviridir.

Böylece, Kronecker teoremine takviye niteliği taşıyan şu teoremi ispatlamış olduk:

Teorem 3.3.2. K bir cisim ve $f(x) \in K[x]$, $K[x]$ te asal bir polinom olsun. Bu takdirde K nın, $u \in K(u)$, $f(x)$ in bir kökü olacak şekilde bir $K(u)$ basit genişlemesi vardır. Üstelik, $K(t)$, $t \in K(t)$, $f(x)$ in bir kökü olmak üzere, K nın bir basit genişlemesi ise $K(u) \cong K(t)$ dir ve gerçekte K ya kısıtlanmışı, K nın idantik tasviri olan bir $\varphi : K(u) \to K(t)$ izomorfisi vardır.

Tanım 3.3.3. K bir cisim ve $f(x)$, $K[x]$ te bir asal polinom olsun. Bu durumda u, $f(x)$ in bir kökü olmak üzere, K nın bir $K(u)$ basit genişlemesine (Teorem 3.3.2 ye göre böyle bir cisim vardır ve K ya kısıtlanmışı, K nın idantik tasviri ile çakışan bir izomorfiden vazgeçildiği takdirde, tek türlü belirlidir), *f(x) in bir kökünü K ya katmakla elde edilen cisim* denir.

Not 3.3.4. K bir cisim ve $f(x)$, $K[x]$ te bir asal polinom olsun. $K(u)$ nun, K ya $f(x)$ in bir u kökünü katmakla elde edilen cisim olduğunu varsayalım. c, $f(x)$ in baş katsayısı olsun. Teorem 3.2.3 ten $\frac{1_K}{c} f(x)$ in, u nun K üzerindeki minimal polinomu olduğunu biliyoruz. O halde Teorem 3.2.8 den $|K(u) : K| = deg\ \frac{1_K}{c} f(x) = deg\ f(x)$ elde edilir, yani K ya asal bir $f(x) \in K[x]$ polinomunun bir kökünü katmakla elde edilen cismin K üzerindeki derecesi, $f(x)$ in derecesine eşittir.

Teorem 3.3.5 (Kronecker). K bir cisim ve $f(x)$, $K[x]\backslash K$ da derecesi n olan (K üzerinde asal olması gerekmeyen) bir polinom olsun. Bu takdirde K nın öyle bir E genişleme cismi vardır ki, $f(x)$ in bir kökünü içerir ve $|E : K| \le n$ dir.

İspat. $f(x) \notin K[x]$ olduğundan $f(x)$, ne sıfır polinomudur, ne de $K[x]$ te bir aritmetik birimdir. $K[x]$, asal çarpanlara ayrılışın tek olduğu bir tamlık bölgesi olduğundan, $f(x)$ i asal polinomların çarpımı olarak yazabiliriz ve $f(x)$ in asal bölenlerinden birinin bir kökünü K ya katabiliriz. Bu şekilde elde edilen E cismi, $f(x)$ in o asal böleninin ve dolayısıyla $f(x)$ in bir kökünü içerecektir. Üstelik, $|E : K|$, $f(x)$ in o asal böleninin derecesine eşit olacaktır; şu halde $|E : K|$, en çok $f(x)$ in derecesine eşittir.

Örnek 3.3.6. $f(x) = x^2 - 2 \in \mathrm{F}_5[x]$ polinomunu gözönüne alalım. $f(x)$, F_5 üzerinde asaldır, çünkü aksi halde $f(x)$ in F_5 te bir kökü bulunurdu, oysa F_5 te karesi $2 \in \mathrm{F}_5$ olan hiçbir eleman yoktur. Şimdi $f(x)$ in bir u kökünü F_5 e katalım. Oluşan $\mathrm{F}_5(u)$ cismi, F_5-tabanı $\{1, u\}$ olan bir F_5-vektör uzayıdır ve $u^2 = 2 \in \mathrm{F}_5$ tir. Şimdi $\mathrm{F}_5(u)$ da birkaç örnek hesaplama yapalım:

$$(4+2u)(3+u) = 12 + 4u + 6u + 3u^2 = 2 + 10u + 3 \cdot 2 = 2 + 0 \cdot u + 1 = 3,$$
$$(3+2u)(2+4u) = 6 + 12u + 4u + 8u^2 = 1 + 2u + 4u + 3 \cdot 2 = 7 + 6u = 2 + u.$$

$u^2 = 2$ $(\in \mathrm{F}_5)$ denkleminden dolayı $\mathrm{F}_5(u)$ da u yerine $\sqrt{2}$ yazma konusunda anlaşacağız. Burada $\sqrt{2}$ nin sadece hesaplanan u nesnesinin diğer ismi olduğunu

tabii ki unutmayacağız, yani $\sqrt{2}$, sayısal değeri 1,414... olan reel sayı değil, karesi 2 olan bir semboldür.

Şimdi $(1+2\sqrt{2})(3+\sqrt{2})$ ve $(4+\sqrt{2})^{-1}$ i $\{1,\sqrt{2}\}$ F_5-tabanı cinsinden hesaplayalım.

$$(1+2\sqrt{2})(3+\sqrt{2}) = 3+\sqrt{2}+6\sqrt{2}+2\cdot 2 = (3+4)+(1+6)\sqrt{2} = 2+2\sqrt{2} \ ,$$

$$\frac{1}{4+\sqrt{2}} = \frac{1}{4+\sqrt{2}}\cdot\frac{4-\sqrt{2}}{4-\sqrt{2}} = \frac{4-\sqrt{2}}{16-2} = \frac{4-\sqrt{2}}{14} = \frac{4-\sqrt{2}}{4}$$

$$= \frac{1}{4}(4-\sqrt{2}) = 4(4-\sqrt{2}) = 16-4\sqrt{2} = 1+\sqrt{2}.$$

$$\varphi : F_5(\sqrt{2}) \to F_5(\sqrt{2})$$
$$a+b\sqrt{2} \to a-b\sqrt{2}$$

tasviri, $F_5(\sqrt{2})$ nin bir otomorfisidir, çünkü her $a+b\sqrt{2}$, $c+d\sqrt{2} \in F_5(\sqrt{2})$ için

$$\varphi[(a+b\sqrt{2})+(c+d\sqrt{2})] = \varphi[(a+c)+(b+d)\sqrt{2}] = (a+c)-(b+d)\sqrt{2}$$
$$= (a-b\sqrt{2})+(c-d\sqrt{2}) = \varphi(a+b\sqrt{2})+\varphi(c+d\sqrt{2})$$

ve

$$\varphi[(a+b\sqrt{2})\cdot(c+d\sqrt{2})] = \varphi[(ac+2bd)+(ad+bc)\sqrt{2}] = (ac+2bd)-(ad+bc)\sqrt{2}$$
$$= (ac+2(-b)(-d))+(a(-d)+(-b)c)\sqrt{2}$$
$$= (a-b\sqrt{2})\cdot(c-d\sqrt{2})$$
$$= \varphi(a+b\sqrt{2})\cdot\varphi(c+d\sqrt{2})$$

dir. φ aşikar olarak üzerinedir ve $Ker\varphi \neq F_5(\sqrt{2})$ dir.

Binom teoremine (Teorem 2.48) göre her $a+b\sqrt{2} \in F_5(\sqrt{2})$ için

$$(a+b\sqrt{2})^5 = a^5+5a^4b\sqrt{2}+10a^3b^2\cdot 2+10a^2b^3\cdot 2\sqrt{2}+5ab^4\cdot 4+b^5\cdot 4\sqrt{2}$$
$$= a^5+4b^5\sqrt{2} = a+4b\sqrt{2} = a-b\sqrt{2}$$

dir. O halde φ aynı zamanda

$$\varphi : F_5(\sqrt{2}) \to F_5(\sqrt{2})$$
$$t \ \to t^5$$

olarak da tanımlanabilir.

Örnek 3.3.7. $g(x) = x^2-3 \in F_5[x]$ polinomu da F_5 üzerinde asaldır. $g(x)$ in bir kökü olan $\sqrt{3}$ ü F_5 e katmakla $F_5(\sqrt{3})$ cismi elde edilir ki, bu cisim bir F_5-vektör uzayı olup, F_5 üzerindeki bir tabanı $\{1,\sqrt{3}\}$ tür ve $(\sqrt{3})^2 = 3 \in F_5$ tir. Tabii ki, $\sqrt{3}$ ün 1,732... reel sayısı olmadığını, sadece karesi 3 olan, hesaplanabilen bir nesne olduğunu unutmamalıyız. $F_5(\sqrt{3})$ te

$$(3+2\sqrt{3})(1+4\sqrt{3}) = 3+12\sqrt{3}+2\sqrt{3}+8\cdot 3 = 27+14\sqrt{3} = 2+4\sqrt{3}\ ,$$
$$(2+3\sqrt{3})(2+4\sqrt{3}) = 4+8\sqrt{3}+6\sqrt{3}+12\cdot 3 = 4+3\sqrt{3}+\sqrt{3}+36 = 4\sqrt{3}\ ,$$
$$\frac{1}{1+3\sqrt{3}} = \frac{1}{1+3\sqrt{3}}\cdot\frac{1-3\sqrt{3}}{1-3\sqrt{3}} = \frac{1-3\sqrt{3}}{1-27} = \frac{1+2\sqrt{3}}{4} = \frac{1}{4}(1+2\sqrt{3}) = 4(1+2\sqrt{3}) = 4+3\sqrt{3}$$

tür.

F_5 te 8=3 olduğu gibi, $\sqrt{3}$ için de $\sqrt{8}$ yazabiliriz. Burada $\sqrt{8} \in F_5(\sqrt{3})$, $(\sqrt{8})^2 = 8 = 3$ ü sağlayan, hesaplanabilen bir nesnedir, yani $\sqrt{8}$, 2,828... reel sayısı değildir, karesi $8 \in$ □ olan bir nesnedir. $\sqrt{8}$ i $\sqrt{8} = \sqrt{4\cdot 2} = 2\sqrt{2}$ şeklinde yazmaya kalkışabiliriz. Ancak, bu doğru değildir. Çünkü $\sqrt{8} \in F_5(\sqrt{3})$ ve $2\sqrt{2} \in F_5(\sqrt{2})$ dir, yani $\sqrt{8}$ ve $2\sqrt{2}$, iki farklı cismin elemanıdır ve bu iki cismin kesişimi F_5 e eşit olmadığından, $\sqrt{8} = 2\sqrt{2}$ yazmak anlamlı değildir.

Burada

$$\psi : F_5(\sqrt{3}) \to F_5(\sqrt{2})$$
$$a+b\sqrt{3} \to a+2b\sqrt{2}$$

tasviri, ilginç bir tasvirdir. Gerçekten, her $a+b\sqrt{3}, c+d\sqrt{3} \in F_5(\sqrt{3})$ için

$$\psi[(a+b\sqrt{3})+(c+d\sqrt{3})] = \psi[(a+c)+(b+d)\sqrt{3}] = (a+c)+2(b+d)\sqrt{2}$$
$$= (a+2b\sqrt{2})+(c+2d\sqrt{2}) = \psi(a+b\sqrt{3})+\psi(c+d\sqrt{3})$$

ve

$$\psi[(a+b\sqrt{3})\cdot(c+d\sqrt{3})] = \psi[(ac+3bd)+(ad+bc)\sqrt{3}] = (ac+3bd)+2(ad+bc)\sqrt{2}$$
$$= (ac+2\cdot 2b\cdot 2d)+(a\cdot 2d+2b\cdot c)\sqrt{2}$$
$$= (a+2b\sqrt{2})\cdot(c+2d\sqrt{2})$$
$$= \psi(a+b\sqrt{3})\cdot\psi(c+d\sqrt{3})$$

tür ve dolayısıyla ψ bir halka homomorfisidir. ψ nin üzerine (1-1) olduğu açıktır, şu halde ψ bir cisim izomorfisidir. O halde $F_5(\sqrt{3})$ ve $F_5(\sqrt{2})$, izomorf cisimlerdir, yani $F_5(\sqrt{3}) \cong F_5(\sqrt{2})$ dir. Bu iki cismi ψ izomorfisi nedeniyle özdeşleştirebiliriz, yani her $a,b \in F_5$ için $a+b\sqrt{3} = a+2b\sqrt{2}$ yazabiliriz. Ancak o zaman $\sqrt{3} = 2\sqrt{2}$ yazabiliriz.

Bu iki cismi her $a,b \in F_5$ için $a+b\sqrt{3} = a-2b\sqrt{2}$ diyerek, yani $\varphi\psi : F_5(\sqrt{3}) \to F_5(\sqrt{2})$ izomorfisi yardımıyla özdeşleştirebilirdik. Bunları nasıl özdeşleştirdiğimiz önemli değildir, fakat tutarlı bir şekilde, hep aynı özdeşleştirmeyi kullanmalıyız.

$F_5(\sqrt{3})$ ve $F_5(\sqrt{2})$ cisimlerini, her $a,b \in F_5$ için $a+b\sqrt{3} = a+2b\sqrt{2}$ yazarak özdeşleştirdiğimiz takdirde, örneğin $\sqrt{18}$ i karesi $18 \in F_5$ olan, hesaplanabilen bir nesne olarak yorumlayamayız, çünkü $F_5(\sqrt{3}) = F_5(\sqrt{2})$ de karesi 18 olan iki eleman vardır ki, bunlar $2\sqrt{2}$ ve $-2\sqrt{2} = 3\sqrt{2}$ dir. $\sqrt{18}$ olarak $2\sqrt{2}$ ve $3\sqrt{2}$ den hangisini kastettiğimizi mutlaka belirtmeliyiz. Aksi takdirde, □ deki

$$-7 = \sqrt{(-7)^2} = \sqrt{49} = 7$$

ye benzer bir hata olarak, $F_5(\sqrt{2})$ de

$$3\sqrt{2} = \sqrt{9\cdot 2} = \sqrt{18} = \sqrt{9\cdot 2} = \sqrt{4\cdot 2} = 2\sqrt{2}$$

gibi hatalar yapabiliriz. □ de karesi 49 olan iki sayı vardır ki, bunlar 7 ve -7 dir ve $\sqrt{49}$, 7 ve -7 sayılarından pozitif olanı olarak anlaşılır. Şu halde $\sqrt{49}$ yazdığımızda $\sqrt{49}$ olarak 7 ve -7 nin hangisini kastettiğimizi kesinlikle belirtiriz. Bu, $-7 = \sqrt{(-7)^2}$ hatasını yapmamızı önler. $F_5(\sqrt{2})$ de de, $\sqrt{18}$ olarak $2\sqrt{2}$ ve $3\sqrt{2}$ den hangisini aldığımızı belirtmek, $3\sqrt{2} = 2\sqrt{2}$ hatasına düşmemizi önler.

§ 4. Sonlu Cisimler

Sonlu cisimlerin, yani sonlu elemanlı cisimlerin bazı örneklerini daha önce görmüştük. Bu paragrafta sonlu cisimlerin bazı özeliklerini ele alacağız.

Son zamanlarda, sonlu cisimlerle Galois teorisinden sonra uğraşmak adet haline gelmiştir. Bizim sonlu cisimlere yaklaşımımız, alışılmıştan daha elemanter ve daha somut olacaktır. Bu da Galois teorisinin daha iyi anlaşılmasını sağlayacaktır.

Bir sonlu cismin mertebesini asal sayı kuvvetlerine kısıtlayarak işe başlayalım.

Lemma 3.4.1. *q* bir doğal sayı ve *K*, *q* elemanlı bir cisim olsun. Bu takdirde uygun bir *p* asal sayısı ve uygun bir *n* doğal sayısı için $q = p^n$ dir.

İspat. *K*, *q* elemanlı bir cisim olsun. *K* nın $\mathbb{Q}$ ya izomorf olduğunu bildiğimiz asal alt cismi $\mathbb{Q}$ olamaz, çünkü aksi halde *K* sonsuz eleman içerirdi. O halde *K* nın asal alt cismi, uygun bir *p* asal sayısı için F_p olmak zorundadır. Şimdi *K* yı bir F_p-vektör uzayı olarak gözönüne alalım. *K* nın F_p üzerindeki boyutu sonlu olmak zorundadır. Bu sonlu boyuta $\left|K : \mathrm{F}_p\right| = n \in \mathbb{N}$ diyelim. *K* nın bir F_p-tabanı $\{k_1, k_2, ..., k_n\}$ olsun. Bu takdirde *K*, a_i $(i = 1, 2, ..., n)$ ler birbirinden bağımsız olarak F_p yi dolaşmak üzere,

$$a_1 \cdot k_1 + a_2 \cdot k_2 + ... + a_n \cdot k_n$$

elemanlarından oluşur ve $(a_1, a_2, ..., a_n) \neq (b_1, b_2, ..., b_n)$ olduğunda

$$a_1 \cdot k_1 + a_2 \cdot k_2 + ... + a_n \cdot k_n \neq b_1 \cdot k_1 + b_2 \cdot k_2 + ... + b_n \cdot k_n$$

olur. Böylece $a_1, a_2, ..., a_n$ den her biri için *p* tane olası seçim vardır ve dolayısıyla *K* da tam p^n tane eleman vardır.

O halde $q = p^n$ koşulu, *q* elemanlı bir cismin varlığı için gerek bir koşuldur. Bu paragraftaki asıl amaçlarımızdan biri, bu koşulun aynı zamanda yeter bir koşul olduğunu göstermektir.

Lemma 3.4.1 in ispatından, p^n elemanlı bir cismin karakteristiğinin *p* olduğunu biliyoruz. Şimdi karakteristiği asal olan (sonlu olmaları gerekmeyen) cisimlere ilişkin iki lemma ispatlayacağız.

Lemma 3.4.2. *K*, karakteristiği $p \neq 0$ olan bir cisim olsun. Bu durumda her $a, b \in K$ için

$$(a+b)^p = a^p + b^p \quad , \quad (a \cdot b)^p = a^p \cdot b^p$$

dir.

İspat. Binom teoremini kullanacağız. Burada p bir asal sayıdır ve k=1,2,...,$p-1$ için $\binom{p}{k}$ binom katsayıları, p ile bölünebilen tam sayılardır. Çünkü $p!$, p ile bölünebilir, yani $k!(p-k)!\binom{p}{k}$, p ile bölünebilir; fakat $k!(p-k)!$ ile p aralarında asal olduğundan, Aritmetiğin Esas Yardımcı Teoremine göre p, $\binom{p}{k}$ yı böler. O halde her $a,b \in K$ için

$$(a+b)^p = a^p + \sum_{k=1}^{p-1}\binom{p}{k}a^{p-k}b^k + b^p = a^p + \sum_{k=1}^{p-1} 0_K + b^p = a^p + b^p$$

dir, çünkü $\binom{p}{k}$, p nin bir katıdır ve *karK*=*p* olduğundan, $\binom{p}{k}a^{p-k}b^k = 0_K$ $(k = 1,2,..., p-1)$ dır. Böylece $(a+b)^p = a^p + b^p$ eşitliği ispatlanmış olur. $(a\cdot b)^p = a^p \cdot b^p$ iddiası ise Lemma 2.27(5) ten dolayı doğrudur.

Lemma 3.4.2 den dolayı

$$\varphi : K \to K$$
$$a \to a^p$$

tasviri, bir cisim homomorfisidir ($1_K^p = 1_K \neq 0_K$ olduğu açıktır). Karakteristiği bir p asal sayısı olan bir cismin $a_1, a_2, ..., a_m$ gibi m tane elemanı için

$$(a_1 + a_2 + ... + a_m)^p = a_1^p + a_2^p + ... + a_m^p$$

olduğu, m ye göre tümevarımla ispat edilir.

Lemma 3.4.3. K, karakteristiği $p \neq 0$ olan bir cisim ve $n \in \mathbb{N}$ olsun. Bu takdirde her $a,b \in K$ için

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

dir.

İspat. İspatı n ye göre tümevarımla yapacağız. Lemma 3.4.2 ye göre $(a+b)^p = a^p + b^p$ dir, yani iddia n=1 için doğrudur. Şimdi n>1 alalım ve iddiayı n=k için doğru varsayalım, yani

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

olsun. Bu takdirde her $a,b \in K$ için

$$(a+b)^{p^{k+1}} = [(a+b)^{p^k}]^p = [a^{p^k} + b^{p^k}]^p = (a^{p^k})^p + (b^{p^k})^p = a^{p^{k+1}} + b^{p^{k+1}}$$

olur, yani iddia n=k+1 için de doğrudur. Şu halde iddia her $n \in \mathbb{N}$ için doğrudur.

Lemma 3.4.5. $q \in \mathbb{N}$ ve K, q elemanlı bir cisim olsun. Bu takdirde:

(1) Her $a \in K^*$ için $a^{q-1} = 1_K$ dır.

(2) Her $a \in K$ için $a^q = a$ dır.

(3) $K[x]$ te $x^q - x = \prod_{a \in K} (x - a)$ dır.

(4) $f(x)$, $K[x]$ te derecesi d olan, sıfırdan farklı bir polinom olsun. $K[x]$ te $f(x) \mid x^q - x$ ise, $f(x)$ in K da tam d tane kökü vardır ve bu kökler, ikişer ikişer birbirinden farklıdır.

İspat. (1) K^* bir çarpım grubu olup, $|K^*| = |K \setminus \{0_K\}| = q - 1$ dir. Şu halde her $a \in K^*$ için $a^{q-1} = 1_K$ dır.

(2) $a \neq 0_K$ ise (1) den, $a = 0_K$ ise $0_K^q = 0_K$ eşitliğinden $a^q = a$ elde edilir.

(3) K nın her a elemanı, (2) den dolayı, $x^q - x \in K[x]$ polinomunun bir köküdür. O halde hem $x^q - x$, hem de $\prod_{a \in K} (x - a)$, $K[x]$ te, K nın q tane a elemanını kök olarak kabul eden, q. dereceden bir monik polinomdur. $x^q - x \neq \prod_{a \in K} (x - a)$ olsaydı $(x^q - x) - \prod_{a \in K} (x - a)$ polinomu, derecesi q dan küçük olan ve birbirinden farklı en az q tane kökü olan, sıfırdan farklı bir polinom olurdu ki, bu Teorem 2.89 ile çelişir. Şu halde $x^q - x = \prod_{a \in K} (x - a)$ olmak zorundadır.

(4) $f(x) \mid x^q - x$ olduğundan $x^q - x = f(x) \cdot g(x)$ olacak şekilde bir $g(x) \in K[x]$ vardır ve $deg\, g(x) = q - d$ dir. (3) e göre $x^q - x$ in kökleri ikişer ikişer birbirinden farklıdır ve $f(x)$ in her kökü, aynı zamanda $x^q - x$ in de bir kökü olduğundan, $f(x)$ in köklerinin de ikişer ikişer birbirinden farklı olduğu görülür. Benzer şekilde, $g(x)$ in kökleri de ikişer ikişer birbirinden farklıdır. Teorem 2.89 a göre $g(x)$ in K da en fazla $q - d$ tane kökü vardır. $f(x)$ in K da r tane kökü bulunsaydı ve $r<d$ olsaydı $x^q - x = f(x) \cdot g(x)$ in K da en fazla $r+(q-d)(<q)$ tane kökü olurdu. Bu ise K nın, sayıları q olan tüm elemanlarının, $x^q - x$ in kökleri oluşuna aykırıdır. O halde $f(x)$ in K da en az d tane kökü vardır. Oysa Teorem 2.89 a göre $f(x)$ in K da en fazla d tane kökü bulunabilir. Şu halde $f(x)$ in K da tam d tane kökü vardır.

Lemma 3.4.6. L/K bir cisim genişlemesi olsun ve K nın $q(\in \square)$ tane elemanının bulunduğunu varsayalım. b, L nin herhangi bir elemanı olsun. $b \in K$ olması için gerek ve yeter koşul, $b^q = b$ olmasıdır.

İspat. $b \in K$ olması için gerek ve yeter koşul, b nin, $\prod_{a \in K} (x - a)$ polinomunun bir kökü olması, dolayısıyla $x^q - x$ in bir kökü olması, yani $b^q = b$ olmasıdır.

Son iki lemma, sonlu bir cismin alt cisimleri hakkında bilgi sahibi olmamızı sağlayacaktır. K_1 ve K_2, sırasıyla p^{m_1} ve p^{m_2} elemanlı iki sonlu cisim ve $K_1 \subset K_2$ olsun. Bu takdirde $K_1^* \underset{a.g.}{\subset} K_2^*$ dır ve dolayısıyla Lagrange teoremine göre

$\left|K_1^*\right| = p^{m_1} - 1, \left|K_2^*\right| = p^{m_2} - 1$ i böler. Şimdi bunun olabilmesi için gerek ve yeter koşulun $m_1 | m_2$ olduğunu göstereceğiz.

Lemma 3.4.7. $m, n \in \mathbb{Z}$ olsun ve $d = (m, n)$ diyelim. Bu takdirde:

(1) Her $k \in \mathbb{Z}$ için $(k^m - 1, k^n - 1) = k^d - 1$ dir.

(2) *K* herhangi bir cisim ve *x*, *K* üzerinde bir değişken ise asal çarpanlara ayrılışın tek olduğu *K*[*x*] tamlık bölgesinde $(x^m - 1_K, x^n - 1_K) \approx x^d - 1_K$ dir.

İspat. (1) $e = (k^m - 1, k^n - 1)$ diyelim.

$$k^m - 1 = (k^d - 1)[(k^d)^{(m/d)-1} + (k^d)^{(m/d)-2} + \ldots + k^d + 1]$$

olduğundan $k^d - 1 \left| k^m - 1 \right.$ dir. Benzer şekilde $k^d - 1 \left| k^n - 1 \right.$ dir, dolayısıyla $k^d - 1 | e$ dir. Diğer taraftan, $k^m \equiv 1(e)$ dir, o halde $\mathbb{Z}_e^*$ da $\left(\overline{k}\right)^m = \overline{1}$ dir ve dolayısıyla $\left|\overline{k}\right| | m$ dir. Benzer şekilde $\left|\overline{k}\right| | n$ dir, o halde $\left|\overline{k}\right| | d$ ve dolayısıyla $\mathbb{Z}_e^*$ da $\left(\overline{k}\right)^d = \overline{1}$ dir ki, bu da $k^d \equiv 1(e)$, yani $e \left| k^d - 1 \right.$ demektir. $k^d - 1 | e$ ve $e \left| k^d - 1 \right.$ den $e = k^d - 1$ sonucu çıkar.

(2) $f(x) = (x^m - 1_K, x^n - 1_K)$ diyelim.

$$x^m - 1_K = (x^d - 1_K)[(x^d)^{(m/d)-1} + (x^d)^{(m/d)-2} + \ldots + x^d + 1_K]$$

olduğundan *K*[*x*] te $x^d - 1_K \left| x^m - 1_K \right.$ dır. Benzer şekilde $x^d - 1_K \left| x^n - 1_K \right.$ dır ve dolayısıyla $x^d - 1_K \left| f(x) \right.$ tir. Diğer taraftan $f(x) \left| x^m - 1_K \right.$ olduğundan $K[x]/(f(x))$ te $(x + (f))^m = x^m + (f) = 1_K + (f)$ dir, dolayısıyla $x + (f)$, $K[x]/(f)$ te bir aritmetik birimdir ve $x + (f) \in (K[x]/(f))^*$ ın mertebesi *m* ile, benzer şekilde *n* ile ve dolayısıyla *d* ile bölünebilir. O halde $x^d + (f) = (x + (f))^d = 1_K + (f)$ dir ve *K*[*x*] te $f(x) \left| x^d - 1_K \right.$ dır. $x^d - 1_K \left| f(x) \right.$ ve $f(x) \left| x^d - 1_K \right.$ dan $f(x) \approx x^d - 1_K$ sonucu çıkar.

Lemma 3.4.8. $m, n, p \in \mathbb{Z}$, *K* bir cisim ve *x*, *K* üzerinde bir değişken olsun.

(1) Her $k \in \mathbb{Z}$ için, $k^m - 1 \left| k^n - 1 \right.$ olması için gerek ve yeter koşul, $m | n$ olmasıdır.

(2) *K*[*x*] polinom halkasında $x^m - 1_K \left| x^n - 1_K \right.$ olması için gerek ve yeter koşul, $m | n$ olmasıdır.

(3) *K*[*x*] polinom halkasında $x^{p^m} - x \left| x^{p^n} - x \right.$ olması için gerek ve yeter koşul, $m | n$ olmasıdır.

İspat.

(1) $k^m - 1 \left| k^n - 1 \right. \Leftrightarrow (k^m - 1, k^n - 1) = k^m - 1 \Leftrightarrow k^{(m,n)} - 1 = k^m - 1$

$$\Leftrightarrow (m, n) = m \Leftrightarrow m | n$$

(2) $x^m - 1_K \mid x^n - 1_K \Leftrightarrow (x^m - 1_K, x^n - 1_K) \approx x^m - 1_K \Leftrightarrow x^{(m,n)} - 1_K = x^m - 1_K$

$\Leftrightarrow (m,n) = m \Leftrightarrow m \mid n$

(3) $x^{p^m} - x \mid x^{p^n} - x \Leftrightarrow x^{p^m-1} - 1_K \mid x^{p^n-1} - 1_K \overset{(2)}{\Leftrightarrow} p^m - 1 \mid p^n - 1 \overset{(1)}{\Leftrightarrow} m \mid n$

Teorem 3.4.9. K, p^n (p asal) elemanlı bir cisim olsun. K nın p^m elemanlı bir alt cisminin bulunabilmesi için gerek ve yeter koşul, $m \mid n$ olmasıdır. $m \mid n$ olması durumunda K nın p^m elemanlı bir ve bir tek alt cismi vardır ve bu alt cisim

$$\left\{ a \in K \mid a^{p^m} = a \right\}$$

dır.

İspat. *Gereklik.* p^n elemanlı K cisminin p^m elemanlı bir alt cismi varsa $m \mid n$ dir: Daha önce de ifade edildiği gibi, K nın p^m elemanlı bir H alt cismi varsa H^*, K^* ın bir alt grubudur ve dolayısıyla Lagrange teoremine göre $|H^*| = p^m - 1$, $|K^*| = p^n - 1$ i böler. $p^m - 1 \mid p^n - 1$ den Lemma 3.4.8(1) e göre $m \mid n$ elde edilir.

Yeterlik. $m \mid n$ ise p^n elemanlı K cisminin p^m elemanlı bir alt cismi vardır: Lemma 3.4.6 daki gibi, K da $a^{p^m} = a$ koşulunu gerçekleyen bütün a elemanlarının kümesini gözönüne alalım ve $K_1 = \left\{ a \in K \mid a^{p^m} = a \right\}$ diyelim. $1_K \in K_1$ olduğundan K_1 boş değildir ve her $a, b \in K_1$ için

$(a+b)^{p^m} = a^{p^m} + b^{p^m} = a + b$ (Lemma 3.4.3 e göre) olduğundan $a + b \in K_1$,

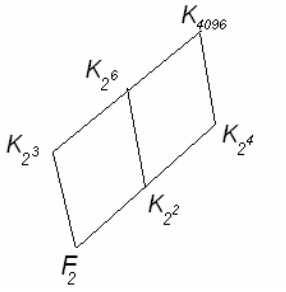
$(-b)^{p^m} = [(-1_K) \cdot b]^{p^m} = (-1_K)^{p^m} \cdot b^{p^m} = (-1_K) \cdot b$ " $-b \in K_1$,

$(a \cdot b)^{p^m} = a^{p^m} \cdot b^{p^m} = a \cdot b$ " $a \cdot b \in K_1$,

$(1_K / b)^{p^m} = 1_K / b^{p^m} = 1_K / b$ ($b \neq 0_K$ olmak koşuluyla) " $1_K / b \in K_1$

dir, dolayısıyla K_1, K nın bir alt cismidir. Şimdi K_1 in tam p^m tane elemanının bulunduğunu gösterelim. $m \mid n$ olduğundan Lemma 3.4.8(3) e göre $K[x]$ te $x^{p^m} - x \mid x^{p^n} - x$ tir. O halde Lemma 3.4.5(4) e göre $x^{p^m} - x$ polinomunun tam p^m tane kökü vardır ve bu kökler, ikişer ikişer birbirinden farklıdır ve $x^{p^m} - x$ in kökleri, K_1 in elemanlarından ibarettir. Şu halde K_1 in gerçekten tam p^m tane elemanı vardır. Bu ise $m \mid n$ olduğunda K nın p^m elemanlı bir K_1 alt cisminin mevcut olduğunu kanıtlar. Üstelik, p^m elemanlı tek alt cisim vardır. K_2, K nın bir alt cismi ve $|K_2| = p^m$ ise, K_2 nin herhangi bir b elemanı, Lemma 3.4.6 ya göre $b^{p^m} = b$ eşitliğini gerçekler ve dolayısıyla $K_2 \subset K_1$ dir ki, buradan da $K_1 = K_2$ sonucu çıkar.

Teorem 3.4.9 a bir örnek olarak, K_{4096} nın $4096 = 2^{12}$ elemanlı bir cisim olduğunu farzedelim. Bu takdirde K_q, q elemanlı bir cismi göstermek üzere, K_{4096} nın bütün alt cisimleri, aşağıdaki şekilde görüldüğü gibidir:



Özellikle, 4096 elemanlı bir cismin varlığını kabul etmekle, aynı zamanda $2^1, 2^2, 2^3, 2^4, 2^6$ elemanlı bir cismin de varlığı sonucuna varabiliriz. Fakat 4096 elemanlı bir cismin gerçekten var olup olmadığını bilmiyoruz, dolayısıyla yukarıki iddia çok zayıftır. Aslında herhangi bir *p* asal sayısı ve herhangi bir *n* doğal sayısı için p^n elemanlı bir cismin varlığı doğrudur. Bu iddiayı ispat edeceğiz. Bunun için elemanter sayılar teorisinden bazı sonuçlara ihtiyacımız vardır.

Aşağıda $\sum_{d|n} a_d$ gösterimini kullanacağız. Bu şu anlama gelmektedir: $n \in \mathbb{N}$ dir ve *d*, *n* nin (1 ve *n* de dahil) bütün pozitif bölenlerini dolaşmak üzere, a_d terimlerinin toplamı alınmaktadır. Örneğin $\sum_{d|12} a_d = a_1 + a_2 + a_3 + a_4 + a_6 + a_{12}$ ve $\sum_{d|15} a_d = a_1 + a_3 + a_5 + a_{15}$ tir. Aşikar olarak $\sum_{d|n} a_d = \sum_{d|n} a_{n/d}$ dir. $\prod_{d|n} a_d$ ve $\bigcup_{d|n} S_d$ gösterimleri, benzer anlamlar taşıyacaktır.

Lemma 3.4.10. φ, Euler fonksiyonu olmak üzere, her $n \in \mathbb{N}$ için

$$\sum_{d|n} \varphi(d) = n$$

dir.

İspat. Her $k \in \mathbb{N}$ için $\varphi(k)$, *k* yı geçmeyen ve *k* ile aralarında asal olan doğal sayıların sayısı olarak tanımlanmıştır. $1, 2, ..., n$ sayılarından herhangi birinin *n* ile en büyük ortak böleni, *n* nin *d* gibi bir pozitif bölenidir. Dolayısıyla

$$S_d = \left\{ k \in \mathbb{N} \mid k \le n \ , \ (k, n) = d \right\}$$

olmak üzere,

$$\{1, 2, ..., n\} = \bigcup_{d|n} S_d$$

dir. Son eşitlikten $n = \left| \{1, 2, ..., n\} \right| = \sum_{d|n} |S_d|$ elde edilir. Burada

$$
\begin{aligned}
S_d &= \{k \in \mathbb{N} : k \le n,\ (k,n) = d\} \\
&= \{k \in \mathbb{N} : k \le n,\ d \mid k,\ (k,n) = d\} \\
&= \{k \in \mathbb{N} : k \le n,\ k = db\ (b \in \mathbb{N}),\ (k,n) = d\} \\
&= \{db \in \mathbb{N} : db \le n,\ (db,n) = d\} \\
&= \left\{db \in \mathbb{N} : db \le n,\ \left(db, d \cdot \frac{n}{d}\right) = d\right\} \\
&= \left\{db \in \mathbb{N} : 1 \le b \le \frac{n}{d},\ \left(b, \frac{n}{d}\right) = 1\right\}
\end{aligned}
$$

dir. O halde $|S_d|$, $1 \le b \le \frac{n}{d}$ ve $\left(b, \frac{n}{d}\right) = 1$ koşullarına uyan *b* doğal sayılarının sayısına, yani $\varphi(n/d)$ ye eşittir. Buradan

$$n = \sum_{d|n} |S_d| = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d)$$

elde edilir.

Bir sonraki lemmanın ifadesinde kolaylık sağlaması açısından bazı tanımlamalar yapacağız: $m \in \mathbb{N}$ olmak üzere, bir *mod.m tam kalan sistemi, m* tane tam sayıdan oluşan bir küme olarak tanımlanır, öyle ki,bu tam sayılardan her biri, $1, 2, ..., m$ den bir ve yalnız birine *mod.m* kongrüdür. O halde *mod.m* bir tam kalan sistemi öyle bir $\{r_1, r_2, ..., r_m\} \subset \mathbb{N}$ kümesidir ki, $r_1, r_2, ..., r_m$ nin mod.*m* kalan sınıfları, $\mathbb{Z}_m$ yi oluştururlar. Özellikle r_i $(i = 1, ..., m)$ tam sayıları *mod.m* birbirlerine kongrü değildirler (ve tabii ki, birbirlerinden farklıdırlar). $r_1, r_2, ..., r_m$ *mod.m* birbirine kongrü olmayan tam sayılar ise $\{r_1, r_2, ..., r_m\}$ kümesi *mod.m* bir tam kalan sistemidir. Aynı zamanda, her tam sayı $r_1, r_2, ..., r_m$ tam sayılarından birine *mod.m* kongrü ise, $\{r_1, r_2, ..., r_m\}$ kümesi gene *mod.m* bir tam kalan sistemi oluşturur.

Mod.m bir indirgenmiş kalan sistemi, $\varphi(m)$ tane tam sayıdan oluşan bir küme olarak tanımlanır, öyle ki, tam sayılardan herbiri, $1, 2, ..., m$ tam sayıları içinde *m* ile aralarında asal olanlardan bir ve yalnız birine *mod.m* kongrüdür. O halde *mod.m* bir indirgenmiş kalan sistemi öyle bir $\{a_1, a_2, ..., a_{\varphi(m)}\} \subset \mathbb{N}$ kümesidir ki, $a_1, a_2, ..., a_{\varphi(m)}$ nin *mod.m* kalan sınıfları, $\mathbb{Z}_m^*$ ı oluştururlar. Özellikle a_i $(i = 1, ..., \varphi(m))$ ler birbirlerine *mod.m* kongrü değildirler (ve tabii ki, birbirlerinden farklıdırlar). $a_1, a_2, ..., a_{\varphi(m)}$ *m* ile aralarında asal olan ve *mod.m* birbirlerine kongrü olmayan tam sayılar ise, $\{a_1, a_2, ..., a_{\varphi(m)}\}$ *mod.m* bir indirgenmiş kalan sistemidir. Aynı zamanda, *m* ile aralarında asal olan her tam sayı $a_1, a_2, ..., a_{\varphi(m)}$ tam sayılarından birine *mod.m* kongrü ise $\{a_1, a_2, ..., a_{\varphi(m)}\}$ kümesi gene bir *mod.m* indirgenmiş kalan sistemidir.

Lemma 3.4.11. $m,n \in \mathbb{Z}$ ve (*m,n*)=1 olsun. Bu takdirde:

(1) $\{r_1, r_2, ..., r_m\} \subset \mathbb{Z}$ bir *mod.m* tam kalan sistemi ve $\{s_1, s_2, ..., s_n\} \subset \mathbb{Z}$ bir *mod.n* tam kalan sistemi ise

$$\{ms_i + nr_j : i = 1, ..., m; j = 1, ..., n\} \subset \mathbb{Z}$$

bir *mod.mn* tam kalan sistemidir.

(2) $\{a_1, a_2, ..., a_{\varphi(m)}\} \subset \mathbb{Z}$ bir *mod.m* indirgenmiş kalan sistemi ve $\{b_1, b_2, ..., b_{\varphi(n)}\} \subset \mathbb{Z}$ bir *mod.n* indirgenmiş kalan sistemi ise

$$\{ma_i + nb_j : i = 1, ..., \varphi(m); j = 1, ..., \varphi(n)\} \subset \mathbb{Z}$$

bir *mod.mn* indirgenmiş kalan sistemidir.

(3) $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

İspat. (1) *mn* tane $ms_i + nr_j$ tam sayılarının birbirinden farklı herhangi iki tanesinin mod.*mn* birbirine kongrü olmadığını göstermek yeterlidir. Gerçekten,

$$ms_i + nr_j \equiv ms_{i'} + nr_{j'} \ (mn)$$

ise

$$ms_i + nr_j \equiv ms_{i'} + nr_{j'} \ (m) \text{ ve } ms_i + nr_j \equiv ms_{i'} + nr_{j'} \ (n)$$

$$nr_j \equiv nr_{j'} \ (m) \text{ ve } ms_i \equiv ms_{i'} \ (n)$$

((*m,n*)=1 olduğundan) $r_j \equiv r_{j'} \ (m)$ ve $s_i \equiv s_{i'} \ (n)$

$$r_j = r_{j'} \text{ ve } s_i = s_{i'}$$

olacağından

$$ms_i + nr_j = ms_{i'} + nr_{j'}$$

dür.

(2) $\{a_1, a_2, ..., a_{\varphi(m)}\} \subset \{r_1, r_2, ..., r_m\}$ ve $\{b_1, b_2, ..., b_{\varphi(n)}\} \subset \{s_1, s_2, ..., s_n\}$ olacak şekilde bir $\{r_1, r_2, ..., r_m\}$ *mod.m* ve bir $\{s_1, s_2, ..., s_n\}$ *mod.n* tam kalan sistemi alalım. Burada $\{a_1, a_2, ..., a_{\varphi(m)}\} = \{r_j \,|\, j = 1, ..., m, \ (r_j, m) = 1\}$ ve $\{b_1, b_2, ..., b_{\varphi(n)}\} = \{s_i \,|\, i = 1, ..., n, \ (s_i, n) = 1\}$ dir. Bu durumda $\{ms_i + nr_j \,|\, i = 1, ..., m; j = 1, ..., n\}$, *mod.mn* bir tam kalan sistemidir. O halde $ms_i + nr_j$ ile *mn* nin aralarında asal olması için gerek ve yeter koşulun $(s_i, n) = 1$ ve $(r_j, m) = 1$ olması olduğunu göstermek yeterli olacaktır.

Gereklik. $(ms_i + nr_j, mn) = 1$ ise $(s_i, n) = 1$ ve $(r_j, m) = 1$ dir:

$(s_i, n) > 1$ olsa

$$\left.\begin{array}{l} (s_i, n) \,|\, ms_i + nr_j \\ (s_i, n) \,|\, mn \end{array}\right\} \Rightarrow (s_i, n) \,|\, (ms_i + nr_j, mn) \Rightarrow (ms_i + nr_j, mn) > 1$$

olur. Benzer şekilde $(r_j, m) > 1$ olsa $(ms_i + nr_j, mn) > 1$ olur. Oysa hipoteze göre $(ms_i + nr_j, mn) = 1$ dir. Şu halde $(s_i, n) = 1$ ve $(r_j, m) = 1$ olmak zorundadır.

Yeterlik. $(s_i, n) = 1$ ve $(r_j, m) = 1$ ise $(ms_i + nr_j, mn) = 1$ dir:

d=$(ms_i + nr_j, mn)$ diyelim. $d > 1$ olsa $p \mid d$ olacak şekilde bir *p* asal sayısı bulunur.

$$p \mid d \Rightarrow p \mid mn \Rightarrow p \mid m \vee p \mid n$$

$$p \mid m \text{ ise } p \mid ms_i \;;\; p \mid d \Rightarrow \left.\begin{matrix} p \mid ms_i + nr_j \\ p \mid ms_i \end{matrix}\right\} \Rightarrow p \mid nr_j$$

$$p \mid m,\ (m,n) = 1 \Rightarrow (p,n) = 1$$

$$p \mid nr_j \ ,\ (p,n) = 1 \overset{A.E.Y.T.}{\Rightarrow} p \mid r_j$$

olur ve $p \mid m$, $p \mid r_j$ den $p \mid (m, r_j) = 1$ gibi bir çelişki elde edilir. Benzer şekilde, $p \mid n$ ise $p \mid (n, s_i) = 1$ gibi bir çelişki elde edilir. O halde $(ms_i + nr_j, mn) = 1$ olmak zorundadır.

(3) (2) ye göre *mod.mn* bir indirgenmiş kalan sisteminin eleman sayısı $\varphi(m) \cdot \varphi(n)$ dir. O halde *m* ile *n* aralarında asal olduğunda $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ dir.

k ya göre tümevarımla şu genelleştirmeye varabiliriz: İkişer ikişer aralarında asal olan $m_1, m_2, ..., m_k$ doğal sayıları için

$$\varphi(m_1.m_2...m_k) = \varphi(m_1).\varphi(m_2)...\varphi(m_k)$$

dır. Özellikle $n \in \square$ ise ve *n* nin kanonik ayrılışı $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ şeklinde ise

$$\varphi(n) = \varphi(p_1^{\alpha_1}).\varphi(p_2^{\alpha_2})...\varphi(p_k^{\alpha_k})$$

dır.

Şimdi, *p* bir asal sayı olmak üzere, $\varphi(p^\alpha)$ yı kapalı şekilde bulmak kolaydır: p^α tane $1, 2, ..., p^\alpha$ tam sayısı içinde tam $p^{\alpha-1}$ tanesi, yani

$$p \cdot 1, p \cdot 2, ..., p \cdot p^{\alpha-1}$$

tam sayıları, *p* ile aralarında asal değildir, dolayısıyla tam $p^\alpha - p^{\alpha-1}$ tanesi *p* ile aralarında asaldır. Bu ise $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ demektir. $\varphi(p^\alpha)$ aynı zamanda

$$\varphi(p^\alpha) = p^\alpha \left(1 - \frac{1}{p}\right)$$

olarak da yazılabilir.

O halde $n \in \square$, $n > 1$ ise ve *n* nin kanonik ayrılışı $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ şeklinde ise

$$\begin{aligned}\varphi(n) &= (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1})...(p_k^{\alpha_k} - p_k^{\alpha_k-1}) \\ &= p_1^{\alpha_1-1}p_2^{\alpha_2-1}...p_k^{\alpha_k-1}(p_1-1)(p_2-1)...(p_k-1) \\ &= p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right) \\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right)\end{aligned}$$

dır. Son ifadeyi açarak

$$\varphi(n) = n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_k}\right) + \left(\frac{n}{p_1p_2} + \frac{n}{p_1p_3} + \cdots + \frac{n}{p_{k-1}p_k}\right) + - \cdots + (-1)^k\left(\frac{n}{p_1p_2\cdots p_k}\right)$$

elde ederiz. O halde *d*, *n* nin farklı asal bölenlerinin bir çarpımını göstermek üzere, $\varphi(n)$, $\mp\frac{n}{d}$ biçimindeki terimlerin toplamına eşittir ve işaret, asal bölenlerin sayısının tek veya çift oluşuna göre "$-$" veya "+" dır. Şu halde $\varphi(n)$,

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

şeklinde yazılabilir. Burada, *d* uygun bir asal sayının karesi ile bölünebilir ise $\mu(d) = 0$ dır, aksi halde *d* nin farklı asal bölenlerinin sayısının çift veya tek oluşuna göre $\mu(d) = 1$ veya $\mu(d) = -1$ dir.

Tanım 3.4.12.

$\mu(1) = 1,$
$\mu(n) = (-1)^r$ (*n*, *r* tane farklı asal sayının çarpımı biçiminde ise)
$\mu(n) = 0$ (*n*, bir asal sayının karesi ile bölünebiliyorsa)

şeklinde tanımlanan $\mu : \square \to \square$ fonksiyonuna *Möbius fonksiyonu* denir.

Örneğin

$$\mu(1) = 1, \quad \mu(2) = -1, \quad \mu(3) = -1, \quad \mu(4) = 0, \quad \mu(5) = -1,$$
$$\mu(6) = 1, \quad \mu(7) = -1, \quad \mu(8) = 0, \quad \mu(9) = 0, \quad \mu(10) = 1$$

dir.

$n = \sum_{d|n} \varphi(d)$ ve $\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$ formülleri birbirine eşdeğerdir. Bu, *Möbius Ters Çevirme Formülü* olarak bilinen ve $\sum_{d|n} a_d$ bölenler toplanı ile a_d yi birbirine bağlayan bir formülün özel halidir. Bu formülü vermeden önce şu lemmaya ihtiyacımız vardır:

Lemma 3.4.13. Bir $n \in \square$ verildiğine göre, $\sum_{d|n} \mu(d)$ toplamı, $n = 1$ için 1 e, $n > 1$ için 0 a eşittir.

İspat. $n=1$ ise

$$\sum_{d|n}\mu(d)=\sum_{d|1}\mu(d)=\mu(1)=1$$

dir. $n>1$ ise ve n nin kanonik ayrılışı $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ biçiminde ise

$$\begin{aligned}\sum_{d|n}\mu(d)=\sum_{d|p_1p_2\cdots p_k}\mu(d)&=\mu(1)+(\mu(p_1)+\mu(p_2)+...+\mu(p_k))\\&\quad+(\mu(p_1p_2)+\mu(p_1p_3)+...+\mu(p_{k-1}p_k))\\&\quad+(\mu(p_1p_2p_3)+...+\mu(p_{k-2}p_{k-1}p_k))\\&\quad+...+\mu(p_1p_2...p_k)\\&=1+\binom{k}{1}(-1)^1+\binom{k}{2}(-1)^2+\binom{k}{3}(-1)^3+...+\binom{k}{k}(-1)^k\\&=(1-1)^k=0\end{aligned}$$

dır.

Lemma 3.4.14 (Möbius Ters Çevirme Formülü). K bir cisim ve $f:\mathbb{N}\to K$ herhangi bir fonksiyon olsun. $F:\mathbb{N}\to K$ fonksiyonunu

$$F(n)=\sum_{d|n}f(d)\qquad(\forall n\in\mathbb{N})$$

şeklinde tanımlayalım. Bu durumda her $n\in\mathbb{N}$ için

$$f(n)=\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)$$

dir.

İspat. $n\in\mathbb{N}$ olsun. n nin herhangi bir d pozitif böleni için

$$F\left(\frac{n}{d}\right)=\sum_{b\left|\frac{n}{d}\right.}f(b),$$

$$\mu(d)F\left(\frac{n}{d}\right)=\sum_{b\left|\frac{n}{d}\right.}\mu(d)f(b),$$

$$\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d|n}\sum_{b\left|\frac{n}{d}\right.}\mu(d)f(b)$$

dir. Son toplam, n nin $db\,|\,n$ koşuluna uyan pozitif bölenlerinin bütün (d,b) sıralı ikilileri üzerinden alınmaktadır. Bu toplam, aynı zamanda n nin $bd\,|\,n$ koşuluna uyan pozitif bölenlerinin bütün (b,d) sıralı ikilileri üzerinden alınan toplamdır. O halde

$$\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{b|n}\sum_{d\left|\frac{n}{b}\right.}\mu(d)f(b)=\sum_{b|n}f(b)\left(\sum_{d|n/b}\mu(d)\right)=f(n)$$

dir, çünkü Lemma 3.4.13 e göre, $\sum_{d|n/b} \mu(d)$ toplamı $b=n$ için 1 e, *b, n* nin bir has böleni ise 0 a eşittir.

Lemma 3.4.15. *K* bir cisim ve $f:\mathbb{N}\to K^*$ herhangi bir fonksiyon olsun. $F:\mathbb{N}\to K$ fonksiyonunu

$$F(n)=\prod_{d|n} f(d) \quad (\forall n\in\mathbb{N})$$

şeklinde tanımlayalım. Bu durumda her $n\in\mathbb{N}$ için

$$f(n)=\prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)} =\prod_{d|n} F(d)^{\mu\left(\frac{n}{d}\right)}$$

dir.

İspat. $n\in\mathbb{N}$ olsun.

$$F\left(\frac{n}{d}\right)=\prod_{b\left|\frac{n}{d}\right.} f(b)$$

olduğundan

$$F\left(\frac{n}{d}\right)^{\mu(d)} =\prod_{b\left|\frac{n}{d}\right.} f(b)^{\mu(d)},$$

$$\prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)} =\prod_{d|n}\prod_{b\left|\frac{n}{d}\right.} f(b)^{\mu(d)}$$

ve dolayısıyla

$$\prod_{d|n} F\left(\frac{n}{d}\right)^{\mu(d)} =\prod_{b|n}\prod_{d\left|\frac{n}{b}\right.} f(b)^{\mu(d)} =\prod_{b|n}\left(f(b)^{\sum_{d|n/b}\mu(d)}\right)=f(n)$$

dir.

Şimdi tekrar sonlu cisimlere dönelim. Her *p* asal sayısı ve her *n* doğal sayısı için, p^n elemanlı bir sonlu cismin bulunduğunu ve eleman sayıları aynı olan herhangi iki sonlu cismin birbirine izomorf olduğunu ispatlayacağız. Öncelikle, asal çarpanlara ayrılışın tek olduğu $\mathrm{F}_p[x]$ halkasında $x^{p^n}-x\in\mathrm{F}_p[x]$ in asal polinomlara ayrılışıyla işe başlayalım. Burada $x^{p^n}-x$ in bütün asal çarpanlarının birbirinden farklı olduğu ve $\mathrm{F}_p[x]$ te bir asal polinomun $x^{p^n}-x$ i bölmesi için gerek ve yeter koşulun, derecesinin *n* yi bölmesi olduğu sonucu çıkacaktır.

Teorem 3.4.16. *p* bir pozitif asal sayı olsun ve $F_d(x)$, $\mathrm{F}_p[x]$ te dereceleri *d* olan bütün monik asal polinomların çarpımı olsun ($\mathrm{F}_p[x]$ te derecesi *d* olan hiçbir monik asal polinom yoksa $F_d(x)$, $1\in\mathrm{F}_p[x]$ sabit polinomuna eşit olsun). Bu takdirde $\mathrm{F}_p[x]$ te

$$x^{p^n} - x = \prod_{d|n} F_d(x)$$

tir.

İspat. $x^{p^n} - x$ in bütün kökleri basittir, çünkü $x^{p^n} - x$ ile $x^{p^n-1} - 1$ türevi, aralarında asaldır. Şu halde $x^{p^n} - x$, $\mathrm{F}_p[x]$ te herhangi bir polinomun karesi ile bölünemez. Özellikle $x^{p^n} - x$, $\mathrm{F}_p[x]$ te asal çarpanlarından herhangi birinin karesi ile bölünemez.

$f(x)$ in $\mathrm{F}_p[x]$ te bir monik asal polinom olduğunu farzedelim ve $d = deg\, f(x)$ olsun. *f*(*x*) in bir *a* kökünü F_p ye katarak $\mathrm{F}_p(a)$ cismini oluşturalım. *f*(*x*), *a* nın F_p üzerindeki minimal polinomudur, dolayısıyla $\left|\mathrm{F}_p(a) : \mathrm{F}_p\right| = deg\, f(x) = d$ dir ve $\mathrm{F}_p(a)$, p^a elemanlı bir cisimdir. Bu nedenle, Lemma 3.4.5(3) e göre, her $b \in \mathrm{F}_p(a)$ için $b^{p^a} = b$ dir. Şimdi, $\mathrm{F}_p[x]$ te $f(x) \left| x^{p^n} - x \right.$ olması için gerek ve yeter koşulun □ de $d|n$ olması olduğunu ispatlamalıyız.

Yeterlik. □ de $d|n$ ise $\mathrm{F}_p[x]$ te $f(x) \left| x^{p^n} - x \right.$ tir: $a \in \mathrm{F}_p(a)$ olduğundan $a^{p^d} = a$ dır, dolayısıyla *a*, $x^{p^d} - x \in \mathrm{F}_p[x]$ in bir köküdür. *f*(*x*), *a* nın F_p üzerindeki minimal polinomu olduğundan, $f(x) \left| x^{p^d} - x \right.$ olmak zorundadır. $d|n$ olduğundan Lemma 3.4.8(3) e göre $x^{p^d} - x \left| x^{p^n} - x \right.$ tir ki, buradan da $f(x) \left| x^{p^n} - x \right.$ sonucu çıkar.

Gereklik. $\mathrm{F}_p[x]$ te $f(x) \left| x^{p^n} - x \right.$ ise □ de $d|n$ dir: $f(x) \left| x^{p^n} - x \right.$ olduğunu varsayalım. Bu durumda uygun bir $g(x) \in \mathrm{F}_p[x]$ için $f(x) \cdot g(x) = x^{p^n} - x$ ve dolayısıyla $f(a) \cdot g(a) = a^{p^n} - a = 0_K$ dır. O halde *a*, $x^{p^n} - x$ in bir köküdür. Diğer taraftan $\mathrm{F}_p(a)$ nın her elemanı, $x^{p^n} - x$ in bir köküdür. Çünkü $b \in \mathrm{F}_p(a)$ ise $f_0, f_1, ..., f_{d-1} \in \mathrm{F}_p$ olmak üzere, $b = f_0 + f_1.a + f_2.a^2 + ... + f_{d-1}.a^{d-1}$ dir ki, buradan

$$\begin{aligned} b^{p^n} &= (f_0 + f_1.a + f_2.a^2 + ... + f_{d-1}.a^{d-1})^{p^n} \\ &= {f_0}^{p^n} + {f_1}^{p^n}.a^{p^n} + {f_2}^{p^n}.(a^2)^{p^n} + ... + {f_{d-1}}^{p^n}.(a^{d-1})^{p^n} \\ &= f_0 + f_1.a + f_2.a^2 + ... + f_{d-1}.a^{d-1} \\ &= b \end{aligned}$$

elde edilir. Lemma 3.4.5(3) e göre $\mathrm{F}_p(a)$ nın elemanları, $x^{p^d} - x$ in kökleriyle çakıştığından, $x^{p^d} - x$ in her kökünün $x^{p^n} - x$ in de bir kökü olduğu görülür. O halde $x^{p^d} - x \left| x^{p^n} - x \right.$ tir ve dolayısıyla Lemma 3.4.8(3) e göre $d|n$ dir.

Lemma 3.4.17. *p* bir asal sayı, N_d de $\mathrm{F}_p[x]$ te derecesi *d* olan monik asal polinomların sayısı olsun. $F_d(x)$ ise $\mathrm{F}_p[x]$ te derecesi *d* olan N_d tane monik asal polinomun çarpımı olsun ($N_d = 0$ ise $F_d(x) = 1_F$ dir). Bu takdirde her $n \in \mathbb{N}$ için

(1) $p^n = \sum_{d|n} dN_d$,

(2) $F_n(x) = \prod_{d|n} (x^{p^d} - x)^{\mu(n/d)}$,

(3) $N_n = \frac{1}{n} \sum_{d|n} \mu(n/d) p^d$,

(4) $N_n > 0$

dır.

İspat. (1) $x^{p^n} - x = \prod_{d|n} F_d(x)$ eşitliğinin her iki tarafındaki polinomların dereceleri eşitlenerek, formülün doğru olduğu görülür.

(2) Lemma 3.4.15, $n \in \mathbb{N}$ yi $F_n(x)$ e götüren $F : \mathbb{N} \to \mathrm{F}_p(x)$ tasviri ile uygulanarak, $x^{p^n} - x = \prod_{d|n} F_d(x)$ eşitliğinden sonuç elde edilir.

(3) (1) den Möbius Ters Çevirme Formülü yardımıyla istenen eşitlik elde edilir.

(4) Tanım gereği $N_n \geq 0$ dır. $N_n = 0$ olsa, (3) e göre $\sum_{d|n} \mu(n/d) p^d = 0$ olur. Bu eşitliğin her iki tarafı $\mu(n/d) \neq 0$ koşuluna uyan p^d lerin en küçüğü olan p^{d_0} ile bölünerek $-\mu(n/d_0) = \sum_{\substack{d|n \\ d \neq d_0}} \mu(n/d) p^{d-d_0}$ şeklinde bir eşitlik elde edilir ki, bu eşitliğin sağ tarafı *p* ile bölünebilir, ancak sol tarafı *p* ile bölünemez. Şu halde $N_n > 0$ olmak zorundadır.

Teorem 3.4.18. *n* bir doğal sayı ve *p* bir asal sayı olsun. Bu takdirde p^n elemanlı bir sonlu cisim vardır.

İspat. Lemma 3.4.17(4) e göre $\mathrm{F}_p[x]$ te *n*. dereceden bir *f*(*x*) asal polinomu vardır. *K*, *f*(*x*) in bir kökünü F_p ye katmakla elde edilen cisim olsun. Bu takdirde Teorem 3.2.8 e göre $|K : \mathrm{F}_p| = n$ dir ve *K*, p^n elemanlı bir cisimdir.

Teorem 3.4.19. *K* bir cisim ve *G*, K^* ın sonlu bir alt grubu olsun. Bu durumda *G* devreseldir. Özellikle, *K* sonlu bir cisim ise K^* da devreseldir.

İspat. $n=|G|$ olsun. *G* nin herhangi bir *g* elemanının mertebesi, *n* nin bir bölenidir. O halde *G* yi bir ayrık birleşim olarak

$$G=\bigcup_{d|n}\{g\in G:|g|=d\}$$

şeklinde yazabiliriz. Buradan, $\psi(d)$, *G* de mertebesi *d* olan elemanların sayısını göstermek üzere,

$$n=|G|=\sum_{d|n}\psi(d)$$

elde edilir.

Şimdi $\psi(d)$ nin ya sıfıra ya da $\varphi(d)$ ye eşit olduğunu göstereceğiz. *G* de mertebesi *d* olan hiçbir eleman yoksa tabii ki, $\psi(d)=0$ dır. *G* de mertebesi *d* olan bir *g* elemanı varsa, bu takdirde *g* tarafından doğurulan <*g*> devresel grubundaki *d* tane elemanın herbiri $g^d=1_G$ eşitliğini sağlar. O halde bu elemanlar, $x^d-1\in K[x]$ polinomunun köküdür, dolayısıyla bu polinomun *K* da en az *d* tane kökü vardır. Diğer taraftan, bu polinomun *K* da en fazla *d* tane kökü bulunabilir. Şu halde bu polinomun *K* da tam *d* tane kökü vardır ki, bu kökler <*g*> nin elemanlarıdır. O halde *G* nin mertebesi *d* olan her elemanı (ki, bu eleman x^d-1 polinomunun bir kökü olmak zorundadır) <*g*> alt grubunun bir elemanıdır ve <*g*> deki bir elemanın mertebesinin *d* olması için gerek ve yeter koşul, o elemanın <*g*> nin bir doğurayı olmasıdır. O halde *G* nin mertebesi *d* olan elemanları, <*g*> nin doğurayları ile çakışır. <*g*> nin $\varphi(d)$ tane doğurayı olduğuna göre, *G* de mertebesi *d* olan $\varphi(d)$ tane eleman vardır, yani iddia edildiği gibi, $\psi(d)=\varphi(d)$ dir.

n nin herhangi bir pozitif *d* böleni için $\psi(d)\le\varphi(d)$ olduğundan, $n=\sum_{d|n}\psi(d)\le\sum_{d|n}\varphi(d)=n$ elde edilir. Buradan *n* nin her *d* pozitif böleni için $\psi(d)=\varphi(d)$ sonucu çıkar. Özellikle $\psi(n)=\varphi(n)>0$ ise G de mertebesi *n* olan bir *a* elemanı vardır. Şu halde *G*, *a* tarafından doğurulan devresel gruptur, yani *G*=<*a*> dır.

Teorem 3.4.20. *K*, p^n elemanlı bir cisim ve *t*, K^* devresel grubunun bir doğurayı olsun. Bu takdirde

(1) $K=\mathrm{F}_p(t)$,

(2) *t* nin F_p üzerindeki minimal polinomunun derecesi *n* dir,

(3) K_1, p^n elemanlı herhangi bir cisim ise, *t* nin F_p üzerindeki minimal polinomunun K_1 de bir kökü vardır.

İspat. (1) $0_K\in\mathrm{F}_p(t)$ olduğundan ve *K* nın 0_K dan farklı her elemanı, *t* nin bir kuvveti şeklinde olması nedeniyle $\mathrm{F}_p(t)$ ye ait olduğundan $K\subset\mathrm{F}_p(t)$ dir. Buradan $K=\mathrm{F}_p(t)$ elde edilir.

(2) t nin F_p üzerindeki minimal polinomunun derecesi, $\left|\mathrm{F}_p(t):\mathrm{F}_p\right| = \left|K:\mathrm{F}_p\right| = n$ dir.

(3) t nin F_p üzerindeki minimal polinomunun derecesi n ye eşit ve dolayısıyla n nin bir böleni olduğundan, Teorem 3.4.16 ya göre bu polinom, $x^{p^n} - x$ in bir bölenidir ve Lemma 3.4.5(3) e göre bu polinomun K_1 de birbirinden farklı n tane kökü vardır, dolayısıyla bu polinomun K_1 de bir kökü bulunur.

Teorem 3.4.21. Eleman sayıları aynı olan herhangi iki sonlu cisim, birbirine izomorftur.

İspat. K ve K_1, p^n elemanlı iki cisim olsun. Bu takdirde Teorem 3.4.19 a göre K^* bir devresel gruptur. t, K^* ın bir doğurayı olsun. Bu durumda Teorem 3.4.20(1) e göre $K = \mathrm{F}_p(t)$ dir. t nin F_p üzerindeki minimal polinomu $f(x) \in \mathrm{F}_p[x]$ olsun. Teorem 3.4.20(3) e göre $f(x)$ in K_1 de c gibi bir kökü vardır. K_1 in F_p üzerinde c tarafından doğurulan alt cismi $\mathrm{F}_p(c) \subset K_1$ olsun. Bu takdirde $n = deg\ f(x) = \left|\mathrm{F}_p(c):\mathrm{F}_p\right| \le \left|K_1:\mathrm{F}_p\right| = n$ den $\mathrm{F}_p(c) = K_1$ olduğu sonucu çıkar. O halde Teorem 3.2.7 den

$$K_1 = \mathrm{F}_p(c) \cong \mathrm{F}_p[x]/(f(x)) \cong \mathrm{F}_p(t) = K$$

elde edilir. Şu halde $K_1 \cong K$ dır.

Bu teorem sayesinde, eleman sayıları aynı olan bütün sonlu cisimleri özdeşleştirebiliriz. O halde q $(q = p^n)$ elemanlı bir tek cisim vardır ki, bu cisim, bundan böyle F_q ile gösterilecektir.

§ 5. Parçalanış Cisimleri

Bu paragrafta, verilen bir K cismi ve bir $f(x) \in K[x] \setminus K$ polinomu için $f(x)$, $E[x]$ te birinci dereceden polinomların bir çarpımı olarak yazılabilecek şekilde, K nın bir E genişleme cisminin bulunmasının mümkün olup olmayacağını araştıracağız.

Bu problem , cisim genişlemeleri teorisindeki şu önemli soruyla bağlantılıdır: Bir cisim izomorfisi, genişleme cisminin bir cisim izomorfisine uzatılabilir mi? Daha açık olarak , E_1 / K_1 ve E_2 / K_2 iki cisim genişlemesi ve $\varphi : K_1 \to K_2$ bir cisim izomorfisi ise $\psi_{|K_1} = \varphi$ olacak şekilde bir $\psi : E_1 \to E_2$ cisim izomorfisi bulunabilir mi? Genel olarak cevap negatiftir, fakat genişlemelerin basit cebirsel genişlemeler olduğu önemli durumda cevap, pozitife döner.

Herhangi bir $\varphi : K_1 \to K_2$ cisim izomorfisi için $\hat{\varphi}\left(\sum_{i=0}^{m} a_i x^i\right) = \sum_{i=0}^{m} \varphi(a_i) x^i$ eşitliği ile tanımlanan $\hat{\varphi} : K_1[x] \to K_2[x]$ tasviri, bir halka izomorfisi idi (Lemma 2.73 , Teorem 2.75).

Lemma 3.5.1. E_1 / K_1 ve E_2 / K_2 iki cisim genişlemesi ve $\varphi : K_1 \to K_2$ bir cisim izomorfisi olsun. $f_1(x) \in K_1[x]$ in $K_1[x]$ te asal bir polinom olduğunu varsayalım ve $f_2(x), f_1(x)$ in $\hat{\varphi}$ tasvirindeki görüntüsü , yani $f_2(x) = \hat{\varphi}(f_1(x)) \in K_2[x]$ olsun. $u_1 \in E_1$, $f_1(x)$ in bir kökü , $u_2 \in E_2$ de $f_2(x)$ in bir kökü olsun. Bundan başka, $K_1(u_1) \subset E_1$, E_1 in u_1 tarafından doğurulan alt cismi , $K_2(u_2) \subset E_2$ de E_2 nin u_2 tarafından doğurulan alt cismi olsun. Bu takdirde φ, $K_1(u_1)$ cismini $K_2(u_2)$ cismine resmeden ve u_1 i u_2 ye götüren bir izomorfiye uzatılabilir, yani $\psi(u_1) = u_2$ ve $\psi_{|K_1} = \varphi$ olacak şekilde bir $\psi : K_1(u_1) \to K_2(u_2)$ cisim izomorfisi vardır. Üstelik, bu özelikleri taşıyan ψ izomorfisi, tek türlü belirlidir.

İspat. İspatta Teorem 3.2.7 ve Teorem 2.54 ü kullanacağız. $u_1, f_1(x)$ in bir kökü ve $f_1(x)$ $K_1[x]$ te asal olduğundan , $c_0, f_1(x)$ in baş katsayısı olmak üzere $c_0^{-1} f_1(x)$, Teorem 3.2.3 e göre u_1 in K_1 üzerindeki minimal polinomudur ($f_1(x)$ asal olduğundan sıfır polinomu veya derecesi sıfır olan bir polinom değildir) Aşikar olarak, $(c_0^{-1} f_1) = (f_1)$ dir. Teorem 3.2.7 den ve Teorem 2.54 ile Tanım 2.55 e dayanan ispatından

$$\alpha : K_1(u_1) \to K_1[x]/(f_1)$$
$$\sum_i a_i u_1^i \to \sum_i a_i (x + (f_1))^i$$

tasvirinin bir cisim izomorfisi olduğunu biliyoruz. Benzer şekilde

$$\beta : K_2(u_2) \to K_2[x]/(f_2)$$
$$\sum_i a_i u_2^i \to \sum_i a_i (x + (f_2))^i$$

tasviri de bir cisim izomorfisidir. Ayrıca

$$\hat{\varphi} : K_1[x] \to K_2[x]$$

gibi bir halka izomorfisi vardır. Burada (f_1), $K_1[x]$ in bir idealidir, bu nedenle $\operatorname{Im}\hat{\varphi}_{|(f_1)} = (f_2)$ de $K_2[x]$ in bir idealidir ve Teorem 2.57(7) ye göre

$$K_1[x]/(f_1) \cong K_2[x]/\operatorname{Im}\hat{\varphi}_{|(f_1)} = K_2[x]/(f_2)$$

dir. Daha açık olarak,

$$\lambda : K_1[x]/(f_1) \to K_2[x]/(f_2)$$
$$g + (f_1) \to \hat{\varphi}(g) + (f_2)$$

tasviri, söz konusu izomorfidir.

O halde , $\beta^{-1}\lambda\alpha : K_1(u_1) \to K_2(u_2)$ tasviri bir halka , aynı zamanda bir cisim izomorfisidir. $\psi = \beta^{-1}\lambda\alpha$ diyelim. Bu takdirde herhangi bir $a \in K_1$ için

$$\psi(a) = (\beta^{-1}\lambda)(\alpha(a)) = (\beta^{-1}\lambda)(a) = (\beta^{-1}\lambda)([a + (f_1)]) = \beta^{-1}[a + (f_2)] = \beta^{-1}(a) = a$$

olur (burada K_1 ve K_2, Kronecker teoreminde olduğu gibi, sırasıyla $K_1[x]/(f_1)$ ve $K_2[x]/(f_2)$ nin bir alt cismi olarak alınmaktadır) ve

$$\psi(u_1) = (\beta^{-1}\lambda)(\alpha(u_1)) = (\beta^{-1}\lambda)([x + (f_1)]) = \beta^{-1}(x + (f_2)) = u_2$$

elde edilir. O halde ψ, φ nin bir uzatılmışı olup, $\psi(u_1) = \psi(u_2)$ dir.

Şimdi ψ nin, istenen koşullara uyan tek izomorfi olduğunu gösterelim. u_1 in kuvvetleri, Teorem 3.2.8 e göre $K_1(u_1)$ in bir K_1-tabanını oluştururlar. $\mu : K_1(u_1) \to K_2(u_2)$, $\mu(u_1) = u_2$ ve $\mu_{|K_1} = \varphi$ koşullarına uyan bir cisim izomorfisi ise μ, $K_1(u_1)$ in herhangi bir $t = \sum_i a_i u_1^i$ $(a_i \in K_1)$ elemanını $\mu(t) = \sum_i \mu(a_i u_1^i) =$ $\sum_i \mu(a_i)(\mu(u_1))^i = \sum_i \varphi(a_i) u_2^i = \psi(\sum_i a_i u_1^i) = \psi(t)$ ye resmeder, dolayısıyla $\mu = \psi$ dir.

Teorem 3.5.2. E_1 / K ve E_2 / K iki cisim genişlemesi olsun. Bundan başka, $u_1 \in E_1$ ve $u_2 \in E_2$, K üzerinde cebirsel olsun. Bu takdirde u_1 in K üzerindeki minimal polinomunun, u_2 nin K üzerindeki minimal polinomu ile çakışması için gerek ve yeter koşul, u_1 i u_2 ye resmeden ve K ya kısıtlanmışı K nın idantik tasviri olan bir (ve sonuçta bir tek) $\psi : K(u_1) \to K(u_2)$ cisim izomorfisinin bulunmasıdır.

İspat. *Gereklik.* u_1 ve u_2 nin K üzerindeki minimal polinomları aynı ise yukarıdaki özelikleri sağlayan bir ψ izomorfisi vardır: Lemma 3.5.1 deki φ yerine $I_K : K \to K$ idantik tasvirini alırsak, bu tasvir, $\psi(u_1) = u_2$ koşuluna uyan, tek türlü belirli bir $\psi : K(u_1) \to K(u_2)$ izomorfisine uzatılabilir.

Yeterlik. $\psi : K(u_1) \to K(u_2)$ tasviri, $\psi(u_1) = u_2$ ve $\psi(a) = a$ $(\forall a \in K)$ koşullarını sağlayan bir cisim izomorfisi ise u_1 ve u_2 nin K üzerindeki minimal polinomları aynıdır: $f(x) = \sum_{i=0}^{m} a_i x^i$, u_1 in K üzerindeki minimal polinomu olsun. Bu takdirde $f(u_1) = \sum_{i=0}^{m} a_i . u_1^i = 0_K$ dır. Buradan

$$0_K = \psi(0_K) = \psi(\sum_{i=0}^{m} a_i . u_1^i) = \sum_{i=0}^{m} \psi(a_i . u_1^i) = \sum_{i=0}^{m} \psi(a_i).\psi(u_1^i) = \sum_{i=0}^{m} a_i . (\psi(u_1))^i$$

$$= \sum_{i=0}^{m} a_i . u_2^i = f(u_2)$$

elde edilir. O halde u_2, $f(x)$ in bir köküdür. Fakat $f(x) \in K[x]$ bir monik asal polinomdur. Bu ise $f(x)$ in, u_2 nin K üzerindeki minimal polinomu olması anlamına gelir.

Not 3.5.3. Lemma 3.5.1 den, her cisim izomorfisinin daha geniş cisimlere uzatılabileceği sonucu çıkarılmamalıdır. Örneğin

$$\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$$
$$a + b\sqrt{2} \to a - b\sqrt{2} \qquad (a, b \in \mathbb{Q})$$

izomorfisini gözönüne alalım. $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt{2})$ nin bir genişleme cismidir. φ izomorfisi, bir $\psi : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ izomorfisine uzatılabilseydi, $-\sqrt{2} = \varphi(\sqrt{2}) = \psi(\sqrt{2}) = \psi((\sqrt[4]{2})^2) = \psi((\sqrt[4]{2}))^2$ olurdu ki, bu bir çelişkidir, çünkü $\psi(\sqrt[4]{2}) (\in \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q})$ nin karesi pozitif olmak zorundadır. O halde φ, $\mathbb{Q}(\sqrt[4]{2})$ cisminin bir izomorfisine uzatılamaz.

Bir polinomun herhangi iki parçalanış cisminin birbirine izomorf oluşu, Lemma 3.5.1 in en önemli uygulamasıdır. Şimdi bu konuyu ele alacağız.

Tanım 3.5.4. E / K bir cisim genişlemesi ve $f(x) \in K[x] \setminus K$ olsun. $f(x)$, $E[x]$ te lineer polinomların bir çarpımı şeklinde yazılabilirse, yani $f(x) = a_0 (x - a_1)(x - a_2)...(x - a_m)$ olacak şekilde $a_0, a_1, a_2, ..., a_m \in E$ varsa $f(x)$ E *de parçalanıyor* denir. $f(x)$, E de parçalanır, fakat E nin K yı kapsayan hiçbir has alt cisminde parçalanmaz ise E ye $f(x)$ *in* K *üzerinde bir parçalanış cismi* denir.

Örnek 3.5.5. $x^2 + 1 \in \mathbb{Q}[x]$ i gözönüne alalım. $\mathbb{Q}[x]$ te $x^2 + 1 = (x + i)(x - i)$ dir ve dolayısıyla $x^2 + 1$, $\mathbb{Q}$ de parçalanır. Fakat $x^2 + 1$, $\mathbb{Q}$ nin $\mathbb{Q}$ yi kapsayan hiçbir has alt cisminde parçalanamaz, çünkü $\mathbb{Q}$, $\mathbb{Q}$ nin $\mathbb{Q}$ yi kapsayan tek has alt cismidir, öyle ki, $x^2 + 1$, $\mathbb{Q}[x]$ te parçalanmaz. O halde $\mathbb{Q}$, $x^2 + 1$ in $\mathbb{Q}$ üzerinde bir parçalanış cismidir.

$\mathbb{R}$, x^2+1 in $\mathbb{R}$ üzerinde bir parçalanış cismi değildir, çünkü x^2+1, $\mathbb{R}(i)\subset\mathbb{C}$ cisminde parçalanır. x^2+1, $\mathbb{R}(i)$ nin $\mathbb{R}$ yu kapsayan tek has alt cismi olan $\mathbb{R}$ da parçalanmaz. Şu halde $\mathbb{R}(i)$, x^2+1 in $\mathbb{R}$ üzerinde bir parçalanış cismidir.

Örnek 3.5.6. $\mathbb{Q}(\sqrt{2})$, $x^2-2\in\mathbb{Q}[x]$ in $\mathbb{Q}$ üzerinde bir parçalanış cismidir.

Örnek 3.5.7. $x^3-2\in\mathbb{Q}[x]$, $\mathbb{Q}(\sqrt[3]{2})$ de parçalanmaz, çünkü $\mathbb{Q}(\sqrt[3]{2})[x]$ te $x^3-2=(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+(\sqrt[3]{2})^2)$ dir ve buradaki ikinci çarpan, $\mathbb{Q}(\sqrt[3]{2})[x]$ te asaldır. Diğer taraftan, $\mathbb{Q}(\sqrt[3]{2},\omega)[x]$ te $x^3-2=(x-\sqrt[3]{2})(x-\omega\sqrt[3]{2})(x-\omega^2\sqrt[3]{2})$ dir ve dolayısıyla x^3-2, $\mathbb{Q}(\sqrt[3]{2},\omega)[x]$ te parçalanır. Aslında $\mathbb{Q}(\sqrt[3]{2},\omega)$, x^3-2 nin $\mathbb{Q}$ üzerindeki bir parçalanış cismidir. Burada $\mathbb{Q}(\sqrt[3]{2},\omega)=\mathbb{Q}(\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2})$ nin $\mathbb{Q}$ üzerinde x^3-2 nin kökleri tarafından doğurulan cisim olduğuna dikkat edelim.

Örnek 3.5.8. E/K bir cisim genişlemesi ve $f(x)\in K[x]$, $n>0$ dereceli bir polinom olsun. E nin $f(x)$ in (çokkatlılıklarıyla sayılan) $a_1,a_2,...,a_n$ köklerini içerdiğini varsayalım. Bu takdirde $H=K(a_1,a_2,...,a_n)$, $f(x)$ in K üzerinde bir parçalanış cismidir. Gerçekten, $a_0\in K$, $f(x)$ in baş katsayısı olmak üzere, $f(x)$, $H[x]$ te $f(x)=a_0(x-a_1)(x-a_2)...(x-a_n)$ şeklinde çarpanlara ayrılır, çünkü her $x-a_k$ çarpanı $H[x]$ e aittir. O halde $f(x)$, $H[x]$ te parçalanır. Diğer taraftan L, E/K nın, $f(x)$ in parçalandığı bir ara cismi ise her k için $x-a_k$, $L[x]$ e ait ve dolayısıyla a_k, L ye aittir. Şu halde $\{a_1,a_2,...,a_n\}\subset L$ ve dolayısıyla $H=K(a_1,a_2,...,a_n)\subset L$ dir. O halde $f(x)$, H nın K yı kapsayan hiçbir has alt cisminde parçalanmaz. Şu halde H, $f(x)$ in K üzerinde bir parçalanış cismidir. Bu aslında, $K(a_1,a_2,...,a_n)$ nin, E/K nın $f(x)$ in K üzerinde bir parçalanış cismi olan tek ara cismi olduğunu gösterir. Özellikle, E nin, $f(x)$ in K üzerinde bir parçalanış cismi olması için gerek ve yeter koşul, $E=K(a_1,a_2,...,a_n)$ olmasıdır.

Örnek 3.5.9. E/K bir cisim genişlemesi, L, bu genişlemenin bir ara cismi ve $f(x)\in K[x]\setminus K$ olsun. E nin, $f(x)$ in K üzerinde bir parçalanış cismi olduğunu varsayalım. Bu takdirde E, aynı zamanda $f(x)$ in L üzerinde bir parçalanış cismidir, çünkü $f(x)$, E de parçalanır, fakat E nin K yı kapsayan hiçbir has alt cisminde parçalanmaz, hatta bunun da ötesinde, E nin L yi kapsayan hiçbir has alt cisminde de parçalanmaz.

Örnek 3.5.10. p bir asal sayı olsun. $x^{p^n}-x$ ile $p^n x^{p^n-1}-1$ türevinin herhangi bir en büyük ortak böleni, $\mathrm{F}_p[x]$ te bir aritmetik birimdir, yani bu polinomlar aralarında asaldır. O halde Teorem 2.92(2) ye göre $x^{p^n}-x\in\mathrm{F}_p[x]$ in

çokkatlı kökü yoktur. Bu durumda $x^{p^n} - x$ in parçalandığı, F_p nin bir genişleme cismi, en azından, $f(x)$ in birbirinden farklı p^n tane kökünü içermek zorundadır. Lemma 3.4.5(3) ten $x^{p^n} - x$ in p^n elemanlı F_{p^n} cisminde parçalandığını biliyoruz. Şu halde F_{p^n}, $x^{p^n} - x$ in F_p üzerinde bir parçalanış cismidir.

Örnek 3.5.11. E/K bir cisim genişlemesi ve $f(x) \in K[x] \setminus K$ olsun. $a_1 \in E$, $f(x)$ in bir kökü ve $L = K(a_1)$, uygun bir $g(x) \in L[x]$ için $f(x) = (x - a_1)g(x)$ olacak şekilde, E nin K üzerinde a_1 tarafından doğurulan alt cismi olsun. $g(x)$ in derecesi pozitif ise ve E, $g(x)$ in L üzerinde bir parçalanış cismi ise E aynı zamanda $f(x)$ in K üzerinde bir parçalanış cismidir. Gerçekten, E, $g(x)$ in L üzerinde bir parçalanış cismi ise $c \in K$ ve $a_2, ..., a_n \in E$ olmak üzere, $g(x) = c(x - a_2)...(x - a_n)$ dir. Örnek 3.5.8 den $E = L(a_2, ..., a_n)$ olduğunu biliyoruz. O halde $E[x]$ te $f(x) = c(x - a_1)(x - a_2)...(x - a_n)$ dir, dolayısıyla $f(x)$, $E[x]$ te parçalanır. Diğer taraftan, E', E/K nın herhangi bir ara cismi ise ve $f(x)$, E' de parçalanırsa, bu takdirde $c(x - a_1)(x - a_2)...(x - a_n)$, $E'[x]$ e aittir, o halde, $a_1 \in E'$, $L = K(a_1) \subset E'$ ve $a_2, ..., a_n \in E'$ dür; buradan $L(a_2, ..., a_n) \subset E'$ ve $E \subset E'$ elde edilir. O halde $f(x)$, E nin K yı kapsayan hiçbir has alt cisminde parçalanmaz. Bu durumda E, $f(x)$ in K üzerinde bir parçalanış cismidir.

Örnek 3.5.12. Örnek 3.5.7 de $\mathbb{Q}(\sqrt[3]{2}, \omega)$ nın, $x^3 - 2$ nin $\mathbb{Q}$ üzerinde bir parçalanış cismi olduğunu görmüştük. Benzer şekilde, $\mathbb{Q}(\sqrt[3]{2})[y]/(y^2 + y + 1)$ ve $\mathbb{Q}(\omega)[y]/(y^3 - 2)$, $x^3 - 2$ nin $\mathbb{Q}$ üzerinde birer parçalanış cismidir (burada y, $\mathbb{Q}$ üzerinde bir değişkendir). Bu cisimlerde $x^3 - 2$, sırasıyla

$$[x - (\sqrt[3]{2} + (y^2 + y + 1))][x - (\sqrt[3]{2}y + (y^2 + y + 1))][x - (\sqrt[3]{2}y^2 + (y^2 + y + 1))]$$

ve

$$[x - (y + (y^3 - 2))][x - (\omega y + (y^3 - 2))][x - (\omega^2 y + (y^3 - 2))]$$

şeklinde parçalanır.

Herhangi bir polinomun bir parçalanış cisminin bulunup bulunmadığı sorusu, doğal olarak insanın aklına geliyor. Şimdi, bu sorunun yanıtının olumlu olduğunu, Kronecker'e ait şu teoremle göstereceğiz:

Teorem 3.5.13. $f(x)$, keyfi bir K cismi üzerinde pozitif dereceli herhangi bir polinom olsun. Bu takdirde K nın bir E genişleme cismi vardır, öyle ki, $|E : K| \leq (deg\, f(x))!$ dir ve E, $f(x)$ in K üzerinde bir parçalanış cismidir.

İspat. İspatı $deg\, f(x) = n$ ye göre tümevarımla yapalım. $n = 1$ ise uygun bir $a, c \in K$ çifti için $f(x) = c(x - a)$ dır, şu halde K, $f(x)$ in K üzerinde bir parçalanış cismidir ve $|E : K| = 1 \leq 1! = 1$ dir. O halde iddia $n = 1$ için doğrudur.

Şimdi $deg\, f(x) = n \geq 2$ olduğunu ve teoremin herhangi bir cisim üzerinde, derecesi $n-1$ olan herhangi bir polinom için doğru olduğunu varsayalım. Teorem 3.3.5 e göre *K* nın, $f(x)$ in bir a kökünü içerecek ve $|L:K| \leq n$ olacak şekilde bir L genişleme cismini oluşturabiliriz. O halde Teorem 2.88 e göre *L*[*x*] te uygun bir $g(x)$ polinomu için $f(x) = (x-a)g(x)$ tir. $deg\, f(x) = n-1$ olduğundan tümevarım hipotezine göre L nin öyle bir E genişleme cismi vardır ki, E, $g(x)$ in L üzerinde bir parçalanış cismidir ve $|E:L| \leq (n-1)!$ dir. Örnek 3.5.11 den E nin, $f(x)$ in K üzerinde bir parçalanış cismi olduğu sonucuna varırız.Üstelik, $|E:K| = |E:L||L:K| \leq (n-1)!|L:K| \leq (n-1)!n = n!$ dir.

Görüyoruz ki, Teorem 3.5.13 te yapılan, Kronecker teoreminin ardarda uygulanmasından başka birşey değildir. $f(x)$ in bütün köklerini içeren bir cisim bulana kadar Teorem 3.3.5 i ard arda kullanırız. Teorem 3.5.13 ün ispatında kökleri ardarda katmak yerine tümevarım yöntemi uygulanmaktadır.

Şimdi teklik sorusuna dönelim. Örnek 3.5.12, bir polinomun birbirinden farklı birçok parçalanış cisminin bulunabileceğini ortaya çıkarmıştır. Ancak, daha önce de işaret ettiğimiz üzere, bir polinomun bütün parçalanış cisimleri, birbirine izomorftur. Bununla ilgili olarak, şu daha genel teoremi ispatlayalım:

Teorem 3.5.14. E_1 / K_1 ve E_2 / K_2 iki cisim genişlemesi ve $\varphi : K_1 \to K_2$ bir cisim izomorfisi olsun. $f_1(x)$, $K_1[x] \setminus K_1$ e ait bir polinom ve $f_2(x) = \hat{\varphi}(f_1(x)) \in K_2[x] \setminus K_2$, $f_1(x)$ in $\hat{\varphi}$ tasvirindeki görüntüsü olsun. E_1, $f_1(x)$ in K_1 üzerinde bir parçalanış cismi ve E_2, $f_2(x)$ in K_2 üzerinde bir parçalanış cismi ise φ, bir $\Phi : E_1 \to E_2$ cisim izomorfisine uzatılabilir ve dolayısıyla $E_1 \cong E_2$ dir.

İspat. E_1, K_1 üzerinde $f_1(x)$ in kökleri tarafından doğurulmuştur. $f_1(x)$ in her kökü K_1 üzerinde cebirsel olduğundan ve sonlu sayıda kök bulunduğundan, Teorem 3.2.16 dan $|E_1 : K_1|$ in sonlu olduğu sonucu çıkar. İspatı $|E_1 : K_1|$ e göre tümevarımla yapacağız. $|E_1 : K_1| = 1$ ise $E_1 = K_1$ dir ve $f_1(x), K_1$ de parçalanır. $f_2(x)$ de K_2 de parçalanır ve $K_2 = E_2$ dir. O halde $E_1 = K_1 \overset{\varphi}{\to} K_2 = E_2$, istenen izomorfidir.

Şimdi $|E_1 : K_1| \geq 2$ olduğunu ve derecesi en çok $n-1$ olan bir parçalanış cismi için, herhangi bir cisim izomorfisinin, o cisimlere karşılık gelen polinomların parçalanış cisimlerinin bir izomorfisine uzatılabildiğini varsayalım. $|E_1 : K_1| \geq 2$ olduğundan ve E_1, K_1 üzerinde $f_1(x)$ in kökleri tarafından doğurulduğundan, $f_1(x)$ in E_1 de olup, K_1 de olmayan bir kökü bulunmalıdır. O halde $u_1, f_1(x)$ in $E_1 \setminus K_1$ e ait bir kökü olsun. $g_1(x) \in K_1[x]$ in, u_1 in K_1 üzerindeki minimal polinomu olduğunu varsayalım ve u_2, $\hat{\varphi}\,(g_1(x)) = g_2(x) \in K_2[x]$ in E_2 deki bir

kökü olsun. Lemma 3.5.1 den φ nin bir $\psi : K_1(u_1) \to K(u_2)$ izomorfisine uzatılabileceğini biliyoruz. $u_1 \in E_1 \setminus K_1$ olduğundan $|K_1(u_1) : K_1| > 1$, Teorem 3.1.21 e göre de $|E_1 : K_1(u_1)| < n$ dir. Örnek 3.5.9 a göre $E_1, f_1(x)$ in $K_1(u_1)$ üzerinde bir parçalanış cismi ve $E_2, f_2(x)$ in $K_2(u_2)$ üzerinde bir parçalanış cismi olduğundan buradan tümevarımla ψ nin bir $\Phi : E_1 \to E_2$ izomorfisine uzatılabileceği sonucuna varırız. Bu Φ tasviri, φ nin istenen uzatılmışıdır.

Teorem 3.5.15. *K* bir cisim ve *f*(*x*), *K*[*x*] te pozitif dereceli herhangi bir polinom olsun. Bu takdirde *f*(*x*) in *K* üzerinde herhangi iki parçalanış cismi, birbirine izomorftur ve bu izomorfi, *K* nın her elemanını sabit bırakan bir izomorfidir.

İspat. E_1 ve E_2 *f*(*x*) in *K* üzerinde iki parçalanış cismi olsun. Teorem 3.5.14 te $K_1 = K = K_2$ ve $\varphi = I_K$ alınırsa, buradan E_1 ile E_2 nin birbirine izomorf olduğu sonucu çıkar.

Bu paragrafın kalan kısmında cebirsel kapalı cisimleri inceleyeceğiz.

Tanım 3.5.16. Bir *K* cisminin hiçbir has cebirsel genişlemesi yoksa, yani *K* nın her *E* cebirsel genişlemesi, *K* ile çakışıyorsa *K* ya *cebirsel kapalı bir cisim* denir.

Teorem 3.5.17. *K* bir cisim olsun. Bu durumda aşağıdaki ifadeler, birbirine denktir:

(1) *K*, cebirsel kapalıdır.
(2) *K*[*x*] teki her asal polinomun derecesi 1 dir.
(3) *K*[*x*] teki pozitif dereceli her polinomun *K* da bir kökü vardır.
(4) *K*[*x*] teki pozitif dereceli her polinom, *K* da parçalanır.

İspat. (1)$\Rightarrow$(2): *K* cebirsel kapalı olsun. *K*[*x*] te derecesi 1 den büyük bir *f*(*x*) asal polinomu bulunsaydı, $E = K[x]/(f)$, *K* nın bir cebirsel genişlemesi ve $K \subset E$ olurdu ki, bu *K* nın hiçbir has cebirsel genişlemesinin bulunmaması varsayımıyla çelişir. O halde *K*[*x*] te her asal polinomun derecesi 1 dir.

(2)$\Rightarrow$(1): *K*[*x*] te her asal polinomun derecesinin 1 olduğunu varsayalım. *K* nın hiçbir has cebirsel genişlemesinin bulunmadığını göstermek istiyoruz. *E*, *K* nın bir has cebirsel genişlemesi olsaydı, bir $a \in E \setminus K$ bulunurdu. Şimdi *a*, *K* üzerinde cebirseldir ve $a \notin K$ olduğundan Lemma 3.1.28(1) e göre *K*(*a*), *K* nın bir has üst cismidir.

$$1 < |K(a) : K| = a \text{ nın } K \text{ üzerindeki minimal polinomunun derecesi}$$
$$= K[x] \text{ teki bir asal polinomun derecesi}=1$$

olur ki, bu da 1<1 çelişkisine neden olur. Şu halde *K* cebirsel kapalıdır.

(2)$\Rightarrow$(3): *K*[*x*] teki her asal polinomun derecesinin 1 olduğunu varsayalım. *f*(*x*), *K*[*x*] te pozitif dereceli herhangi bir polinom olsun. *f*(*x*) in *K* da bir kökünün bulunduğunu göstereceğiz. Gerçekten, *f*(*x*) in her asal böleni $c(x-a)$ $(c, a \in K)$

biçimindedir, o halde bu asal bölenin K da bir a kökü vardır; buradan $f(x)$ in de K da bir a kökünün bulunduğu sonucu çıkar.

$(3) \Rightarrow (4)$: $K[x]$ teki pozitif dereceli her polinomun K da bir kökünün bulunduğunu varsayalım ve $f_1(x) \in K[x] \backslash K$ olsun. Bu takdirde K da, $f_1(x)$ in a_1 gibi bir kökü vardır, dolayısıyla uygun bir $f_2(x) \in K[x]$ için $f_1(x) = (x - a_1) f_2(x)$ tir. $f_2(x)$ pozitif dereceli ise $f_2(x)$ in K da bir a_2 kökü vardır ve uygun bir $f_3(x) \in K[x]$ için $f_2(x) = (x - a_2) f_3(x)$ tir; bu durumda $f_1(x) = (x - a_1)(x - a_2) f_3(x)$ tir. $f_3(x)$ pozitif dereceli ise $f_3(x)$ in K da a_3 gibi bir kökü vardır ve uygun bir $f_4(x) \in K[x]$ için $f_3(x) = (x - a_3) f_4(x)$ tir, dolayısıyla $f_1(x) = (x - a_1)(x - a_2)(x - a_3) f_4(x)$ tir. Bu şekilde derecesi sıfır olan bir $f_n(x)$ polinomu bulunana kadar devam edersek, sonuçta $f_1(x) = (x - a_1)(x - a_2)(x - a_3)...(x - a_{n-1}) f_n$ elde edilir, buradan da $f_1(x)$ in K da parçalandığı sonucu çıkar.

$(4) \Rightarrow (2)$: $K[x]$ te pozitif dereceli her polinomun K da parçalandığını varsayalım ve $f(x)$, $K[x]$ te bir asal polinom olsun. Bu takdirde varsayıma göre $f(x)$, $deg\, f(x)$ tane birinci deceden polinoma parçalanır. $f(x)$ asal olduğundan buradan çarpan sayısı olan $deg\, f(x)$ in 1 olduğu sonucu çıkar. Şu halde $K[x]$ teki her asal polinom, birinci derecedendir.

Cebirsel kapalı bir cisme örnek olarak □ verilebilir. Bu, kompleks katsayılı her polinomun □ de bir kökünün bulunduğunu ifade eden ve *Cebirin Esas Teoremi* olarak bilinen önemli teoremin bir sonucudur. "Cebirin Esas Teoremi" ismi biraz gariptir, çünkü bu teorem ne bir esas teoremdir, ne de cebirin bir teoremidir! Bu teoremin herhangi bir ispatında analizden bazı sonuçlar kullanılmaktadır.

Lemma 3.5.18. E/K bir cisim genişlemesi olsun ve E nin cebirsel kapalı olduğunu varsayalım. K nın E deki cebirsel kapanışı A olsun. Bu takdirde A cebirsel kapalı bir cisimdir.

İspat. $A[x] \backslash A$ daki her polinomun A da bir kökünün bulunduğunu göstermek yeterlidir. $f(x)$, $A[x]$ te pozitif dereceli herhangi bir polinom olsun. Bu takdirde $f(x)$, $E[x]$ te pozitif dereceli bir polinomdur ve dolayısıyla Teorem 3.5.17 ye göre $f(x)$ in E de b gibi bir kökü vardır. Bu durumda $A(b)$, A nın bir cebirsel genişlemesidir ve A, K nın bir cebirsel genişlemesidir; şu halde Teorem 3.2.20 ye göre $A(b)$, K nın bir cebirsel genişlemesidir. Sonuçta $b \in A(b)$, K üzerinde cebirseldir ve buradan A nın tanımı gereğince $b \in A$ olduğu sonucu çıkar, yani $f(x)$ in A da bir kökü vardır.

Tanım 3.5.19. E/K bir cisim genişlemesi olsun. E, K nın bir cebirsel genişlemesi ise ve cebirsel kapalı ise E ye *K nın bir cebirsel kapanışı* denir.

Her K cisminin bir cebirsel kapanışı var mıdır? Bu sorunun yanıtı "evet" tir ve ispatı Zorn Lemması yardımıyla yapılır. Bir K cisminin cebirsel kapanışı şu anlamda tek türlü belirlidir: K nın herhangi iki cebirsel kapanışı arasında, K nın her elemanını sabit bırakan bir izomorfi kurulabilir.

§ 6. Galois Teorisi

Bu paragrafta Galois teorisine bir giriş yapacağız. Herhangi bir *E/K* cisim genişlemesi verildiğine göre, *E/K* nın ara cisimleri ile *genişlemenin Galois grubu* denilen bir grubun alt grupları arasında ilişki kuracağız. Böylece genişlemenin ara cisim yapısı ile ilgili pek çok soru, Galois grubunun alt grup yapısı ile ilgili sorulara indirgenebilecektir. Biz burada tamamen I. Kaplansky'nin yaklaşımını izleyeceğiz.

E/K bir cisim genişlemesi ise *E* bir cisimdir ve aynı zamanda bir *K*-vektör uzayıdır. *E* nin aynı anda hem cisim, hem de vektör uzayı yapısıyla çalışmak çok verimli olacaktır. Bu nedenle, bu yapıların her ikisini de koruyan tasvirleri gözönüne alacağız.

E bir cisim olsun. *E* nin bir φ cisim otomorfisinin *E* nin kendi üzerine (1-1) bir halka homomorfisi olduğunu hatırlayalım. Buna denk olarak, *E* nin bir cisim otomorfisi, <*E*,+> grubunun bir otomorfisidir ki, bu aynı zamanda *E* nin bir halka izomorfisidir. *E* nin idantik tasvirinin *E* nin bir cisim otomorfisi olduğu açıktır, dolayısıyla *E* nin bütün cisim otomorfilerinin oluşturduğu küme boş değildir. Üstelik, φ ve ψ, E nin herhangi iki cisim otomorfisi ise $\varphi\psi$ ve φ^{-1} tasvirleri, <*E*,+> grubunun birer otomorfisidir ki, Lemma 2.56 ya göre bu tasvirler, aynı zamanda *E* nin kendi üzerine birer halka izomorfisidir. Şu halde $\varphi\psi$ ve φ^{-1} tasvirleri, *E* nin cisim otomorfileridir. Bundan dolayı *E* nin bütün cisim otomorfilerinin kümesi, <*E*,+> grubunun bütün otomorfilerinin oluşturduğu grubun bir alt grubudur. *E* nin bütün cisim otomorfilerinin grubunu *Aut*(*E*) ile göstereceğiz. O halde *E* nin toplam grubunun otomorfilerinin grubu ile *E* nin cisim otomorfilerinin grubu için (birbiriyle karıştırmamak koşuluyla) aynı gösterimi kullanacağız.

Aut(E), E yi kendi üzerine resmeden ve *E* nin cisim yapısını koruyan tasvirlerin ailesidir. Bu cisim otomorfilerinden *E* nin vektör uzayı yapısını koruyan tasvirleri seçeceğiz.

Tanım 3.6.1. *E/K* ve *F/K* iki cisim genişlemesi olsun. Bir $\varphi : E \to F$ tasviri hem bir cisim homomorfisi, hem de bir *K*-vektör uzayı homomorfisi ise φ ye bir *K-homomorfi* denir. Bir $\varphi : E \to F$ *K*-homomorfisi (1-1) ve üzerine ise φ ye bir *K-izomorfi* denir. *E* nin kendi üzerine bir *K*-izomorfisine *E nin bir K-otomorfisi* denir. *E* nin bütün *K*-otomorfilerinin kümesini $Aut_K E$ veya *G*(*E/K*) ile göstereceğiz.

$\varphi : E \to F$ bir *K*-homomorfi ise Tanım 3.1.15 e göre $\varphi(1_E) = 1_F$ dir, çünkü φ bir cisim homomorfisidir ve φ bir *K*-lineer transformasyon olduğundan her $k \in K$ için $\varphi(k) = \varphi(k \cdot 1_E) = k \cdot \varphi(1_E) = k \cdot 1_F = k$ eşitliği sağlanır. O halde her $k \in K$ için $\varphi(k) = k$ dır. Tersine, $\varphi : E \to F$ tasviri, her $k \in K$ için $\varphi(k) = k$ koşulunu sağlayan bir *K*-homomorfi ise bu takdirde her $k \in K$ ve $e \in E$ için $\varphi(k \cdot e) = \varphi(k) \cdot \varphi(e) = k \cdot \varphi(e)$ dir ve dolayısıyla φ, bir *K*-lineer transformasyondur. Sonuç olarak, bir $\varphi : E \to F$ cisim homomorfisinin bir *K*-homomorfi olması için gerek ve yeter koşul, φ nin *K* nın her elemanını sabit bırakmasıdır.

Lemma 3.6.2. *E/K* bir cisim genişlemesi ise *E* nin *K* üzerindeki bütün K-otomorfilerinin $Aut_K E$ kümesi bir gruptur.

İspat. $I_E \in Aut_K E \subset Aut(E)$ dir ve *Aut*(*E*) bir gruptur. Teorem 2.100 e göre iki vektör uzayı izomorfisinin bileşkesi ve bir vektör uzayı izomorfisinin tersi gene bir vektör uzayı izomorfisi olduğundan $Aut_K E$, bileşke ve ters alma işlemlerine göre kapalıdır. Şu halde $Aut_K E$, *Aut*(*E*) nin bir alt grubudur.

Tanım 3.6.3. *E/K* bir cisim genişlemesi olsun. $Aut_K E = G(E/K)$ grubuna *E nin K üzerindeki Galois grubu* denir.

Örnek 3.6.4. *E* herhangi bir cisim ve *P*, *E* nin asal alt cismi olsun.*E* nin her φ cisim otomorfisi, 1_E yi sabit bırakır. Buradan φ nin, *P* nin her elemanını sabit bıraktığı sonucu çıkar. O halde *E* nin her cisim otomorfisi, *E* nin bir *P*-otomorfisidir ve $Aut(E) = Aut_P E$ dir.

Örnek 3.6.5.
$$\varphi: \mathbb{C} \to \mathbb{C}$$
$$a+bi \to a-bi \qquad (a,b \in \mathbb{R})$$
eşlenik alma tasviri, $\mathbb{C}$ nin bir $\mathbb{R}$ -otomorfisidir.

Örnek 3.6.6.
$$\varphi: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$$
$$a+b\sqrt{2} \to a-b\sqrt{2} \qquad (a,b \in \mathbb{Q})$$
tasviri, $\mathbb{Q}(\sqrt{2})$ nin bir $\mathbb{Q}$ -otomorfisidir.

Örnek 3.6.7. *K* bir cisim ve *x*, *K* üzerinde bir değişken olsun. Bu takdirde *K*(*x*), *K* nın bir cisim genişlemesidir. $a \in K^*$ ise *ax, K* üzerinde transandanttır ve Teorem 3.1.37 ye göre
$$\sigma_a : K(x) \to K(x)$$
$$\frac{f(x)}{g(x)} \to \frac{f(ax)}{g(ax)}$$
tasviri, *K*(*x*) in bir cisim otomorfisidir. σ_a nın aslında *K*(*x*) in bir *K*-otomorfisi olduğunu görmek zor değildir. Benzer şekilde, herhangi bir $b \in K$ için
$$\tau_b : K(x) \to K(x)$$
$$\frac{f(x)}{g(x)} \to \frac{f(x+b)}{g(x+b)}$$
tasviri, *K*(*x*) in bir *K*-otomorfisidir. $a \neq 1_K$ ve $b \neq 0_K$ için
$(\tau_b \sigma_a)(x) = \tau_b(\sigma_a(x)) = \tau_b(ax) = a(x+b) \neq ax+b = \sigma_a(x+b) = \sigma_a(\tau_b(x)) = (\sigma_a \tau_b)(x)$
olduğundan $Aut_K K(x)$, komütatif olmayan bir gruptur.

Şimdi $Aut_K K(x)$ grubunu bulacağız. Aşağıda *y* ve *z* yi, *K* üzerinde birbirinden farklı iki yeni değişken olarak kullanacağız.

u, $K(x)\backslash K$ nın keyfi bir elemanı olsun, yani $p(x)$ ve $q(x)$, $K[x]$ te aralarında asal iki polinom ve $q(x) \neq 0_K$ olmak üzere, $u = p(x)/q(x)$ diyelim. u nun K üzerinde transandant olduğunu ve $K(x)$ in $K(u)$ üzerinde sonlu boyutlu (dolayısıyla cebirsel) olduğunu iddia ediyoruz.

Önce ilk iddiayı, yani u nun K üzerinde transansant olduğunu ispat edelim. u, K üzerinde cebirsel olsaydı, u nun K üzerinde

$$H(y) = y^k + c_{k-1}y^{k-1} + ... + c_1 y + c_0 \in K[y]$$

gibi bir minimal polinomu bulunurdu. $H(u) = 0_K$ eşitliğinden

$$(p(x)/q(x))^k + c_{k-1}(p(x)/q(x))^{k-1} + ... + c_1(p(x)/q(x)) + c_0 = 0_K ,$$

$$\left(p(x)\right)^k + c_{k-1}\left(p(x)\right)^{k-1} q(x) + ... + c_1 p(x)\left(q(x)\right)^{k-1} + c_0\left(q(x)\right)^k = 0_K$$

elde edilirdi ve buradan

$$K[x] \text{ te } q(x) \Big| \left(p(x)\right)^k \text{ ve } (p(x), q(x)) \approx 1,$$

$q(x)$, $K[x]$ te bir aritmetik birim ve dolayısıyla $q(x) \in K$,

$$u = p(x)/q(x) \in K[x]$$

sonucu çıkardı. O halde $H(u) = u^k + c_{k-1}u^{k-1} + ... + c_1 u + c_0$, derecesi $k(deg\ p(x))$ olan bir polinom olurdu ki, bu $H(u) = 0_K$ oluşuyla çelişir. Şu halde u, K üzerinde transandanttır.

İkinci olarak, $\left|K(x) : K(u)\right|$ nun sonlu olduğunu ispatlayalım.

$u = p(x)/q(x)$ te

$p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, $q(x) = b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0$

$(a_n \neq 0_K$, $b_m \neq 0_K)$ olsun. $uq(x) - p(x) = 0_K$ eşitliğinden dolayı x, $K(u)[y]$ de

$$F(y) = (b_m u)y^m + (b_{m-1}u)y^{m-1} + ... + (b_1 u)y + b_0$$

$$- a_n y^n - a_{n-1}y^{n-1} - ... - a_1 y - a_0$$

polinomunun bir köküdür. Şu halde x, $K(u)$ üzerinde cebirseldir. Üstelik, $deg\ F(y) = max(m,n) = max(deg\ p(x), deg\ q(x))$ olduğu görülür, çünkü $u \notin K$ olduğundan $b_m u - a_n \neq 0_K$ dır. Şimdi $F(y)$ nin $K(u)$ üzerinde asal olduğunu göstereceğiz. Buradan, $1_K / c, F(y)$ nin baş katsayısı olmak üzere, $cF(y)$ nin, x in $K(u)$ üzerindeki minimal polinomu olduğu ve dolayısıyla $\left|K(x) : K(u)\right| = deg\ cF(y)$ $= deg\ F(y) = max(deg\ p(x), deg\ q(x))$ olduğu sonucu çıkacaktır.

u, K üzerinde transandant olduğundan, Teorem 3.1.37 ye göre $z \to u$ sübstitüsyon homomorfisi, aslında $K(z)$ nin $K(u) \subset K(x)$ üzerine bir cisim izomorfisidir. O halde $K(u) \cong K(z)$ dir ve Teorem 2.75 e göre $K(u)[y] \cong K(z)[y]$ dir. Bu durumda $F(y)$ nin $K(u)[y]$ de asal olabilmesi için gerek ve yeter koşul, $F(z) \in K(z)[y]$ görüntüsünün $K(z)[y]$ de asal olmasıdır. Lemma 2.87 den, $F(z)$ nin $K(z)[y]$ de asal olması için gerek ve yeter koşulun, $F(z) = q(y)z - p(y)$ nin $K[z][y] = K[y][z]$ de asal olması olduğu sonucunu çıkarırız. Fakat $F(z) = q(y)z - p(y)$, $K[y][z]$ de tabii ki asaldır, çünkü $q(y)z - p(y)$, $K[y][z]$ de

birinci derecedendir, $q(y)$ ve $-p(y)$ katsayıları, $K[y]$ de aralarında asaldır (çünkü $p(x)$ ve $q(x)$, $K[x]$ te aralarında asaldır).

O halde $p(x)$ ve $q(x)$, $K[x]$ te aralarında asal iki polinom ve $q(x) \neq 0_K$ olmak üzere, $K(x)\backslash K$ ya ait her $u = p(x)/q(x)$ elemanı için
$|K(x) : K(u)| = max(deg\ p(x), deg\ q(x))$ tir.

Şimdi $\varphi \in Aut_K K(x)$ ve $\varphi(x) = u$ olsun. Yukarıdaki gibi $u = p(x)/q(x)$ yazalım.

$$\begin{aligned} K(u) = K(\varphi(x)) &= \{ f(\varphi(x))/g(\varphi(x)) \,|\, f, g \in K[x],\ g \neq 0_K \} \\ &= \{ \varphi(f(x))/\varphi(g(x)) \,|\, f, g \in K[x],\ g \neq 0_K \} \\ &= \{ \varphi(f(x)/g(x)) \,|\, f, g \in K[x],\ g \neq 0_K \} \\ &= \varphi(K(x)) = K(x) \neq K \end{aligned}$$

olduğundan $u \in K(x)\backslash K$ dır ve

$$1 = |K(x) : K(x)| = |K(x) : K(u)| = max(deg\ p(x), deg\ q(x))$$

eşitliğinden uygun $a, b, c, d \in K$ ile $p(x) = ax + b$, $q(x) = cx + d$ olduğu sonucu çıkar. Burada $ad - bc \neq 0_K$ dır, çünkü $ad - bc = 0_K$ olsa
$u = p(x)/q(x) = (ax + b)/(cx + d) \in K$ gibi bir çelişki elde edilir.

O halde $Aut_K K(x)$ teki her otomorfi, $a, b, c, d \in K$, $ad - bc \neq 0_K$ koşulunu sağlayan uygun elemanlar olmak üzere, x i $(ax + b)/(cx + d)$ ye götüren bir sübstitüsyon homomorfisidir. Tersine, φ, $\varphi(x) = (ax + b)/(cx + d)$ $(a, b, c, d \in K,$ $ad - bc \neq 0_K)$ biçiminde bir sübstitüsyon homomorfisi ise $(ax + b)/(cx + d) =: u$, K ya ait değildir, dolayısıyla u, K üzerinde transandanttır ve φ, $K(x)$ ten $K(u)$ üzerine bir cisim homomorfisidir. $ad - bc \neq 0_K$ olduğundan hem a, hem de c, 0_K olamaz, o halde $|K(x) : K(u)| = max(deg\,(ax + b)), deg\,(cx + d)) = 1$ ve $K(u) = K(x)$ tir. Şu halde φ, $K(x)$ in kendi üzerine bir cisim homomorfisidir. φ, K nın her elemanını sabit bıraktığından, buradan φ nin $Aut_K K(x)$ e ait olduğu sonucu çıkar. Bu nedenle $Aut_K K(x)$, tamamen $x \to (ax + b)/(cx + d)$ $(a, b, c, d \in K$, $ad - bc \neq 0_K)$ sübstitüsyon homomorfilerinden oluşur.

Bir sonraki lemma, şu bilinen gerçeğin bir genelleştirilmişidir: Reel katsayılı bir polinomun herhangi bir kompleks kökünün eşleniği de o polinomun bir köküdür.

Lemma 3.6.8. E/K bir cisim genişlemesi ve $f(x) \in K[x]$ olsun. $u \in E$, $f(x)$ in bir kökü ise herhangi bir $\varphi \in Aut_K E$ için E nin $\varphi(u)$ elemanı da $f(x)$ in bir köküdür.

İspat. $f(x) = \sum_{i=0}^{m} a_i x^i$ ise $f(u) = 0_K$ dan $0_K = \varphi(0_K) = \varphi(f(u)) = \varphi(\sum_{i=0}^{m} a_i u^i)$

$= \sum_{i=0}^{m} \varphi(a_i) \cdot \varphi(u^i) = \sum_{i=0}^{m} a_i \cdot (\varphi(u))^i = f(\varphi(u))$ sonucu çıkar. Şu halde $\varphi(u)$, $f(x)$ in bir köküdür.

E/K sonlu boyutlu bir genişleme olsun ve $\{a_1, a_2, ..., a_m\}$ nin *E* nin bir *K*-tabanı olduğunu varsayalım. Bu takdirde *E* nin her *K*-otomorfisi, bu otomorfinin taban elemanları üzerindeki etkisiyle tamamen belirlenir, çünkü φ ve ψ , *E* nin iki *K*-otomorfisi ve $\varphi(a_i) = \psi(a_i)$ $(i = 1, 2, ..., m)$ ise, $\sum_{i=0}^{m} k_i.a_i$ biçiminde yazdığımız herhangi bir $a \in E$ için

$$\varphi(a) = \varphi(\sum_{i=0}^{m} k_i.a_i) = \sum_{i=0}^{m} \varphi(k_i) \cdot \varphi(a_i) = \sum_{i=0}^{m} k_i \cdot \varphi(a_i) = \sum_{i=0}^{m} k_i \cdot \psi(a_i) = \sum_{i=0}^{m} \psi(k_i) \cdot \psi(a_i) =$$

$$\psi(\sum_{i=0}^{m} k_i.a_i) = \psi(a)$$

dır. Bundan dolayı, *E* nin *K*-otomorfilerini, taban elemanlarının görüntülerini vererek tanımlayacağız. O halde eşlenik alma tasvirini $i \to -i$ ile, Örnek 3.6.6 daki tasviri $\sqrt{2} \to -\sqrt{2}$ ile göstereceğiz.

Özellikle, *E/K* basit bir genişleme ve *a* bir primitif eleman ise, Teorem 3.2.8 e göre *n, a* nın *K* üzerindeki minimal polinomunun derecesi olmak üzere $\{1_K, a, a^2, ..., a^{n-1}\}$, *E*=*K*(*a*) nın bir *K*-tabanıdır. Şimdi $\varphi \in Aut_K E$ olsun. $\varphi(a^i) = (\varphi(a))^i$ $(i = 1, 2, ..., n-1)$ olduğundan φ tasviri, φ nin *a* üzerindeki etkisiyle tamamen belirlenir. $\varphi(a)$, *a* nın *K* üzerindeki minimal polinomunun $K(a)$ ya ait bir köküdür. O halde *r*, *a* nın *K* üzerindeki minimal polinomunun $K(a)$ daki birbirinden farklı köklerinin sayısını göstermek üzere, $|Aut_K E| \le r$ dir. Böylece aşağıdaki lemmayı ispatlamış olduk:

Lemma 3.6.9. *K* bir cisim olsun. *a, K* üzerinde cebirsel ve *a* nın *K* üzerindeki minimal polinomu *f* ise *r*, *f* nin *K*(*a*) daki birbirinden farklı köklerinin sayısı olmak üzere, $|Aut_K K(a)| \le r \le deg\ f = |K(a) : K|$ dır.

Örnek 3.6.10. $\sqrt[3]{2}$, 2 nin pozitif reel küpkökü olsun. O halde $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ dir. Şimdi $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})$ grubunu bulalım. $\varphi \in Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2})$ ise $\varphi(\sqrt[3]{2}) \in \mathbb{Q}$, $\sqrt[3]{2}$ nin $\mathbb{Q}$ üzerindeki $x^3 - 2$ minimal polinomunun bir köküdür. $x^3 - 2$ nin $\sqrt[3]{2}$ den farklı kökleri kompleks olduğundan, $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$ olmak zorundadır. Şu halde φ, $\mathbb{Q}(\sqrt[3]{2})$ nin idantik tasviridir ve dolayısıyla $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2}) = \{I_{\mathbb{Q}(\sqrt[3]{2})}\}$ dir.

Örnek 3.6.11. $\mathbb{C} = \mathbb{R}(i)$ dir ve *i* nin $\mathbb{R}$ üzerindeki minimal polinomu, $\mathbb{R}$ de iki kökü bulunan $x^2 + 1$ dir. Şu halde $|Aut_{\mathbb{R}}\mathbb{C}| \le 2$ dir. İdantik tasvir ve eşlenik alma tasviri, $\mathbb{C}$ nin iki $\mathbb{R}$ -otomorfisi olduğundan buradan $|Aut_{\mathbb{R}}\mathbb{C}| = 2$ sonucu çıkar ve dolayısıyla $Aut_{\mathbb{R}}\mathbb{C} \cong C_2$ (C_2, ikinci mertebeden bir devresel grubu göstermektedir) elde edilir. Benzer şekilde, $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}) \cong C_2$ dir.

Örnek 3.6.12. $Aut_{\square}\square(\sqrt{2},\sqrt{3})$ grubunu bulalım. $\square(\sqrt{2},\sqrt{3})=\square(\sqrt{2})(\sqrt{3})$ tür. Burada $\{1,\sqrt{2}\}$, $\square(\sqrt{2})$ nin bir $\square$ -tabanı, $\{1,\sqrt{3}\}$ ise $\square(\sqrt{2})(\sqrt{3})$ ün bir $\square(\sqrt{2})$-tabanıdır (çünkü x^2-3, $\square(\sqrt{2})$ üzerinde asaldır) ve dolayısıyla Teorem 3.1.21 e göre $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$, $\square(\sqrt{2},\sqrt{3})$ ün bir $\square$ -tabanıdır. Şimdi herhangi bir $\varphi\in Aut_{\square}\square(\sqrt{2},\sqrt{3})$ tasviri, $\sqrt{2}$ yi $\sqrt{2}$ veya $-\sqrt{2}$ ye, $\sqrt{3}$ ü ise $\sqrt{3}$ veya $-\sqrt{3}$ e götürür. Şu halde φ için 4 olası durum vardır:

$$\varphi_1(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$$
$$\varphi_2(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$$
$$\varphi_3(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$$
$$\varphi_4(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}\qquad(a,b,c,d\in\square).$$

$\varphi_1,\varphi_2,\varphi_3,\varphi_4$ ün gerçekten $\square(\sqrt{2},\sqrt{3})$ ün $\square$ -otomorfileri olduğu kolayca görülür, o halde $Aut_{\square}\square(\sqrt{2},\sqrt{3})=\{\varphi_1,\varphi_2,\varphi_3,\varphi_4\}$ tür. Burada φ_1, $\square(\sqrt{2},\sqrt{3})$ ün idantik tasviridir ve $\{i,j,k\}=\{2,3,4\}$ için $(\varphi_i)^2=\varphi_1$, $\varphi_i\varphi_j=\varphi_k$ dır. O halde $Aut_{\square}\square(\sqrt{2},\sqrt{3})\cong C_2\times C_2\cong V_4$ ($V_4=\{I,(12)(34),(13)(24),(14)(23)\}$ grubu, Klein'ın dörtlü grubudur) tür.

Şimdi bir *E/K* genişlemesinin ara cisimleri ile $Aut_K E$ nin alt grupları arasındaki ilişkiyi göreceğiz.

Lemma 3.6.13. *E/K* bir cisim genişlemesi olsun ve $G=Aut_K E$ diyelim.

(1) *L, E/K* nın bir ara cismi ise

$$L'=\{\varphi\in G:\varphi(l)=l\ (\forall l\in L)\}$$

G nin bir alt grubudur.

(2) $H\underset{a.g.}{\subset}G$ ise

$$H'=\{a\in E:\varphi(a)=a\ (\forall\varphi\in G)\}$$

E/K nın bir ara cismidir.

İspat. (1) $I_E\in L'$ olduğu açıktır, şu halde $L'\neq\varnothing$ dir. $\varphi,\psi\in L'$ ise her $l\in L$ için $(\psi\varphi)(l)=\psi(\varphi(l))=\psi(l)=l$ olduğundan $\psi\varphi\in L'$ dür. Her $l\in L$ için $\varphi(l)=l$ ve dolayısıyla $\varphi^{-1}(l)=l$ dir, şu halde $\varphi^{-1}\in L'$ dür. O halde L', $Aut_K E$ nin bir alt grubudur (aslında $L'=Aut_L E$ dir).

(2) Her $\varphi\in H'\subset Aut_K E$, *K* nın elemanlarını sabit bıraktığından $K\subset H'$ dür. $a,b\in H'$ ise her $\varphi\in H$ için $\varphi(a)=a$ ve $\varphi(b)=b$ dir, dolayısıyla

$$\varphi(a+b)=\varphi(a)+\varphi(b)=a+b \quad \Rightarrow \quad a+b\in H',$$
$$\varphi(-b)=-\varphi(b)=-b \quad \Rightarrow \quad -b\in H',$$
$$\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)=a\cdot b \quad \Rightarrow \quad a\cdot b\in H',$$
$$\varphi(1_E/b)=1_E/\varphi(b)=1_E/b \ \ (b\neq 0_K \text{ olmak koşuluyla}) \Rightarrow \quad 1_E/b\in H'$$

dür. Şu halde H', E nin bir alt cismidir ve dolayısıyla H', E/K nın bir ara cismidir.

Örneğin, Örnek 3.6.12 daki gösterimle

$$\square(\sqrt{2},\sqrt{3})'=\{1_G\}\underset{a.g.}{\subset}G=Aut_{\square}\square(\sqrt{2},\sqrt{3}),$$

$$\square(\sqrt{2})'=\{\varphi_1,\varphi_2\},\qquad \square(\sqrt{3})'=\{\varphi_1,\varphi_3\},\qquad \square(\sqrt{6})'=\{\varphi_1,\varphi_4\},\qquad \square'=G$$

ve

$$\{1_G\}'=\square(\sqrt{2},\sqrt{3}) \quad , \quad \{\varphi_1,\varphi_2\}'=\square(\sqrt{2}) \quad , \quad \{\varphi_1,\varphi_3\}'=\square(\sqrt{3}),$$
$$\{\varphi_1,\varphi_4\}'=\square(\sqrt{6}) \quad , \quad G'=\square$$

dur.

E/K bir cisim genişlemesi ve $H\underset{a.g.}{\subset}Aut_K E$ ise H' ye *H nın sabit bıraktığı cisim* denir. Şimdi Lemma 3.6.13 teki üs alma işleminin 4 uç durumunu gözönüne alalım.

Lemma 3.6.14. E/K bir cisim genişlemesi ve $G=Aut_K E$ olsun. Bu takdirde

(1) $\{1_G\}'=E$,

(2) $E'=\{1_G\}$,

(3) $K'=G$,

(4) $K\subset G'$ dür.

İspat. (1) $\{1_G\}'=\{a\in E\,|\,\varphi(a)=a\ (\forall\varphi\in\{1_G\})\}=\{a\in E\,|\,I_E(a)=a\}=E$.

(2) $E'=\{\varphi\in G\,|\,\varphi(a)=a\ (\forall a\in E)\}=\{I_E\}=\{1_G\}$.

(3) $K'=\{\varphi\in G\,|\,\varphi(a)=a(\forall a\in K)\}=G$.

(4) Tabii ki, $K\subset G'$ dür. Örnek 3.6.10 dan $Aut_{\square}\square(\sqrt[3]{2})=\{I_{\square(\sqrt[3]{2})}\}$ olduğunu biliyoruz, şu halde $\square(\sqrt[3]{2})/\square$ genişlemesi için $G=\{1_G\}$ ve

$K=\square\underset{\neq}{\subset}\square(\sqrt[3]{2})=\{I_{\square(\sqrt[3]{2})}\}'=G'$ dür. Şu halde G' her zaman K ya eşit değildir.

Şekil 3.1

Tanım 3.6.15. *E/K* bir cisim genişlemesi olsun ve $G = Aut_K E$ diyelim. G', K ya eşit ise *E/K* ya bir *Galois genişlemesi* denir.

Buna denk olarak, *E/K* nın bir Galois genişlemesi olması için gerek ve yeter koşul, *E/K* nın her *a* elemanı için $\varphi(a) \neq a$ olacak şekilde bir $\varphi \in Aut_K E$ nin bulunmasıdır. Örneğin □ , □ nin, □ $(\sqrt{2}, \sqrt{3})$ ve □ $(\sqrt{2})$ ise □ nun birer Galois genişlemesidir.

Lemma 3.6.16. *E/K* bir cisim genişlemesi olsun ve $G = Aut_K E$ diyelim. *L* ve *M*, *E/K* nın iki ara cismi, *H* ve *J* de *G* nin iki alt grubu olsun. *X*, *E/K* nın bir ara cismi veya *G* nin bir alt grubu ise $(X')'$ yü kısaca X'' ile gösterelim. Bu takdirde aşağıdakiler sağlanır:

(1) $L \underset{a.c.}{\subset} M$ ise $M' \underset{a.g.}{\subset} L'$ dür,

(2) $H \underset{a.g.}{\subset} J$ ise $J' \underset{a.c.}{\subset} H'$ dür,

(3) $L \underset{a.c.}{\subset} L''$ ve $H \underset{a.g.}{\subset} H''$ dür,

(4) $L''' = L'$ ve $H''' = H'$ dür.

İspat. (1) $L \underset{a.c.}{\subset} M$ olduğunu varsayalım. $\varphi \in M'$ ise her $a \in M$ ve dolayısıyla her $a \in L$ için $\varphi(a) = a$ dır, şu halde $\varphi \in L'$ ve sonuç olarak $M' \underset{a.g.}{\subset} L'$ dür.

(2) $H \underset{a.g.}{\subset} J$ olduğunu varsayalım. $a \in J'$ ise her $\varphi \in J$ ve dolayısıyla her $\varphi \in H$ için $\varphi(a) = a$ dır, şu halde $a \in H'$ ve sonuç olarak $J' \underset{a.c.}{\subset} H'$ dür.

(3) Herhangi bir $a \in L$ alalım. L' nün tanımı gereğince her $\varphi \in L'$ için $\varphi(a) = a$ dır, o halde *a*, L' deki bütün *K*-otomorfilerde sabit kalır. Bu durumda *a*, L' nün sabit bıraktığı cisme aittir, yani $a \in L''$ dür. Buradan $L \subset L''$ olduğu sonucu çıkar. Şimdi herhangi bir $\varphi \in H$ alalım. H' nün tanımı gereğince her $a \in H'$ için $\varphi(a) = a$ dır, dolayısıyla φ, H' deki her elemanı sabit bırakır, o halde $\varphi \in H''$ dür. Buradan $H \underset{a.g.}{\subset} H''$ elde edilir.

(4) (3) e göre $L \underset{a.c.}{\subset} L''$ ve $H \underset{a.g.}{\subset} H''$ dür. Şu halde (1) e göre $L''' \underset{a.g.}{\subset} L'$ ve (2) ye göre $H''' \underset{a.c.}{\subset} H'$ dür. (3) te *L* yerine H', *H* yerine L' koyarsak $H' \underset{a.c.}{\subset} H'''$ ve $L' \underset{a.g.}{\subset} L'''$ elde edilir. Buradan da $L''' = L'$ ve $H''' = H'$ olduğu sonucu çıkar.

Şekil 3.2

Genelde L, L'' nün, H da H'' nün bir has alt kümesi olabilir. Eşitlik durumu için bir tanım verelim.

Tanım 3.6.17. *E/K* bir cisim genişlemesi ve $G = Aut_K E$ olsun. *E/K* nın bir *L* ara cismine $L = L''$ olması halinde *kapalı bir ara cisim* denir ve *G* nin bir *H* alt grubuna da $H = H''$ olması halinde *kapalı bir alt grup* denir.

Şu halde *E* nin, *K* nın bir Galois genişlemesi olması için gerek ve yeter koşul, *K* nın kapalı olmasıdır. Lemma 3.6.16(4) e göre her üslü nesne, kapalıdır.

Teorem 3.6.18. *E/K* bir cisim genişlemesi ve $G = Aut_K E$ olsun. Bu takdirde E/K nın bütün kapalı ara cisimlerinin kümesi ile *G* nin bütün kapalı alt gruplarının kümesi arasında $L \to L'$ şeklinde verilen (1-1) bir tekabül vardır.

İspat. *L, E/K* nın bir kapalı ara cismi ise Lemma 3.6.13(1) e göre L' *G* nin bir alt grubudur ve Lemma 3.6.16(4) e göre de L' kapalıdır. Şu halde üs alma, genişlemenin bütün kapalı ara cisimlerinin kümesinden *G* nin bütün kapalı alt gruplarının kümesi içine bir tasvirdir. Bu tasvir (1-1) dir, çünkü $L' = M'$ den $(L')'' = (M')''$ çıkar ve buradan gene Lemma 3.6.16(4) e göre *L=M* elde edilir. Son olarak, üs alma tasviri, üzerinedir, çünkü *H, G* nin herhangi bir kapalı alt grubu ise H' kapalı bir ara cisimdir ve $(H')' = H$ dır.

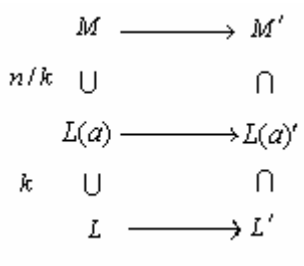
Bu teorem , hangi ara cisimlerin ve hangi alt grupların kapalı olduğunu belirtmediğimiz sürece "hemen hemen faydasız" dır. En önemli durumda, yani *E/K* sonlu boyutlu bir Galois genişlemesi olduğunda bütün ara cisimler ve alt gruplar kapalı hale gelecektir.

Şimdiki amacımız, bir nesnenin kapalı bir nesneden "sonlu miktarda büyük" olması halinde kapalı olduğunu göstermektir. Bunun için iki teknik lemmaya ihtiyaç duymaktayız.

E/K bir cisim genişlemesi, *L* ve *M*, $L \underset{a.c.}{\subset} M$ koşuluna uyan iki ara cisim ise *M* nin *L* üzerindeki $|M : L|$ boyutuna *L ve M nin göreceli boyutu* denir. *G*, bu genişlemenin Galois grubu, *H* ve *J, G* nin $H \underset{a.g.}{\subset} J$ koşuluna uyan iki alt grubu ise, *H* nın *J* içindeki $|J : H|$ indeksine *H ve J nin göreceli indeksi* denir.

Lemma 3.6.19. *E/K* bir cisim genişlemesi, *L* ve *M*, $L \underset{a.c.}{\subset} M$ koşuluna uyan iki ara cisim olsun. *L* ve *M* nin $|M:L|$ göreceli boyutu sonlu ise M' ve L' nün göreceli indeksleri de sonludur. Gerçekte, $|L':M'| \le |M:L|$ dir. Özellikle, *E/K* sonlu boyutlu bir genişleme ise $|Aut_K E| \le |E:K|$ dır.

İspat. İspatı $n=|M:L|$ ye göre tümevarımla yapalım. $n=1$ ise $M = L$ ve $L' = M'$ dür, dolayısıyla $|L':M'| = 1$ dir. Şimdi $n \ge 2$ alalım ve teoremin her $i<n$ için ispat edilmiş olduğunu varsayalım. $|M:L| > 1$ olduğundan bir $a \in M \backslash L$ bulabiliriz. Hipotez gereğince $|M:L|$ sonludur, o halde Teorem 3.2.14 e göre *M, L* nin bir cebirsel genişlemesidir ve dolayısıyla *a, L* üzerinde cebirseldir. $f(x) \in L[x]$, *a* nın *L* üzerindeki minimal polinomu olsun ve $k = deg\, f(x)$ diyelim. Lemma 3.1.28 e göre $k > 1$ dir, çünkü $a \notin L$ dir. Teorem 3.2.8 den $|L(a):L| = k$ sonucu çıkar ve Teorem 3.1.21 den $|M:L(a)| = n/k$ elde edilir. Bu durum, aşağıdaki şemada gösterilmiştir:



Şekil 3.3

$k < n$ durumunda tümevarım herşeyi sağlar: $n/k < n$ ve $k < n$ den $|L(a)':M'| \le |M:L(a)|$, $|L':L(a)'| \le |L(a):L|$ ve sonuçta $|L':M'| = |L':L(a)'| \cdot |L(a)':M'| \le |L(a):L| \cdot |M:L(a)| = k(n/k) = n = |M:L|$ elde edilir. *k=n* durumu için ayrı bir ispat gereklidir.

Şimdi *k=n* olduğunu varsayalım. Bu takdirde $|M:L(a)| = 1$ ve dolayısıyla $M = L(a)$ dır. $|L':M'| \le n$ olduğunu ispatlamak için, M' nün L' deki bütün sağ kalan sınıflarının $\Re$ kümesinden, *f*(*x*) in birbirinden farklı bütün köklerinden oluşan küme içine (1-1) bir tasvir kuracağız. $\Re$ da $|L':M'|$ tane sağ kalan sınıfı bulunduğundan buradan, *r*, *f*(*x*) in *M* deki birbirinden farklı köklerinin sayısını göstermek üzere, $|L':M'| \le r$ olduğu sonucu çıkacaktır.
$r \le deg\, f = |L(a):L| = |M:L|$ olduğundan teorem, böylece ispatlanmış olacaktır.

İstenen tasvirin ne olması gerektiğini Lemma 3.6.8 verecektir.

$$\alpha : \quad \Re \to \{ b \in M \mid f(b) = 0_K \}$$
$$M'\varphi \to \varphi(a) \qquad (\varphi \in L')$$

tasvirini gözönüne alalım. a, $f(x)$ in bir kökü ve $\varphi \in L' \underset{a.g.}{\subset} G = Aut_K E$ olduğundan Lemma 3.6.8 e göre $\varphi(a)$, gerçekten $f(x)$ in bir köküdür. α tasviri iyi tanımlıdır, çünkü $M'\varphi = M'\psi$ $(\varphi, \psi \in L')$ ise uygun bir $\mu \in M'$ için $\varphi = \mu\psi$ dir, şu halde μ, M nin her elemanını ve dolayısıyla a yı sabit bırakır ve $\alpha(M'\varphi) = \varphi(a) = (\mu\psi)(a) = \mu(\psi(a)) = \psi(a) = \alpha(M'\psi)$ eşitliği elde edilir. α, üstelik (1-1) dir, çünkü $\alpha(M'\varphi) = \alpha(M'\psi)$ ise $\varphi(a) = \psi(a)$ ve dolayısıyla $\psi^{-1}(\varphi(a)) = a$ dır; o halde $\psi^{-1}\varphi$, a yı ve sonuçta $L(a) = M$ nin her elemanını sabit bırakır, şu halde $\psi^{-1}\varphi \in M'$ ve $M'\varphi = M'\psi$ dir. Böylece $|L' : M'| \le |M : L|$ nin ispatı tamamlanmış olur.

$|Aut_K E| \le |E : K|$ iddiası da gerçekten doğrudur, çünkü $|Aut_K E| = |Aut_K E : \{1_G\}| = |K' : \{1_G\}| = |K' : E'| \le |E : K|$ dır.

Lemma 3.6.20. E/K bir cisim genişlemesi, H ve J, $G = Aut_K E$ nin $H \underset{a.g.}{\subset} J$ koşuluna uyan iki alt grubu olsun. H ve J nin $|J : H|$ göreceli indeksi sonlu ise J' ve H' nün göreceli boyutu da sonludur. Gerçekte $|H' : J'| \le |J : H|$ dır.

İspat. $|J : H| = n$ olsun ve $|H' : J'| > n$ olduğunu varsayalım. Bu takdirde H' de J' üzerinde lineer bağımsız olan $a_1, a_2, ..., a_n, a_{n+1}$ gibi $n+1$ tane eleman vardır. $\bigcup_{i=1}^{n} H\varphi_i$, J nin H ya göre sağ kalan sınıflarına ayrılışı olsun.

$\varphi_j(a_i) \in E$ $(j = 1, 2, ..., n$, $i = 1, 2, ..., n+1)$ olmak üzere, $n+1$ bilinmeyenli n tane lineer denklemden oluşan

$$\begin{cases} \varphi_1(a_1)x_1 + \varphi_1(a_2)x_2 + \varphi_1(a_3)x_3 + ... + \varphi_1(a_{n+1})x_{n+1} = 0_E \\ \varphi_2(a_1)x_1 + \varphi_2(a_2)x_2 + \varphi_2(a_3)x_3 + ... + \varphi_2(a_{n+1})x_{n+1} = 0_E \\ \qquad\qquad\qquad ..... \\ \varphi_n(a_1)x_1 + \varphi_n(a_2)x_2 + \varphi_n(a_3)x_3 + ... + \varphi_n(a_{n+1})x_{n+1} = 0_E \end{cases} \tag{3.8}$$

sistemini gözönüne alalım. Bilinmeyen sayısı, denklem sayısından büyük olduğundan, (3.8) sisteminin E de triviyal olmayan bir çözümü vardır. (3.8) in triviyal olmayan çözümlerinden, x_i ler arasında sıfırların sayısı mümkün olduğunca az olan bir tanesini seçelim. Bu çözüm, $x_1 = b_1$, $x_2 = b_2$, $x_3 = b_3, ..., x_{n+1} = b_{n+1}$ olsun. b_j lerin r $(r \le n+1)$ tanesinin 0_E den farklı olduğunu varsayalım. b_j lerin seçimi gereğince, (3.8) sisteminin, 0_E den farklı c_j lerin sayısı r den küçük olacak şekilde hiçbir $x_1 = c_1$, $x_2 = c_2$, $x_3 = c_3, ..., x_{n+1} = c_{n+1}$ çözümü yoktur.

Gerektiğinde b_j lerin numaralarını değiştirerek, $b_1,...,b_r$ nin 0_E den farklı ve ($n+1>r$ olması durumunda) $b_{r+1}=...=b_{n+1}=0_E$ olduğunu varsayabiliriz. Ayrıca $b_1=1_E$ olduğunu varsayabiliriz, çünkü $b_1\neq 1_E$ ise $b_1,b_2,...,b_{n+1}$ çözümü yerine $b_1/b_1,b_2/b_1,...,b_{n+1}/b_1$ çözümünü de alabiliriz; kuşkusuz her iki çözümde de 0_E den farklı elemanların sayısı aynıdır.

Şimdi $\psi\in J$ olsun.

$$\begin{cases}\psi(\varphi_1(a_1))x_1+\psi(\varphi_1(a_2))x_2+\psi(\varphi_1(a_3))x_3+...+\psi(\varphi_1(a_{n+1}))x_{n+1}=0_E\\ \psi(\varphi_2(a_1))x_1+\psi(\varphi_2(a_2))x_2+\psi(\varphi_2(a_3))x_3+...+\psi(\varphi_2(a_{n+1}))x_{n+1}=0_E\\ \qquad\qquad .....\\ \psi(\varphi_n(a_1))x_1+\psi(\varphi_n(a_2))x_2+\psi(\varphi_n(a_3))x_3+...+\psi(\varphi_n(a_{n+1}))x_{n+1}=0_E\end{cases} \tag{3.9}$$

sistemini gözönüne alalım. Bu sistem ile ilgili olarak iki gözlem yapalım. Birincisi, $x_1=b_1=1_E,\ x_2=b_2,\ x_3=b_3,...,x_{n+1}=b_{n+1}$, (3.8) in çözümü ve ψ bir homomorfi olduğundan $x_1=\psi(b_1)=1_E, x_2=\psi(b_2), x_3=\psi(b_3),...,x_{n+1}=\psi(b_{n+1})$ de (3.9) un bir çözümüdür. İkincisi, (3.9) sistemi ile (3.8) sistemi birbirine eşdeğerdir. Bu iddiayı ispatlamak için $\psi\varphi_1,\psi\varphi_2,\psi\varphi_3,...,\psi\varphi_n$ nin, H nın J içindeki birbirinden farklı sağ kalan sınıflarının elemanları olduğuna dikkat edelim, çünkü $H\psi\varphi_i=H\psi\varphi_j$ ise $(\psi\varphi_i)(\psi\varphi_j)^{-1}\in H$ ve dolayısıyla $\varphi_i\varphi_j^{-1}\in H$ dır; buradan $H\varphi_i=H\varphi_j$ ve dolayısıyla $i=j$ sonucu çıkar. O halde

$$H\psi\varphi_1=H\varphi_{i_1},\ H\psi\varphi_2=H\varphi_{i_2},\ H\psi\varphi_3=H\varphi_{i_3},...,H\psi\varphi_n=H\varphi_{i_n}$$

olsun. Bu takdirde uygun $\eta_1,\eta_2,\eta_3,...,\eta_n\in H$ ile

$$\psi\varphi_1=\eta_1\varphi_{i_1},\ \psi\varphi_2=\eta_2\varphi_{i_2},\ \psi\varphi_3=\eta_3\varphi_{i_3},...,\psi\varphi_n=\eta_n\varphi_{i_n}\ \left(\{i_1,i_2,...,i_n\}=\{1,2,...,n\}\right)$$

yazabiliriz. Herbir η_k, H' deki herbir a_m yi sabit bıraktığından (3.8) deki i_k. denklem olan

$$\varphi_{i_k}(a_1)x_1+\varphi_{i_k}(a_2)x_2+\varphi_{i_k}(a_3)x_3+...+\varphi_{i_k}(a_{n+1})x_{n+1}=0_E$$

denklemi,

$$(\eta_k\varphi_{i_k})(a_1)x_1+(\eta_k\varphi_{i_k})(a_2)x_2+(\eta_k\varphi_{i_k})(a_3)x_3+...+(\eta_k\varphi_{i_k})(a_{n+1})x_{n+1}=0_E$$

denklemine ve dolayısıyla (3.9) daki *k*. denklem olan

$$\psi(\varphi_k(a_1))x_1+\psi(\varphi_k(a_2))x_2+\psi(\varphi_k(a_3))x_3+...+\psi(\varphi_k(a_{n+1}))x_{n+1}=0_E$$

denklemine eşdeğerdir. Buradan (3.8) ve (3.9) sistemlerinin birbirine eşdeğer olduğu sonucu çıkar.

Şu halde (3.9) sisteminin $x_1=\psi(b_1)=1_E, x_2=\psi(b_2), x_3=\psi(b_3),...,$ $x_{n+1}=\psi(b_{n+1})$ çözümü, aynı zamanda (3.8) sisteminin de bir çözümüdür. Diğer taraftan $x_1=b_1=1_E,\ x_2=b_2,\ x_3=b_3,...,x_{n+1}=b_{n+1}$ de (3.8) in bir çözümüdür. O halde bu iki çözümün farkı

$$x_1=0_E, x_2=b_2-\psi(b_2), x_3=b_3-\psi(b_3),...,x_{n+1}=b_{n+1}-\psi(b_{n+1}),$$

yani

$$x_1 = 0_E, x_2 = b_2 - \psi(b_2), ..., x_r = b_r - \psi(b_r), x_{r+1} = 0_E, ..., x_{n+1} = 0_E \qquad (3.10)$$

de (3.8) in bir çözümüdür.

ψ yi J nin keyfi bir elemanı olarak almıştık. Şimdi ψ için makul bir seçim yapacağız. $\varphi_1, \varphi_2, \varphi_3, ..., \varphi_n$ den biri H ya aittir; örneğin $\varphi_1 \in H$ olsun. Bu takdirde $\varphi_1(a_m) = a_m$ dir, çünkü $a_m \in H'$ $(m = 1, 2, ..., n, n+1)$ dür. $x_1 = b_1$, $x_2 = b_2, x_3 = b_3, ...,$ $x_{n+1} = b_{n+1}$ (3.8) in bir çözümü olduğundan (3.8) deki ilk denklemden

$$a_1.b_1 + a_2.b_2 + a_3.b_3 + ... + a_{n+1}.b_{n+1} = 0_E$$

elde edilir. Burada $\{a_1, a_2, a_3, ..., a_{n+1}\}$, J' üzerinde lineer bağımsızdır ve $b_1 = 1_E \neq 0_E$ dir. Şu halde $b_1, b_2, ..., b_{n+1}$ lerin tamamı J' ye ait olamaz. Bunlardan biri, örneğin b_2, J' ye ait değildir, dolayısıyla $\psi(b_2) \neq b_2$ olacak şekilde bir $\psi \in J$ vardır.

Şimdi $\psi \in J$ yi $\psi(b_2) \neq b_2$ olacak şekilde seçelim. Bu takdirde (3.8) sisteminin (3.10) çözümü, triviyal çözümden farklı bir çözümdür ki, bu çözümde 0_E den farklı elemanların sayısı, r den küçüktür; bu ise r nin tanımı ile çelişir. Bu çelişki, $|H' : J'| > n$ olamayacağını gösterir. O halde $|H' : J'| \leq n = |J : H|$ dır.

Teorem 3.6.21. *E/K* bir cisim genişlemesi ve $G = Aut_K E$ olsun. *L* ve *M, E/K* nın $L \underset{a.c.}{\subset} M$ koşuluna uyan iki ara cismi, *H* ve *J* de $G = Aut_K E$ nin $H \underset{a.g.}{\subset} J$ koşuluna uyan iki alt grubu olsun. Bu takdirde

(1) *L* kapalı ve $|M : L|$ sonlu ise *M* kapalıdır ve $|L' : M'| = |M : L|$ dir,

(2) *H* kapalı ve $|J : H|$ sonlu ise *J* kapalıdır ve $|H' : J'| = |J : H|$ dır.

İspat. (1) Lemma 3.6.16(3) e göre $M \subset M''$, hipoteze göre de $L = L''$ dür. O halde Lemma 3.6.19 ve Lemma 3.6.20 den

$$|M : L| \leq |M'' : M||M : L| = |M'' : L| = |M'' : L''| = |(M')' : (L')'| \leq |L' : M'| \leq |M : L|$$

elde edilir. Böylece $|L' : M'| = |M : L|$ olduğu ispat edilmiş olur. (2) nin ispatı da tamamen benzer şekilde yapılır.

Şimdi bu paragrafın en büyük teoremini ifade ve ispat edeceğiz.

Teorem 3.6.22 (Galois Teorisinin Esas Teoremi). *E/K* sonlu boyutlu bir Galois genişlemesi ve $G = Aut_K E$ olsun. Bu takdirde *E/K* nın bütün ara cisimlerinin kümesi ile *G* nin bütün alt gruplarının kümesi arasında $L \to L'$ şeklinde (1-1) bir tasvir kurulabilir. Bu tasvirde iki ara cismin göreceli boyutu, onlara karşılık gelen alt grupların göreceli indeksine eşittir. Özellikle, $|G| = |Aut_K E| = |E : K|$ dır.

İspat. Teorem 3.6.18 e göre, *E/K* nın bütün kapalı ara cisimlerinin kümesi ile *G* nin bütün kapalı alt gruplarının kümesi arasında $L \to L'$ şeklinde (1-1) bir tekabül vardır. *E/K* bir Galois genişlemesi olduğundan hipoteze göre *K* kapalıdır ve bütün ara cisimler, *K* üzerinde sonlu boyutlu olduklarından Teorem 3.6.21(1) e göre

kapalıdırlar. Bundan başka, M herhangi bir ara cisim ise $|K':M'|=|M:K|$ dır. Özellikle, E kapalıdır ve $|Aut_K E|=|G|=|G:\{1_G\}|=|G:E'|=|K':E'|=|E:K|$ dır. O halde G sonludur. $\{1_G\}$ kapalı olduğundan Teorem 3.6.21(2) den G nin bütün alt gruplarının kapalı olduğu sonucu çıkar, çünkü bunlar, G nin sonlu alt gruplarıdır. Şu halde üs alma tasviri, E/K nın bütün ara cisimlerinin kümesi ile G nin bütün alt gruplarının kümesi arasında (1-1) bir tasvirdir. Teorem 3.6.21 e göre, $L \underset{a.c.}{\subset} M$ koşuluna uyan iki ara cismin $|M:L|$ göreceli boyutu, G nin onlara karşılık gelen alt gruplarının $|L':M'|$ göreceli indeksine eşittir ve G nin $H \underset{a.g.}{\subset} J$ koşuluna uyan iki alt grubunun $|J:H|$ göreceli indeksi de bu alt gruplara karşılık gelen ara cisimlerin $|H':J'|$ göreceli boyutuna eşittir.

Örnek 3.6.23. $\sqrt[3]{2}$, 2 nin reel küp kökü olsun ve $\mathbb{Q}$ üzerinde $\mathbb{Q}(\sqrt[3]{2},\omega)$ genişlemesini gözönüne alalım. $\mathbb{Q}(\sqrt[3]{2},\omega)$ nın $\mathbb{Q}$ -otomorfileri şunlardır:

$$\varphi_1:\sqrt[3]{2}\to\sqrt[3]{2},\quad \omega\to\omega \qquad \varphi_4:\sqrt[3]{2}\to\sqrt[3]{2}\omega,\quad \omega\to\omega^2=-1-\omega$$

$$\varphi_2:\sqrt[3]{2}\to\sqrt[3]{2},\quad \omega\to\omega^2=-1-\omega \qquad \varphi_5:\sqrt[3]{2}\to\sqrt[3]{2}\omega^2=\sqrt[3]{2}(-1-\omega),\quad \omega\to\omega$$

$$\varphi_3:\sqrt[3]{2}\to\sqrt[3]{2}\omega,\quad \omega\to\omega \qquad \varphi_6:\sqrt[3]{2}\to\sqrt[3]{2}\omega^2=\sqrt[3]{2}(-1-\omega),\quad \omega\to\omega^2=-1-\omega$$

$\mathbb{Q}(\sqrt[3]{2},\omega)$ nın her u elemanı,

$$u=a+b\sqrt[3]{2}+c\sqrt[3]{4}+d\omega+e\sqrt[3]{2}\omega+f\sqrt[3]{4}\omega \qquad (a,b,c,d,e,f\in\mathbb{Q})$$

biçiminde tek türlü yazılabilir. Şimdi $\mathbb{Q}(\sqrt[3]{2},\omega)$ nın, $\mathbb{Q}$ nun bir Galois genişlemesi olduğunu göstereceğiz. Bunun için G nin sabit cisminin tam olarak $\mathbb{Q}$ olduğunu göstermeliyiz.

$$\begin{aligned}&\varphi_2(a+b\sqrt[3]{2}+c\sqrt[3]{4}+d\omega+e\sqrt[3]{2}\omega+f\sqrt[3]{4}\omega)\\&=a+b\sqrt[3]{2}+c\sqrt[3]{4}+(d+e\sqrt[3]{2}+f\sqrt[3]{4})\omega^2\\&=a+b\sqrt[3]{2}+c\sqrt[3]{4}+(d+e\sqrt[3]{2}+f\sqrt[3]{4})(-1-\omega)\\&=(a-d)+(b-e)\sqrt[3]{2}+(c-f)\sqrt[3]{4}-d\omega-e\sqrt[3]{2}\omega-f\sqrt[3]{4}\omega\end{aligned}$$

olduğundan, $\mathbb{Q}(\sqrt[3]{2},\omega)$ nın bir $u=a+b\sqrt[3]{2}+c\sqrt[3]{4}+d\omega+e\sqrt[3]{2}\omega+f\sqrt[3]{4}\omega$ elemanının φ_2 tasvirinde sabit kalması için gerek ve yeter koşul,

$$\begin{aligned}a&=a-d, & d&=-d\\b&=b-e, & e&=-e\\c&=c-f, & f&=-f\end{aligned}$$

eşitliklerinin sağlanmasıdır. O halde $\mathbb{Q}(\sqrt[3]{2},\omega)$ nın φ_2 ile sabit kalan bir *u* elemanı $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ biçimindedir. φ_3 de *u* yu sabit bırakıyorsa, bu takdirde

$$\begin{aligned} a+b\sqrt[3]{2}+c\sqrt[3]{4} &= \varphi_3(a+b\sqrt[3]{2}+c\sqrt[3]{4}) \\ &= a+b\sqrt[3]{2}\omega+c\sqrt[3]{4}\omega^2 \\ &= a+b\sqrt[3]{2}\omega+c\sqrt[3]{4}(-1-\omega) \\ &= a-c\sqrt[3]{4}+b\sqrt[3]{2}\omega-c\sqrt[3]{4}\omega \end{aligned}$$

olur ki, buradan $b=0_E$, $c=-c$, $-c=0_E$ ve dolayısıyla $u=a\in\mathbb{Q}$ sonucu çıkar. *G* nin sabit bıraktığı cisimde bir *u* elemanı ister istemez φ_2 ve φ_3 tarafından sabit kalacağından, o *u* elemanı rasyonel olmak zorundadır. O halde *G* nin sabit bıraktığı cisim, $\mathbb{Q}$ dur. Bu ise $\mathbb{Q}(\sqrt[3]{2},\omega)$ nın, $\mathbb{Q}$ nun bir Galois genişlemesi olduğunu gösterir.

$G(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ grubunun çarpım tablosu kolayca oluşturulabilir. $(\varphi_3\varphi_2)(\sqrt[3]{2})=\varphi_3(\sqrt[3]{2})=\sqrt[3]{2}\omega$ ve $(\varphi_3\varphi_2)(\omega)=\varphi_3(\omega^2)=\omega^2$ olduğundan, $\varphi_3\varphi_2=\varphi_4$ tür, v.s. Şu halde $G(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ nun çarpım tablosu şu şekildedir:

	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_1	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_2	φ_2	φ_1	φ_4	φ_3	φ_6	φ_5
φ_3	φ_3	φ_6	φ_5	φ_2	φ_1	φ_4
φ_4	φ_4	φ_5	φ_6	φ_1	φ_2	φ_3
φ_5	φ_5	φ_4	φ_1	φ_6	φ_3	φ_2
φ_6	φ_6	φ_3	φ_2	φ_5	φ_4	φ_1

Şekil 3.4

O halde $G(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$, 6. mertebeden komütatif olmayan bir gruptur ve yukarıdaki tablo ile S_3 ün aşağıdaki çarpım tablosu karşılaştırılarak, $G(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ nun S_3 e izomorf olduğu kolayca görülebilir:

	ι	(23)	(123)	(12)	(132)	(13)
ι	ι	(23)	(123)	(12)	(132)	(13)
(23)	(23)	ι	(12)	(123)	(13)	(132)
(123)	(123)	(13)	(132)	(23)	ι	(12)
(12)	(12)	(132)	(13)	ι	(23)	(123)
(132)	(132)	(12)	ι	(13)	(123)	(23)
(13)	(13)	(123)	(23)	(132)	(12)	ι

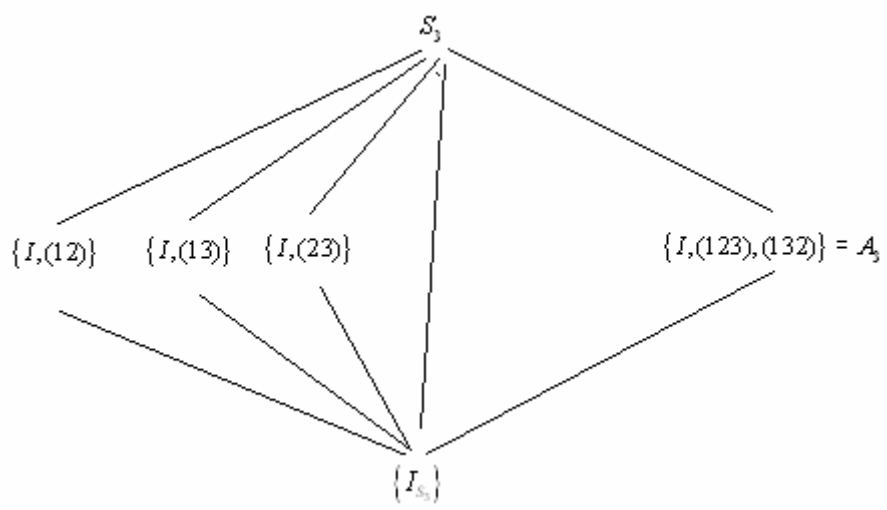
Şekil 3.5

$G(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})\cong S_3$ izomorfisi, $G(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ daki her otomorfinin, x^3-2 nin kökleri üzerindeki etkisiyle tamamen belirlendiğini gözlemleyerek daha

güzel bir yolla bulunabilir. x^3-2 nin kökleri $u_1=\sqrt[3]{2},\ u_2=\sqrt[3]{2}\omega,\ u_3=\sqrt[3]{2}\omega^2$ dir. φ_2, u_1 i u_1 e, u_2 yi u_3 e ve u_3 ü u_2 ye resmettiğinden

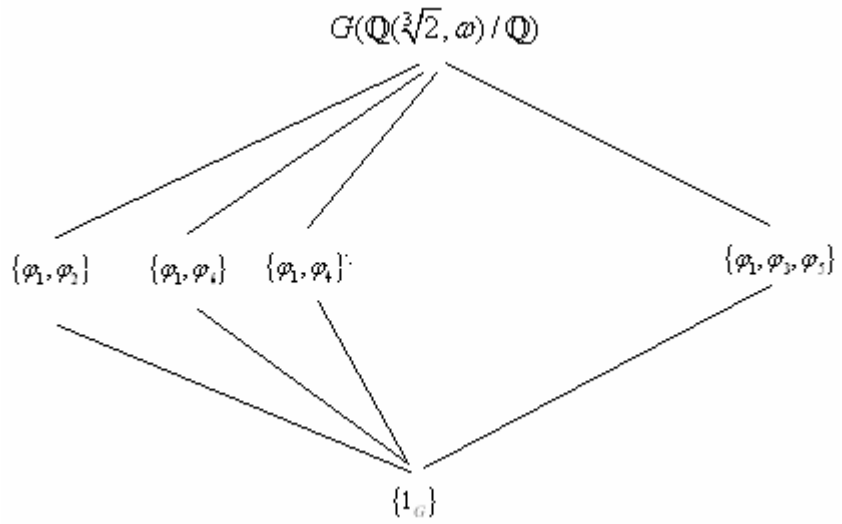
$$\begin{pmatrix} u_1 & u_2 & u_3 \\ u_1 & u_3 & u_2 \end{pmatrix} = (u_2u_3)$$

permütasyonuyla, yani S_3 teki (23) permütasyonuyla gösterilebilir Diğer φ_j ler de benzer şekilde S_3 te birer permütasyon olarak düşünülebilir ve buradan $G(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}) \cong S_3$ olduğu sonucu çıkar. Yukarıdaki çarpım tablolarında, φ_j ile onun bu izomorfideki görüntüsü, mütekabil yerler işgal eder. S_3 ün çok iyi bilinen alt grup şeması şu şekildedir:



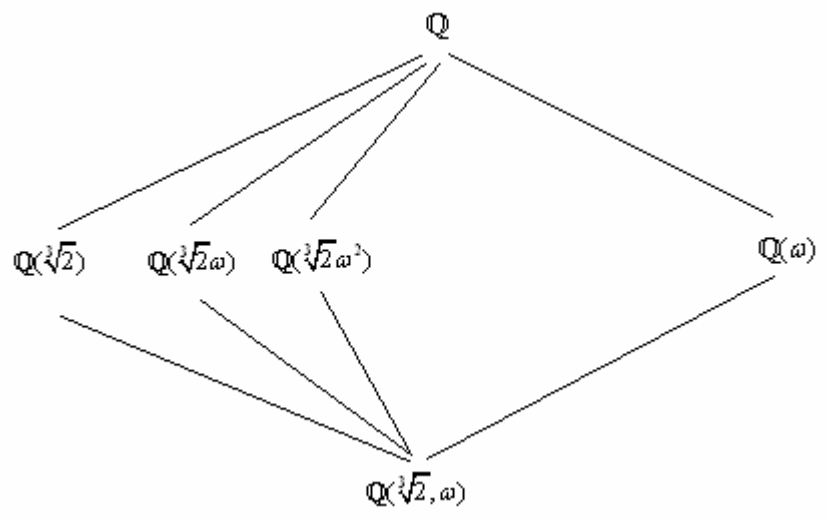
Şekil 3.6

O halde $G(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ nun alt gruplar şeması



Şekil 3.7

şeklindedir ve üs alma işleminden



Şekil 3.8

elde edilir.

Örnek 3.6.24. $\sqrt[4]{2}$, 2 nin dördüncü dereceden reel kökü olsun ve $\mathbb{Q}$ üzerinde $\mathbb{Q}(\sqrt[4]{2}, i)$ genişlemesini gözönüne alalım. $\mathbb{Q}(\sqrt[4]{2}, i)$ nin $\mathbb{Q}$ -otomorfileri

$$\varphi_1 : \sqrt[4]{2} \to \sqrt[4]{2}, \quad i \to i \qquad \varphi_5 : \sqrt[4]{2} \to -\sqrt[4]{2}, \quad i \to i$$

$$\varphi_2 : \sqrt[4]{2} \to \sqrt[4]{2}, \quad i \to -i \qquad \varphi_6 : \sqrt[4]{2} \to -\sqrt[4]{2}, \quad i \to -i$$

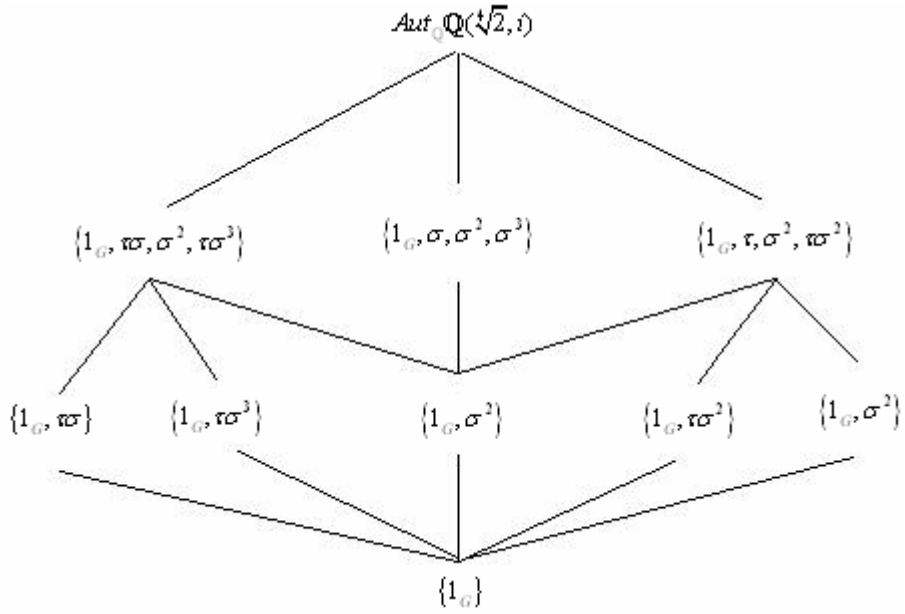
$$\varphi_3 : \sqrt[4]{2} \to \sqrt[4]{2}i, \quad i \to i \qquad \varphi_7 : \sqrt[4]{2} \to -\sqrt[4]{2}i, \quad i \to i$$

$$\varphi_4 : \sqrt[4]{2} \to \sqrt[4]{2}i, \quad i \to -i \qquad \varphi_8 : \sqrt[4]{2} \to -\sqrt[4]{2}i, \quad i \to -i$$

Şimdi $\varphi_2 = \tau$ ve $\varphi_3 = \sigma$ diyelim. Bu durumda $|\tau| = 2$, $|\sigma| = 4$ ve $\sigma^\tau = \sigma^{-1}$ dir. O halde $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$, 8. mertebeden bir dihedral gruptur. $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ daki her otomorfi, $x^4 - 2$ nin $u_1 = \sqrt[4]{2}$, $u_2 = \sqrt[4]{2}i, u_3 = -\sqrt[4]{2}$, $u_4 = -\sqrt[4]{2}i$ kökleri üzerindeki etkisiyle tamamen belirlendiğinden, $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ grubu, S_4 ün bir alt grubuna izomorftur. $\sigma = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 \\ u_2 & u_3 & u_4 & u_1 \end{pmatrix} = (u_1 u_2 u_3 u_4)$, $\tau = \begin{pmatrix} u_1 & u_2 & u_3 & u_4 \\ u_1 & u_4 & u_3 & u_2 \end{pmatrix} = (u_2 u_4)$ olduğundan bir

$$\varphi_2 = \tau \to (24)$$
$$\varphi_3 = \sigma \to (1234)$$

izomorfisi ile $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) \cong <(24),(1234)> =$
$\{I,(13),(24),(12)(34),(13)(24),(14)(23),(1234),(1432)\} \underset{a.g.}{\subset} S_4$ tür. $G(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ grubunun alt gruplar şeması şu şekildedir:



Şekil 3.9

Şimdi $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ genişlemesinin $\{1_G, \tau\sigma^2\}$ alt grubuna karşılık gelen ara cismini bulalım. Kısalık açısından $u = \sqrt[4]{2}$ yazalım. Bu takdirde
$(\tau\sigma^2)(u) = (\tau\sigma)(\sigma(u)) = (\tau\sigma)(ui) = \tau(\sigma(u)\cdot\sigma(i)) = \tau(ui\cdot i) = \tau(-u) = -\tau(u) = -u$ ve
$(\tau\sigma^2)(i) = (\tau\sigma)(\sigma(i)) = \tau(\sigma(i)) = \tau(i) = -i$ dir. Şimdi $a,b,c,d,e,f,g,h \in \mathbb{Q}$ olmak üzere, $s = a + bu + cu^2 + du^3 + ei + fui + gu^2 i + hu^3 i$ olsun. Bu takdirde

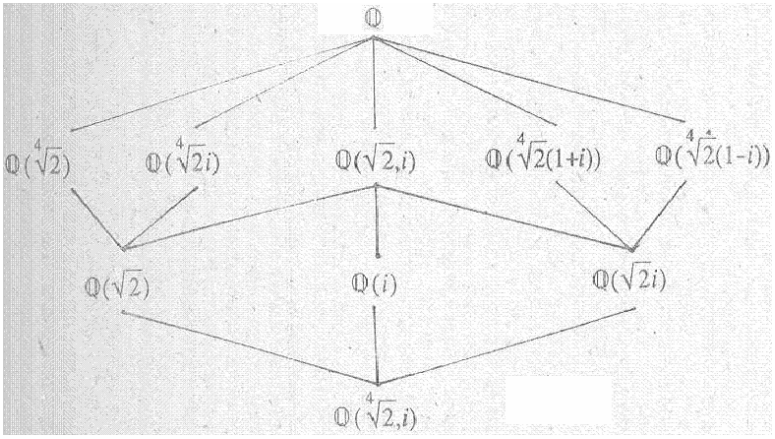
$$\begin{aligned}(\tau\sigma^2)(s) &= (\tau\sigma^2)(a + bu + cu^2 + du^3 + ei + fui + gu^2 i + hu^3 i)\\ &= a + b(-u) + c(-u)^2 + d(-u)^3 + e(-i) + f(-u)(-i) + g(-u)^2(-i) + h(-u)^3(-i)\\ &= a - bu + cu^2 - du^3 - ei + fui - gu^2 i + hu^3 i\end{aligned}$$

dir; o halde s nin $\tau\sigma^2$ tasvirinde sabit kalması için gerek ve yeter koşul,

$$a = a, \quad b = -b, \quad c = c, \quad d = -d,$$
$$e = -e, \quad f = f, \quad g = -g, \quad h = h,$$

olması, yani $b = d = e = g = 0$ olması, yani
$s = a + cu^2 + fui + hu^3 i = a + f(ui) - c(ui)^2 - h(ui)^3$, yani $s \in \mathbb{Q}(ui)$ olmasıdır. O halde $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ genişlemesinin $\{1_G, \tau\sigma^2\}$ alt grubuna karşılık gelen ara cismi,

$\{1_G, \tau\sigma^2\}' = \mathbb{Q}(ui) = \mathbb{Q}(\sqrt[4]{2}i)$ dir. Benzer hesaplamalar sonucu Galois tekabülü, aşağıdaki şemada görüldüğü şekilde bulunur (burada ara cisimler ile kendilerine karşılık gelen alt gruplar, her iki şemada aynı yerleri işgal etmektedir):



Şekil 3.10

Örnek 3.6.25. p bir asal sayı ve $n \in$ olsun. F_{p^n} / F_p genişlemesini gözönüne alalım.

$$\sigma : F_{p^n} \to F_{p^n}$$
$$a \to a^p$$

tasviri, Lemma 3.4.2 ye göre bir cisim homomorfisidir ve Teorem 3.4.9 a göre F_p nin her elemanını sabit bırakır. O halde σ F_p -lineerdir ve $\left|F_{p^n} : F_p\right|$ sonlu olduğundan Teorem 2.107 ye göre σ, F_{p^n} in kendi üzerine bir tasviridir. Şu halde σ, F_{p^n} in bir F_p -otomorfisidir.

Şimdi $G = Aut_K E$ diyelim. $G =< \sigma >$ olduğunu göstermek istiyoruz. Önce $|\sigma| = n$ olduğunu ispatlayalım. Lemma 3.4.5(2) veya Teorem 3.4.9 a göre her $a \in F_{p^n}$ için $\sigma^n(a) = a^{p^n} = a$ olduğundan $\sigma^n = 1_G$ dir ki, buradan $|\sigma| | n$ elde edilir. Diğer taraftan *m, n* nin bir pozitif has böleni ise Teorem 3.4.9 a göre F_{p^n} nin p^m elemanlı F_{p^m} has alt cismi bulunur ve $\sigma^m(b) = b^{p^m} \neq b$ olacak şekilde bir $b \in F_{p^n} \setminus F_{p^m}$ elemanı vardır, dolayısıyla $\sigma^m \neq 1_G$ dir. Buradan $|\sigma| = n$ olduğu sonucu çıkar. $\left|F_{p^n} : F_p\right|$ sonlu olduğundan Lemma 3.6.19 dan

$$n = |\sigma| = |< \sigma >| \leq |G| = \left|G : \{1_G\}\right| = \left|(F_p)' : (F_{p^n})'\right| \leq \left|F_{p^n} : F_p\right| = n$$

elde edilir, o halde $|< \sigma >| = |G| = n$ ve $G =< \sigma >$ dir.

Şimdi F_{p^n} nin, F_p nin bir Galois genişlemesi olduğunu göstermek kolaydır. Teorem 3.4.9 a göre

$$G' =< \sigma >' = \left\{a \in F_{p^n} \,|\, \sigma(a) = a\right\} = F_p$$

dir, şu halde F_{p^n}, F_p nin bir Galois genişlemesidir.

Şimdi Galois tekabülünü belirleyelim. $<\sigma>$ nın alt grupları, n nin pozitif bölenleriyle (1-1) tekabül halindedir ve Teorem 2.34 e göre G nin her H alt grubu, $H =<\sigma^m>$ biçimindedir. F_{p^n} nin, $H =<\sigma^m>$ alt grubuna tekabül eden alt cismi, F_{p^n} nin p^m elemanlı tek alt cismi olan

$$H' =<\sigma^m>'=\left\{a \in \mathrm{F}_{p^n} \middle| \sigma^m(a) = a\right\} = \left\{a \in \mathrm{F}_{p^n} \middle| a^{p^m} = a\right\} = \mathrm{F}_{p^m}$$

cismidir.

Şekil 3.11

Bütün bu örneklerde, öncelikle Galois grubunun alt gruplarını belirledik, daha sonra bu alt gruplara tekabül eden ara cisimleri bulduk. Tabii ki, bunun tersi de yapılabilir, yani önce ara cisimler belirlenip, sonra bu ara cisimlere tekabül eden alt gruplar bulunabilir. Fakat bir genişlemenin bütün ara cisimlerini bulmak, genellikle daha zordur, bazı ara cisimlerin gözden kaçırılması muhtemeldir. Aynı zamanda benzer olanları ayırt etmek de zordur. Örneğin Örnek 3.6.25 te $\square(\sqrt{2}(1+i))$ ve $\square(\sqrt{2}(1-i))$ cisimlerinin nerede bulunduklarını ve $\square(\sqrt{2}(1+i)) = \square(\sqrt{2}(1-i))$ olup olmadığını hemen görmek kolay değildir. Alt grupları listelemek, ara cisimleri listelemekten çok daha kolaydır.

Bir genişlemenin Galois grubunun normal alt gruplarına hangi ara cisimlerin tekabül ettiği sorusunu sormak gayet doğaldır. Aynı zamanda Galois grubunun bölüm grupları hakkında ne söylenebilir? Şimdi bu sorulara cevap vereceğiz.

Tanım 3.6.26. *E/K* bir cisim genişlemesi ve $G = Aut_K E$ bu genişlemenin Galois grubu olsun. *E* nin her $\varphi \in Aut_K E$ *K*-otomorfisi, bu genişlemenin bir *L* ara cismini kendi içine resmediyorsa *L, K ve E ye göre stabildir* veya *L,* (*K,E*)*-stabildir* denir.

Tanım 3.6.26 daki durumda *L* bir (*K,E*)-stabil ara cisim ise, *E* nin herhangi bir φ *K*-otomorfisinin φ^{-1} tersi de *L* yi *L* içine resmeder. O halde *E* nin herhangi bir φ *K*-otomorfisinin *L* ye kısıtlanmışı olan $\varphi_{|L}$, *L* nin bir *K*-otomorfisidir. Şu halde

$$res : Aut_K E \to Aut_K L$$
$$\varphi \to \varphi_{|L}$$

şeklinde bir "kısıtlama" tasviri vardır.

L nin bir λ K-otomorfisi verildiğine göre, E nin $\lambda = \varphi_{|L}$ koşulunu sağlayan bir φ K-otomorfisi varsa λ *otomorfisi E ye uzatılabilir* denir. Buna göre *res*, L nin bütün uzatılabilir K-otomorfilerinin kümesi üzerine bir tasvirdir.

Teorem 3.6.27. *E/K* bir cisim genişlemesi olsun.

(1) L bir (K,E)-stabil ara cisim ise L', $Aut_K E$ Galois grubunun bir normal alt grubudur.

(2) H, $Aut_K E$ nin bir normal alt grubu ise H', genişlemenin bir (K,E)-stabil ara cismidir.

İspat. (1) Her $\varphi \in Aut_K E$ ve her $\lambda \in L'$ için $\varphi\lambda\varphi^{-1} \in L'$ olduğunu göstermeliyiz. O halde her $a \in L$ için $(\varphi\lambda\varphi^{-1})(a) = a$ olduğunu göstermeliyiz. Gerçekten, $a \in L$, $\lambda \in L'$ ve $\varphi \in Aut_K E$ ise L, (K,E)-stabil olduğundan $\varphi^{-1}(a) \in L$ dir, şu halde $\lambda(\varphi^{-1}(a)) = \varphi^{-1}(a)$ ve dolayısıyla $(\varphi\lambda\varphi^{-1})(a) = \varphi(\lambda(\varphi^{-1}(a))) = \varphi(\varphi^{-1}(a)) = a$ dır. Buradan $L' \lhd Aut_K E$ olduğu sonucu çıkar.

(2) Her $\varphi \in Aut_K E$ ve $a \in H'$ için $\varphi(a) \in H'$ olduğunu göstermeliyiz. O halde her $\eta \in H$ için $\eta(\varphi(a)) = \varphi(a)$ olduğunu göstermeliyiz. Gerçekten, $a \in H'$, $\eta \in H$ ve $\varphi \in Aut_K E$ ise, $H \lhd Aut_K E$ olduğundan $\varphi^{-1}\eta\varphi \in H$ dır, şu halde $(\varphi^{-1}\eta\varphi)(a) = a$ ve dolayısıyla $\varphi^{-1}((\eta\varphi)(a)) = a$, $(\eta\varphi)(a) = \varphi(a)$ dır. Buradan H' nün (K,E)-stabil olduğu sonucu çıkar.

Teorem 3.6.28. *E/K* bir Galois genişlemesi ve L bir ara cisim olsun. L, (K,E)-stabil ise K nın bir Galois genişlemesidir.

İspat. Her $a \in L \backslash K$ için $\lambda(a) \neq a$ koşuluna uyan bir $\lambda \in Aut_K L$ bulmalıyız. *E, K* nın bir Galois genişlemesi olduğundan $\varphi(a) \neq a$ koşuluna uyan bir $\varphi \in Aut_K E$ vardır. L, (K,E)-stabil olduğundan $\varphi_{|L} \in Aut_K L$ dir. Şu halde λ olarak $\varphi_{|L}$ alınabilir.

Teorem 3.6.29. *E/K* bir Galois genişlemesi ve $f(x)$, $K[x]$ te asal bir polinom olsun. $f(x)$ in E de bir kökü varsa $f(x)$, E de parçalanır ve $f(x)$ in köklerinin hepsi basittir.

İspat. $a_1 \in E$, $f(x)$ in bir kökü olsun. $deg\, f(x) = n$ diyelim. E nin uygun $c, a_1, a_2, .., a_n$ elemanları için $f(x) = c(x-a_1)(x-a_2)...(x-a_n)$ olduğunu göstermek istiyoruz. Bu amaçla $a_1, a_2, .., a_m$, $f(x)$ in E deki birbirinden farklı bütün kökleri olmak üzere, $g(x) = c(x-a_1)(x-a_2)...(x-a_m) \in E[x]$ diyelim. Teorem 2.89 dan $m \leq n$ olduğunu biliyoruz.

Lemma 3.6.8 e göre E nin her K-otomorfisi, $f(x)$ in bir kökünü gene $f(x)$ in bir köküne resmeder. O halde $g(x)$ in $a_1, a_2, .., a_m$ köklerinin simetrik fonksiyonları olan katsayıları, E nin her K-otomorfisinde sabit kalır. Bu, $g(x)$ in

katsayılarının $E' = K$ ya ait olduğunu gösterir. O halde $g(x) \in K[x]$ tir. Bu durumda $f(x)$ ve $g(x)$, $K[x]$ e ait ve a_1 köküne sahip iki polinomdur ve $f(x)$, K üzerinde asaldır. Şu halde Teorem 2.92(1),(3) e göre $f(x) \mid g(x)$ ve dolayısıyla $n = deg\, f(x) \le deg\, g(x) = m$ dir. Buradan $n \le m$ sonucu çıkar; daha önce de $m \le n$ olduğunu belirtmiştik. O halde $m = n$ dir. Buna göre $f(x) \mid g(x)$ ten $f(x) \cong g(x)$ elde edilir. O halde uygun bir $c \in K^*$ için $f(x) = c(x - a_1)(x - a_2)...(x - a_m)$ dir ve $f(x)$ in $a_1, a_2, .., a_m \in E$ köklerinin hepsi birbirinden farklıdır, yani $f(x)$ in bütün kökleri basittir.

Bir sonraki teorem, Teorem 3.6.28 in bir tür tersidir. *L* nin cebirsel olması hipotezi olmadan sonucun kesin doğru olduğu söylenemez.

Teorem 3.6.30. *E/K* bir cisim genişlemesi ve *L* bir ara cisim olsun. *L* cebirsel ise ve *K* nın bir Galois genişlemesi ise *L*, (*K,E*)- stabildir.

İspat. Her $a \in L$ ve her $\varphi \in Aut_K E$ için $\varphi(a) \in L$ olduğunu göstermek istiyoruz. $a \in L$ ise *L*, *K* üzerinde cebirsel olduğundan *a, K* üzerinde cebirseldir. $f(x)$, *a* nın *K* üzerindeki minimal polinomu olsun. Bu takdirde Teorem 3.6.29 a göre $f(x)$, $L[x]$ te birinci dereceden *n* tane birbirinden farklı polinomun çarpımıdır, çünkü *L, K* nın bir Galois genişlemesidir. Şu halde $f(x)$ in bütün kökleri, *L* ye aittir. Şimdi $\varphi \in Aut_K E$ ise $\varphi(a)$, $f(x)$ in bir köküdür ve dolayısıyla, ispat edilmek istendiği gibi, $\varphi(a) \in L$ dir.

E/K bir cisim genişlemesi ve *L, E/K* nın bir (*K,E*)-stabil ara cismi olsun

$$res : Aut_K E \to Aut_K L$$

$$\varphi \to \varphi_{|L}$$

kısıtlama tasvirini gözönüne alalım. *E* nin herhangi iki φ, ψ *K*-otomorfisi için $(\psi\varphi)_{|L} = \psi_{|L}\varphi_{|L}$ olduğundan, buradan *res* tasvirinin bir homomorfi olduğu sonucu çıkar. O halde $(Aut_K E)/Ker\, res = \mathrm{Im}\, res$ tir. Burada $\mathrm{Im}\, res$, *L* nin *E* ye uzatılabilen bütün *K*-otomorfilerinin kümesidir (dolayısıyla *L* nin *E* ye uzatılabilen bütün *K*-otomorfilerinin kümesi, $Aut_K E$ nin bir alt grubudur) ve

$$Ker\, res = \left\{\varphi \in Aut_K E : \varphi_{|L} = I_L\right\} = \left\{\varphi \in Aut_K E : \varphi(a) = a\ (\forall\, a \in L)\right\} = L' = Aut_L E$$

dir. Buradan $(Aut_K E)/(Aut_L E)$ nin, *L* nin *E* ye uzatılabilen bütün *K*-otomorfilerinin grubuna izomorf olduğu sonucu çıkar. Böylelikle şu teoremi ispat etmiş olduk:

Teorem 3.6.31. *E/K* bir cisim genişlemesi ve *L* bir ara cisim olsun. *L, (K,E)*-stabil ise bu takdirde $L' = Aut_L E$, $Aut_K E$ nin bir normal alt grubudur ve $G(E/K)/G(E/L) = (Aut_K E)/(Aut_L E)$ bölüm grubu, $Aut_K L$ nin, *L* nin *E* ye uzatılabilen *K*-otomorfilerinden oluşan alt grubuna izomorftur.

Şimdi bir ara cisme göre durumu belirleyerek, esas teoreme bir ek yapabiliriz:

Teorem 3.6.32. *E/K*, sonlu boyutlu bir Galois genişlemesi ve $G = Aut_K E$ olsun. *L* de *E/K* nın bir ara cismi olsun. Bu takdirde:

(1) *E*, *L* nin bir Galois genişlemesidir.

(2) *L* nin *K* nın bir Galois genişlemesi olması için gerek ve yeter koşul, $L' = Aut_L E$ nin, $G = Aut_K E$ nin bir normal alt grubu olmasıdır. Bu durumda $G / L' = (Aut_K E)/(Aut_L E)$, L nin K üzerindeki $Aut_K L$ Galois grubuna izomorftur. O halde $G(E/K)/G(E/L) \cong G(L/K)$ dır.

İspat. Burada esas teoremin hipotezleri gerçeklenir. Esas teorem, *E/K* nın herhangi bir ara cisminin ve *G* nin her alt grubunun kapalı olduğunu belirtir.

(1) *E* nin, *L* nin bir Galois genişlemesi olduğunu göstermek için $L'' = L$ olduğunu, yani *L* nin kapalı olduğunu ispatlamalıyız. Esas teoremin ispatında her ara cismin kapalı olduğunu bulmuştuk. *L* de *E/K* nın bir ara cismidir ve sonuçta *L* de kapalıdır.

(2) *Gereklik. L, K* nın bir Galois genişlemesi ise L', $G = Aut_K E$ nin bir normal alt grubudur: Hipoteze göre *E/K* sonlu boyutlu bir genişlemedir, şu halde *L/K* da sonlu boyutlu bir genişlemedir. O halde Teorem 3.2.14 e göre *L, K* üzerinde cebirseldir. *L, K* nın bir Galois genişlemesi ise Teorem 3.6.31 e göre *L*, (*K,E*)-stabildir ve dolayısıyla Teorem 3.6.27(1) e göre L', $Aut_K E$ nin bir normal alt grubudur.

Yeterlik. L', $G = Aut_K E$ nin bir normal alt grubu ise *L, K* nın bir Galois genişlemesidir: L', $Aut_K E$ nin bir normal alt grubu ise Teorem 3.6.27(2) ye göre L'' bir (*K,E*)-stabil ara cisimdir. Burada $L'' = L$ dir, çünkü bütün ara cisimler kapalıdır. Şu halde *L*, (*K,E*)-stabildir. Buradan Teorem 3.6.28 e göre *L* nin, *K* nın bir Galois genişlemesi olduğu sonucu çıkar.

Şimdi *L* nin, *K* nın bir Galois genişlemesi olduğunu ve $L' \lhd G = Aut_K E$ olduğunu varsayalım. Bu takdirde esas teoreme göre (*E* yerine *L* alınarak) $|Aut_K L| = |L : K|$ eşitliği elde edilir. Teorem 3.6.30 a göre $G / L' = (Aut_K E)/(Aut_L E)$, $Aut_K L$ nin bir alt grubuna izomorftur. $L'' = L$ (yani L kapalı) ve $G' = K$ (yani *L*, *K* nın bir Galois genişlemesi) olduğunu kullanırsak esas teoreme göre $|G / L'| = |G : L'| = |L'' : G'| = |L : K| = |Aut_K L|$ olduğunu görürüz. O halde $Aut_K L$ nin bir alt grubuna izomorf olan G / L' nün mertebesi, $Aut_K L$ nin mertebesi ile aynıdır. $|L : K| = |Aut_K L|$ sonlu olduğundan buradan G / L' nün aslında $Aut_K L$ nin kendisine izomorf olduğu sonucu çıkar.

Teorem 3.6.33. F_q, *q* elemanlı bir cisim ve *E*, F_q nun sonlu boyutlu bir genişlemesi olsun. Bu takdirde *E*, F_q nun bir Galois genişlemesidir ve $Aut_{F_q} E$, her $a \in E$ için $\varphi : a \to a^q$ olacak şekilde tanımlanan φ otomorfisi tarafından doğurulan devresel gruptur.

İspat. $\left|E:\mathrm{F}_q\right|=r$ ve $kar\,\mathrm{F}_q=p$ olsun, yani F_p, F_q nun (ve E nin) asal alt cismi olsun. Bu takdirde $m=\left|\mathrm{F}_q:\mathrm{F}_p\right|$ olmak üzere, $q=p^m$ dir. Şimdi E/F_p genişlemesini gözönüne alalım. E, F_q üzerinde r boyutlu bir vektör uzayı ve F_q, F_p üzerinde m boyutlu bir vektör uzayı olduğundan Teorem 3.1.21 e göre E, F_p üzerinde rm boyutlu bir vektör uzayıdır ve dolayısıyla $\left|E\right|=p^{rm}$ dir. Şu halde E sonlu bir cisimdir ve Örnek 3.6.25 e göre E, F_p nin bir Galois genişlemesidir. O halde Teorem 3.6.32(1) e göre E, E/F_p nin herhangi bir ara cisminin bir Galois genişlemesidir. Özellikle E, F_q nun bir Galois genişlemesidir. Bundan başka, Örnek 3.6.25 ten σ, $\varphi:a\to a^q$ $(\forall a\in E)$ cisim izomorfisi olmak üzere, $Aut_{\mathrm{F}_p}E=<\sigma>$ olduğunu ve p^m elemanlı F_q ara cismine tekabül eden $(\mathrm{F}_q)'$ grubunun $<\sigma^m>$ olduğunu biliyoruz. Şu halde $\varphi=\sigma^m:a\to a^{p^m}=a^q$ $(\forall a\in E)$ olmak üzere, $Aut_{\mathrm{F}_p}E=(\mathrm{F}_q)'=<\varphi>$ dir.

SONUÇLAR ve TARTIŞMA

Bu çalışmada Galois Teorisinin temellerini oluşturan, cisim genişlemeleri teorisi ayrıntılı bir şekilde verilmiş ve Galois teorisine bir giriş yapılmıştır.

KAYNAKLAR

Kitap ve Kitap Bölümleri için gösterim

[1] **Feyzioğlu, Ahmet,** 1990. A Course on Algebra I, Boğaziçi University Printing Office, İstanbul.

[2] **Feyzioğlu, Ahmet,** 1990. A Course on Algebra II, Boğaziçi University Printing Office, İstanbul.

[3] **Foote, Richard M. and Dummit, David S.**, Abstract Algebra, Prentice-Hall International Editions

[4] **Şenkon, Hülya,** 1990. Soyut Cebir Dersleri I, İ.Ü. Fen Fakültesi Basımevi, İstanbul

[5] **Şenkon, Hülya,** 1993. Soyut Cebir Dersleri II, İ.Ü. Fen Fakültesi Basımevi, İstanbul

Mehmet Fatih UÇAR: 29 Aralık 1981 Salı günü Erzincan'da doğdu.Vali Metin İlyas AKSOY İlköğretim Okulu'ndan 1993 yılında, Anadolu Lisesinin Ortaokul bölümünden 1997 yılında, Erzincan Nevzat Ayaz Fen Lisesi'nden 2000 yılında mezun oldu. 2001-2005 yılları arasında İstanbul Kültür Üniversitesi Fen-Edebiyat Fakültesi Matematik-Bilgisayar Bölümü'nde ve 2002-2005 yılları arasında İstanbul Kültür Üniversitesi İktisadi ve İdari Bilimler Fakültesi İşletme Bölümü'nde(çap) lisans eğitimini tamamladı. 2005 yılında İKÜ Fen Bilimleri Enstitüsü'nde yükseklisans eğitimine başladı.Halen İKÜ Fen-Edebiyat Fakültesi Matematik-Bilgisayar Bölümü'nde Araştırma Görevlisi olarak yükseklisans eğitimine devam etmektedir.