EGE ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ
(YÜKSEK LİSANS TEZİ)

Q CİSMİ ÜZERİNDEKİ TRİNOMİAL GENİŞLEMELER

NURETTİN BAĞIRMAZ

Matematik Anabilim Dalı

Bilim Dalı Kodu : 403.01.01

Sunuş Tarihi : 27.06.2006

Tez Danışmanı : Prof. Dr. Gönül USLU

Bornova – İZMİR

I I I

Nurettin BAĞIRMAZ tarafından yüksek lisans tezi olarak sunulan ‘‘Q Cismi Üzerindeki Trinomial Genişlemeler’’ başlıklı bu çalışma E.Ü. Lisansüstü Eğitim ve Öğretim Yönetmeliği ile E.Ü. Fen Bilimleri Enstitüsü Eğitim ve Öğretim Yönergesi’nin ilgili hükümleri uyarınca tarafımızdan değerlendirilerek savunmaya değer bulunmuş ve 27/06/2006 tarihinde yapılan tez savunma sınavında aday oybirliği/oyçokluğu ile başarılı bulunmuştur.

JüriÜyeleri:	**İmza**
Jüri Başkanı : Prof. Dr. Gönül USLU	**……**
Raportör Üye: Yrd. Doç. Alev FIRAT	**……**
Üye : Yrd. Doç. Sevgi MORALI	**……**

ÖZET

Q CİSMİ ÜZERİNDEKİ TRİNOMİAL GENİŞLEMELER

BAĞIRMAZ,Nurettin

Yüksek Lisans Tezi Matematik Bölümü

Tez Yöneticisi:Prof. Dr. Gönül USLU

Haziran 2006

Bu tez esas olarak beş bölümden oluşmaktadır. Birinci bölümle tez konusu tanıtılmış, ikinci bölümde cisim genişlemeleri hakkında genel bir özet ve temel teoremler ispatlarıyla verilmiştir.

Üçüncü bölümde Galois teorisinin esasları ve dördüncü bölümde bir polinomun diskriminantı ile Galois grubu arasındaki ilişkiler ele alınmıştır.

Beşinci bölümde başta Galois grubu A_n alternatif grubu tarafından kapsanan trinomialler incelenmiş olup,daha sonra asal sayılardan oluşan bir küme S olmak üzere, diskriminantı p ¿ S asal sayıları ile bölünmeyen f(x) ¿ Z[x] indirgenemez trinomiallerin varlığı ispatlanmıştır.

Anahtar sözcükler: Galois grubu,trinomial, A_n ,diskriminant.

ABSTRACT

TRINOMIAL EXTENSIONS OF Q

BAĞIRMAZ, Nurettin
Yüksek Lisans Tezi Matematik Bölümü
Tez Yöneticisi: Prof. Dr. Gönül USLU
Haziran 2006

This thesis essentially consists of five chapters. In the first chapter, the subject of the thesis is explained. In the second chapter, a general summary of field extension and theorems are given with their proofs.

In the third chapter, basics of Galois theory are examined. In the fourth chapter, the relations between discriminant of a given trinomial with it's Galois group are explained.

In the fifth chapter, the trinomial which Galois group subset of it's A_n is proved. S is a set of primes, f(x) is trinomial with coeffifients a,b ¿ Z , p ¿ S such that there exist diskriminant .

Keywords: Galois group, Trinomial, A_n , Discriminant.

TEŞEKKÜR

Değerli hocam sayın Prof. Dr. Gönül USLU'ya araştırma boyunca anlayış ve rehberliği için en derin teşekkürlerimi sunarım.

Sevgili eşim Mehtap'a bana karşı duyduğu sarsılmaz inancından ve bana en çekilmez olduğum anlarda tahammül etmesinden dolayı teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

ÖZET……..... V

ABSTRACT……..…….....VII

TEŞEKKÜR…….....IX

1.GİRİŞ……..... 1

2.ÖNBİLGİLER…….……..... 3

2.1 Cisim Genişlemeleri……... 3

2.2 Cebirsel Genişlemeler…….....8

2.3 Parçalanış Cisimleri……..... 12

2.4 Ayrılabilir Genişlemeler……..... 14

3.GALOİS TEORİSİ……..... 17

3.1 Bir Cismin Otomorfizma Grubu……..... 17

3.2 Normal Genişlemeler……... 19

3.3 Galois Genişlemeleri…….…….....19

4.DİSKRİMİNANTLAR……..... 31

4.1 Bir Polinomun Diskriminantı…….....31

4.2 Bir Trinomialin Diskriminantı…….....39

5.SONUÇ…….…….....41
5.1 Galois Grubu Çift Olan Trinomialler…….....41
5.2 Diskriminantı,Asal Sayılardan Oluşan Bir Küme S
Olmak Üzere,p ¿ S Asal Sayıları İle Aralarında
Asal Trinomialler…….....44

YARARLANILAN KAYNAKLAR……..... 54
ÖZGEÇMİŞ…….....55

1.GİRİŞ

Q rasyonel sayılar cisminin trinomial genişlemeleri, rasyonel trinomiallerin parçalanış cisimleridir. Her n ≥2 tam sayısı için Q üzerindeki Galois grubu A_n alterne grubuna izomorf olan Q cisminin sonsuz genişlemeleri olduğunu ilk olarak 1892 yılında Hilbert ispatlamıştır (Hermez,A.,Salinier,A.,2001).

Bu çalışmada öncelikle Q cismi üzerindeki Galois grubu A_n alterne grubuna izomorf olan rasyonel trinomiallerin varlığı gösterildi. Daha sonra asal sayılardan oluşan bir küme S olmak üzere, Q cismi üzerindeki Galois grubu A_n alterne grubuna izomorf olan ve diskriminantı p ¿ S asal sayıları ile bölünmeyen f(x) ¿ Z[X] indirgenemez trinomiallerin varlığı ispatlanmıştır.

Bu amaca ulaşmak için ikinci bölümde cisim genişlemeleri ve parçalanış cisimleri hakkında tanımlar ve ilgili teoremler ispatları ile birlikte açıklandı. Üçüncü bölümde Galois teorisinin temel tanım ve teoremleri ele alındı. Dördüncü bölümde ise bir polinomun diskriminantı ve özel olarak 2. ve 3. dereceden polinomların diskriminantları ispatları ile birlikte verildi.

Sonuç bölümde Galois grubu A_n alterne grubu tarafından kapsanan trinomiallerin varlığı incelendi. Daha sonra asal sayılardan oluşan bir küme S olmak üzere , diskriminantı p ¿ S asal sayıları ile bölünmeyen f(x) ¿ Z[x] indirgenemez trinomiallerin varlığı ispatlandı.

2. ÖN BİLGİLER

2.1 Cisim Genişlemeleri

Tanım 2.1.1:E bir cisim ve F, E'nin alt cismi olsun. O zaman E ye F'nin bir cisim genişlemesi denir ve E/F ile gösterilir.

Tanım 2.1.2: E /F bir cisim genişlemesi S⊂E bir alt kümesi olsun E'nin F ve S'yi kapsayan bütün alt cisimlerinin ara kesiti F(S) ile gösterilir. F(S) cismine F ye S'nin elemanları katılarak elde edilen cisim veya F ve S ile doğrulan cisim denir.

Teorem 2.1.1: E/F bir cisim genişlemesi olsun. O zaman E, F üzerinde bir vektör uzayıdır.

İspat : Bir skalerle çarpma işlemini E'deki çarpma olarak alırsak, vektör uzayı olma şartlarının sağlandığı açıktır.

Tanım 2.1.3: E/ F bir cisim genişlemesi olsun. E nin F-uzayı olarak boyutuna E nin F üzerindeki derecesi denir ve $boy_F E = [E, F]$ ile gösterilir.

Tanım 2.1.4: $[E, F]$ sonlu ise E ye F nin sonlu cisim genişlemesi ve $[E, F]$ sonsuz ise E ye F nin sonsuz cisim genişlemesi denir.

Örnek 2.1.1:*C*/R(*C*:Kompleks cisim,R:Reel cisim) sonlu cisim genişlemesidir.

$$C = \{a + ib : a, b \in R\}$$

$\{1, i\}$ kümesi *C*'yi R- uzayı olarak gerer ve lineer bağımsızdır. Dolayısıyla $\{1, i\}$ *C'* nin *R* üzerindeki bir tabanıdır.

boy $_R(C)=2 \Rightarrow [C:R]=2$ dir.

Tanım 2.1.5: E / F bir cisim genişlemesi ve $u \in E$ olsun. $f(u)=0$ olacak şekilde bir $0 \neq f(x) \in F[x]$ polinomu varsa, *u*' ya F üzerinde cebirsel eleman denir. Eğer böyle bir f(x) ¿ 0(x) polinomu yoksa, o zaman *u*' ya F üzerinde transandant eleman denir.

Tanım 2.1.6: *C* nin *Q*(rasyonel sayılar cismi) üzerinde cebirsel olan elemanına cebirsel sayı, transandant olan elemanına transandant sayı denir.

Örnek 2.1.2: $u \in F$ ise, u, F üzerinde cebirsel olur; çünkü u elemanı $f(x)=x-u \in F[x]$ polinomunun köküdür.

Örnek 2.1.3: $\sqrt{2} \in R$, Q üzerinde cebirseldir; çünkü $\sqrt{2}$, $x^2-2 \in Q[x]$ polinomunun bir köküdür.

Tanım 2.1.7: E / F cisim genişlemesi olsun. Eğer *u, F* üzerinde cebirsel ise, *F* ve *u'* yu içeren en küçük alt cisim olan *F*(*u*)'ya *F*'nin basit cebirsel genişlemesi denir.

$F(u)=\left\{ \frac{f(u)}{g(u)} \mid f(x), g(x) \neq 0 \in F[x] \right\}$ dır.

Teorem 2.1.2: E/F cisim genişlemesi ve $u \in E$ cebirsel olsun O zaman öyle bir $p(x) \in F[x]$ monik indirgenemez polinom vardır ki

$p(u)=0$ dır. $p(x)$ tektir. Ayrıca $g(x)\in F[x]$ ve $g(u) = 0$ ise, $p(x)$ |g(x) dir.

İspat : u,E üzerinde cebirsel olduğundan öyle bir $0\neq p(x)\in F[x]$ vardır ki $p(u) = 0$ dır. der(p(x)) ¿ 1 ve $F[x]$ bir tek türlü çarpanlara ayırma bölgesi olduğundan öyle $p_1(x),\ldots\ldots p_r(x)\in F[x]$ indirgenemez polinomları vardır ki

p(x)= $p_1(x)\,p_2(x)\ldots p_r(x)$ dir.

Buradan $0=p(u)=p_1(u)\,p_2(u)\ldots p_r(u)\,olur.$ $p_i(u)$ ¿ E ve E sıfır bölensiz olduğundan bir 1 ¿ $k\leq r$ için $p_k(u)=0$ dır.Şimdi $p(x)$ = p_k (x) olsun. p(x) in başka katsayısını tersi ile çarparak p(x)'i monik yapabiliriz. g(x) ¿ $F[x]$ olmak üzere g(u) = 0 olsun. g(x)= $q(x)\,p(x)+r(x)$ *ve* der $(r(x))<der(p(x))$ olacak biçimde q(x) , r(x) ¿ $F[x]$ vardır. Buradan $0=g(u)=q(u)\,p(u)+r(u)=0+r(u)$ olur. r(x) = 0 olsun.

Öyleyse $p(u)=r(u)=0$ dır.Ayrıca $(p(x),r(x))=d(x)$ olsun.O zaman

$p(x)\,a(x)+r(x)\,b(x)=d(x)$ ve $d(u)$= 0 ise der(d(x)) ¿ 1 dir. Ayrıca $d(x)|\,p(x)$ ve p(x) indirgenemez olduğunda der(d(x)) = der(p(x)) dır.Aynı zamanda d(x)|r(x) olduğundan der(d(x)) ¿ $der(r(x))<der(p(x))$ ise, $r(x)\neq 0$ bu ise çelişkidir.

Bundan dolayı $r(x)=0$ ve $g(x)=q(x)\,p(x)$ dir. Şimdi p(x) in tekliğini gösterelim g(x) indirgemez; monik ve g(u)= 0 olsun.

Yukarıdaki açıklamalardan dolayı $p(x)|g(x) \Rightarrow g(x)=cp(x)$ $\Rightarrow c=1 \Rightarrow g(x)=p(x)$ olur.

Tanım 2.1.8: *E/F* bir cisim genişlemesi ve $u \in E, F$ üzerinde cebirsel olsun. u için bir önceki teoremden elde edilen *u*'yu kök kabul eden en küçük dereceli p(x) polinomuna minimal polinom denir ve *ind*(*u*,*F*) = *p*(x) ile gösterilir. *der*(*p*(x))'e de *u*'nun *F* üzerindeki derecesi denir.

Teorem 2.1.3: *F* bir cisim ve $f(x) \in F[x]$ bir indirgenemez polinom olsun. O zaman *F* nin öyle bir cisim genişlemesi *E* vardır ki *f*(x)' in *E* içinde bir kökü vardır.

İspat: *F*[x] esas idealler bölgesi ve $f(x) \in F[x]$ indirgenemez olduğundan (*f*)=(*f*(x)) esal ideal olup, dolayısıyla maksimal ideal olur.(*f*(x)) maksimal ideal olduğundan *F*[x]/(*f*) bir cisimdir.

E=*F*[x]/(*f*) olarak alalım.

$\sigma : F \to E$

$a \mapsto a + (f)$

örten dönüşümü bir halka homomorfizmasıdır. Çünkü; her a,b $\in$ F için

σ (a+b)=(a+b)+(*f*) = (a+(*f*)) + (b+(*f*)) = $\sigma(a)+\sigma(b)$ ve

$\sigma(a.b)=$ a.b+(*f*) = (a+(*f*)).(b+(*f*)) = σ (a). σ (b) dır.

σ (1) = 1+(*f*) $\in$ 0 +(*f*) ise $1_E \in 0_E$ olduğundan σ bir cisim homomorfizmasıdır. Her $a \in F$ elemanını a +(*f*) ile özdeş kılınırsa *F*

¿ E olur. F ¿ E ise E, F nin bir cisim genişlemesidir. u = x+(f) ¿ E olsun. Şimdi u ¿ E nin f(x) in bir kökü olduğunu gösterelim:

f (x) = $c_0+c_1x+\ldots+c_nx^n\in F[x],(c_n\neq 0)$ olsun. O zaman

f (u) = $c_0+c_1(x+(f))+c_2(x+(f))^2+\ldots+c_n(x+(f))^n$

= $c_0+c_1+c_2x^2+\ldots+c_nx^n+(f)$

= $f(x)+(f)$

= $(f(x))=0_E\in E$ dir.

Sonuç olarak $u\in E$, $f(x)$ in bir köküdür.

Teorem 2.1.4*:* *E/F* bir cisim genişlemesi ve u ¿ E , F üzerinde cebirsel olmak üzere $E=F(u)$ *ve* $der(ind(u,F))=n$ olsun.O zaman $1,u,\ldots,u^{n-1}$ E'nin bir F-uzayının bazını oluşturur. Böylece her b ¿ E elemanı $c_0+c_1u+\ldots+c_{n-1}u^{n-1}\in F$ olmak üzere tek türlü $b=c_0+c_1u+\ldots+c_{n-1}u^{n-1}$ biçiminde yazılabilir.

İspat : *ind*(u,F) = p(x) olsun, *der*(p(x)) = n dir. $f(x)\in F[x]$ olsun. $f(x)=q(x)p(x)+r(x)$ ve der(r(x)) ¿ $n-1$ olacak biçimde tek q(x),r(x) ¿ $F[x]$ vardır.

İki tarafa ψ_u değer homomorfizması uygulanırsa

$f(u)$=q(u)p(u)+r(u)

=0+r(u)=r(u) ise $f(u)$ = r(u) olur.

$r(x)=c_0+c_1x+\ldots+c_{n-1}x^{n-1}$ olacak biçimde $c_0,c_1,\ldots,c_{n-1}\in F$ vardır.

$f(u)=r(u)=c_0+c_1u+\ldots+c_{n-1}+u^{n-1}$ ve $1,u,\ldots,u^{n-1}$ kümesi,*E*'yi *F*-uzayı olarak gerer. Mümkünse lineer bağımsız olmasın.O zaman en az biri sıfırdan farklı olan öyle $c_0,c_1,\ldots,c_{n-1}\in F$ vardır ki $c_0+c_1u+\ldots+c_{n-1}u^{n-1}=0$ olur.Bu durumda *r*(x)'in katsayılarından en az biri sıfırdan farklı olduğundan $r(x)\neq 0$ dır.Böylece *r*(*u*)=0ve $p(u)=0\Rightarrow p(x)|r(x)$ olur. der $r(x)<der\ p(x)$ olduğundan bu bir çelişkidir.Bundan dolayı $c_0=c_1=\ldots=c_{n-1}=0$ olacağından $1,u,\ldots,u^{n-1}$ lineer bağımsız olur.

Örnek 2.1.4: $Q\left(\sqrt[3]{2}\right)$ cismini ve Q - tabanını bulalım. $\sqrt[3]{2}$ = u olsun. O zaman ind$\left(\sqrt[3]{2},Q\right)=x^3-2$ olur. Teorem 2.1.4'den $\left\{1,\sqrt[3]{2},\sqrt[3]{4}\right\}$, $Q\left(\sqrt[3]{2}\right)$'nin bir Q -bazıdır.Böylece Q $\left(\sqrt[3]{2}\right)=\left\{a+b\sqrt[3]{2}+c\sqrt[3]{4}:a,b,c\in Q\right\}$ olarak bulunur.

2.2 Cebirsel Genişlemeler

Tanım 2.2.1: E/ F bir cisim genişlemesi olsun. E nin her elemanı F üzerinde cebirsel ise, E ye F nın bir cebirsel genişlemesi denir.

Teorem 2.2.1: Her sonlu cisim genişlemesi bir cebirsel genişlemedir.

İspat:E / F bir sonlu cisim genişlemesi ve u ¿ E olsun. $[E:F]$ = n olacak biçimde $n \geq 1$ tamsayı vardır.Burada n+1 tane $1, u, \ldots, u^n$ elemanları F üzerinde lineer bağımlıdır.Dolayısıyla en az biri sıfırdan farklı olan $c_0, c_1, \ldots, c_n \in F$ vardır ki $c_0 + c_1 u + \ldots + c_n u_1^n = 0$ dır.

f(x)= $c_0 + c_1 x + \ldots + c_n x^n$ olsun. Buradan $f(x) \neq 0$ *ve* $f(u) = 0$ olur. Bundan dolayı u, F üzerinde cebirseldir.

Teorem 2.2.2: F ¿ $E \leq K$ bir cisim kulesi ve E /F,K/E birer sonlu cisim genişlemesi olsun. O zaman K/ F sonlu cisim genişlemesi ve $[K:F] = [K:E].[E:F]$ dir.

İspat: $[E:F] = m$ *ve* $[K:E] = n$ olsun.

$[K:F] = m \cdot n$ olduğunu göstermek yeter. E nin bir F-bazı $\{u_i : 1 \leq i \leq m\}$ ve K nın bir E-bazı $\{v_j : 1 \leq j \leq n\}$ olsun. $\{u_i . v_j : 1 \leq i \leq m,\ 1 \leq j \leq n\}$ nin R nın F –bazı olduğunu göstermek yeter.

$y \in K$ *ve* $y = \sum_{j=1}^{n} b_J v_J$, $b_j \in E$

ile $b_j = \sum_{i=1}^{m} a_{ij} u_i$, $a_{ij} \in F$ *olsun*.

Böylece;

$$y=\sum_{j=1}^{n}\left(\sum_{i=1}^{m}a_{ij}u_i\right)v_j$$

$$=\sum_{j=1}^{n}\sum_{i=1}^{m}a_{ij}u_iv_j \text{ bu bir lineer kombinasyondur.}$$

$$\sum_{\substack{1\le j\le n\\ 1\le i\le m}} ¿¿u_Iv_J=0\Rightarrow\sum_{j=1}^{n}\left(\sum_{i=1}^{m}c_{ij}u_i\right)v_j=0¿$$

$$\Rightarrow\sum_{j=1}^{n}c_{ij}u_i=0 \quad , \quad j=1,2,\ldots,n$$

$$\Rightarrow c_{ij}=0 \quad ; \quad \begin{matrix} i=1,2,\ldots,n \\ j=1,2,\ldots,n \end{matrix}$$

dır. Bundan dolayı $\{u_iv_j\}$ kümesi F üzerinde lineer bağımsızdır.

Örnek 2.2.1: E=Q$(\sqrt{2},\sqrt{3})$ ve B= Q$(\sqrt{2})$ olsun . $\sqrt{3}$ 'ün Q (rasyonel sayılar cismi) üzerindeki minimal polinomu x^2-3 tür. Bunun yanında $\sqrt{3}$, $B=Q(\sqrt{2})$ üzerinde cebirsel ve $\sqrt{3}$ ün B üzerindeki indirgenemez polinomu x^2-3 'ün bir bölenidir. Teorem den $[E:Q(\sqrt{2})]\le 2$ dir.Gerçekte $[E:Q(\sqrt{2})]=2$ dir. Çünkü

$\sqrt{3} \notin Q(\sqrt{2})$ dir. Tersine $\sqrt{3} \in Q(\sqrt{2})$ olsaydı a,b∈Q olmak üzere

$$\sqrt{3} = a + b\sqrt{2} \Rightarrow 3 = a^2 + 2ab\sqrt{2} + 2b^2 \Rightarrow \sqrt{2} = \frac{3 - a^2 + 2ab\sqrt{2} + 2b^2}{a \cdot b}$$

olurdu.

Bu ise, $\sqrt{2}$ irrasyonel olduğundan bir çelişkidir. Teorem 2.2.2'den $[E:Q] = [E:Q(\sqrt{2})] \cdot [Q(\sqrt{2}):Q]$

= 2.2=4 tür.

Sonuç 2.2.1:E/F bir cisim genişlemesi ve u ¿ E olsun.Eğer u ,F üzerinde cebirsel ise, F(u)/F sonlu ve dolayısıyla cebirseldir. Ayrıca [F(u):F]=der((u,F)) dir.

İspat :der(ind(u,F))=n olsun.Teorem 2.1.4'den {1, $u, u^2, \ldots, u^{n-1}$ } kümesi F(u)'nun bir F bazıdır. Böylece [F(u):F] = n dir.Teorem 2.2.1'den F(u)/F cebirsel genişlemedir.

Sonuç 2.2.2:E/F bir cisim genişlemesi ve $u_1, u_2, \ldots, u_n \in E$, F üzerinde cebirsel olsun. O zaman F($u_1, u_2, \ldots, u_n)/F$ sonlu ve bir cebirsel genişlemedir.

İspat :İspatı n üzerinden indiksiyon ile yapalım. n=1 için sonuç 2.2.1'den doğru olur. Kabul edelim ki sonuç2.2.1'den n>1 ve n-1 için doğru olsun. O zaman [F($u_1, u_2, \ldots, u_{n-1}): F$] sonludur. u_n , F üzerinde cebirsel ve F[x] ¿ F($u_1, u_2, \ldots, u_{n_{-1}}$) [x] olduğundan u_n , $F(u_1, u_2, \ldots, u_{n_{-1}})$ üzerinde cebirseldir. Sonuç 2.2.1'den

$[F(u_1,u_2,\ldots,u_{n-1},u_n):F(u_1,u_2,\ldots,u_{n-1})]$ sonlu ve dolayısıyla cebirseldir.

Sonuç 2.2.3:E/F bir cisim genişlemesi ve u,v ¿ E , F üzerinde cebirsel olsun. O zaman u+v , u-v , u.v ve u/v (v ¿ 0) elemanları da F üzerinde cebirseldir.

İspat: Sonuç 2.2.2'den F(u,v) , F üzerinde cebirseldir. u+v , u-v , u.v ve u/v (v ¿ 0) elamanları F(u,v) cisminin elamanları olduğundan tanım 2.2.1'den bu elemanlar da F üzerinde cebirseldir.

2.3 Parçalanış Cisimleri

Tanım 2.3.1:F bir cisim ve $f(x)\in F[x]$ indirgenemez bir polinom olsun. F cisminin bir E cisim genişlemesi verildiğinde E[x] içinde $f(x)=(x-u_1)(x-u_2)\ldots(x-u_n),u_i\in E$ olursa ve E= $F(u_1,u_2,\ldots,u_n)$ ise, yani E cismi $f(x)$ in kökleri tarafından üretilirse E/F genişlemesine $f(x)$ 'in F üzerinde parçalanış cismi denir. Burada E, $f(x)$ in köklerini katarak elde edilen en küçük cisimdir.

Teorem 2.3.1:F bir cisim olsun. Pozitif dereceli her bir $f(x)\in F[x]$ polinomunun E/F gibi bir parçalanış cismi vardır.

İspat: $f(x)\in F[x]$ monik ve der $f(x)=n$ verilsin. $f(x)$ polinomu $f(x)=f_1(x).f_2(x)\ldots f_k(x)$ şeklinde indirgenemez polinomların bir çarpımı şeklinde yazılsın. $f_i(x)$ ler , F üzerinde

indirgenemez monik polinomlardır.İspatı n-k üzerindeki indiksiyon ile yapalım.

i) n-k=0 ise , yani $f_i(x)$ lerin her biri lineer ise $f(x)$ in $u_1, u_2, \ldots, u_n$ köklerinin hepsi F cisminde olduğundan $f(x)$ in F üzerindeki parçalanış cismi kendisidir.

ii) $f_i(x)$ lerden en az birisi diyelim ki $f_1(x)$ lineer polinom değilse $k < n$ olur ve buradan da $n-k$ >0 olur.Teorem2.1.3 de gösterildiği gibi $f_1(x)$ indirgenemez olduğundan K= $F[X]/(f_1(x))$ bir cisimdir.Ayrıca K/F bir cisim genişlemesi ve $u=x+(f_1(x)) \in$ K dersek u , $f_1(x)$ in bir köküdür. $u \in$ K , $f_1(x)$ in kökü olduğundan $f_1(x)=(x-u)g(x) \in$ K[X] ise $f(x)=f(x)f_2(x)\ldots f_k(x) \in$ $F[X]$ = $(x-u)g(x)f_1(x)f_2(x)\ldots f_k(x) \in$ K[X] dir.

f(x) in K[X] deki çarpanlara ayrılışındaki indirgenemez çarpanların sayısı m ise, o zaman $m>k$ dır. O halde n-m<n-k olduğundan teorem tümevarım hipotezine göre f(x) ve K için doğrudur.Böylece E[X]'de $f(x)=\prod_{i=1}^{n}(x-u_i)$ şartını sağlayan bir E=K($u_1, u_2, \ldots, u_n$) genişlemesini bulabiliriz. Ayrıca K=F(u) dır. Çünkü $f_1(u)=0$ ve

$f_1(x) \mid f(x)$ ise, $f(u)=0$ dır. Burada bazı i ler için $u = u_i$ dır O zaman E=K($u_1, u_2, \ldots, u_n$)$=F(u)(u_1, u_2, \ldots, u_n)=F(u, u_1, u_2, \ldots, u_n)$

$$= F(u_1, u_2, \ldots, u_n)$$

olur. Dolayısıyla E, $f(x)$'in F üzerindeki bir parçalanış cismidir.

Örnek 2.3.1: $f(x)=x^2+1 \in R[x]$ polinomun R üzerindeki parçalanış cismi C dir. Çünkü $f(x)=(x-i)(x+i) \in C[x]$ polinomun kökleri i ve $-i$ dir. Şu halde $f(x)$ in parçalanış cismi

$E = R(-i,i)=R(i)=C$ dir. Diğer yandan $f(x)=x^2+1 \in Q[x]$ polinomun Q üzerindeki parçalanış cismi $E=Q(i) \subset C$ dir. Çünkü E, $f(x)$ in köklerini Q cismine katarak elde edilen en küçük cisimdir.

2.4 Ayrılabilir Genişlemeler

Tanım 2.4.1: E/F bir cisim genişlemesi ve $f(x) \in F[x]$ olsun. $u \in E$ için $f(u)=0$ ise u' ya $f(x)$'in bir sıfırı (kökü) denir. $f(x)=(x-u)^s . g(x)$ için u ya s-katlı kök denir. Eğer $s=1$ ise, u ya basit (tek katlı kök) denir.

Tanım 2.4.2: $f(x)=a_0+a_1 x+\ldots+a_n x^n \in F[x]$ için $f'(x)=a_1+2a_2 x+\ldots+na_n x^{n-1}$ polinomuna $f(x)$ in türevi denir.

Teorem 2.4.1: $f(x)\in F[x]$ ve F' in E parçalanış cismi içindeki bir kökü u olsun. O zaman u' nun çok katlı kök olması için gerek ve yeter şart $f'(u)=0$ olmasıdır.

İspat: u , s-katlı kök olsun. Önce $f(x)=(x-u)^s f_1(x)$ olacak biçimde $f_1(x)\in E$ vardır. Türev alma kurallarından $f'(x)=s(x-u)^{s-1}f_1(x)+(x-u)^s f_1'(x)$, $(s-1\geq 1)$ dir.

Böylece $f'(u)=s(u-u)^{s-1}f_1(u)+(u-u)^s f_1'(u)=0$ olur. Karşıt olarak $f'(u)=0$ kabul edelim. $f(x)=(x-u)^s f_1(x)$ ve $s\geq 1$ mümkünse $s=1$ olsun. $f(x)=(x-u)^s f_1(x)\Rightarrow f'(x)=f_1(x)+(x-u)f_1'(x)$ dir. Böylece

$$0=f'(u)=f_1(u)+(u-u)f_1'(u)=f_1(u)\Rightarrow(x-u)\,|\,f_1(x)$$

$$\Rightarrow f_1(x)=(x-u)f_2(x)$$

olacak biçimde $f_2(x)\in E[x]$ vardır. Bu durumda $f(x)=(x-u)^2 f_2(x)\Rightarrow s\geq 2$ olur. Bu ise, bir çelişkidir.

Teorem 2.4.2: $f(x)\in F[x]$ indirgenemez polinom olsun. Char(F)=0 ise, $f(x)$'in E/F parçalanış cismi içinde çok katlı kökü yoktur.

İspat: $f(x)=a_0+a_1x+\ldots+a_nx^n, a_n\neq 0$ olsun. Bu durumda $f'(x)=a_1+2a_2x+\ldots+na_nx^{n-1}$ dır. $u\in E, f(x)$ in çok katlı bir kökü olsun. O zaman $f(u)=f'(u)=0\Rightarrow(x-u)|f(x)$ ve $(x-u)|f'(x)$ dir. $(f(x),f'(x))=d(x)$ olacak biçimde $d(x)\in F[x]$ vardır. Böylece $(x-u)|d(x)\Rightarrow der(d(x))\geq 1, d(x)|f(x)$ ve $f(x)$ indirgenemez olduğundan $der(d(x))=n$ ise, $d(x)=f(x)$ dir. Diğer yandan $der(f'(x))\leq n-1\Rightarrow f'(x)=0$ dır. Ancak Char(F)=0 ise, $na_n\neq 0$ olduğundan $f'(x)\neq 0$ olmalı. Bu ise bir çelişki olduğundan u , $f(x)$ in tek katlı köküdür.

Tanım 2.4.3: $f(x)\in F[x]$ indirgenemez bir polinom olsun. $f(x)$ in E parçalanış cismi içerisinde hiçbir katlı kökü yoksa $f(x)$ polinomuna ayrılabilir polinom denir.

Tanım 2.4.4: $F\subset E$ 'nin alt cismi ve $u\in E$, F üzerinde cebirsel olsun. Eğer $ind(u,F)$ ayrılabilir polinom ise u'ya F üzerinde ayrılabilir eleman denir. Eğer E nin her elemanı F üzerinde ayrılabilir ise, E ye F' nin ayrılabilir genişlemesi denir.

Teorem 2.4.3: E , F cisminin parçalanış cismi ve Char(F)=0 olsun.O zaman E/F ayrılabilir genişlemedir.

İspat: $u\in E$ ve $f(x)=ind(u,F)$ olsun.Char(F)=0 olduğundan bir önceki teoremden u, F üzerinde ayrılabilirdir.

Örnek 2.4.1: Q'nun sonlu genişlemeleri ayrılabilirdir.

Tanım 2.4.5:Eğer *F*[x] içinde her bir polinom ayrılabilir ise, *F* cismine mükemmel cisim denir.

Teorem 2.4.4: Karakteristiği sıfır olan bütün cisimler mükemmeldir.

İspat: Teorem 2.4.2'den Char(*F*) =0 ise, *F*[x] deki indirgenemez bir polinomun parçalanış cismi içerisindeki bütün kökleri basittir.Böylece *F*[x] deki her polinom ayrılabilirdir.Tanımdan *F* mükemmeldir

3. GALOİS TEORİSİ

3.1 Bir Cismin Otomorfizma Grubu

Tanım 3.1.1. : E bir cisim olsun. E'den E'ye tanımlı bir σ izomorfizmasına E cisminin bir otomorfizması denir. Bu otomorfizmaların kümesi Aut (E) ile gösterilir.

Teorem 3.1.1. : E bir cisim olsun. Aut(E) kümesi fonksiyon birleşimi işlemine göre gruptur.

İspat: Aut(E) = $\{\sigma_i \mid \sigma_i : E \to E, \sigma$ otomorfizma$\}$

(i) Her $\Im, \sigma \in$ Aut(E) ve a, b $\in$ E için;

$\Im(a+b) = \Im(a) + \Im(b)$

$\Im(a.b) = \Im(a)\,\Im(b)$

$\Im\sigma(a+b) = \Im(\sigma(a) + \sigma(b))$

$= (\Im\sigma)(a) + (\Im\sigma)(b)$

$\Im\sigma(a.b) = \Im(\sigma(a).\sigma(b))$

$= \Im(\sigma(a).\sigma(b))$

$= \Im(\sigma(a)).(\Im\sigma(b))$

$= (\Im\sigma)(a).(\Im\sigma)(b)$ olduğundan

$\Im\sigma : E \to E$ bir halka homomorfizmasıdır. σ ve $\Im$ bire-bir ve örten olduğundan $\Im\sigma$ da bire-bir örtendir.

Böylece $\sigma\Im \in Aut(E)$ dir.

(ii) Her $a \in E$ için $I_E(a)=a$ olduğundan $I_E \in Aut(E)$ dir.

(iii) Her $\Im_1, \Im_2, \Im_3 \in Aut(E)$ için

$\Im_1(\Im_2\Im_3)=(\Im_1\Im_2)\Im_3$ olduğundan birleşme özelliği sağlanır.

(iv) Her $\Im \in Aut(E)$ bire-bir örten olduğundan $\Im^{-1} \in Aut(E)$ vardır.

Sonuç olarak Aut(E) fonksiyon birleşimi işlemine göre bir grupur.

Tanım 3.1.2 : F bir cisim ve f(x) ¿ F[x] polinomunun F üzerindeki parçalanış cismi E olsun.

$Gal(E/F) = Aut_F(E) = \{\sigma \in Aut(E) : \sigma(a) = a, \text{ her } a \in F \text{ için}\}$

grubuna E'nin F'yi sabit bırakan otomorfizmaların grubu veya E'nin F üzerindeki Galois grubu denir.

Ayrıca $Gal(E/F) \subset Aut(E)$ olduğu açıktır.

Teorem 3.1.2 : E/F bir cisim genişlemesi ve $f(x) \in F[x]$ olsun. Eğer $u \in E$, f(x) in bir kökü ve $\sigma \in Gal(E/F)$ ise o zaman $\sigma(u)$'da f(x) polinomunun bir köküdür.

İspat : $f(x) = c_0 + c_1x + \ldots + c_nx^n \quad (c_n \neq 0)$ ve $f(u) = 0$ olsun.

O zaman

$0 = \sigma(f(u)) = \sigma(c_0) + \sigma(c_1u) + \ldots + \sigma(c_nu^n)$

$= \sigma(c_0) + \sigma(c_1)\,\sigma(u) + \ldots + \sigma(c_n)\,\sigma(u)^n$

$= c_0 + c_1\,\sigma(u) + \ldots + c_n\,\sigma(u)^n$

$= f(\sigma(u))$

olduğundan $\sigma(u)$, $f(x)$'in bir köküdür.

3.2 Normal Genişlemeler

Tanım 3.2.1 : E/F bir cebirsel genişleme olsun. Eğer E'de bir kökü olan F[x] içindeki her bir indirgenemez polinom E[x] içinde tamamen parçalanabilirse E'ye F cisminin bir normal genişlemesi denir.

Örnek 3.2.1: $f(x)=x^3 - 2 \in Q$ [x] polinomunun köklerinden biri $\alpha = \sqrt[3]{2}$ reel olup

$f(x) = (x - \sqrt[3]{2}\,).(x^2 + \sqrt[3]{2}\,x + \sqrt[3]{4}\,) \in Q(\sqrt[3]{2}\,)[x]$

$= (x - \sqrt[3]{2}\,).\, g(x)$ dir.

g(x)'in reel kökü olmadığından ve $Q(\sqrt[3]{2}) \subset R$ olduğundan $Q(\sqrt[3]{2}\,)[x]$ de indirgenemezdir. Dolayısıyla g(x) in kökleri $w = \dfrac{-1 + i\sqrt{3}}{2}$ olmak üzere αw ve αw^2 dir. Böylece f(x) in parçalanış cismi

$E = Q(\alpha,\ \alpha w, \alpha w^2) = Q(\alpha, w) = Q(\sqrt[3]{2}\,, i\sqrt{3}\,)$ tür.

Sonuç olarak E/Q normal genişleme olup $Q(\sqrt[3]{2})/Q$ normal genişleme değildir. Çünkü f(x), $Q(\sqrt[3]{2})$ [x] te tamamen parçalanmaz.

3.3 Galois Genişlemeleri

Tanım 3.3.1 : E/F bir sonlu cisim genişlemesi olsun.Eğer E, F üzerinde bir ayrılabilir parçalanış cismi yani;$[E:F] = |Gal(E/F)|$ ise, E'ye F'nin Galois genişlemesi denir.

Örnek 3.3.1 : $F = Q$ ve $E = Q(i\sqrt{3}) \subset C$ olsun. Bu durumda E/F genişlemesi sonlu ve $ind(i\sqrt{3}, Q) = x^2 + x + 1 \in Q$ [x] dir.

$[E : F] = der(ind(i\sqrt{3})) = 2$ dir.

$f(x) = ind(i\sqrt{3}, Q) = (x + \frac{1}{2}(1+i\sqrt{3})).(x - \frac{1}{2}(1-i\sqrt{3})) \in Q(i\sqrt{3})[x]$ ayrılabilir bir polinomdur.

$\sigma : E \to E$, $\quad \Im : E \to E$,

$i\sqrt{3} \to i\sqrt{3}$ $\quad$ $i\sqrt{3} \to -i\sqrt{3}$

olmak üzere E nin iki tane Q otomorfizmalarıdır. Bu durumda $Gal(E/F) = \{\sigma, \Im\}$ ve $|Gal(E/F)| = 2$ dir.

Sonuç olarak $|Gal(E/F)| = [E:F] = 2$ olup E/F Galois genişlemesidir.

Tanım 3.3.2 : E/F bir cisim genişlemesi ve $G = Gal(E/F)$ olsun.

İnv G = $\{a \in E \mid \sigma(a) = a, \forall \sigma \in G\} \subset E$ bir alt cisimdir.

i) $\forall$ a, b $\in$ İnv G için σ (a-b) = σ(a) - σ(b) = a – b $\in$ inv G

ii) $\forall$ a, b $\in$ İnv G için σ (a.b) = σ(a) . σ(b) = a.b $\in$ inv G

iii) $\forall$ a $\neq 0 \in$ İnv G için σ (a^{-1}) = $(\sigma(a))^{-1} = a^{-1} \in$ inv G dir.

Yukarıdaki şekilde tanımlanan inv G $\subset E$ alt cismine G = Gal(E/F) nin sabit cismi denir.

Teorem 3.3.1 : E/F bir cisim genişlemesi ve G = Gal(E/F) olsun. O zaman aşağıdaki özellikler vardır:

i) $G_1 \supset G_2 \Rightarrow$ inv $G_1 \subset$ inv G_2

ii) $F_1 \supset F_2 \Rightarrow$ Gal(E/F_1) $\subset$ Gal (E/F_2)

iii) inv (Gal (E/F)) $\supset F$ dir.

iv) inv Gal (E/inv G) $\supset F$ dir.

İspat :

i) $G_1 \supset G_2$ olsun. a $\in$ inv G_1 $\Rightarrow \forall \sigma \in G_1$ için σ(a) = a

$\Rightarrow \forall \sigma \in G_2$ için σ(a) = a

$\Rightarrow$ a $\in$ inv G_2

$\Rightarrow$ inv $G_1 \subset$ inv G_2

ii) $F_1 \supset F_2$ olsun.

$\sigma \in$ Gal (E/F_1) $\Rightarrow \sigma$ (a)=a, her a $\in F_1$

$\Rightarrow F_1 \supset F_2$ olduğundan σ(a) = a, her a $\in F_2$

$\Rightarrow \sigma \in$ Gal (E/F_2)

$\Rightarrow$ Gal (E/F_1) $\subset$ Gal (E/F_2)

iii) $\sigma \in$ Gal $(E/F) \Rightarrow \forall\, a \in F, \sigma(a) = a$

$\Rightarrow a \in$ inv Gal (E/F)

$\Rightarrow F \subset$ inv Gal (E/F)

iv) $\forall\, a \in F$ için $\sigma(a) = a, \sigma \in G \Rightarrow a \in$ inv G

$\Rightarrow \sigma \in$ Gal $(E/\text{inv } G)$

$\Rightarrow a \in$ inv Gal $(E/\text{inv } G)$

Yardımcı özellik 3.3.1 : *E/F* bir sonlu Galois genişlemesi ve K bir ara cisim olsun. O zaman E/K bir Galois genişlemesidir.

Teorem 3.3.2 : E/F bir sonlu Galois genişlemesi olsun.O zaman F = inv Gal (E/F) dir.

İspat : Gal (E/F) = $\{\sigma \in$ Aut(E): $\sigma(a) = a$, her $a \in$ F için$\}$

K = inv Gal (E/F) olsun.

Gal (E/K) = $\{\sigma \in$ Aut(E): $\sigma(b) = b$, her $b \in$ K için$\}$

E/F sonlu Galois genişlemesi olduğundan

|Gal(E/F)|=[E:F]dir ..... (*)

$\sigma \in$ Gal (E/F) olsun. $\sigma(b) = b$, her $b \in$ K için;

Diğer yandan Teorem 3.3.1 (iv) ten $F \subset K$ ise

Gal (E/F) $\geq$ Gal (E/K) olur. .....(**)

Bir önceki yardımcı özellikten E/K Galois genişlemesi dolayısıyla

$|Gal\ (E/K)| = [E:K]$ dir. .....(***)

(*), (**) ve (***) dan $[E:F] = [E:K]$ olur.

Diğer taraftan $[E:F] = [E:K].[K:F] \Rightarrow [K:F] = 1 \Rightarrow K = F$ dir.

Yardımcı özellik 3.3.2 : E/F bir sonlu Galois genişlemesi ve K bir ara cisim olsun.

K/F Galois $\Leftrightarrow$ Gal(E/K) $\triangleleft$ Gal (E/F) dir.

Bu durumda $Gal\ (K/F) \cong \dfrac{Gal\,(E/F)}{Gal\,(E/K)}$

Teorem 3.3.3 : E/F bir cisim genişlemesi ve E'nin F üzerinde Galois grubu

G = Gal (E/F) olsun.

Γ : G nin alt gruplarının kümesi, ve

Σ : $F \leq K \leq E$ şartını sağlayan K cisimlerinin kümesi olsun

O zaman;

$f: \Gamma \rightarrow \Sigma$ ve $g: \Sigma \rightarrow \Gamma$

$H \rightarrow inv\ H$ $K \rightarrow Gal\ (E/K)$

dönüşümleri birbirinin tersidirler ve dolayısıyla bire-bir örten dönüşümlerdir.

Üstelik şu özellikler vardır:

a) $H_1 \supset H_2 \Rightarrow \text{inv } H_1 \leq \text{inv} H_2$

b) $|H| = [E: \text{inv } H]$

c) $H \triangleleft G \Leftrightarrow$ inv H/F normal genişlemedir.

Bu durumda $Gal(\text{inv } H/F) \cong G/H$ dir.

İspat : $H \subset G$ nin alt grubu olsun. Teorem 3.3.2 den

$G = Gal(E/F) = Gal(E/\text{inv } G)$ dir.

Burada G yerine H alınırsa $Gal(E/\text{inv } H) = H$ olur.

$\Gamma \xrightarrow{f} \Sigma \xrightarrow{g} \Gamma$, $H \xrightarrow{f} \text{inv } H \xrightarrow{g} H$

$(gf)(H) = g(f(H)) = g(\text{inv } H) = Gal(E/\text{inv } H) = H = 1_\Gamma(H)$

böylece her $H \subset G$ için $gf = 1_\Gamma$ olur. ..... (*)

Yardımcı özellik 3.3.1 den $[E: \text{inv } H] = |Gal(E/\text{inv } H)| = |H|$ dir.

$H \subset G$ olduğundan $H \in \Gamma$dir.

$K \in \Sigma$ olsun. $H = Gal(E/K)$ diyelim.

E/F Galois genişlemesi olduğundan Yardımcı özellik 3.3.1 den E/K Galois genişlemesi ve Teorem 3.3.2 den de

$K = \text{inv } Gal(E/K)$ dir. .....(1)

$H = Gal(E/K)$ olduğundan Teorem 3.3.1 den $\text{inv } H = \text{inv } Gal(E/K)$...(2)

(1) ve (2) den $K = \text{inv } H = \text{inv } Gal(E/K)$ olur.

Böylece $(fg)(K) = f(g(K))$

$= F(Gal(E/K))$

$= \text{inv } Gal(E/K)$

$= \text{inv } H$

= K

= 1_Σ(K) dır. .....(**)

Sonuç olarak (*) ve (**) dan gf = 1_Γ ve fg = 1_Σ

$\Rightarrow$ f ve g tersinirdirler ancak ve ancak f ve g bire-bir ve örtendir.

(a) Teorem 3.3.1 den bulunur.

(b) Yukarıda gösterildi.

(c) F $\leq$ K $\leq$E ve H = Gal(E/K) olsun. Yukarıda K = inv H olduğu gösterildi. Yardımcı özellik 3.3.2 den H $\triangleleft$ G $\Leftrightarrow$ inv H/F normal genişlemedir. Dolayısıyla Gal(inv H/F) $\cong$ G/H dir.

Teorem 3.3.4: $f(x)\in F[x]$ in parçalanış cismi E olsun. O zaman Gal(E/F) grubu S_n simetrik grubun bir alt grubuna izomorflur .

İspat: $f(x)\in F[x]$ in E de ki bütün köklerin kümesi $x=\{\alpha_1,.....\alpha_n\}$ olsun,

$a,\sigma\in Gal(E/F)$ *olsun. O zaman* $\sigma_a(x)=a(x)=x$ *tir.*

$\psi : Gal(E/F)\to S_X$, $\psi(a)=\sigma_a$ olarak tanımlayalım.

ψ bir homomorfizmadır: $\forall a,b\in Gal(E/F)$ için,

$\sigma_{ab}(x)=(ab)(x)=a(\sigma_b(x))=\sigma_a(\sigma_b(x))$

$=(\sigma_a\cdot\sigma_b)(x)$ olduğundan

$\psi(ab)=\psi(a)\cdot\psi(b)$ tir.

ψ 1−1 dir. $a, b \in$ ¿ ¿ $Gal(E/F)$ için;

$\psi(a)=\psi(b) \Rightarrow \sigma_a(x)=\sigma_b(x) \Rightarrow a=b$ dir.

Böylece homomorfizma teoremine göre Gal(E/F) ¿ S_x ve $S_x \subset S_n$ olduğundan istenilen elde edilir.

Örnek 3.3.2: f(x) = $x^3 - 2 \in Q$ [x] polinomunun Q rasyonel sayılar cismi üzerinde parçalanış cismini,Gal(E/ Q) grubunu ve bu grubun alt grupları ile alt gruplarının sabit bıraktıkları ara cisimleri bulalım.

Çözüm 3.3.1: f(x)= $x^3 - 2$ polinomunun Q rasyonel sayılar cismi üzerindeki parçalanış cismi E olsun. f(x) in reel kökü $\sqrt[3]{2}$ olduğundan

f(x) = $(x - \sqrt[3]{2}).[x^2 + \sqrt[3]{2}\, x + (\sqrt[3]{2})^2] \in Q(\sqrt[3]{2})[x]$

$= (x - \sqrt[3]{2}).g(x) \in Q(\sqrt[3]{2})[x]$ dir.

$Q(\sqrt[3]{2}) \subset R$ ve g(x) in reel kökü olmadığında g(x), $Q(\sqrt[3]{2})[x]$ de indirgenemezdir. g(x)'in kökleri w = $\frac{-1+i\sqrt{3}}{2}$ olmak üzere $\sqrt[3]{2}$ w ve $\sqrt[3]{2}\, w^2$ dir. Şu halde f(x) in tüm kökleri $\sqrt[3]{2}$, $\sqrt[3]{2}$ w ve $\sqrt[3]{2}\, w^2$ olup parçalanış cismi $E(\sqrt[3]{2}, \sqrt[3]{2}\, w, \sqrt[3]{2}\, w^2) = Q(\sqrt[3]{2}, i\sqrt{3})$ tür.

Q mükemmel cisim olduğundan E/Q Galois genişlemesi olup [E:Q] = |Gal(E/Q)| = 6 dır. Bunu daha ayrıntılı inceleyelim:

E'nin Q otomorfizmaları $\sqrt[3]{2}$ ve $i\sqrt{3}$ ile belirlidir.

Bu otomorfizmalar:

$\sigma_1 : \sqrt[3]{2} \rightarrow \sqrt[3]{2}\ , \quad i\sqrt{3} \rightarrow i\sqrt{3}$

$\sigma_2 : \sqrt[3]{2} \rightarrow \sqrt[3]{2}\ w, \quad i\sqrt{3} \rightarrow i\sqrt{3}$

$\sigma_3 : \sqrt[3]{2} \rightarrow \sqrt[3]{2}\ w^2, \quad i\sqrt{3} \rightarrow i\sqrt{3}$

$\sigma_4 : \sqrt[3]{2} \rightarrow \sqrt[3]{2}\ , \quad i\sqrt{3} \rightarrow -i\sqrt{3}$

$\sigma_5 : \sqrt[3]{2} \rightarrow \sqrt[3]{2}\ w, \quad i\sqrt{3} \rightarrow -i\sqrt{3}$

$\sigma_6 : \sqrt[3]{2} \rightarrow \sqrt[3]{2}\ w^2 \quad i\sqrt{3} \rightarrow -i\sqrt{3}$

$\sigma = \sigma_2$ ve $\Im = \sigma_4$ diyelim.

$\sigma\,\Im\,(\sqrt[3]{2}) = \sigma\,(\sqrt[3]{2}) = \sqrt[3]{2}\ w,$

$\sigma\,\Im\,(i\sqrt{3}) = \sigma\,(-i\sqrt{3}) = -i\sqrt{3}$

$\sigma\,\Im : \sqrt[3]{2} \rightarrow \sqrt[3]{2}\ w,\ i\sqrt{3} \rightarrow -i\sqrt{3}$ olduğundan $\sigma\,\Im = \sigma_5$ tir.

$\sigma^2\,(\sqrt[3]{2}) = \sigma\,(\sqrt[3]{2}\ w) = \sqrt[3]{2}\ w^2$

$\sigma^2\,(i\sqrt{3}) = \sigma(i\sqrt{3}) = i\sqrt{3}$

$\sigma^2 : \sqrt[3]{2} \rightarrow \sqrt[3]{2}\ w^2, \quad i\sqrt{3} \rightarrow i\sqrt{3}$

olduğundan $\sigma^2 = \sigma_3$ tür.

$\sigma^2\,\Im\,(\sqrt[3]{2}) = \sigma^2\,(\sqrt[3]{2}) = \sqrt[3]{2}\ w^2,$

$\sigma^2\,\Im\,(i\sqrt{3}) = \sigma^2\,(-i\sqrt{3}) = -i\sqrt{3}$

$\sigma^2\,\Im : \sqrt[3]{2} \rightarrow \sqrt[3]{2}\ w^2,\ i\sqrt{3} \rightarrow -i\sqrt{3}$ olduğundan $\sigma^2\,\Im = \sigma_6$ dır.

$\sigma^3(\sqrt[3]{2}) = \sqrt[3]{2}$

$\sigma^3(i\sqrt{3}) = i\sqrt{3}$

$\sigma^3 : \sqrt[3]{2} \rightarrow \sqrt[3]{2}$, $i\sqrt{3} \rightarrow i\sqrt{3} \Rightarrow \sigma^3 = \sigma_1 = I$ dır.

$\Im^2 : \sqrt[3]{2} \rightarrow \sqrt[3]{2}$, $i\sqrt{3} \rightarrow i\sqrt{3} \Rightarrow \Im^2 = \sigma_1 = I$ dır.

Böylece $Gal(E/Q) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$

$= \{I, \sigma, \sigma^2, \Im, \sigma\Im, \sigma^2\Im\}$ olur.

θ ¿ $Gal(E/Q)$ için $\overline{\theta} \in S_3$ aşağıdaki gibi tanımlansın:

123
123
¿
righ
¿
¿
¿
123
231
¿
righ
¿
¿
¿
123
312
¿
righ
¿
¿
¿
123
132
¿
righ
¿
¿
¿
()
¿

¿

¿
123
213
¿
righ
¿
¿

Bu durumda

S_3 = {(1), (123), (132), (23), (12), (13)}= { I, $\bar{\sigma}$, $\bar{\sigma^2}$, $\overline{\Im}$, $\overline{\sigma\Im}$, $\overline{\sigma^2\Im}$ }tür.

$u_1 = \sqrt[3]{2}$, $u_2 = \sqrt[3]{2}\ w$, $u_3 = \sqrt[3]{2}\ w^2$, $w = \frac{-1+i\sqrt{3}}{2}$ olsun.

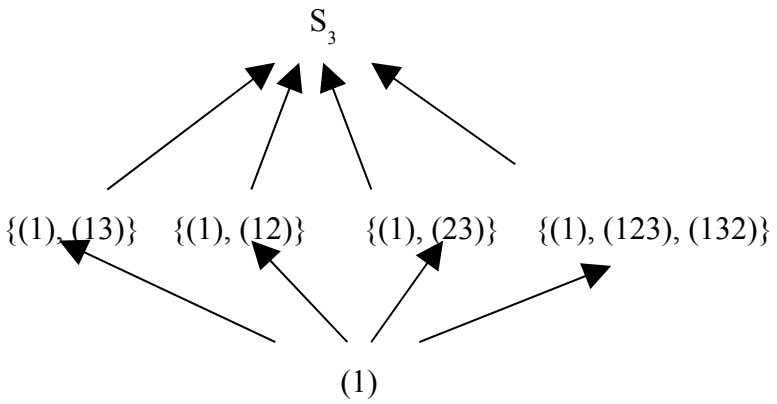
$\sigma : \sqrt[3]{2} \to \sqrt[3]{2}\ w, \quad \sqrt[3]{2}\ w \to \sqrt[3]{2}\ w^2, \quad \sqrt[3]{2}\ w^2 \to \sqrt[3]{2}$

$u_1 \to u_2, \qquad u_2 \to u_3 , \qquad u_3 \to u_1$

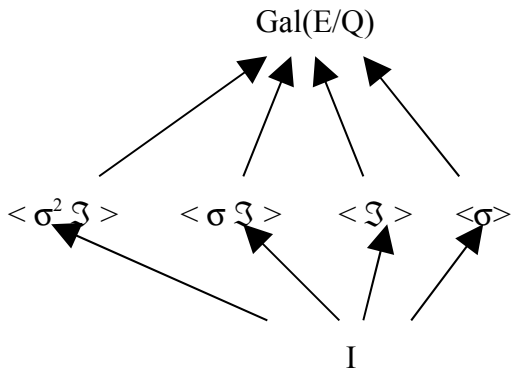
$\bar{\sigma} : \ 1 \to 2, \qquad 2 \to 3, \qquad 3 \to 1$

olduğundan benzer yolla $\psi : Gal(E/Q) \to S_3 \ , \theta \to \bar{\theta}$ dönüşümünün bir izomorfizma olduğu görülür.S_3 ve Gal(E/Q) grubunun alt gruplarının kafes diyagramları aşağıdaki gibi olur.

S_3'ün kafes diyagramı



Gal(E/Q) nun alt grup kafes diyagramı



Son olarak Gal(E/Q) grubunun alt gruplarına karşılık gelen ara cisimleri bulalım:

$E = Q(\sqrt[3]{2}, i\sqrt{3})$

İnv Gal(E/Q) = Q ve inv I = E olduğu açık.

$F_1 = inv < \sigma >$ diyelim.

Teorem 3.3.3 (b) den $[E:F_1] = | < \sigma > | = 3$ tür.

Diğer yandan $[E:Q] = [E:F_1].[F_1:Q]$, 6 = 3.2 ve $Q(i\sqrt{3}) \subset F_1$ ve $[Q(i\sqrt{3}):Q] = 2$ olduğundan $F_1 = Q(i\sqrt{3})$ tür. Aynı zamanda $\frac{|Gal|(E/Q)}{|<\sigma>|} = 2$ yani $< \sigma > \triangleleft$ Gal(E/Q) olduğundan Teorem 3.3.3 (c) den $Q(i\sqrt{3}/Q)$ normal genişlemedir.

$F_2 = inv < \Im >$ diyelim.

Teorem 3.3.3 (b) den $[E:F_2] = | < \Im > | = 2$ ise $[F_2 : Q] = 3$ tür.

Diğer yandan $Q(\sqrt[3]{2}) \subseteq F_2$ ve $[Q(\sqrt[3]{2}:Q)] = 3$ olduğundan $F_2 = Q(\sqrt[3]{2})$ dir.

$F_3 = inv < \Im >$ diyelim.

$\Im(w) = \Im\left(\frac{-1+i\sqrt{3}}{2}\right) = \frac{-1-i\sqrt{3}}{2} = w^2$

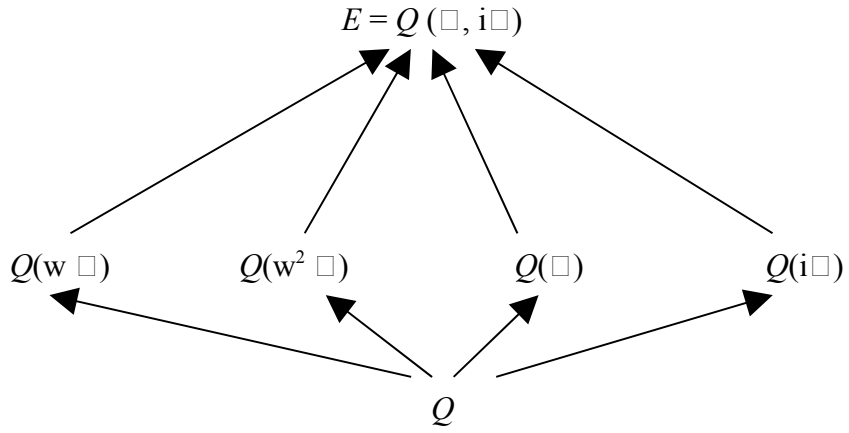
$\Im(w^2) = (\Im(w))^2 = w^4 = w$, $(w^3 = 1)$

$\sigma\,\Im(w^2\ \sqrt[3]{2}) = \sigma(w.\ \sqrt[3]{2}) = w^2\ \sqrt[3]{2}$ olduğundan $F_3 = Q(w^2\ \sqrt[3]{2})$ dir.

$F_4 = inv < \sigma^2\ \Im >$ diyelim.

$\sigma^2\ \Im\ (w\ \sqrt[3]{2}) = \sigma^2\ (w^2\ \sqrt[3]{2}) = w^2\ \sqrt[3]{2}\ w^2 = w\ \sqrt[3]{2}$ olduğundan

$F_4 = Q(w\ \sqrt[3]{2})$ dir. Bu durumda ara cisim kafes diyagramı



şeklinde olur.

4.DİSKRİMİNANTLAR

4.1 Bir Polinomun Diskriminantı

Tanım 4.1.1: F bir cisim ,f(x) = $a_0+a_1x+\ldots+a_{n-1}x^{n-1}+a_nx^n\in F[x]$ $(a_n\neq 0)$ polinomunun F üzerindeki parçalanış cismi E ve f(x)'in E'deki kökleri $\alpha_1,\alpha_2,\ldots,\alpha_n$ olsun.

$$D(f)=\prod_{1\leq i\leq j\leq n} a_n^{2(n-1)}(\alpha_i-\alpha_j)^2$$

ifadesine f(x) polinomunun diskriminantı denir.

Teorem 4.1.1: F bir cisim ,f(x) ¿$F[x]$, $der(f(x))=n\geq 1$ *ve* $f(x)$ 'in F cismi üzerindeki parçalanış cismi E olsun :

(i) $D(f)\neq 0$ gerek ve yeter koşul f(x)'in köklerinin farklı olmasıdır.

(ii) $D(f)\in F$ dır.

İspat:f(x)'in E'deki kökleri $\alpha_1,\alpha_2,\ldots,\alpha_n$ ve başkatsayısı $a_n\neq 0$ olsun.

(i) $(\Rightarrow)\quad D(f)=a_n^{2(n-1)}\cdot \prod_{i<j}(\alpha_i-\alpha_j)^2\neq 0\Rightarrow(\alpha_i-\alpha_j)^2\neq 0$

$\Rightarrow(\alpha_i-\alpha_j)\neq 0 \Rightarrow \alpha_i\neq\alpha_j\ ,\quad i\neq j$ için

$(\Leftarrow)\qquad i\neq j$ için $\alpha_i\neq\alpha_j\Rightarrow(\alpha_i-\alpha_j)\neq 0$

$\Rightarrow(\alpha_i-\alpha_j)^2\neq 0$

$\Rightarrow D(f)\neq 0$ dır.

(ii) D(f) ifadesi elemanter simetrik fonksiyonlardan oluştuğundan $a_i\in F$ ' ler cinsinden yazabiliriz.

Örnek 4.1.1 :F bir cisim olsun. $f(x)=x^2+bx+c\in F[x]$ polinomunun diskriminantını hesaplayalım.f(x)' in kökleri $\alpha_{1,2}=\frac{1}{2}\left(-b\mp\sqrt{b^2-4c}\right)$ olarak verilir.

Böylece $D(f)=(\alpha_1-\alpha_2)^2=(\alpha_1+\alpha_2)^2-4\alpha_1\cdot\alpha_2=b^2-4c$ olarak bulunur.

Örnek 4.1.2: $f(x)=x^2-\sqrt{5}\in R[x]$ polinomun diskriminantını inceleyelim. $f(x)=x^2-\sqrt{5}=\left(x-\sqrt[4]{5}\right)\left(x+\sqrt[4]{5}\right)\in R[x]$ olduğundan f(x)' in kökleri $x=\sqrt[4]{5}$ ve $x=-\sqrt[4]{5}$ olur.

Böylece $D(f)=(x_1-x_2)^2$

$=\left(\sqrt[4]{5}-\left(-\sqrt[4]{5}\right)\right)^2$

$$= \left(2\sqrt[4]{5}\right)^2 = 4\sqrt{5} \in R \quad \text{olur.}$$

Örnek 4.1.3:F bir cisim olsun. $f(x) = x^3 + qx + r \in F[x]$ polinomun diskriminantını inceleyelim.f(x)' in kökleri $\alpha_1, \alpha_2, \alpha_3$ y= $\sqrt[3]{\frac{1}{2}\left(-r + \sqrt{r^2 + 4q^3/27}\right)}$, $z = -q/3y$ ve birimin üçüncü dereceden kökü $\left(w = \frac{-1 + i\sqrt{3}}{2}\right)$ olmak üzere $\alpha_1 = y + z$, $\alpha_2 = wy + w^2 z$ $\alpha_3 = w^2 y + wz$ olarak verilir. $w^3 = 1$, $\left(w = \frac{-1 + i\sqrt{3}}{2}\right)$ olduğunu kullanarak

$$\alpha_1 - \alpha_2 = y + z - wy - w^2 z$$

$$= \left(y - w^2 z\right) - \left(wy - z\right)$$

$$= \left(y - w^2 z\right) - \left(y - w^2 z\right) w$$

$$= \left(y - w^2 z\right)(1 - w) \quad \text{bulunur.}$$

Benzer şekilde,

$$\alpha_1 - \alpha_3 = y + z - w^2 y - wz = \left(y - wz\right)\left(1 - w^2\right) \text{ ve}$$

$$\alpha_2 - \alpha_3 = wy + w^2 z - w^2 y - wz = \left(y - z\right) w \left(1 - w\right)$$

olarak bulunur.

Yukarıdaki değerleri $\Delta=[D(f)]^{1/2}=(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)$

ifadesinde yerine koyarak

$$\Delta=(y-z)(y-wz)(y-w^2z)w(1-w^2)(1-w)^2 \ldots\ldots\ldots\ldots \quad (*)$$

eşitliğini buluruz.

Burada

$$w(1-w^2)(1-w)^2=3i\sqrt{3},(i^2=-1), \quad ve \quad x^3-1=(x-1)(x-w)(x-w^2)$$

eşitliğinde $x=\frac{y}{z}$ yazarak

$(y-z)(y-wz)(y-w^2z)=y^3-z^3=\sqrt{r^2+4q^3/27}$ olarak bulunur.

Bu değerleri (*) da yerine koyarsak

$D(f)=\Delta^2=\left(3i\sqrt{3}\sqrt{r^2+4q^3/27}\right)^2=-27r^2-4q^3$ olarak bulunur.

Örnek 4.1.4: $f(x)=x^3-3x+1\in R[x]$ polinomun diskriminantını hesaplayalım.

f(x)'in diskriminantı

$$D(f)=-27r^2-4q^3=-27\cdot 1^2-4(-3)^3=-27+4\cdot 27=81$$

olarak bulunur.

Teorem 4.1.2: $\tau\in S_n$ çift permütasyon $(\tau\in A_n)$ ise

$$\delta=\prod_{i\le i\le j\le n}(\alpha_i-\alpha_j)$$

ifadesi τ altında sabit kalır. $\tau \in S_n$ tek permütasyon ise δ 'nın işareti değişir.

İspat: $\tau \in A_n$ olsun τ çift sayıda transpozisyonun (2-linin) çarpımıdır. i<j ,(ij) 2-lisi için $\alpha_i - \alpha_j$ çarpanı τ altında $\alpha_{\tau(i)} - \alpha_{\tau_{(j)}} = \alpha_j - \alpha_i = -(\alpha_i - \alpha_j)$ çarpımına dönüşür ve diğer çarpanlar değişmez.Şu halde $\tau \in A_n$ ise $\tau\ (\delta) = \delta$ ve $\tau \notin A_n$ ise $\tau\ (\delta) = -\delta$ olur.

Teorem 4.1.3: $f(x) \in F[x]$ monik ,E / F f(x)'in parçalanış cismi ve f(x)'in F üzerinde Galois grubu $Gal(E/F) \subset A_n$ olmasıdır $\Leftrightarrow D(f)$ diskiriminantı F'deki bir elemanın karesidir.

İspat $(\Rightarrow)$ **:** $Gal(E/F) \subset A_n$ ise bir önceki teoreme göre $\tau \in Gal(E/F)$ için $\tau(\delta) = \delta$,

Şu halde δ, τ altında değişmediğinden $\delta \in F$ dir.D(f)= δ^2 olduğundan D(f) , F'de karedir.

$(\Leftarrow)$ Tersine D(f) kare ise $\delta \in F$ dir. $\tau \in Gal(E/F)$ fakat $\tau \notin A_n$ olsa bir önceki teoremden $\tau(\delta) = -\delta$ olurdu.Bu ise $\delta \in F$ ile çelişir.Şu halde $Gal(E/F) \subset A_n$ dır.

Tanım 4.1.2: F bir cisim ve f(x) ¿ F[x] polinomunun F üzerindeki parçalanış cismi E olsun.Gal(E/F) grubuna, f(x)'in F üzerindeki Galois grubu denir ve Gal_F (f) ile gösterilir.

Teorem 4.1.4: $f(x)\in Q[x]$,der f(x)=2 olsun. O zaman

G= $Gal_Q(f)$ grubun derecesi 1 ya da 2 dir.

İspat: $f(x)=x^2+bx+c \in Q[x]$ polinomun Q cisminde kökü varsa 1.dereceden iki çarpanı olur ve $f(x)=x^2+bx+c=(x-d)(x-e)$ $d,e\in Q$ polinomun Galois grubu $1:Q\to Q$ birim grubundan oluşur.

$f(x)=x^2+bx+c \in Q[x]$ polinomun Q cisminde kökü yoksa indirgenemez ve Q üzerinde $\alpha\in C$ ve $\bar{\alpha}$, α nın eşleniği olmak üzere $f(x)=x^2+bx+c=(x-\alpha)\left(x-\bar{\alpha}\right)$ biçiminde çarpanlara ayrılır.f(x)'in Galois grubu $1:\alpha\to\alpha$ ve $\tau:\alpha\to\bar{\alpha}$ ile belirli olup $Gal_Q(f)\simeq S_2$ *bulunur*.

Örnek 4.1.5: $f(x)=x^2+1\in Q[x]$ polinomu Q cismi üzerinde $x^2+1=(x-i)(x+i)$ biçiminde çarpanlara ayrılır ve parçalanış cismi Q(i,-i) =Q(i)dir.

Böylece $|Gal(Q(i)/Q)|=2$ ve

$Gal(Q(i)/Q)\simeq S_2$ dir.

Teorem 4.1.5: $f(x)\in Q[x]$ indirgenemez, Galois grubu G, diskriminantı D(f) ve der(f(x))=3 olsun.

(i) f(x) in tek bir reel kökü vardır $\Leftrightarrow D(f)<0$ dır.Bu durumda $G\simeq S_3$ olur.

(ii) f(x) in bütün kökleri reeldir $\Leftrightarrow D(f)>0$ dır.Bu durumda $\sqrt{D(f)}\in Q$ ise $G\simeq A_3$ veya $\sqrt{D(f)}\notin Q$ ise $G\simeq S_3$ tür.

İspat: char$Q$ = 0 ve Q mükemmel bir cisim dolayısıyla Q üzerindeki indirgenemez polinomun çok katlı kökü yoktur.Bundan dolayı D(f) ¿ 0 dır.Eğer f(x) in üç kökü de reel ise δ reel ve $D(f)=\delta^2>0$ dır.

Tersine kabul edelim ki f(x) in tek bir reel kökü α ve komleks kökleri $\beta=u+iv$ *ve* $\bar{\beta}=u-iv$ olsun.Bu durumda $\beta-\bar{\beta}$ =2iv , $\alpha=\bar{\alpha}$ ve

$$\delta=(\alpha-\beta).(\alpha-\overline{\beta})\left(\beta-\bar{\beta}\right)$$

$$=(\alpha-\beta)(\overline{\alpha-\beta})(\beta-\bar{\beta})$$

$$=(\alpha-\beta)^2(2iv)\ \ dir.$$

Böylece $D(f)=\delta^2=-4v^2|\alpha-\beta|^4<0$ olur.

E/Q ,f(x)' in parçalanış cismi olsun. f(x)' in tek bir reel kökü α olsun.O zaman $E \neq Q(\alpha)$ dir.Böylece $|G|>3$ *ve* $G \simeq S_3$ tır. Eğer f(x) in tüm kökleri reel ise D(f)>0 ve $\sqrt{D(f)}$ *reeldir*.

Teorem 4.1.3'den $G \simeq A_3 \Leftrightarrow \sqrt{D}$ rasyoneldir. $\sqrt{D}$ irrasyonel ise $G \simeq S_3$ tür.

Örnek 4.1.6: $f(x)=x^3-2 \in Q[x]$ polinomu $Q[x]$ 'te indirgenemezdir.

D(f) = $-27(-2)^2-4\cdot 0^2=-108<0$ dır.Yukarıdaki teoremden f(x)'in Galois grubu S_3 simetrik grubuna izomorftur.

f(x)= $x^3-x+\frac{1}{3} \in Q[x]$ polinomu indirgenemez ve D(f) = 1 dir. $\sqrt{1}$ rasyonel olduğundan $f(x)=x^3-x+\frac{1}{3}$ polinomun Galois grubu A_3 alterne grubuna izomorftur.

4.2 Bir Trinomialin Diskriminantı

F herhangi bir cisim ,0<m<n , (n,m)= 1, ve charF ∣ nm(n-m) olsun.F'nin cebirsel kapanışı $\bar{F}$ içindeki bütün kökleri basit olan,

$$f(x) = x^n + ax^m + b \in F[x] \quad (ab \neq 0)$$

trinomialini alalım. Böylece ,f 'nin Galois grubu iyi tanımlıdır.Ayrıca $f(x) = x^n + ax^m + b$ trinomialin diskriminantı

$$D(f) = (-1)^{\frac{n(n-1)}{2}} b^{m-1}\left(n^n b^{n-m} + (-1)^{n-1} m^m a^n\right) \quad \ldots\ldots\ldots\ldots$$

…(1)

olarak verilir [Swam R.G., teorem 2].

$$s(n-m) - rn = 1 \ , \quad 0 < s < n \quad ve \quad 0 \leq r < n-m \quad \ldots\ldots\ldots\ldots\ldots (2)$$

olacak şekilde r ve s tam sayıları daima bulunabilir. F cisminden alınan t ve μ elemanları;

$$t = \frac{b^{n-m}}{a^n} \in F \ . \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

.(3) ve $\mu = \frac{a^s}{b^r}$ olarak tanımlayalım.

O zaman ;

$$a = t^r \mu^{n-m} \quad ve \quad b = t^s \mu^s \quad \text{olur.}$$

Böylece θ ,f(x) nin bir kökü olmak üzere $\theta \rightarrow \frac{b^r}{a^s}\theta$

dönüşümü f(x) trinomialin her bir kökünü;

$$f_t(x)=a^{-sn}\cdot b^{rn} f\left(\frac{a^s}{b^r}x\right)=x^n+t^r x^m+t^s\in F[x]\ldots\ldots\ldots\ldots\ldots(4)$$

trinomialin bir köküne götüren bire-bir örten bir dönüşümdür.

Bu dönüşüm f(x)'in F cismi üzerindeki $Gal_F(f)$ Galois grubu ile $f_t(x)$ 'in F cismi üzerindeki $Gal_F(f_t)$ Galois grubu arasında bir izomorfizma oluşturur.

$f_t(x)=x^n+t^r x^m+t^s\in F[x]$ trinomialin diskriminantı

$$D\left(f_t(x)\right)=(-1)^{\frac{n(n-1)}{2}}\cdot t^{s(m-1)+rn}\cdot\left[n^n t+(-1)^{n-1}\cdot m^m(n-m)^{n-m}\right]$$

olarak verilir.Buna ek olarak

$$t_0=(-1)^n\cdot\frac{m^m(n-m)^{n-m}}{n^n}\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

.(5) alırsak

$$D\left(f_t(x)\right)=(-1)^{\frac{n(n-1)}{2}}\cdot n^n\cdot t^{s(m-1)+rn}\cdot\left(t-t_0\right)$$ olarak bulunur.

5.SONUÇ

5.1 Galois Grubu Çift olan Trinomialler

Teorem 5.1.1:F bir cisim, (n,m)=1, char F | nm(n-m) ve $f(x)=x^n+ax^m+b\in F[x],(ab\neq 0)$ ayrılabilir bir polinom olsun .O zaman ,

$Gal_F(f)\subseteq$ ¿ ¿ A_n olması ancak ve ancak

(i) n tek tamsayı ise ;r,s ve t_0 bölüm 4.2 , (2) ve (5) deki gibi olmak üzere

$$a=t^r\mu^{n-m},\ b=t^s\mu^n \quad \text{ve} \quad t=\frac{nt_0}{n+(-1)^{\frac{n+1}{2}}\lambda^2} \qquad \ldots\ldots\ldots\ldots\ldots\ldots \ldots(6)$$

şartlarını sağlayan F cismin de λ ve μ elemanların var olmasıdır.

(ii) n çift tamsayı ise ;

r,s ve t_0 (2) ve (5) teki gibi olmak üzere

$a=t^r\mu^{n-m}$

$b = t^s \mu^n$ ve $t = t_0 + (-1)^{n/2} \lambda^2$ ..... .(7)

olacak şekilde F cismin de μ ve λ elemanların var olmasıdır.

İspat: Teorem 4.1.3'ten $Gal_F(f_t) \subseteq A_n$ *olması* $D(f_t(x))$ diskriminantın F cisminde kare olmasına denktir.

i) n tek tamsayı olma durumu :

(2) şartından $s(m-1)+rn = sm-s+rn = sn-s-1 = s(n-1)-1$

tek tamsayı olarak bulunur.Böylece ; $D(f_t(x))$ in kare olması

$(-1)^{\frac{(n-1)}{2}} nt(t-t_0) = \lambda^2 t^2$ .....(8)

olacak şekilde bir $\lambda \in F$ elemanın varlığına denktir.(8) ifadesinden

$$t = \frac{nt_0}{n + (-1)^{\frac{(n+1)}{2}} \lambda^2}$$ olarak bulunur.

ii) n çift tamsayı olma durumu :

(n,m)=1 olduğundan m-1 çift tamsayıdır. $s(m-1)+rn$ çift tamsayı olduğundan $t^{s(m-1)+rn}$ F cismin de karedir.Bu durumda $D(f_t(x))$ ' in

kare olması $t=t_0+(-1)^{n/2}\lambda^2$ olacak şekilde bir $\lambda\in F$ elemanın varlığına denktir.

Örnek 5.1.1: F = Q , n=7 ,m=1 $\mu=\frac{7^6}{3^5}$ ve $\lambda=21$ alalım.

Yukarıdaki bilgiler ışığında ;

$\mu=\frac{a^s}{b^r}$ olduğundan s= 6 ve r = 5 tir.

Bunun yanında

$$t_0=(-1)^n\frac{m^m(n-m)^{n-m}}{n^n}=(-1)^7\frac{1^1(7-1)^{7-1}}{7^7}=\frac{-6^6}{7^7}$$ ve

$$t=\frac{nt_0}{n+(-1)^{n+1/2}\lambda^2}=\frac{7(-6^6)}{7+(-1)^4 21^2}=\frac{3^6}{-7^7}$$ olur.

Ayrıca $t=\frac{b^{n-m}}{a^n}$ olduğundan da $b=3,\ ve\ a=-3,$

olarak bulunur. Böylece $f(x)=x^7-7x+3\in Q[x]$ trinomiali elde edilir.f(x)'in diskriminantı

$$D(f(x))=(-1)^{\frac{n(n-1)}{2}}\cdot b^{m-1}\cdot\left(n^n b^{n-m}+(-1)^{n-1}\cdot(n-m)^{n-m}\cdot m^m a^n\right)$$

formülünden

$$D(f(x))=(-1)^{21}\cdot 3^6\left(7^7 3^6+6^6 1^1(-7)^7\right)$$

$$=-3^6\cdot 7^7\left(3^6-6^6\right)$$

$= 3^8 \cdot 7^8 \in Q$ olarak bulunur.

D(f(x)) ,Q rasyonel sayılar cisminde kare olduğundan f(x)'in Q üzerindeki Galois grubu $Gal_Q(f) \subseteq A_7$ *dir*.

Teorem 5.1.2: F bir cisim ,0<m<n ve char F | nm(n-m) olsun.

r ve s tamsayıları

$s(n-m)-rn=1$, $0<s<n$ *ve* $0 \le r < n-m$ şartlarını sağlasın.

Bir λ değişkeni için (6)(n tek tamsayı) veya (7) (n çift tamsayı) denklemlerinde olduğu gibi bir t ¿ $F(\lambda)$ tanımlansın, o zaman $f_t = x^n + t^r x^m + t^s \in F(\lambda)[x]$ trinomialin F(λ) üzerindeki Galois grubu A_n alternatif grubuna izomorftur.

5.2 Diskriminantı, Asal Sayılardan Oluşan Bir Küme S Olmak Üzere, $p \in S$ Asal Sayıları İle Aralarında Asal Trinomialler

Tanım 5.2.1: F bir sonlu cebirsel sayı cismi(charF= p ¿ 0) olsun.Herhangi bir indirgenemez $f(t,x) \in F(t)[x]$ polinomu için $U_{f,F}$ ile gösterilen küme : f(s,x) polinomu $F[x]$ 'te tanımlı ve indirgenemez olacak şekilde bütün $s \in F$, cebirsel sayılardan oluşsun.

Teorem 5.2.1(Hilbert indirgenmezlik teoremi**) :** $E=Q\left(T_1,T_2,\ldots,T_n\right)$, T_i'ler değişken $f\in E[x]$ indirgenemez bir polinom ve $\alpha_1,\alpha_2,\ldots,\alpha_n\in E$ olsun. O zaman $\bar{f}\in Q[x]$ indirgenemez bir polinom olmak üzere , f nin katsayılarını ve tüm α_i leri içeren bir bölgede tanımlı , $f\to\bar{f}$ ye götüren bir özel homomorfizma vardır.

Tanım 5.2.2: p asal sayı $a\in Z$ ve $0\le a_i<p$ olsun

$a_0+a_1p+a_2p^2+\ldots+a_kp^k+\ldots$ sonsuz toplama p-adik tam sayı denir.

p-adik tamsayılar halkası Z_p ile gösterilir. Z_p halkasının bölüm cismi Q_p olarak yazılır.Q_p nin her elemanına p-adik sayı denir.p-adik bir sayı ,bir $n\in Z$ ve a_i ¿$\{0,1,\ldots,p-1\}$ için, $\sum_{i=n}^{\infty}a_ip^i$ olarak yazılır.

Teorem 5.2.2: S sonlu asal sayılardan oluşan bir küme olsun. Her n pozitif tamsayısı için,Q rasyonel sayılar cismi üzerindeki Galois grubu S_n simetrik grubuna izomorf ve D(f) diskriminantı $p\in S$ asal sayıları ile bölünmeyen bir $f(x)=x^n+ax^m+b\in Z[x]$ trinomiali vardır.

İspat: T_1,T_2 değişkenler olsun.Her n pozitif tamsayısı için $x^n+T_1x+T_2$ trinomialin $Q(T_1,T_2)$ üzerindeki Galois grubu

$$Gal_{Q(T_1,T_2)}\left(x^n+T_1\mathrm{x},\mathrm{T}_2\right)\simeq S_n \quad \text{dir.}$$

Hilbert 'in indirgenmezlik teoreminden, Q rasyonel sayıların cismi üzerindeki Galois grubu, S_n olan $x^n+t_1x+t_2$ özel trinomiali için (t_1,t_2) ¿ Q^2 aralığı Q^2 içinde her p ¿ Z idealine göre p-adik olarak yoğundur.Bu yüzden $a_0,b_0\in Q$ rasyonel sayıları verildiğinde her $p\in S$ için,

$f(x)\equiv x^n+a_0x+b_0(\mathrm{mod}\ p)$ olacak şekilde Q rasyonel sayıların cismi üzerindeki Galois grubu S_n ye izomorf olan bir $f(x)=x^n+ax+b\in Q[x]$ trinomiali vardır.

Örneğin;

$a_0=1$ ve

$$\begin{array}{l} 0(\mathrm{mod}\ p) \quad , \quad p|n-1 \quad ise \\ 1(\mathrm{mod}\ p) \quad , \quad p|n-1 \quad ise \end{array}$$

¿

$b_0=$¿〔¿¿¿

¿

olarak alalım.Bu durumda $a_0=1$ olduğundan

$D(f)=(-1)^{\frac{n(n-1)}{2}}\cdot\left(n^n b_{0^{n-1}}+(-1)^{n-1}\cdot(n-1)^{n-1}\right)$ bulunur.

i) p | n-1 ise $p \mid b_0$ olur.Bu durumda p | D(f)dir

ii) p | n-1 ise $p \mid b_0$ olur.Bu durumda da p | D(f) dir.

Sonuç olarak her $p \in S$ asal sayısı için p | D(f) dir.Üstelik uygun bir $m \in Z$ tamsayısını alarak f(x) trinomialini $m^n f(x/m)$ trinomialine dönüştürerek f(x)' in katsayılarını tam sayı yapabiliriz.

Uyarı 5.2.1:u,v ¿ Z ve v tek olmak üzere $\left(\frac{u}{v}\right)$ ye Jacobi sembolü denir

Örnek 5.2.1: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ *ve*

$\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{4}$ tür.

Tanım 5.2.3: p bir asal sayı olsun. Her $0 \neq n \in Q$ rasyonel sayısı; (u,v) = 1, p | u, p | v ve u,v ¿ Z olmak üzere tek türlü olarak $n = p^h \cdot \frac{u}{v}$ $(h \in Z)$ şeklinde yazılabilir. $n = p^h \cdot \frac{u}{v}$ yazılışındaki h tamsayısı $V_p(n)$ ile gösterilsin.

Teorem 5.2.3: k ile n aralarında asal pozitif tamsayılar ve k<n olsun.Bir p asal sayısı için aşağıdakiler denktir.

i) Z tamsayılar halkasında , diskriminantı kare olan ve p ile bölünmeyen bir $f(x)=x^n+ax^k+b\in Z[x]$ trinomiali vardır.

ii) Eğer n çift ve p tek ise, $V_p(n)=0$ *veya* $\left(\frac{-1}{p}\right)^{\frac{n}{2}}=1$

Eğer n çift ve p=2 ise $(-1)^{n/2}(1-kn)\equiv 1(\mathrm{mod}\,8)$

Eğer n tek ve p tek ise $V_p(k(n-k))=0$ *veya* $\left(\frac{p}{n}\right)=1$

Eğer n tek ve p=2 ise $(-1)^{\frac{n-1}{2}}n\equiv 1(\mathrm{mod}\,8)$ *veya* $(-1)^{\frac{n-1}{2}}n\equiv 5(\mathrm{mod}\,8)$ *ve* $k(n-k)=2(n-2)$ *dir*.

İspat: (i) $\Rightarrow(ii)$:n pozitif çift tamsayı olsun. $r, s\in N$ doğal sayıları

$s(n-k)-rn=1$, $0<s<n$ *ve* $0\le r<n-k$ şartlarını sağlasın. $n=mp^h$, $V_p(n)=h$ $(m,h\in Z)$ olsun ve $a=mt^r, b=t^s$ alalım. O zaman $f(x)=x^n+ax^k+b$ trinomialin diskriminantı (1)'den

$D(f)=t^{s(k-1)+rn}\cdot m^n\left((-1)^{n/2}\cdot(k-n)^{n-k}+(-1)^{n/2}\cdot p^{hn}\cdot t\right)$ olarak bulunur.

n çift tamsayı olsun;

p tek ve p|n ise p = 4z+1 $(z \in Z)$ biçiminde bir asal sayı olarak alırsak

$\left(\frac{-1}{p}\right)^{n/2} = (-1)^{\frac{p-1}{2}\cdot\frac{n}{2}} = 1$ olarak bulunur.

p tek ve p | n ise $v_p(h) = 0$ dır.

p=2 ise (i) şartından p | D(f) olacağından

$2 \mid (-1)^{n/2} \cdot (k-n)^{n-k} k^k$

$\Rightarrow (-1)^{n/2} (k-n)^{k-n} k^k \equiv 1 (\mathrm{mod}\, 2)$ bazı k ve n ler için

$\Rightarrow (-1)^{n/2} (k-n)^{n-k} k^k \equiv 1 (\mathrm{mod}\, 8)$

$\Rightarrow (-1)^{\frac{n}{2}} (k-n).k \equiv 1 (\mathrm{mod}\, 8)$

$\Rightarrow$ $(-1)^{n/2}$ (1-nk) ≡ 1(mod 8) (Çünkü her k tek tamsayısı için $k^2 \equiv 1 (\mathrm{mod}\, 8)$ dir.)olur.

n pozitif tek tamsayı durumu da benzer yolla incelenir.

(ii) ⇒ (i) n çift tamsayı olma durumu: $r, s \in N$ doğal sayıları $s(n-k) - rn = 1$,$0 < s < n$ *ve* $0 \le r < n-k$ şartları sağlasın. $v_p(n) = h$, $n = mp^h$ olsun ve $a = mt^r$, $b = t^s$ olarak alalım.

Bu değerleri $f(x) = x^n + ax^k + b$ trinomialin (1)'deki diskriminantında yazılırsa D(f) diskriminantı $D(f) = t^{s(k-1)+rn} \cdot m^n \left((-1)^{n/2} \cdot (k-n)^{n-k} . k^k + (-1)^{n/2} \cdot p^{hn} \cdot t \right)$ olarak bulunur.

n tam sayısını bölen p asal sayısı için (ii)'deki $(-1)^{n/2}(1-kn)\equiv 1 \pmod 8$ bağıntısından

$$y^2-\left((-1)^{n/2}(k-n)^{n-k}k^k\right)\equiv 0 \pmod{p^{hn}}$$

denklemin tamsayı çözümleri vardır.p | n ve (n,k)=1 oluğundan p | $(k-n)^{n-k}k^k$ (n>2)dir.Sonuç olarak p asal sayısı ile bölünmeyen Z de kare olan D(f) diskriminantı için bir $t\in Z$ vardır. p | n durumun da ise h=0 ve p^{hn}=1 olacağından aynı sonuç çıkar.

n tek tamsayı olma durumu:

$r, s\in N$ doğal sayıları

$rn-s(n-k)=1$, $0<s<n$ ve $0<r\le n-k$ şartlarını sağlasın.

$(n-k)^{n-k}\cdot k^k=mp^h$, $vp((n-k)^{n-k}\cdot k^k)=h$ olsun ve $a=mp^h t^r$, $b=m^{n+1}\cdot t^s$ olarak alalım.

Bu değerleri $f(x)=x^n+ax^k+b$ trinomialin (1)'deki diskriminantında yazılırsa D(f) diskriminantı

$$D(f)=t^{s(n-1)}m^{(n+1)k}\left((-1)^{\frac{n-1}{2}}n^n m^{(n+1)(n-k-1)}+(-1)^{\frac{n-1}{2}}p^{h(n+1)}t\right)$$

olarak bulunur.

Her p | k(n-k) asal sayısı için

$V_p(k(n-k))\neq 0\Rightarrow p=2$ dir.(ii) p=2 ise $(-1)^{\frac{n-1}{2}}n\equiv 1 \pmod 8$ için

$y^2-(-1)^{\frac{n-1}{2}}$ n^n $m^{(n+1)(n-k-1)}$ ¿ $0 \pmod{p^n}$ denkleminin tamsayı çözümleri vardır.

p|k(n-k), (n,k)=1 olduğundan p | $n^n m^{(n+1)(n-k-1)}$,(n+1>2) dir. Sonuç olarak p asal sayısı ile bölünmeyen Z de kare olan D(f) diskriminantı için bir t ¿ Z tamsayısı vardır.

p | k(n-k) durumunda ise h = 0 olacağından aynı sonuca ulaşılır.

Uyarı 5.2.2: Bölüm 4.2'den (n,k)=1; r,s ¿ N doğal sayıları

s(n-k)-rn=1, 0<s<n ve 0≤r<n-k şartlarını sağlamak üzere

$f(x) = x^n + ax^k + b$ trinomialini $T = \frac{b^{n-k}}{a^n}$ parametresine göre düzenleyerek

$$\left(\frac{b^r}{a^s}\right)^n f\left(\frac{a^s}{b^r}x\right) = x^n + \left(\frac{b^{n-k}}{a^n}\right)x^k + \left(\frac{b^{n-k}}{a^n}\right)^s = x^n + T^r x^k + T^s \in Q(T)[x]$$

trinomiali elde ederiz. Sonuç olarak Q rasyonel sayılar cisminde diskriminantı kare olan ve katsayıları $a=a(t)^r\mu^{n-k}$,$b= a(t)^s\mu^n$, t, $\mu \in Q$ ile verilen herhangi bir $x^n+ax^k+b \in Q[x]$ trinomiali için $a(T) \in Q(T)$ elemanları vardır.

Teorem 5.2.4:n ile k aralarında asal pozitif tamsayılar ve k<n olsun. Asal sayılardan oluşan her sonlu S kümesi için aşağıdaki özellikler birbirine denktir.

i) D(f) diskriminantı herhangi bir $p \in S$ asal sayısı ile bölünmeyen ve Galois grubu $Gal_Q(f(x)) \subset A_n$ olan bir

$f(x) = x^n+ax^k+b \in Z[x]$ trinomiali vardır.

ii) Her $p \in S$ asal sayısı için, diskriminantı kare tamsayı ve diskriminantı $p \in S$ asal sayısı ile bölünmeyen bir $x^n+a_px^k+b_p \in Z[x]$ trinomiali vardır.

İspat: (i) $\Rightarrow$ (ii) İspat için diskriminantın kare tamsayı olduğunu göstermek yeterlidir. (i) den $Gal_Q(f(x)) \subset A_n$ olduğundan D(f) karedir.

(ii) $\Rightarrow$ (i) yukarıdaki uyarıdan her $p \in S$ asal sayısı için, $a_p = a(t_p)^r\mu_p^{n-k}$ ve $b_p = a(t_p)^s\mu_p^n$ olacak şekilde $t_p, \mu_p \in Q$ rasyonel sayıları vardır.

Kabul edelim ki T_1, T_2 değişkenler olsun ve

$f(T_1, T_2, x)=x^n+a(T_1)^rT_2^{n-k}x^k+a(T_1)^sT_2^n \in Q(T)[x]$ polinomunu oluşturalım.

Her $p \in S$ asal sayısı için, eğer $t_1, t_2 \in Q$ rasyonel sayıları p-adik olarak t_p ve μ_p rasyonel sayılarına yeteri kadar yakın ise, o zaman, $f(t_1, t_2, x)= x^n+a_px^k+b_p \pmod p$, ($\forall p \in S$ için) dir.

Teorem 5.1.2'den $Gal_{Q(T_1,T_2)}(f(T_1, T_2, x)) \subset A_n$ olduğunu biliyoruz.

Hilbert'in indirgenmezlik teoreminden $Gal_Q(f(t_1,t_2,x)) \subset A_n$ olacak şekilde yukarıdaki gibi $t_1, t_2 \in Q$ rasyonel sayılarını alabiliriz.

Sonuç olarak, M tamsayısını $M \equiv 1 \pmod{\prod_{p \in S} p}$ şeklinde seçerek, (i) şartını sağlayan ve katsayıları tamsayılardan oluşan $f(x) = M^n f(t_1, t_2, x/M)$ trinomialini elde ederiz.

Teorem 5.2.5 : Bir n pozitif tamsayısı için aşağıdaki özellikler denktir.

i) Asal sayılardan oluşmuş her sonlu S kümesi için,Q rasyonel sayılar cismi üzerindeki Galois grubu A_n alternatif grubuna izomorf ve diskriminantı $p \in S$ asal sayıları ile bölünmeyen bir $f(x) = x^n+ax^k+b \in Z[x]$ trinomiali vardır.

ii) Asal sayılardan oluşmuş her sonlu S kümesi için, Q rasyonel sayılar cismi üzerindeki Galois grubu A_n alterne grubu tarafından içerilen ve diskriminantı $p \in S$ asal sayıları ile bölünmeyen bir $f(x) = x^n+ax^k+b \in Z[x]$ trinomiali vardır.

iii) n pozitif tamsayısı aşağıdaki şartlardan birini sağlar:

$n \equiv 0,1 \pmod 8$

$n \equiv 2 \pmod 8$ ve 2 den farklı her $p|n$ asal sayısı $p \equiv 1 \pmod 4$ şeklindedir.

$n \equiv 3 \pmod 8$ ve her $p|(n-2)$ asal sayısı $p \equiv 1 \pmod 8$ veya $p \equiv 3 \pmod 8$ şeklindedir.

İspat: (ii) ⇒ (iii) Kabul edelim ki $f(x) = x^n+ax^k+b \in Z[x]$ trinomiali n tamsayısına eşit veya n den küçük asal sayıların oluşturduğu S kümesi için (ii) şartını sağlasın ve (n,k)=1 olsun.

Eger n pozitif çift tamsayı ise teorem 5.2.3 den

(a) n tamsayısını bölen her p tek asal sayısı için $\left(-\frac{1}{p}\right)^{n/2} \equiv 1$,

ve (b) $(-1)^{n/2}(1-nk) \equiv 1 \pmod 8$ olduğunu biliyoruz.

(a) şartı sadece n ≡ 0,4 (mod 8) veya n ≡ 2,6 (mod 8) ve p ≡ 1 (mod 4) için mümkün olabilir. n ≡ 6 (mod 8) durumunda p|n olması için p ≡ 3 (mod 4) olmalıki, bu ise (a) şartını sağlamaz. n ≡ 4 (mod 8) için (b) şartı sağlanmaz. Sonuç olarak n pozitif tamsayısının tek tamsayı olma durumu da incelendiğinde sadece (iii) deki şartlar mevcuttur.

(iii) ⇒ (i) n (iii) şartını sağlayan pozitif tamsayı olsun. n ≡ 3 (mod 8) olduğunda k= n-2 ve n ≡ 0,1,2 (mod 8) olduğunda da k = n-1 alalım. O zaman her $p \in S$ asal sayısı teorem 5.2.3 (ii) şartını sağlar.

Sonuç olarak teorem 5.2.3 (ii) ise teorem5.2.4 ve teorem 5.2.4 ise (i) dir

KAYNAKLAR DİZİNİ

Adomson, I.T., 1964,Introduction to field theor, Edinburg.

Çallıalp,F.,1986,Soyut cebir ve sayılar teorisi,Ondokuz Mayıs Üniversitesi.

Feyzioğlu,A.K., 1990,A Course on Algebra,Bogaziçi University Pablication,496.

Hermez ,A.,Saliner A.,2001,Rational trinomials with the alternating group as Galois grup,J.Number Theory 90 ,113-129 p.

Hungerford,T.W.,1974,Graduate Text in Mathematics Algebra, Springer-Verlag ,New York.

Maclane,S.,Birkhoff,G.,Algebra, Harvard University.

Mccarty, P.,1966,Algebraic Extensions of Felds, Toronto.

Morita ,Y.,1990,A Note on the Hilbert Irreducibility Theorem, Proc.Japan Acad.,66 , 101-104 p.

Plans,B.,Vila ,N.,2004,Trinomial extensions of Q with ramification conditions,J.Number Theory 105 ,387-400 p.

Rotman,J.,1988,Galois Theory, Springer-Verlag.

Sere ,J.P., 1992,Topics in Galois Theory, Jones and Barlett, Boston.

Swam ,R.G.,1962,Factorization of polynomials over finite fields,Pacific J.Mth.12 , 1099-1106.

.

ÖZGEÇMİŞ

1979 yılında Ocak'ta doğdu. İlk ve orta öğretimini Merkez Bağıvar İ.Ö.O. ve Diyarbakır Melik Ahmet Lisesinde tamamladı. 2001 yılında Gazi Üniversitesi Gazi Eğitim Fakültesinden mezun olduktan sonra Milli Eğitim Bakanlığına bağlı bir okulda Matematik öğretmeni olarak çalışmaya başladı. 2001 yılında Ege Üniversitesi Fen Bilimleri Enstitüsü Matematik Bölümüne yüksek lisans öğrencisi olarak alındı. Halen İzmir Buca Anadolu Meslek Lisesinde çalışmaktadır.