

Cisimler ve Galois Teorisi

Utkan Utkaner

01/06/2020

İçindekiler

1	Giriş	3
2	Temel Tanımlar ve Sonuçlar	3
2.1	Halkalar	3
2.2	Tamlık Bölgeleri ve Cisimler	4
2.3	Homomorfizmalar ve İdealler	4
3	Cisimlerin Cebirsel Genişlemeleri	6
3.1	Polinomların Çarpanlara Ayrılması	6
3.2	Köklerin İlavesi	7
3.3	Cebirsel Genişlemeler	9
3.4	Cebirsel Kapalı Cisimler	12
4	Normal ve Ayrılabilir Genişlemeler	14
4.1	Parçalanış Cisimleri	14
4.2	Normal Genişlemeler	15
4.3	Katlı Kökler	16
4.4	Sonlu Cisimler	17
4.5	Ayrılabilir Genişlemeler	19
5	Galois Teorisi	21
5.1	Cisimlerin Otomorfizma Grupları	21
5.2	Galois Teorisinin Temel Teoremi	25
5.3	Cebirin Temel Teoremi	27

1 Giriş

Évariste Galois (25 Ekim 1811 - 31 Mayıs 1832) bir Fransız matematikçi ve siyasi aktivisttir. Henüz gençlik yıllarındayken, bir polinomun radikaller tarafından çözülebilmesi için gerekli ve yeterli bir durumu belirleyebildi ve böylece 350 yıldır ayakta olan bir problemi çözdü. Çalışmaları soyut cebirin iki ana dalı olan Galois teorisi ve grup teorisi ile Galois bağlantıları alt dalının temellerini attı. Bir düelloda aldığı yaralardan 20 yaşında öldü.

2 Temel Tanımlar ve Sonuçlar

2.1 Halkalar

Tanım 2.1. Bir R halkası $(r, s) \mapsto r + s$ ile tanımlı toplama ve $(r, s) \mapsto rs$ ile tanımlı çarpma işlemleri altında aşağıdaki koşulları sağlayan bir kümedir:

- (i) Toplama işlemi altında R bir abel gruptur.
- (ii) Çarpma işlemi birleşmelidir.
- (iii) Çarpma işlemi toplama işlemi üzerine dağılmalıdır.

Eğer çarpma işleminin bir birim elemanı varsa, o zaman R halkası birimlidir. Eğer çarpma işlemi değişmeliyse, o zaman R halkası değişmelidir.

Tanım 2.2. Diyelim ki R bir halka olsun. O zaman katsayıları R halkasında olan bir $f(x)$ polinomu yani R halkası üzerinde tanımlı bir $f(x)$ polinomu her i için $a_i \in R$ ve $i > n$ için $a_i = 0$ olmak üzere

$$f(x) = (a_0, a_1, \dots, a_n, 0, 0, \dots)$$

dizisi ile tanımlanır. Burada a_0 $f(x)$ polinomunun sabit terimi, a_n $f(x)$ polinomunun baş katsayısı ve $\partial(f(x)) = n$ $f(x)$ polinomunun derecesi olarak adlandırılır.

Ayrıca R halkası üzerinde tanımlı tüm polinomların kümesi $R[x]$

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$$

ve $k = i + j$ için $c_k = \sum a_i b_j$ olmak üzere

$$(a_0, a_1, \dots)(b_0, b_1, \dots) = (c_0, c_1, \dots)$$

ile tanımlı toplama ve çarpma işlemleri ile birlikte bir halkadır ve R üzerinde polinomlar halkası olarak adlandırılır.

Burada $x = (0, 1, 0, 0, \dots)$ ile tanımlanır ve bir $f(x) = (a_0, a_1, \dots, a_n, 0, 0, \dots)$ polinomu aynı zamanda

$$f(x) = a_0 + a_1x + \dots + a_nx^n$$

olarak ifade edilebilir.

Tanım 2.3. Baş katsayısı 1 olan polinoma monik polinom denir.

Tanım 2.4. Diyelim ki $f(x) = a_0 + a_1x + \cdots + a_n$ bir R halkası üzerinde bir polinom olsun. O zaman $f(x)$ polinomunun R halkasındaki bir kökü

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

eşitliğini sağlayan bir $\alpha \in R$ elemanıdır.

Tanım 2.5. Diyelim ki R bir halka ve $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ olsun. O zaman $f(x)$ polinomunun türevi

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$$

ile tanımlanır. Ayrıca

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

ve

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

eşitlikleri sağlanır.

2.2 Tamlık Bölgeleri ve Cisimler

Tanım 2.6. Bir tamlık bölgesi sıfırdan farklı iki elemanının çarpımının sıfırdan farklı olduğu bir R halkasıdır.

Tanım 2.7. Eğer bir $r \in R$ elemanı için $rs = 1$ olacak şekilde bir $s \in R$ elemanı varsa, o zaman $r \in R$ elemanı tersinirdir.

Tanım 2.8. Sıfırdan farklı her elemanının tersinir olduğu bir halkaya cisim denir.

Tanım 2.9. Diyelim ki R bir tamlık bölgesi olsun. O zaman $a, b \in R$ ve $b \neq 0$ olmak üzere her elemanı $q = ab^{-1}$ olarak yazılabilen ve R tamlık bölgesinin bir alt halkası olduğu cisme R tamlık bölgesinin kesirler cismi denir.

Tanım 2.10. subfield

2.3 Homomorfizmalar ve İdealler

Tanım 2.11. If R and S are rings, then a function $\varphi : R \rightarrow S$ is a ring homomorphism (or ring map) if, for all $r, r' \in R$:

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

$$\varphi(rr') = \varphi(r)\varphi(r');$$

$$\varphi(1) = 1.$$

A ring homomorphism $\varphi : R \rightarrow S$ is an isomorphism if φ is a bijection; in this case, one says that R and S are isomorphic and one writes $R \cong S$.

Tanım 2.12. If $\varphi : R \rightarrow S$ is a ring map, then its kernel is

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

and its image is

$$\operatorname{im} \varphi = \{s \in S : s = \varphi(r) \text{ for some } r \in R\}.$$

Tanım 2.13. An ideal in a ring R is a subset I containing 0 such that:

- (i) $a, b \in I$ imply $a - b \in I$;
- (ii) $a \in I$ and $r \in R$ imply $ra \in I$.

An ideal I in a ring R is a proper ideal if $I \neq R$.

ideal generated by
principal ideal
natural map

Tanım 2.14. If I is an ideal in a ring R , then R/I is called the quotient ring of R modulo I .

xxx

Tanım 2.15. A ring R is called a principal ideal domain (PID) if it is a domain in which every ideal is a principal ideal.

Tanım 2.16. Let R be a domain, and let $f(x), g(x) \in R[x]$. The greatest common divisor (gcd) of $f(x)$ and $g(x)$ is a polynomial $d(x) \in R[x]$ such that:

- (i) $d(x)$ is a common divisor of $f(x)$ and $g(x)$; that is $d|f$ and $d|g$;
- (ii) if $c(x)$ is any common divisor of $f(x)$ and $g(x)$, then $c(x)|d(x)$;
- (iii) $d(x)$ is monic.

One often denotes $d(x)$ by (f, g) . If $(f, g) = 1$, then $f(x)$ and $g(x)$ are called relatively prime.

Tanım 2.17. Let F be a field. A nonzero polynomial $p(x) \in F[x]$ is irreducible over F if $\partial(p) \geq 1$ and there is no factorization $p(x) = f(x)g(x)$ in $F[x]$ with $\partial(f) < \partial(p)$ and $\partial(g) < \partial(p)$.

Tanım 2.18. An ideal I in a ring R is called a prime ideal if it is a proper ideal and $ab \in I$ implies $a \in I$ or $b \in I$.

Tanım 2.19. An ideal I in a ring R is a maximal ideal if it is a proper ideal and there is no ideal J with $I \subsetneq J \subsetneq R$.

Tanım 2.20. The prime field of a field F is the intersection of all the subfields of F .

Tanım 2.21. A field has characteristic 0 if its prime field is isomorphic to \mathbf{Q} ; it has characteristic p if its prime field is isomorphic to \mathbf{Z}_p .

Tanım 2.22. UFD

Tanım 2.23. A polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbf{Z}[x]$ is called primitive if the gcd of its coefficients is 1.

3 Cisimlerin Cebirsel Genişlemeleri

3.1 Polinomların Çarpanlara Ayrılması

Önerme 3.1 (Gauss Lemma (İlkelik)). *İlkel iki polinomun çarpımı da ilkeldir.*

İspat. İlk olarak $f(x)g(x)$ çarpımının ilkel olmadığını kabul edelim. O zaman $f(x)g(x)$ polinomunun her bir katsayısını bölen bir p asalı vardır. $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_p$ doğal homomorfizma olsun ve $\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ halka homomorfizmasını alalım.

$$\phi(f(x)g(x)) = \phi(f(x))\phi(g(x)).$$

Ama $\phi(f(x)) \neq 0$ ve $\phi(g(x)) \neq 0$ iken $\phi(f(x)g(x)) = 0$ olur ve bu $\mathbb{Z}[x]$ polinomlar halkasının tamlık bölgesi olmasıyla çelişir. \square

Önerme 3.2 (Gauss Lemma (İndirgenemezlik)). *Diyelim ki $f(x) \in \mathbb{Z}[x]$ olsun. Eğer $f(x)$ \mathbb{Z} üzerinde indirgenemez ise, o zaman \mathbb{Q} üzerinde de indirgenemezdir.*

İspat. Önermenin karşıt tersini gösterelim. Genellik bozulmadan $f(x)$ polinomunun ilkel olduğunu kabul edebiliriz. İlk olarak $f(x)$ \mathbb{Q} üzerinde indirgenebilir olsun. Diyelim ki $u(x), v(x) \in \mathbb{Q}[x]$ ve $u(x), v(x) \notin \mathbb{Q}$ olmak üzere $f(x) = u(x)v(x)$ olsun. O zaman $\frac{a}{b} \in \mathbb{Q}$ ve $u'(x)$ ile $v'(x)$ $\mathbb{Z}[x]$ polinomlar halkasında ilkel polinomlar olmak üzere $f(x) = (\frac{a}{b})u'(x)v'(x)$ olur. O halde $bf(x) = au'(x)v'(x)$ olur. Burada $bf(x)$ polinomunun katsayılarının en büyük ortak böleni b ve ilkel iki polinomun çarpımı da ilkel olacağından $au'(x)v'(x)$ polinomunun katsayılarının en büyük ortak böleni a olur. O halde $b = \pm a$ ve buradan $f(x) = \pm u'(x)v'(x)$ olur. Demek ki $f(x)$ \mathbb{Z} üzerinde indirgenebilir. \square

Önerme 3.3. *Diyelim ki $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$ monik polinom olsun. Eğer $f(x)$ polinomunun bir $\alpha \in \mathbb{Q}$ kökü varsa, o zaman $\alpha \in \mathbb{Z}$ ve $\alpha|a_0$ olur.*

İspat. Eğer $\alpha \in \mathbb{Q}$ ise, o zaman $c, d \in \mathbb{Z}$ ve $(c, d) = 1$ olmak üzere $\alpha = \frac{c}{d}$ yazabiliriz. O halde

$$a_0 + a_1\left(\frac{c}{d}\right) + \dots + a_{n-1}\left(\frac{c^{n-1}}{d^{n-1}}\right) + \frac{c^n}{d^n} = 0$$

olur. Bu denklemi d^{n-1} ile çarparsak

$$a_0d^{n-1} + a_1cd^{n-2} + \dots + a_{n-1}c^{n-1} = -\frac{c^n}{d}$$

denklemini elde ederiz. Burada $c, d \in \mathbb{Z}$ olduğundan $\frac{c^n}{d} \in \mathbb{Z}$ ve böylece $d = \pm 1$ olmalıdır. Ayrıca $c|a_0$ olduğu görülür. O halde $\alpha = \pm c \in \mathbb{Z}$ ve $\alpha|a_0$ olur. \square

Önerme 3.4 (Eisenstein Kriteri). *Diyelim ki $n \geq 1$ için $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$ olsun. Eğer $p^2 \nmid a_0$, $p|a_1, \dots, p|a_{n-1}$, $p \nmid a_n$ olacak şekilde bir p asalı varsa, o zaman $f(x)$ \mathbb{Q} üzerinde indirgenemezdir.*

İspat. Kabul edelim ki $b_i, c_i \in \mathbb{Z}$, $b_r \neq 0$, $c_s \neq 0$, $r < n$, ve $s < n$ olmak üzere

$$f(x) = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots + c_sx^s),$$

olsun. O zaman $p|a_0$ ve $p^2 \nmid a_0$ olduğundan ya $p|b_0$ ve $p \nmid c_0$ ya da $p|c_0$ ve $p \nmid b_0$ olur. Burada $p|c_0$ ve $p \nmid b_0$ olduğu durumu alalım. Hipotezden $p \nmid a_n$ olduğundan $p \nmid b_r$ ve $p \nmid c_s$ olur. Diyelim ki $c_0 + \cdots + c_sx^s$ polinomunun p asalının bölmediği ilk katsayısı c_m olsun. O zaman $a_m = b_0c_m + b_1c_{m-1} + \cdots + b_mc_0$ olur. Öyleyse $p \nmid a_m$ ve buradan $m = n$ olduğu görülür. O halde $n = m \leq s < n$ olur ki bu imkansızdır. Benzer şekilde $p|b_0$ ve $p \nmid c_0$ olması durumunda da çelişkiye varırız. Önerme 2.2 ile $f(x)$ \mathbb{Q} üzerinde indirgenemezdir. \square

Uyarı 3.1. Son üç önerme \mathbb{Z} halkasının bir R tek türlü çarpanlara ayırma bölgesiyle yer değiştirmesi durumunda da geçerlidir (\mathbb{Q} R halkasının kesirler cismiyle ve p R halkasının bir asal elemanı ile yer değiştirir).

3.2 Köklerin İlavesi

Tanım 3.1. Eğer E bir cisim ve F E cisminin bir alt cismi ise, o zaman E/F cisminin bir cisim genişlemesidir ve E/F ile gösterilir.

Tanım 3.2. Diyelim ki E/F bir cisim genişlemesi olsun. Vektör uzayı olarak E cisminin F üzerindeki boyutuna E cisminin F üzerindeki derecesi denir ve $[E : F]$ ile gösterilir.

Eğer $[E : F]$ sonluysa, o zaman E/F cisim genişlemesine sonlu genişleme denir. Aksi halde E/F cisim genişlemesine sonsuz genişleme denir.

Tanım 3.3. Diyelim ki E ve E' bir F cisminin iki cisim genişlemesi olsun. O zaman her $a \in F$ için $\varphi(a) = a$ olacak şekilde bir $\varphi : E \rightarrow E'$ homomorfizmasına bir F -homomorfizma denir. Eğer φ birebir ve örten bir F -homomorfizması ise, o zaman φ bir F -izomorfizmasıdır.

Önerme 3.5. Eğer $F \subset K \subset E$ cisimleri için $[E : K]$ ve $[K : F]$ sonlu ise, o zaman E/F sonlu genişlemedir ve

$$[E : F] = [E : K][K : F]$$

olur.

İspat. Diyelim ki E/K cisim genişlemesinin bir bazı $\{\alpha_1, \dots, \alpha_n\}$ ve K/F cisim genişlemesinin bir bazı $\{\beta_1, \dots, \beta_m\}$ olsun. O zaman $\{\beta_j\alpha_i : 1 \leq i \leq n, 1 \leq j \leq m\}$ kümesinin E/F cisim genişlemesinin bir bazı olduğunu göstermek yeterlidir.

Bu küme E/F vektör uzayını gerer. Eğer $\gamma \in E$ ise, o zaman $\gamma = \sum b_i\alpha_i$ olacak şekilde $b_i \in K$ vardır. Öyle $c_{ij} \in F$ için $b_i = \sum c_{ij}\beta_j$ olduğundan $\gamma = \sum c_{ij}\beta_j\alpha_i$ olur. Bu kümenin lineer bağımsız olduğunu görmek için $\sum c_{ij}\beta_j\alpha_i = 0$ olduğunu kabul edelim. O zaman $b_i = \sum c_{ij}\beta_j \in K$ ve $\{\alpha_i\}$ K üzerinde lineer bağımsız olduğundan $b_i = 0$ olur. O halde $\sum c_{ij}\beta_j = 0$ ve $\{\beta_j\}$ F üzerinde lineer bağımsız olduğundan $c_{ij} = 0$ olur. \square

Önerme 3.6. *Eğer F bir cisim ve $p(x) \in F[x]$ indirgenemez ise, o zaman $F[x]/(p(x))$ bölüm halkası F cisminin bir izomorfik görüntüsünü ve $p(x)$ polinomunun bir kökünü içeren bir cisimdir.*

İspat. Eğer $p(x)$ indirgenemez ise, o zaman $I = (p(x))$ esas ideali bir asal idealdir. O halde $F[x]$ bir esas idealler bölgesi olduğundan I bir maksimal ideal olur ve böylece $E = F[x]/I$ bir cisimdir. Şimdi $F \rightarrow F' = \{a + I : a \in F\} \subset E$ olmak üzere $a \mapsto a + I$ dönüşümü bir izomorfizmadır.

Diyelim ki $\alpha = x + I \in E$ olsun. Burada α elemanının $p(x)$ polinomunun bir kökü olduğunu göstereceğiz. Eğer $a_i \in F$ için $p(x) = a_0 + a_1x + \cdots + a_nx^n$ dersek, $I = (p(x))$ olduğundan E cisminde

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

olur. Fakat $I = 0 + I$ $F[x]/I$ cisminin sıfır elemanı olduğundan α $p(x)$ polinomunun bir köküdür. \square

Uyarı 3.2. Bir F cisminden bir E cismine birebir homomorfizma varsa, E cismi F cisminin bir cisim genişlemesi olarak alınabilir.

Önerme 3.7 (Kronecker Teoremi). *Diyelim ki F bir cisim olmak üzere $f(x) \in F[x]$ olsun. O zaman $f(x)$ polinomunun üzerinde lineer çarpanlara ayrıldığı F cisminin bir E cisim genişlemesi vardır.*

İspat. Bunu $f(x)$ polinomunun derecesi üzerinden tümevarım ile gösterelim. Eğer $\partial(f(x)) = 1$ ise, o zaman $f(x)$ lineerdir ve $E = F$ alabiliriz. Eğer $\partial(f(x)) > 1$ ise, o zaman $p(x)$ indirgenemez olmak üzere $f(x) = p(x)u(x)$ olsun. Önerme 2.2 den F cismini ve $p(x)$ polinomunun bir α kökünü içeren bir K cismi vardır. Öyleyse $K[x]$ polinomlar halkasında $p(x) = (x - \alpha)v(x)$ olur. Tümevarımdan K cismini içeren ve üzerinde $v(x)u(x)$ polinunun ve böylece $f(x)$ polinomunun lineer çarpanlara ayrıldığı bir E cismi vardır. \square

Önerme 3.8. *Diyelim ki F bir cisim, $p(x) \in F[x]$ polinomlar halkasında indirgenemez bir polinom ve α F cisminin bir E cisim genişlemesinde $p(x)$ polinomunun bir kökü olsun.*

(i) *O zaman $F(\alpha)$, E cisminin F üzerinde α ile üretilen alt cismi*

$$F[\alpha] = \{b_0 + b_1\alpha + \cdots + b_m\alpha^m \in E : b_0 + b_1x + \cdots + b_mx^m \in F[x]\}$$

olur.

- (ii) Eğer $p(x)$ polinomunun derecesi n ise, o zaman $\{1, \alpha, \dots, \alpha^{n-1}\}$ kümesi F üzerinde $F(\alpha)$ için bir baz olur. Öyleyse $F(\alpha)$ cisminin her elemanı $a_i \in F$ olmak üzere $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$ olarak tek türlü yazılır ve $[F(\alpha) : F] = n$ olur.

olur.

İspat. Diyelim ki F cisminin bir E cisim genişlemesinde $p(x) \in F[x]$ indirgenemez polinomunun bir α kökü olsun. O zaman E cisminin F üzerinde α ile üretilen alt cismini, yani E cisminin F cismini ve α elemanını içeren en küçük alt cismini $F(\alpha)$ ile gösterelim. Şimdi $\varphi : F[x] \rightarrow E$ dönüşümü $b_0 + b_1x + \dots + b_mx^m \in F[x]$ için

$$\varphi(b_0 + b_1x + \dots + b_mx^m) = b_0 + b_1\alpha + \dots + b_m\alpha^m$$

ile tanımlansın. Burada $p(\alpha) = 0$ olduğundan φ dönüşümünün çekirdeği $p(x)$ polinomunu içeren bir homomorfizma olduğu açıktır. Şimdi $\text{Ker}\varphi = (p(x))$ olduğunu gösterelim.

Burada $F[x]$ bir esas idealler bölgesi olduğundan öyle $f(x) \in F[x]$ için $\text{Ker}\varphi = (f(x))$ olur. O halde $p(x) \in \text{Ker}\varphi$ olduğundan öyle $g(x) \in F[x]$ için $p(x) = f(x)g(x)$ olur. Burada $p(x)$ F üzerinde indirgenemez olduğundan $g(x) \in F$ olmalıdır. Öyleyse $\text{Ker}\varphi = (f(x)) = (p(x))$ olur.

Birinci İzomorfizma Teoreminden

$$\begin{aligned} F[x]/(p(x)) &\cong \text{Im}\varphi \\ &= \{b_0 + b_1\alpha + \dots + b_m\alpha^m \in E : b_0 + b_1x + \dots + b_mx^m \in F[x]\} \\ &= F[\alpha] \end{aligned}$$

elde edilir. Öyleyse $F[x]/(p(x))$ bir cisim olduğundan $F[\alpha]$ kümesi bir cisimdir. Açıkça $F[\alpha]$ F cismini ve α elemanını içeren en küçük alt cisimdir ve $F(\alpha) = F[\alpha]$ olur. Eğer $p(x)$ polinomunun derecesi n ise, o zaman α $F[x]$ polinomlar halkasında derecesi n doğal sayısından küçük olan hiçbir polinomun kökü olamaz. Bu ise

$$\{1, \alpha, \dots, \alpha^{n-1}\}$$

kümesinin F üzerinde $F(\alpha)$ için bir baz olduğunu gösterir ve $[F(\alpha) : F] = n$ olur. \square

3.3 Cebirsel Genişlemeler

Tanım 3.4. Diyelim ki E F cisminin bir cisim genişlemesi olsun. Eğer bir $\alpha \in E$ elemanı için $f(\alpha) = 0$ olacak şekilde sabit olmayan bir $f(x) \in F[x]$ polinomu varsa, o zaman $\alpha \in E$ F üzerinde cebirseldir.

Eğer $\alpha \in E$ F üzerinde cebirsel değilse, o zaman F üzerinde aşkındır.

Önerme 3.9. Diyelim ki E F cisminin bir cisim genişlemesi ve $\alpha \in E$ F üzerinde cebirsel olsun. Ayrıca $f(x) \in F[x]$ $f(\alpha) = 0$ olacak şekilde en küçük dereceli bir polinom olsun.

- (i) O zaman $f(x)$ F üzerinde indirgenemezdir.
- (ii) Eğer $g(x) \in F[x]$ ve $g(\alpha) = 0$ ise, o zaman $f(x)|g(x)$ olur.
- (iii) O zaman $f(\alpha) = 0$ olacak şekilde en küçük dereceli yalnız bir $f(x) \in F[x]$ monik polinomu vardır.
- İspat.* (i) Diyelim ki $f(x) = u(x)v(x)$, $\partial(u(x)) < \partial(f(x))$ ve $\partial(v(x)) < \partial(f(x))$ olsun. O zaman $0 = f(\alpha) = u(\alpha)v(\alpha)$ olur. Buradan $u(\alpha) = 0$ veya $v(\alpha) = 0$ elde ederiz. Yani α $f(x)$ polinomunun dercesinden daha küçük dereceli bir polinomun kökü olur. Bu bir çelişkidir. O halde $f(x)$ F üzerinde indirgenemezdir.
- (ii) Bölme algoritmasından $g(x) = f(x)q(x) + r(x)$, $r(x) = 0$ veya $\partial(r(x)) < \partial(f(x))$ olur. O zaman $g(\alpha) = f(\alpha)q(\alpha) + r(\alpha)$ yani $r(\alpha) = 0$ olur. Fakat $f(x)$ α elemanını kök kabul eden en küçük dereceli polinomlardan olduğundan $r(x) = 0$ olmalıdır. Öyleyse $f(x)|g(x)$ olur.
- (iii) Diyelim ki $g(x)$ $g(\alpha) = 0$ olacak şekilde en küçük dereceli bir monik polinom olsun. O zaman (ii) şikkından $f(x)|g(x)$ ve $g(x)|f(x)$ ve her ikisi de monik polinom olduğundan $f(x) = g(x)$ elde edilir. \square

Tanım 3.5. Bir F cismi üzerinde bir α elemanını kök kabul eden monik indirgenemez polinom α elemanının F üzerindeki minimal polinomu olarak adlandırılır.

Tanım 3.6. Eğer bir F cisminin bir E cisim genişlemesinin her elemanı F üzerinde cebirsel ise, o zaman E cebirseldir denir.

Cebirsel olmayan genişlemelere aşkın genişleme denir.

Önerme 3.10. Eğer E/F sonlu genişleme ise, o zaman cebirsel genişlemedir.

İspat. Diyelim ki $[E : F] = n$ ve $\alpha \in E$ olsun. Herhangi bir n -boyutlu vektör uzayında herhangi $n + 1$ vektör lineer bağımlıdır. O zaman

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

olacak şekilde hepsi sıfır olmayan $a_i \in F$ skalerleri vardır. Böylece $F[x]$ polinomlar halkasında α elemanını kök kabul eden sıfırdan farklı bir polinom vardır. O halde α F üzerinde cebirseldir. \square

Uyarı 3.3. Her cebirsel genişleme sonlu değildir.

Örnek 1. Cebirsel sayılar kümesi \mathbb{A} \mathbb{Q} üzerinde cebirsel olan kompleks sayıların kümesi olarak tanımlansın. O zaman \mathbb{A}/\mathbb{Q} sonlu olmayan bir cebirsel genişlemedir.

Tanım 3.7. Eğer bir F cisminin bir E cisim genişlemesinde $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ olacak şekilde $\alpha_1, \alpha_2, \dots, \alpha_n$ elemanları varsa, o zaman E/F sonlu üretilmiştir.

Uyarı 3.4. Sonlu üretilmiş bir cisim genişlemesi cebirsel olmak zorunda değildir.

Örnek 2. Diyelim ki $F(x)$ bir F cismi üzerinde bir polinomlar halkası olsun. O zaman $F[x]$ polinomlar halkasının E kesirler cismini alalım. E kesirler cisminin elemanları $a_i, b_i \in F$ ve bazı b_i elemanları sıfırdan farklı olmak üzere

$$(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^m)^{-1}$$

formundadır. Öyleyse E F üzerinde x ile üretilmiştir yani $E = F(x)$ olur. Polinomlar halkası tanımından x elemanının F üzerinde cebirsel olmadığı açıkça görülür. O halde, E bir cebirsel genişleme değildir.

Önerme 3.11. Diyelim ki $E = F(\alpha_1, \dots, \alpha_n)$ F cisminin her α_i F üzerinde cebirsel olmak üzere sonlu üretilmiş bir cisim genişlemesi olsun. O zaman E F üzerinde sonludur ve böylece F cisminin bir cebirsel genişlemesi olur.

İspat. Diyelim ki $E_i = F(\alpha_1, \dots, \alpha_i)$, $1 \leq i \leq n$ olsun. Eğer E cisminin bir elemanı F üzerinde cebirsel ise, aynı zamanda $F \subset B \subset E$ olacak şekilde her B cismi üzerinde de cebirsel olur. O halde $1 \leq i \leq n$ için her α_i E_{i-1} üzerinde cebirsel ve $E_0 = F$ olur. Ayrıca $E_i = E_{i-1}(\alpha_i)$ olur. Öyleyse Önerme 2.8 ile $[E_i : E_{i-1}]$ sonludur. Burada $[E_i : E_{i-1}] = d_i$ diyelim. Önerme 2.5 ile

$$[E : F] = [E : E_{n-1}][E_{n-1} : E_{n-2}] \cdots [E_1 : F]$$

ve buradan

$$[E : F] = d_n d_{n-1} \cdots d_1$$

elde edilir. O halde E F cisminin sonlu genişlemesidir ve böylece F üzerinde cebirseldir. \square

Önerme 3.12. Diyelim ki E F cisminin bir cisim genişlemesi olsun. Eğer K E cisminin F üzerinde cebirsel olan elemanlardan oluşan alt kümesi ise, o zaman K E cisminin bir alt cismidir ve F cisminin bir cebirsel genişlemesidir.

İspat. Eğer $\alpha, \beta \in E$ F üzerinde cebirsel ise, o zaman $\alpha \pm \beta, \alpha\beta$ ve $\beta \neq 0$ olmak üzere $\alpha\beta^{-1}$ elemanlarının da F üzerinde cebirsel olduğunu göstermek yeterlidir. Bu elemanlar $F(\alpha, \beta)$ cisminin elemanlarıdır ve Önerme 2.11 ile $F(\alpha, \beta)$ F cisminin bir cebirsel genişlemesidir.

O halde K E cisminin bir alt cismidir ve F cisminin bir cebirsel genişlemesidir. \square

Önerme 3.13. Diyelim ki E bir F cisminin bir cebirsel genişlemesi ve $\varphi : E \rightarrow E$ birebir homomorfizma olsun. O zaman φ örtendir ve böylece E cisminin bir otomorfizması olur.

İspat. Diyelim ki $p(x)$ bir $\alpha \in E$ elemanının F üzerindeki minimal polinomu olsun. Ayrıca K E cisminin F cismini içeren ve $p(x)$ polinomunun E cismindeki kökleriyle F üzerinde üretilen alt cismi olsun. O zaman K F üzerinde E cisminin F üzerinde cebirsel olan elemanlarının sonlu bir kümesi ile üretilir. Önerme 2.11 ile K F cisminin sonlu bir cebirsel genişlemesidir. Ayrıca φ $p(x)$ polinomunun köklerini birbiriyle eşler. O halde φ birebir olduğundan $\varphi(K) \cong K$ olur. Öyleyse $[\varphi(K) : F] = [K : F]$ olur. Burada $\varphi(K)$ K cisminin bir alt cismi olduğundan $\varphi(K) = K$ olmalıdır. Öyleyse bir $\beta \in K$ için $\varphi(\beta) = \alpha$ olur. O halde φ örtendir ve ispat tamamlanır. \square

3.4 Cebirsel Kapalı Cisimler

Tanım 3.8. Eğer bir F cisminin öz cebirsel genişlemesi yoksa, o zaman F cismi cebirsel kapalıdır.

Tanım 3.9. Eğer bir F cisminin bir E cisim genişlemesi cebirsel kapalı ve F üzerinde cebirsel ise, o zaman E F alt cisminin cebirsel kapanışıdır.

Önerme 3.14. *Diyelim ki F bir cisim olsun. O zaman F cisminin cebirsel kapalı bir E cisim genişlemesi vardır.*

İspat. İlk olarak $F[x]$ polinomlar halkasındaki her sabit olmayan polinomun bir kökünü içeren F cisminin bir F_1 genişlemesini oluşturalım. Bu nedenle her sabit olmayan $p(x) \in F[x]$ polinomu için x_p bir bağımsız değişken olsun ve F üzerinde x_p bağımsız değişkenlerine sahip tüm polinomların halkasını R ile gösterelim. Ayrıca I $p(x_p)$ polinomları ile üretilen ideal olsun. O zaman I idealinin R halkasına eşit olmadığını ileri sürüyoruz. Eğer eşit olsaydı, o zaman

$$q_1 p_1(x_{p_1}) + q_2 p_2(x_{p_2}) + \cdots + q_n p_n(x_{p_n}) = 1$$

olacak şekilde $q_1, \dots, q_n \in R$ ve $p_1, \dots, p_n \in I$ polinomları olurdu. Fakat F cisminin her bir $p_1(x), \dots, p_n(x)$ polinomunun bir $\alpha_1, \dots, \alpha_n$ kökünü içeren bir E cisim genişlemesi vardır. Eğer $x_{p_i} = \alpha_i$ ve diğer değişkenleri 0 alırsak $0 = 1$ elde ederiz. Bu çelişki $I \neq R$ olmasını gerektirir.

Şimdi $I \neq E$ olduğundan $I \subseteq J \subset R$ olacak şekilde bir J maksimal ideali vardır. O zaman $F_1 = R/J$ her $p(x) \in F[x]$ polinomunun bir $x_p + J$ kökünü içereb bir cisimdir. (Burada $\alpha \in F$ elemanını $\alpha + J$ ile eşleyerek F_1 cismini F cisminin bir cisim genişlemesi olarak düşünebiliriz.)

Aynı tekniği kullanarak her sabit olmayan $p(x) \in F_i[x]$ polinomunun F_{i+1} cisminde bir kökünün olduğu

$$F/F_1/F_2/\dots$$

cisim genişlemelerini oluşturabiliriz. O zaman $E = \bigcup F_i$ birleşimi F cisminin bir cisim genişlemesi olur. Ayrıca her $p(x) \in E[x]$ polinomunun katsayıları bir i için F_i cisminde ve böylece $p(x) \in E[x]$ polinomunun F_{i+1} ve dolayısıyla E cisminde bir kökü vardır. Öyleyse her $p(x) \in E[x]$ polinomu E üzerinde lineer çarpanlara ayrılır. O halde E cebirsel kapalıdır. \square

Önerme 3.15. *Diyelim ki E cebirsel kapalı olmak üzere E/F bir cisim genişlemesi olsun. O zaman E cisminin F üzerinde cebirsel elemanlarının K kümesi F cisminin cebirsel kapanışıdır. Ayrıca F cisminin cebirsel kapanışı izomorfizma altında tektir.*

İspat. Önerme 2.12 ile K F cisminin cebirsel genişlemesidir. Diyelim ki $f(x) \in K[x]$ olsun. O zaman E cebirsel kapalı olduğundan $f(x)$ polinomunun bir $\alpha \in E$ kökü vardır. Öyleyse $\alpha \in E$ K üzerinde cebirseldir ve K F üzerinde cebirsel olduğundan α F üzerinde cebirseldir. O halde $\alpha \in K$ olur. Böylece K cebirsel kapalıdır ve F cisminin cebirsel kapanışı olur. \square

Lemma 3.16. *Diyelim ki F bir cisim ve $\varphi : F \rightarrow E$ F cisminden cebirsel kapalı bir E cismine birebir homomorfizma olsun. Ayrıca $K = F(\alpha)$ F cisminin bir cebirsel genişlemesi olsun. O zaman φ bir $\phi : K \rightarrow E$ birebir homomorfizmasına genişletilebilir ve bu genişlemelerin sayısı α elemanının minimal polinomunun farklı köklerinin sayısına eşittir.*

İspat. Diyelim ki $p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$ α elemanının F üzerindeki minimal polinomu olsun. Ayrıca

$$p^\varphi(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_{n-1})x^{n-1} + \varphi(a_n)x^n \in E[x]$$

diyelim. Burada $p^\varphi(x)$ polinomu için E cisminde bir kök β olsun. Eğer $\alpha \in F$ cismi üzerinde cebirsel ise, o zaman $F(\alpha)$ cisminin bir elemanı m α elemanının minimal polinomunun derecesinden küçük olmak üzere $b_0 + b_1\alpha + \cdots + b_m\alpha^m$ olarak tek türlü yazılır.

Şimdi

$$\phi(b_0 + b_1\alpha + \cdots + b_m\alpha^m) = \varphi(b_0) + \varphi(b_1)\beta + \cdots + \varphi(b_m)\beta^m$$

olmak üzere $\phi : F(\alpha) \rightarrow E$ dönüşümünü tanımlayalım.

Burada ϕ dönüşümünün bir homomorfizma olduğu kolayca görülür. O halde ϕ $F(\alpha)$ cisminden E cismine birebir homomorfizmadır ve φ birebir homomorfizmasını genişletir. Açıkça $p^\varphi(x)$ polinomunun E cismindeki farklı köklerinin kümesi ile φ birebir homomorfizmalarının ϕ genişlemelerinin kümesi arasında birebir eşleme vardır. Bu son ifadeyi kanıtlar. \square

Önerme 3.17. *Diyelim ki K bir F cisminin bir cebirsel genişlemesi ve $\varphi : F \rightarrow E$ F cisminden cebirsel kapalı bir E cismine birebir homomorfizma olsun. O zaman φ bir $\phi : K \rightarrow E$ birebir homomorfizmasına genişletilebilir.*

İspat. Diyelim ki L K cisminin F cismini içeren bir alt cismi ve Φ φ birebir homomorfizmasının L cisminden E cismine bir genişlemesi olmak üzere S tüm (L, Φ) ikililerinin kümesi olsun. Eğer (L, Φ) ve (L', Φ') S kümesinde olmak üzere $L \subset L'$ ve Φ' birebir homomorfizmasının L cismine kısıtlanması Φ ise, o zaman $(L, \Phi) \leq (L', \Phi')$ olsun. Burada $(F, \varphi) \in S$ olduğundan $S \neq \emptyset$ olur. Ayrıca $\{(L_i, \Phi_i)\}$ S kümesinde bir zincir olmak üzere $L = \bigcup L_i$ olsun. Eğer $a \in L$ ise, o zaman bir i için $a \in L_i$ olur ve L üzerinde Φ $\Phi(a) = \Phi_i(a)$ olarak tanımlansın. Diyelim ki $a \in L_i$ ve $a \in L_j$ olsun. O zaman S kümesindeki zincir tanımından ya $L_i \subset L_j$ ya da $L_j \subset L_i$ olduğundan $\Phi_i(a) = \Phi_j(a)$ elde edilir. Öyleyse Φ iyi tanımlıdır. O halde (L, Φ) $\{(L_i, \Phi_i)\}$ zinciri için bir üst sınırdır. Zorn Lemmasından (L, ϕ) ikilisinin S kümesindeki bir maksimal eleman olduğunu kabul edelim. O zaman ϕ φ birebir homomorfizmasının bir genişlemesidir ve $L = K$ olur. Aksi halde öyle $\alpha \in K$ için $\alpha \notin L$ olmalıdır. O zaman Lemma 2.15 ile $\phi : L \rightarrow E$ birebir homomorfizmasının bir $\phi^* : L(\alpha) \rightarrow E$ genişlemesi olur ve bu (L, ϕ) ikilisinin maksimalliği ile çelişir. O halde $L = K$ olmalıdır ve ispat tamamlanır. \square

Önerme 3.18. *Diyelim ki E ve E' bir F cisminin cebirsel kapanışları olsun. O zaman F üzerinde birim olan bir izomorfizma altında $E \cong E'$ olur.*

İspat. Diyelim ki $\varphi : F \rightarrow E$ her $a \in F$ için $\varphi(a) = a$ olacak şekilde birebir homomorfizma olsun. Lemma 2.16 ile φ bir $\phi : E' \rightarrow E$ birebir homomorfizmasına genişletilebilir. O zaman $E' \cong \phi(E')$ olur. Öyleyse $\phi(E')$ F cismini içeren cebirsel kapalı bir cisimdir. Burada E F cisminin bir cebirsel genişlemesi olduğundan aynı zamanda $\phi(E')$ cisminin de cebirsel genişlemesidir ve F ile E arasında yer alır. O halde $\phi(E') = E$ yani ϕ E' cisminden E cismine bir izomorfizma olur. \square

4 Normal ve Ayrılabilir Genişlemeler

4.1 Parçalanış Cisimleri

Tanım 4.1. Diyelim ki F bir cisim olsun. Bir $f(x) \in F[x]$ polinomunun parçalanış cismi $f(x)$ polinomunun üzerinde lineer çarpanlara ayrıldığı ama hiçbir öz alt cisminde lineer çarpanlara ayrılmadığı F cisminin bir E cisim genişlemesidir.

Önerme 4.1. *Diyelim ki F bir cisim olsun. O zaman her $f(x) \in F[x]$ polinomunun bir parçalanış cismi vardır.*

İspat. Önerme 2.7 ile $f(x)$ polinomunun üzerinde lineer çarpanlara ayrıldığı F cisminin bir E cisim genişlemesi vardır. Diyelim ki $f(x)$ polinomunun E cismindeki kökleri $\alpha_1, \alpha_2, \dots, \alpha_n$ ve $K = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ olsun. O zaman $f(x)$ polinomunun K üzerinde lineer çarpanlara ayrıldığı ama K cisminin hiçbir öz alt cisminde lineer çarpanlara ayrılmadığı görülür. \square

Önerme 4.2. *Diyelim ki F bir cisim olmak üzere E bir $f(x) \in F[x]$ polinomunun parçalanış cismi olsun. Eğer E' $f(x) \in F[x]$ polinomunun bir diğer parçalanış cismiye, o zaman F üzerinde birim olan bir $\varphi : E' \rightarrow E$ izomorfizması vardır.*

İspat. Diyelim ki K E cisminin bir cebirsel kapanışı olsun. O zaman K E üzerinde cebirselidir. Ayrıca E F üzerinde cebirsel olduğundan K F üzerinde cebirselidir. O halde K F cisminin bir cebirsel kapanışıdır. Önerme 2.11 ile E' F cisminin bir cebirsel genişlemesi olacağından Önerme 2.17 ile F üzerindeki birim dönüşüm bir $\varphi : E' \rightarrow K$ birebir homomorfizmasına genişletilebilir. Diyelim ki $f(x) = a_0 + a_1x + \dots + a_nx^n \in F[x]$ olsun ve $f^\varphi(x) = \varphi(a_0) + \varphi(a_1)x + \dots + \varphi(a_n)x^n$ diyelim. O zaman φ F üzerinde birim olduğundan $f^\varphi(x) = f(x)$ olur. O halde $1 \leq i \leq n$ için $\alpha_i \in E'$ ve $c \in F$ olmak üzere

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

olur. Burada $f^\varphi(x) = f(x)$ ve $c \in F$ olduğundan $f(x)$ polinomu $K[x]$ polinomlar halkasında

$$f(x) = c(x - \varphi(\alpha_1))(x - \varphi(\alpha_2)) \dots (x - \varphi(\alpha_n))$$

olarak tek türlü çarpanlara ayrılır. Ayrıca $1 \leq i \leq n$ için $\beta_i \in E$ olmak üzere $f(x)$ polinomu $E[x]$ polinomlar halkasında

$$f(x) = c(x - \beta_1)(x - \beta_2) \dots (x - \beta_n)$$

olarak çarpanlara ayrıldığından $\{\varphi(\alpha_1), \varphi(\alpha_2), \dots, \varphi(\alpha_n)\}$ ile $\{\beta_1, \beta_2, \dots, \beta_n\}$ kümeleri eşittir. Böylece

$$\begin{aligned} E &= F(\beta_1, \beta_2, \dots, \beta_n) \\ &= F(\varphi(\alpha_1), \varphi(\alpha_2), \dots, \varphi(\alpha_n)) \\ &= \varphi(F(\alpha_1, \alpha_2, \dots, \alpha_n)) \\ &= \varphi(E') \end{aligned}$$

olur. O halde φ E' cisminin E cisminin bir izomorfizmasıdır. \square

4.2 Normal Genişlemeler

Önerme 4.3. *Diyelim ki K bir F cisminin bir E cebirsel kapanışının altında kalan cisim genişlemesi olsun. O zaman aşağıdakiler denktir:*

- (i) *Eğer bir indirgenemez $f(x) \in F[x]$ polinomunun K cisminde bir kökü varsa, o zaman bu polinom K üzerinde lineer çarpanlara ayrılır.*
- (ii) *Bir $\{f_i(x)\}_{i \in I} \subset F[x]$ polinomlar ailesinin parçalanış cismi E olur.*
- (iii) *Eğer bir $\varphi : K \rightarrow E$ birebir homomorfizması F üzerinde birim ise, o zaman φ K cisminin bir otomorfizması olarak alınabilir.*

İspat. İlk olarak (i) \implies (ii) olduğunu görelim. Diyelim ki $\alpha \in K$ ve $p(x) \in F[x]$ polinomunun F üzerindeki minimal polinomu olsun. Eğer (i) sağlanıyorsa, o zaman $p(x)$ K üzerinde lineer bölenlere ayrılır. Öyleyse K $(p(x))$ polinomlar ailesinin bir parçalanış cismidir.

Şimdi (ii) \implies (iii) olduğunu görelim. Diyelim ki K bir $\{f_i(x)\}_{i \in I}$ polinomlar ailesinin parçalanış cismi olsun. Eğer $\alpha \in K$ öyle $f_i(x)$ için bir kök ise, o zaman F üzerinde birim olan bir $\varphi : K \rightarrow E$ birebir homomorfizması için $\varphi(\alpha)$ $f_i(x)$ için bir kök olur. O halde K F üzerinde $f_i(x)$ polinomlarının tüm kökleri ile üretildiğinden Önerme 2.13 ile φ K cisminin bir otomorfizması olur.

Son olarak (iii) \implies (i) olduğunu görelim. Diyelim ki $\alpha \in K$ F üzerinde bir indirgenemez $p(x) \in F[x]$ polinomu için bir kök olsun. Ayrıca $\beta \in E$ $p(x)$ polinomunun bir diğer kökü olsun. O zaman $\beta \in K$ olduğunu gösterelim. Burada α ve β aynı indirgenemez $p(x)$ polinomunun kökleri olduğundan

$$F(\alpha) \cong F[x]/(p(x)) \cong F(\beta)$$

olur. Diyelim ki $\varphi : F(\alpha) \rightarrow F(\beta)$ izomorfizması olsun. O zaman $\varphi(\alpha) = \beta$ ve her $a \in F$ için $\varphi(a) = a$ olur. Önerme 2.16 ile φ bir $\phi : K \rightarrow E$ birebir homomorfizmasına genişletilebilir. Eğer (iii) sağlanıyorsa, o zaman ϕ K cisminin bir otomorfizması ve $\phi(\alpha) = \varphi(\alpha) = \beta \in K$ olur. Böylece ispat tamamlanır. \square

Tanım 4.2. Eğer bir F cisminin bir E genişlemesi için Önerme 3.3 sağlanıyorsa, o zaman E F cisminin bir normal genişlemesidir.

4.3 Katlı Kökler

Tanım 4.3. Diyelim ki F bir cisim olmak üzere bir $f(x) \in F[x]$ polinomunun bir parçalanmış cismi E ve bir kökü α olsun. O zaman $E[x]$ polinomlar halkasında $(x-\alpha)^n | f(x)$ olacak şekilde en büyük pozitif n tam sayısına α elemanının katlılığı denir. Eğer $n = 1$ ise, o zaman α $f(x)$ polinomunun basit köküdür. Eğer $n > 1$ ise, o zaman α $f(x)$ polinomunun katlı köküdür.

Önerme 4.4. Diyelim ki F bir cisim olsun. O zaman sabit olmayan bir indirgenemez $f(x) \in F[x]$ polinomu için aşağıdakiler denktir:

- (i) Bu polinomun katlı kökü vardır.
- (ii) Bu polinomun türevi ile en büyük ortak böleni $(f(x), f'(x))$ olmak üzere $(f(x), f'(x)) \neq 1$ olur.
- (iii) Bir p asalı için F cisminin karakteristiği p ve $g(x) \in F[x]$ olmak üzere $f(x) = g(x^p)$ olur.
- (iv) Bu polinomun tüm kökleri katlıdır.

İspat. İlk olarak (i) \implies (ii) olduğunu görelim. Diyelim ki α $f(x)$ polinomunun katlı bir kökü olsun ve F cisminin bir cisim genişlemesinde $n > 1$ olmak üzere $f(x) = (x - \alpha)^n g(x)$ olsun. O zaman

$$f'(x) = n(x - \alpha)^{n-1}g(x) + (x - \alpha)^n g'(x)$$

olur. Öyleyse $f(x)$ ve $f'(x)$ $x - \alpha$ ortak bölenine sahiptir.

Şimdi (ii) \implies (iii) olduğunu görelim. Burada $f(x)$ indirgenemez olduğundan ve $\partial(f'(x)) < \partial(f(x))$ olacağından

$$(f(x), f'(x)) \neq 1 \implies f'(x) = 0$$

olur. Diyelim ki $n \geq 1$ olmak üzere $f(x) = a_0 + a_1x + \cdots + a_nx^n$ olsun. O zaman $f'(x) = a_1 + a_2x + \cdots + na_nx^{n-1}$ sıfır polinomdur ancak ve ancak bir p asalı için F cisminin karakteristiği p ve $p \nmid i$ olmak üzere her i için $a_i = 0$ olur.

Şimdi (iii) \implies (iv) olduğunu görelim. Hipotezden $g(x) \in F[x]$ olmak üzere $f(x) = g(x^p)$ olur. Diyelim ki F cisminin bir cisim genişlemesinde $g(x) = \prod (x - \alpha_i)^{n_i}$ olsun. O zaman $\alpha_i = \beta_i^p$ olacak şekilde F cisminin bir cisim genişlemesi vardır. Öyleyse

$$f(x) = g(x^p) = \prod (x^p - \alpha_i)^{n_i} = \prod (x - \beta_i)^{pn_i}$$

olur ve buradan $f(x)$ polinomunun her kökünün katlılığının en az p olduğu görülür.

Son olarak (iv) \implies (i) olduğu açıktır. □

Önerme 4.5. Diyelim ki F bir cisim olsun. O zaman sıfırdan farklı bir $f(x) \in F[x]$ polinomu için aşağıdakiler denktir:

(i) Bu polinomun türevi ile en büyük ortak böleni $(f(x), f'(x))$ olmak üzere $(f(x), f'(x)) = 1$ olur.

(ii) Bu polinomun tüm kökleri basittir.

İspat. Diyelim ki E $f(x) \in F[x]$ polinomunun bir parçalanış cismi olsun. Bir önceki ispatta görüldüğü üzere $f(x)$ polinomunun bir $\alpha \in E$ kökü katlıdır ancak ve ancak $\alpha \in E$ $f'(x)$ polinomunun bir köküdür.

Eğer $(f(x), f'(x)) = 1$ ise, o zaman xxx'ten $f(x)$ ve $f'(x)$ polinomlarının $E[x]$ polinomlar halkasında ortak böleni ve dolayısıyla ortak kökü yoktur. O halde $f(x)$ polinomunun tüm kökleri basittir.

Eğer $f(x)$ polinomunun tüm kökleri basitse, o zaman $(f(x), f'(x))$ sabit polinom olmalıdır. Aksi halde E cisminde bir köke sahip olur ve bu kök $f(x)$ ile $f'(x)$ polinomlarının ortak kökü olur. \square

4.4 Sonlu Cisimler

Önerme 4.6. Diyelim ki F bir sonlu cisim olsun.

(i) O zaman bir p asal için F cisminin karakteristiği p olur ve F cisminin $F_p \cong \mathbb{Z}_p$ olacak şekilde bir F_p alt cismi vardır.

(ii) O zaman F cisminin eleman sayısı bir n pozitif tam sayısı için p^n olur.

İspat. Önerme xxx ile (i) şıkkı görülür.

Şimdi (ii) şıkkını görmek için F cismini asal cismi F_p üzerinde bir vektör uzayı olarak alalım. Diyelim ki $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ F_p üzerinde F vektör uzayı için bir baz olsun. O zaman her $\beta \in F$ elemanı $1 \leq i \leq n$ için $a_i \in F_p$ olmak üzere

$$\beta = a_1\alpha_1 + a_2\alpha_2 + \dots + a_n\alpha_n$$

olarak tek türlü yazılır. Burada p F_p cisminin eleman sayısı olmak üzere her a_i elemanı p şekilde seçilebilir. Sonuç olarak F cisminin eleman sayısı p^n olur. \square

Önerme 4.7. Her p^n elemanlı F sonlu cismi $x^{p^n} - x \in F_p[x]$ polinomunun bir parçalanış cismidir. O halde p^n elemanlı iki sonlu cisim izomorftur.

İspat. İlk olarak p^n elemanlı F sonlu cisminin sıfırdan farklı elemanları $p^n - 1$ mertebeli bir çarpımsal grup oluştururlar. O halde $0 \neq \alpha \in F$ olmak üzere $\alpha^{p^n-1} = 1$ ve böylece $\alpha^{p^n} = \alpha$ olur. Ayrıca eğer $\alpha = 0$ ise, o zaman $\alpha^{p^n} = \alpha$ olur. Öyleyse F cisminin her elemanı $x^{p^n} - x$ polinomunun bir köküdür. Burada $x^{p^n} - x \in F_p[x]$ polinomunun sadece p^n kökü olduğundan F cismi $x^{p^n} - x \in F_p[x]$ polinomunun köklerinin kümesiyle örtüşür.

Diyelim ki E ve E' p^n elemanlı iki sonlu cisim olsun. O zaman Önerme 3.6 ile E ve E' cisimlerinin p elemanlı sırasıyla E_p ve E'_p alt cisimleri vardır. Ayrıca E ve E' $x^{p^n} - x$ polinomunun sırasıyla E_p ve E'_p alt cisimleri üzerindeki parçalanış cisimleridir. Fakat $E_p \cong E'_p$ olduğundan ve parçalanış cisimlerinin izomorfizma altında teklüğünden $E \cong E'$ olur. \square

Önerme 4.8. Her p asal ve n pozitif tam sayısı için $x^{p^n} - x \in \mathbb{Z}_p[x]$ polinomunun \mathbb{Z}_p üzerindeki parçalanış cismindeki köklerinin tamamı farklıdır ve p^n elemanlı bir F cismini oluşturur. Ayrıca F $x^{p^n} - x$ polinomunun \mathbb{Z}_p üzerindeki parçalanış cismidir.

İspat. Diyelim ki $f(x) = x^{p^n} - x$ olsun. O zaman $f'(x) = p^n x^{p^n-1} - 1$ olmak üzere $(f(x), f'(x)) = 1$ olduğundan $f(x)$ polinomunun katlı kökleri yoktur. O halde $f(x)$ polinomunun tüm p^n sayıdaki kökleri farklıdır. Bu köklerin $f(x)$ polinomunun \mathbb{Z}_p üzerindeki parçalanış cismini oluşturduğunu görelim. Diyelim ki α ve β iki kök ve $\beta \neq 0$ olsun. O zaman

$$\begin{aligned} (\alpha \pm \beta)^{p^n} &= \alpha^{p^n} \pm \beta^{p^n} \\ &= \alpha \pm \beta \end{aligned}$$

ve

$$\begin{aligned} (\alpha\beta^{-1})^{p^n} &= \alpha^{p^n} (\beta^{p^n})^{-1} \\ &= \alpha\beta^{-1} \end{aligned}$$

olur. Öyleyse köklerin kümesi parçalanış cisminin bir alt cismini oluşturur ve böylece parçalanış cismiyle örtüşür. \square

Önerme 4.9. Diyelim ki F p^n elemanlı bir sonlu cisim ve m bir pozitif tam sayı olsun. O zaman F cisminin $[E : F] = m$ olacak şekilde bir E cisim genişlemesi vardır. Eğer E' F cisminin $[E' : F] = m$ olacak şekilde bir diğer cisim genişlemesi ise, o zaman E ile E' izomorftur.

İspat. Diyelim ki K F cisminin bir cebirsel kapanışı ve $f(x) = x^{p^{mn}} - x \in F[x]$ olsun. Eğer $0 \neq \alpha \in E$ ise, o zaman F cisminin çarpımsal grubunun mertebesi $p^n - 1$ olduğundan $\alpha^{p^n-1} = 1$ olur. Ayrıca $n|mn$ olduğundan $p^n - 1 | p^{mn} - 1$ olur. O halde $\alpha^{p^{mn}-1} = 1$ yani $\alpha^{p^{mn}} = \alpha$ olmalıdır. Buradan F cisminin her elemanının $f(x)$ polinomunun bir kökü olduğu görülür.

Önerme 3.8 ile $f(x)$ polinomunun tüm p^{mn} sayıdaki kökleri farklıdır ve bir E cismini oluşturur. O halde $[F : F_p] = n$ ve $[E : F] = m$ olmak üzere

$$K/E/F/F_p \cong \mathbb{Z}_p$$

cisimlerini genişlemelerini elde ederiz. Önerme 3.7 ile eğer E' F cisminin $[E' : F] = m$ olacak şekilde bir diğer cisim genişlemesi ise, o zaman E ile E' cisimlerinin izomorf olduğu görülür. \square

Önerme 4.10. Bir sonlu cismin sıfırdan farklı elemanlarının çarpımsal grubu devirlidir.

İspat. Diyelim ki F^* F cisminin sıfırdan farklı elemanlarının çarpımsal grubu olsun. O zaman F^* çarpımsal grubunun tüm elemanlarının mertebelerinin en küçük ortak katına n dersek Önerme xxx ile mertebesi n olan bir $\alpha \in F^*$ elemanı vardır. O halde F^* çarpımsal grubunun her elemanının mertebesi n sayısını

böler. Öyleyse her $a \in F^*$ için $a^n = 1$ olur. Böylece $x^n - 1$ polinomunun F cisminde en çok n kökü olduğundan F^* çarpımsal grubunun elemanlarının sayısı n sayısından küçüktür veya n sayısına eşittir. Fakat $1, \alpha, \dots, \alpha^{n-1}$ F^* çarpımsal grubunun farklı elemanları olduğundan F^* α ile üretilir. \square

Sonuç 4.11. *Diyelim ki E bir F sonlu cisminin bir sonlu cisim genişlemesi olsun. O zaman bir $\alpha \in E$ için $E = F(\alpha)$ olur.*

İspat. Diyelim ki E cisminin sıfırdan farklı elemanlarının çarpımsal grubu bir $\alpha \in E$ elemanı ile üretilsin. O zaman E cisminin F cismini ve α elemanını içeren en küçük alt cismi $F(\alpha)$ E cisminin kendisidir. \square

Önerme 4.12. *Diyelim ki F bir sonlu cisim olsun. O zaman F üzerinde her dereceden bir indirgenemez polinom vardır.*

İspat. Önerme 3.9 ile F cisminin derecesi n olan bir E cisim genişlemesini alalım. Sonuç 3.11 ile bir $\alpha \in E$ için $E = F(\alpha)$ olur. Öyleyse E F cisminin bir sonlu genişlemesi olduğundan $\alpha \in E$ F üzerinde cebirseldir. Diyelim ki $p(x)$ α elemanının F üzerindeki minimal polinomu olsun. O zaman $[F(\alpha) : F]$ $p(x)$ polinomunun derecesine eşittir. Fakat $F(\alpha) = E$ ve $[E : F] = n$ olduğundan $p(x)$ F üzerinde derecesi n olan bir indirgenemez polinomdur. \square

4.5 Ayrılabilir Genişlemeler

Tanım 4.4. Eğer bir $f(x) \in F[x]$ indirgenemez polinomunun tüm kökleri basit ise, o zaman $f(x) \in F[x]$ bir ayrılabilir polinomdur. Ayrıca eğer bir $f(x) \in F[x]$ polinomunun tüm indirgenemez bölenleri ayrılabilir ise, o zaman $f(x) \in F[x]$ bir ayrılabilir polinomdur.

Tanım 4.5. Diyelim ki E bir F cisminin bir cisim genişlemesi ve $\alpha \in E$ F üzerinde bir cebirsel eleman olsun. Eğer $\alpha \in E$ elemanının F üzerindeki minimal polinomu ayrılabilir ise, o zaman $\alpha \in E$ F üzerinde ayrılabiliridir.

Tanım 4.6. Diyelim ki E bir F cisminin bir cisim genişlemesi olsun. Eğer E cisminin her elemanı F üzerinde ayrılabilir ise, o zaman E F cisminin bir ayrılabilir genişlemesidir.

Tanım 4.7. Eğer bir F cisminin tüm cebirsel genişlemeleri ayrılabilir ise, o zaman F bir mükemmel cisimdir.

Tanım 4.8. Diyelim ki E/F bir sonlu genişleme olsun. Eğer bir $\alpha \in E$ için $E = F(\alpha)$ ise, o zaman E/F bir basit genişlemedir ve α E cisminin ilkel elemanıdır.

Teorem 4.13. *Eğer E bir F cisminin bir sonlu ayrılabilir genişlemesi ise, o zaman E F cisminin bir basit genişlemesidir.*

İspat. Eğer F bir sonlu cisim ise, o zaman Sonuç 3.11 ile F cisminin her E sonlu genişlemesi basittir. Diyelim ki F sonsuz olsun. O zaman E F cisminin sonlu genişlemesi olduğundan $1 \leq i \leq n$ için $\alpha_i \in E$ olmak üzere

$E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ olur. İlk olarak eğer $E = F(\alpha, \beta)$ ise, o zaman $E = F(\gamma)$ olacak şekilde bir $\gamma \in E$ olduğunu görelim. Buradan tümevarım ile sonuç görülür. Diyelim ki $p(x)$ ve $q(x)$ sırasıyla α ve β elemanlarının F üzerindeki minimal polinomları olsun. Ayrıca $p(x)$ polinomunun kökleri $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ ve $q(x)$ polinomunun kökleri $\beta = \beta_1, \beta_2, \dots, \beta_m$ olsun. O zaman E F cisminin ayrılabilir genişlemesi olduğundan $1 \leq i \leq n$ için α_i ve $1 \leq j \leq m$ için β_j elemanları farklıdır. Burada F sonsuz olduğundan $1 \leq i \leq n$ ve $2 \leq j \leq m$ için $a \neq (\alpha_i - \alpha)(\beta - \beta_j)^{-1}$ olacak şekilde bir $a \in F$ vardır. Öyleyse $j \neq 1$ olmak üzere $a(\beta - \beta_j) \neq \alpha_i - \alpha$ ve buradan $a\beta + \alpha \neq \alpha_i + a\beta_j$ olduğu görülür. Diyelim ki $\gamma = a\beta + \alpha$ olsun. O zaman $1 \leq i \leq n$ ve $2 \leq j \leq m$ için $\gamma - a\beta_j \neq \alpha_i$ olur. Diyelim ki $r(x) = p(\gamma - ax) \in F(\gamma)[x]$ olsun. O zaman $r(\beta) = p(\alpha) = 0$ ve $j \neq 1$ olmak üzere $r(\beta_j) = p(\gamma - a\beta_j) \neq 0$ olur. O halde β $r(x)$ polinomunun bir köküdür fakat $j \neq 1$ olmak üzere β_j $r(x)$ polinomunun bir kökü değildir. Ayrıca β $q(x)$ polinomunun bir köküdür. Burada $q(x) \in F(\gamma)[x]$ olarak alalım. Diyelim ki $s(x) \in F(\gamma)[x]$ β elemanının $F(\gamma)$ üzerindeki minimal polinomu olsun. O zaman $s(x)|q(x)$ ve $s(x)|r(x)$ olur. O halde $s(x)$ polinomunun her kökü $q(x)$ ve $r(x)$ polinomlarının da bir köküdür. Fakat $q(x)$ ve $r(x)$ polinomlarının tek ortak kökü β olduğundan $s(x) = x - \beta$ olur. Öyleyse $\beta \in F(\gamma)$ olmalıdır. O halde $\gamma = a\beta + \alpha$, $\alpha \in F(\gamma)$ ve böylece $F(\alpha, \beta) = F(\gamma)$ olur. \square

Önerme 4.14. *Diyelim ki E bir F cisminin bir sonlu genişlemesi olsun. O zaman aşağıdakiler denktir:*

- (i) *Bir $\alpha \in E$ için $E = F(\alpha)$ olur.*
- (ii) *Sonlu sayıda K için $E/K/F$ olur.*

İspat. İlk olarak (i) \implies (ii) olduğunu görelim. Diyelim ki $f(x) \in F[x]$ α elemanının F üzerindeki minimal polinomu olsun. Ayrıca K E cisminin F cismini içeren bir alt cismi ve $g(x)$ α elemanının K üzerindeki minimal polinomu olsun. O zaman $g(x) \in K[x]$ olduğundan $f(\alpha) = 0$ ve $g(x)|f(x)$ olur. Eğer L K cisminin F cismini ve $g(x)$ polinomunun katsayılarını içeren alt cismi ise, o zaman $g(x) \in L[x]$ K üzerinde indirgenemez olduğundan L üzerinde de indirgenemezdir. Ayrıca $F(\alpha) = E$ olduğundan $K(\alpha) = L(\alpha) = E$ olur. Öyleyse $[E : K]$ ve $[E : L]$ $g(x)$ polinomunun derecesine eşittir. O halde $K = L$ olur.

Diyelim ki $\varphi \varphi(K) = g(x)$ olacak şekilde E ile F arasında kalan K cisimlerinin kümesinden $f(x) \in E[x]$ polinomunun bölenlerinin kümesine bir dönüşüm olsun. O zaman yukarıdan φ birebirdir. Ayrıca $f(x)$ polinomunun sonlu sayıda bölene olduğundan E ile F arasında kalan K cisimlerinin kümesi de sonlu olur.

Diğer taraftan (ii) \implies (i) olduğunu görelim. Eğer F sonlu ise, o zaman E sonludur ve Sonuç 3.11 ile bir $\alpha \in E$ için $E = F(\alpha)$ olduğu görülür. Öyleyse F sonsuz olsun. İlk olarak iki $\alpha, \beta \in E$ için $F(\alpha, \beta) = F(\gamma)$ olacak şekilde bir $\gamma \in E$ olduğunu görelim. Her $a \in F$ için α ve β elemanlarının $\gamma_a = \alpha + a\beta$ lineer kombinasyonunu alalım. O zaman $F(\gamma_a)$ cisimleri E ile F arasındadır. Ayrıca E ile F arasında sonlu sayıda cisim olduğundan öyle $a, b \in F$ için $a \neq b$ olmak üzere $F(\gamma_a) = F(\gamma_b)$ olur. Eğer $\gamma_a, \gamma_b \in F(\gamma_b)$ ise, o zaman $\gamma_a - \gamma_b \in F(\gamma_b)$ olacağından $(a - b)\beta \in F(\gamma_b)$ ve buradan $\beta \in F(\gamma_b)$ elde edilir. O zaman

$\gamma_b = \alpha + b\beta \in F(\gamma_b)$ olduğundan $\alpha \in F(\gamma_b)$ olur. Öyleyse $F(\alpha, \beta) \subset F(\gamma_b)$ olur. Ayrıca $F(\gamma_b) \subset F(\alpha, \beta)$ olduğundan eşitlik görülür.

Şimdi öyle $\alpha \in E$ için $[F(\alpha) : F]$ en büyük olsun. Öyleyse $E = F(\alpha)$ olduğunu ileri sürüyoruz. Aksi halde bir $a \in E$ için $a \notin F(\alpha)$ olur. O zaman öyle $\beta \in E$ için $\alpha \in F(\beta)$ ve $a \in F(\beta)$ olmak üzere $F(\alpha) \subsetneq F(\beta)$ elde edilir. Buradan α elemanının seçilişiyle bir çelişkiye varılır. Öyleyse $E = F(\alpha)$ olmalıdır. \square

5 Galois Teorisi

5.1 Cisimlerin Otomorfizma Grupları

Tanım 5.1. Bir G grubunun bir F cismindeki bir karakteri F cisminin çarpımsal grubu F^* olmak üzere bir $\varphi : G \rightarrow F^*$ homomorfizmasıdır.

Tanım 5.2. Bir G grubunun bir F cismindeki karakterlerinin bir kümesi $\{\varphi_1, \varphi_2, \dots, \varphi_n\}$ olmak üzere her $g \in G$ için

$$a_1\varphi_1(g) + a_2\varphi_2(g) + \dots + a_n\varphi_n(g) = 0$$

olacak şekilde en az biri sıfırdan farklı $a_1, a_2, \dots, a_n \in F$ yoksa, o zaman $\{\varphi_1, \varphi_2, \dots, \varphi_n\}$ kümesi bağımsızdır.

Lemma 5.1 (Dedekind). *Bir G grubunun bir F cismindeki karakterlerinin bir $\{\varphi_1, \varphi_2, \dots, \varphi_n\}$ kümesi bağımsızdır.*

İspat. Bunu n üzerinden tümevarım ile gösterelim. Diyelim ki $n = 1$ olsun. Eğer $a_1 \in F$ olmak üzere her $g \in G$ için $a_1\varphi(g) = 0$ ise, o zaman $\varphi(g) \neq 0$ olduğundan $a_1 = 0$ olur. Diyelim ki $n > 1$ ve her $g \in G$ için

$$a_1\varphi_1(g) + a_2\varphi_2(g) + \dots + a_n\varphi_n(g) = 0$$

olacak şekilde en az biri sıfırdan farklı $a_1, a_2, \dots, a_n \in F$ olsun. Burada her i için $a_i \neq 0$ ve $a_n = 1$ olduğunu kabul edebiliriz. O zaman $\varphi_n \neq \varphi_1$ olduğundan $\varphi_n(h) \neq \varphi_1(h)$ olacak şekilde bir $h \in G$ vardır. Yukarıdaki denklemde g yerine hg yazarak

$$a_1\varphi_1(h)\varphi_1(g) + a_2\varphi_2(h)\varphi_2(g) + \dots + a_{n-1}\varphi_{n-1}(h)\varphi_{n-1}(g) + \varphi_n(h)\varphi_n(g) = 0$$

elde edilir. Her tarafı $\varphi_n(h)^{-1}$ ile çarparak elde edilen

$$\sum_{i=1}^{n-1} a_i\varphi_n(h)^{-1}\varphi_1(h)\varphi_i(g) + \varphi_n(g) = 0$$

denklemini ilk denklemden çıkararak

$$\sum_{i=1}^{n-1} a_i(1 - \varphi_n(h)^{-1}\varphi_1(h))\varphi_i(g) = 0$$

elde edilir. Tümevarımdan her katsayı sıfır olur. Burada $a_1 \neq 0$ olduğundan $1 = \varphi_n(h)^{-1}\varphi_1(h)$ ve böylece $\varphi_n = \varphi_1$ çelişkisine varılır. \square

Sonuç 5.2. Bir F cisminin otomorfizmalarının bir $\{\varphi_1, \varphi_2, \dots, \varphi_n\}$ kümesi bağımsızdır.

İspat. Bir F cisminin bir φ otomorfizması bir $\phi : F^* \rightarrow F^*$ grup homomorfizmasına kısıtlanabilir ve F^* grubunun F cismindeki bir karakteri olur. O halde bir F cisminin otomorfizmalarının bir $\{\varphi_1, \varphi_2, \dots, \varphi_n\}$ kümesi bağımsızdır. \square

Tanım 5.3. Diyelim ki E/F bir cisim genişlemesi olsun. O zaman $\varphi : E \rightarrow E$ F -izomorfizmasına E cisminin bir F -otomorfizması denir.

Ayrıca E cisminin F -otomorfizmalarının kümesi $G(E/F)$ bir grup oluşturur.

Tanım 5.4. Eğer G bir F cisminin otomorfizmalarının grubunun bir alt grubuysa, o zaman

$$F^G = \{a \in F : \varphi(a) = a, \forall \varphi \in G\}$$

G grubunun sabit cismidir.

Lemma 5.3. Eğer $G = \{\varphi_1, \varphi_2, \dots, \varphi_n\}$ bir F cisminin otomorfizmalarının bir kümesiye, o zaman

$$[F : F^G] \geq n$$

olur.

İspat. Diyelim ki $[F : F^G] = m < n$ ve $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ F/F^G için bir baz olsun. O zaman E üzerinde n bilinmeyenli m sayıda denklemden oluşan

$$\begin{aligned} \varphi_1(\alpha_1)x_1 + \varphi_2(\alpha_1)x_2 + \dots + \varphi_n(\alpha_1)x_n &= 0 \\ \varphi_1(\alpha_2)x_1 + \varphi_2(\alpha_2)x_2 + \dots + \varphi_n(\alpha_2)x_n &= 0 \\ &\vdots \\ \varphi_1(\alpha_m)x_1 + \varphi_2(\alpha_m)x_2 + \dots + \varphi_n(\alpha_m)x_n &= 0 \end{aligned}$$

lineer sistemini alalım. Burada $m < n$ olduğundan aşık olmaya bir çözüm vardır. Her $\beta \in F$ için $\beta = \sum b_i \alpha_i$ olacak şekilde $b_i \in F^G$ vardır. Lineer sistemin i 'nci satırı b_i ile çarpılırsa i 'nci satırı

$$b_i \varphi_1(\alpha_1)x_1 + b_i \varphi_2(\alpha_1)x_2 + \dots + b_i \varphi_n(\alpha_1)x_n = 0$$

olan lineer sistem elde edilir. Fakat $b_i \in F^G$ olduğundan her i, j için $b_i = \varphi_j(b_i)$ olur. O halde lineer sistemin i 'nci satırı

$$\varphi_1(b_i \alpha_i)x_1 + \varphi_2(b_i \alpha_i)x_2 + \dots + \varphi_n(b_i \alpha_i)x_n = 0$$

olur. O halde

$$\varphi_1(\beta)x_1 + \varphi_2(\beta)x_2 + \dots + \varphi_n(\beta)x_n = 0$$

olur ve buradan $G = \{\varphi_1, \varphi_2, \dots, \varphi_n\}$ kümesinin bağımsızlığıyla bir çelişkiye varılır. Öyleyse $[F : F^G] \geq n$ olmalıdır. \square

Teorem 5.4. *Eğer $G = \{\varphi_1, \varphi_2, \dots, \varphi_n\}$ bir F cisminin otomorfizmalarının grubunun bir alt grubuysa, o zaman*

$$[F : F^G] = |G|$$

olur.

İspat. Burada $[F : F^G] \leq |G|$ olduğunu göstermek yeterlidir. Aksi halde $[F : F^G] > n$ ise $\{\alpha_1, \alpha_2, \dots, \alpha_{n+1}\}$ F^G üzerinde bir vektör uzayı olarak F cisminde lineer bağımsız vektörlerin bir kümesi olsun. O zaman $n+1$ bilinmeyenli n sayıda denklemden oluşan

$$\begin{aligned}\varphi_1(\alpha_1)x_1 + \varphi_1(\alpha_2)x_2 + \dots + \varphi_1(\alpha_{n+1})x_{n+1} &= 0 \\ \varphi_2(\alpha_1)x_1 + \varphi_2(\alpha_2)x_2 + \dots + \varphi_2(\alpha_{n+1})x_{n+1} &= 0 \\ &\vdots \\ \varphi_n(\alpha_1)x_1 + \varphi_n(\alpha_2)x_2 + \dots + \varphi_n(\alpha_{n+1})x_{n+1} &= 0\end{aligned}$$

lineer sistemini alalım. Bu lineer sistemin F üzerinde aşikar olmayan bir çözümü vardır. En az sayıda sıfırdan farklı eleman içeren bir $(a_1 a_2 \dots a_m 00 \dots 0)$ çözümünü alalım. Burada gerekirse α_i elemanları yeniden indislenerek sıfırdan farklı elemanların başa gelmesi sağlanabilir. Eğer $m = 1$ ise, o zaman $\varphi_1(\alpha_1)a_1 = 0$ olacağından $a_1 = 0$ olur. Diyelim ki $m \neq 1$ olsun. Burada gerekirse denklemler a_m elemanının tersiyle çarpılarak $a_m = 1$ alınabilir. Ayrıca öyle a_i için $a_i \notin F^G$ olmalıdır çünkü aksi halde G grubunun birim elemanının bulunduğu satır $\{\alpha_1, \alpha_2, \dots, \alpha_{n+1}\}$ kümesinin lineer bağımsızlığıyla bir çelişki oluşturur. Tekrar gerekirse α_i elemanları yeniden indislenerek $a_1 \notin F^G$ olduğu kabul edilebilir. O halde $\varphi_k(a_1) \neq a_1$ olacak şekilde φ_k vardır. Lineer sistemin j 'nci satırı için

$$\varphi_j(\alpha_1)a_1 + \varphi_j(\alpha_2)a_2 + \dots + \varphi_j(\alpha_{m-1})a_{m-1} + \varphi_j(\alpha_m) = 0$$

olmak üzere φ_k uygulanırsa

$$\varphi_k \varphi_j(\alpha_1) \varphi_k(a_1) + \varphi_k \varphi_j(\alpha_2) \varphi_k(a_2) + \dots + \varphi_k \varphi_j(\alpha_{m-1}) \varphi_k(a_{m-1}) + \varphi_k \varphi_j(\alpha_m) = 0$$

elde edilir. Burada G bir grup olduğundan $\varphi_k \varphi_1, \varphi_k \varphi_2, \dots, \varphi_k \varphi_n$ $\varphi_1, \varphi_2, \dots, \varphi_n$ elemanlarının bir permütasyonudur. Öyleyse $\varphi_k \varphi_j = \varphi_i$ alınarak lineer sistemin i 'nci satırı

$$\varphi_i(\alpha_1) \varphi_k(a_1) + \varphi_i(\alpha_2) \varphi_k(a_2) + \dots + \varphi_i(\alpha_{m-1}) \varphi_k(a_{m-1}) + \varphi_i(\alpha_m) = 0$$

elde edilir. Bu satır

$$\varphi_i(\alpha_1)a_1 + \varphi_i(\alpha_2)a_2 + \dots + \varphi_i(\alpha_{m-1})a_{m-1} + \varphi_i(\alpha_m) = 0$$

satırından çıkarılarak yeni lineer sistemin i 'nci satırı

$$\varphi_i(\alpha_1)(a_1 - \varphi_k(a_1)) + \varphi_i(\alpha_2)(a_2 - \varphi_k(a_2)) + \dots + \varphi_i(\alpha_{m-1})(a_{m-1} - \varphi_k(a_{m-1})) = 0$$

elde edilir. Burada $a_1 - \varphi_k(a_1) \neq 0$ olduğundan $(a_1 a_2 \dots a_m 00 \dots 0)$ çözümünden daha az sayıda sıfırdan farklı eleman içeren aşikar olmayan bir çözüm bulunur. Bu ise bir çelişkidir. O halde $[F : F^G] \leq |G|$ olmalıdır. \square

Sonuç 5.5. *Eğer G ve H bir F cisminin otomorfizmalarının grubunun $E^G = E^H$ olacak şekilde sonlu alt gruplarıysa, o zaman $G = H$ olur.*

İspat. Eğer $\varphi \in G$ ise, o zaman φ elemanının F^G için birim olduğu açıktır. Diğer taraftan $\varphi \notin G$ olmak üzere $\varphi \in F^G$ için birim olsun. Eğer $G \cup \{\varphi\}$ kümesinin $n + 1$ sayıda elemanı F^G için birimse, o zaman Lemma 4.3 ve Teorem 4.4 ile

$$\begin{aligned} n &= |G| \\ &= [F : F^G] \\ &\geq [F : F^{G \cup \{\varphi\}}] \\ &\geq n + 1 \end{aligned}$$

çelişkisine varılır. O halde eğer $\varphi \in F^G$ için birimse, o zaman $\varphi \in G$ olmalıdır.

Eğer $\varphi \in G$ ise $\varphi \in F^G = F^H$ için birimdir ve buradan $\varphi \in H$ olur. Kap-samanın diğer tarafı da benzer şekilde gösterilir. Sonuç olarak $G = H$ olur. \square

Teorem 5.6. *Diyelim ki E/F bir sonlu genişleme olsun. O zaman aşağıdakiler denktir:*

- (i) *Cisim genişlemesinin F -otomorfizmalarının grubu $G = G(E/F)$ olmak üzere $F = E^G$ olur.*
- (ii) *Eğer bir $p(x) \in F[x]$ indirgenemez polinomunun E cisminde bir kökü varsa, o zaman $p(x)$ ayrılabilir ve $p(x)$ polinomunun tüm kökleri E cisminde.*
- (iii) *Bir $f(x) \in F[x]$ ayrılabilir polinomunun parçalanış cismi E olur.*

İspat. İlk olarak (i) \implies (ii) olduğunu görelim. Diyelim ki $p(x) \in F[x]$ bir $\alpha \in E$ kökü olan bir indirgenemez polinom ve $\{\varphi(\alpha) : \varphi \in G\}$ kümesinin elemanları $\alpha_1, \alpha_2, \dots, \alpha_n$ olsun. Ayrıca bir $f(x) \in E[x]$ polinomunu

$$f(x) = \prod (x - \alpha_i)$$

ile tanımlayalım. Her $\varphi \in G$ elemanı α_i elemanlarını permüte ettiğinden $f(x)$ polinomunun katsayılarını sabitler. O halde $f(x)$ polinomunun katsayıları $E^G = F$ cisminde. Öyleyse $f(x) \in F[x]$ olur. Ayrıca $p(x)$ ve $f(x)$ polinomlarının E üzerinde bir ortak kökü olduğundan bu iki polinomun $E[x]$ polinomlar halkasında en büyük ortak böleni 1 değildir. O zaman Önerme xxx ile bu iki polinomun $F[x]$ polinomlar halkasında da en büyük ortak böleni 1 değildir. Ayrıca $p(x)$ indirgenemez olduğundan $f(x)$ polinomunu böler. Öyleyse $f(x)$ polinomunun katlı kökleri olmadığından $p(x)$ polinomunun da katlı kökleri yoktur. Böylece $p(x)$ ayrılabilir ve $p(x)$ polinomunun tüm kökleri E cisminde.

Şimdi (ii) \implies (iii) olduğunu görelim. Diyelim ki $\alpha_1 \notin F$ olmak üzere $\alpha_1 \in E$ olsun. Burada E/F bir sonlu genişleme olduğundan $\alpha_1 \in F$ üzerinde cebirseldir. Diyelim ki $p_1(x) \in F[x]$ α_1 elemanının minimal polinomu olsun. Hipotezden $p_1(x)$ ayrılabilir ve $p_1(x)$ polinomunun tüm kökleri E cisminde. Diyelim

ki $K_1 \subset E$ $p_1(x)$ polinomunun parçalanış cismi olsun. Eğer $K_1 = E$ ise, o zaman ispat tamamlanır. Aksi halde $\alpha_2 \notin K_1$ olmak üzere $\alpha_2 \in E$ olsun. Hipotezden α_2 elemanını kök kabul eden bir ayrılabilir indirgenemez $p_2(x) \in F[x]$ polinomu vardır. Diyelim ki $K_2 \subset E$ $p_1(x)p_2(x)$ ayrılabilir polinomunun parçalanış cismi olsun. Eğer $K_2 = E$ ise ispat tamamlanır. Aksi halde bu yapı yinelenir. Böylece E/F bir sonlu genişleme olduğundan bir n için $K_n = E$ elde edilir.

Son olarak (iii) \implies (i) olduğunu görelim. Son olarak (iii) \implies (i) olduğunu görelim. Eğer E bir $f(x) \in F[x]$ ayrılabilir polinomunun parçalanış cismiye, o zaman E/F bir sonlu genişleme olduğundan Önerme 3.14 ile bir $\alpha \in E$ için $E = F(\alpha)$ olur. Diyelim ki $p(x)$ α elemanının F üzerindeki minimal polinomu ve $p(x)$ polinomunun derecesi n olsun. O zaman $[E : F] = n$ ve E_0 $G(E/F)$ grubunun sabit cismi olmak üzere $[E : E_0] = |G(E/F)|$ olur. Lemma 2.16 ile F cisminin cebirsel kapanışı K olmak üzere $\varphi : F \rightarrow K$ birebir homomorfizmalarının $\phi : F(\alpha) \rightarrow K$ genişlemelerinin sayısı α elemanının minimal polinomunun farklı köklerinin sayısına eşittir. \square

5.2 Galois Teorisinin Temel Teoremi

Tanım 5.5. Diyelim ki F bir cisim olmak üzere E bir $f(x) \in F[x]$ polinomunun parçalanış cismi olsun. O zaman E cisminin F otomorfizmalarının grubu $G(E/F)$ $f(x)$ polinomunun F üzerindeki Galois grubudur.

Tanım 5.6. Diyelim ki F bir cisim olmak üzere E/F cisminin sonlu, normal ve ayrılabilir genişlemesi olsun. O zaman E/F cisminin bir Galois genişlemesidir.

Teorem 5.7 (Galois Teorisinin Temel Teoremi). *Diyelim ki F bir cisim olmak üzere E/F cisminin bir Galois genişlemesi ve $G = G(E/F)$ olsun. O zaman G grubunun H alt gruplarının kümesiyle E/F cisim genişlemesinin K/F alt genişlemeleri arasında $H \mapsto E^H$ ile tanımlı dönüşüm birebir ve örtendir ve tersi $K \mapsto G(E/K)$ ile tanımlıdır. Ayrıca H_1 ile H_2 G grubunun alt grupları ve $\varphi \in G$ olmak üzere*

$$(i) \quad H_2 \subset H_1 \iff E^{H_1} \subset E^{H_2}$$

$$(ii) \quad (H_1 : H_2) = [E^{H_2} : E^{H_1}]$$

$$(iii) \quad E^{\varphi H \varphi^{-1}} = \varphi(E^H) \text{ ve } G(E/\varphi K) = \varphi G(E/K) \varphi^{-1}$$

$$(iv) \quad H \text{ normal alt grup} \iff E^H/F \text{ normal genişleme ve } G/H \cong G(E^H/F)$$

olur.

İspat. İlk olarak H G grubunun bir alt grubu olsun. Sonuç 4.5 ile $G(E/E^H) = H$ olur. Diyelim ki K/F E/F cisim genişlemesinin bir alt genişlemesi olsun. Eğer E/F cisminin bir Galois genişlemesiye, o zaman E cisminin K cisminin de bir Galois genişlemesi olacağı açıktır. O halde $E^{G(E/K)} = K$ elde edilir.

(i) Burada

$$\begin{aligned} H_2 \subset H_1 &\implies E^{H_1} \subset E^{H_2} \\ &\implies G(E/E^{H_2}) \subset G(E/E^{H_1}) \end{aligned}$$

olduğu açıktır. Ayrıca $G(E/E^{H_i}) = H_i$ olduğundan sonuç görülür.

(ii) Diyelim ki H G grubunun bir alt grubu olsun. Teorem 4.4 ile

$$|H| = [E : E^H]$$

olur ve $H_2 = 1$ için sonuç görülür. Önerme 2.5 ile

$$[E : E^{H_1}] = [E : E^{H_2}][E^{H_2} : E^{H_1}]$$

olur ve genel sonuç

$$\begin{aligned} (H_1 : 1) &= (H_1 : H_2)(H_2 : 1) \\ [E : E^{H_1}] &= [E : E^{H_2}][E^{H_2} : E^{H_1}] \end{aligned}$$

denklemlerinden elde edilir.

(iii) Eğer $\phi \in G$ ve $\alpha \in E$ ise, o zaman

$$\phi\alpha = \alpha \iff \phi\phi\phi^{-1}(\phi\alpha) = \phi\alpha$$

olur. Öyleyse ϕ K üzerinde birimdir ancak ve ancak $\phi\phi\phi^{-1} \phi K$ üzerinde birimdir. Buradan $E^{\phi H \phi^{-1}} = \phi(E^H)$ ve $G(E/\phi K) = \phi G(E/K)\phi^{-1}$ olduğu görülür.

(iv) Diyelim ki H G grubunun bir normal alt grubu olsun. O zaman her $\varphi \in G$ için $\varphi H \varphi^{-1} = H$ olduğundan (iii) ile her $\varphi \in G$ için $\varphi E^H = E^H$ olur. Öyleyse çekirdeği H olan bir

$$\begin{aligned} G &\rightarrow G(E^H/F) \\ \varphi &\mapsto \varphi|E^H \end{aligned}$$

örten grup homomorfizması vardır ve $G/H \cong G(E^H/F)$ olur. Ayrıca $(E^H)^{G/H} = F$ olduğundan Teorem 4.6 ile E^H F cisminin bir normal genişlemesidir.

Diğer taraftan K F cisminin bir normal genişlemesi olsun ve F üzerinde $\alpha_1, \alpha_2, \dots, \alpha_n$ elemanlarıyla üretilsin. O zaman $\varphi \in G$ ve $\varphi\alpha_i$ α_i elemanının F üzerindeki minimal polinomunun bir kökü olduğundan K cisminindedir. Böylece $\varphi K = K$ ve (iii) ile $\varphi H \varphi^{-1} = H$ elde edilir.

□

5.3 Cebirin Temel Teoremi

Teorem 5.8 (Cebirin Temel Teoremi). *Kompleks sayılar cismi \mathbb{C} cebirsel kapalıdır.*

İspat. Kompleks sayılar cismi \mathbb{C} $x^2 + 1 \in \mathbb{R}[x]$ polinomunun parçalanış cismi olarak tanımlansın ve bu polinomun bir kökü $i \in \mathbb{C}$ ile gösterilsin. O zaman $\mathbb{C} = \mathbb{R}(i)$ olur. Her $f(x) \in \mathbb{R}[x]$ polinomunun \mathbb{C} cisminde bir kökünün olduğunu görelim. Diyelim ki $f(x) \in \mathbb{R}[x]$ $x^2 + 1 \in \mathbb{R}[x]$ polinomundan farklı bir monik indirgenemez polinom olsun. Burada Ara Değer Teoreminin doğrudan sonucu olan \mathbb{R} ile ilgili aşağıdaki iki önerme alınsın:

- (i) Pozitif reel sayıların karekökleri vardır.
- (ii) Derecesi tek doğal sayı olan reel katsayılı her polinomun bir reel kökü vardır.

İlk olarak \mathbb{C} cisminin her elemanının bir karekökü olduğunu görelim. Diyelim ki $a, b \in \mathbb{R}$ olmak üzere $\alpha = a + bi \in \mathbb{C}$ olsun ve

$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2}$$

$$d^2 = \frac{-a + \sqrt{a^2 + b^2}}{2}$$

olacak şekilde $c, d \in \mathbb{R}$ alalım. O zaman $c^2 - d^2 = a$ ve $(2cd)^2 = b^2$ olur. Eğer c ile d elemanlarının işaretleri cd ile b elemanlarının işaretleri aynı olacak şekilde seçilirse, o zaman $(c + di)^2 = \alpha$ ve böylece α $c + di \in \mathbb{C}$ elemanının karekökü olur.

Diyelim ki $f(x) \in \mathbb{R}[x]$ ve E $f(x)(x^2 + 1)$ polinomunun bir parçalanış cismi olsun. O zaman E \mathbb{C} cismini içerir. Burada $E = \mathbb{C}$ olduğunu görelim. İlk olarak \mathbb{R} cisminin karakteristiği sıfır olduğundan $f(x) \in \mathbb{R}[x]$ polinomu ayrılabilir. Teorem 4.6 ile E \mathbb{R} cisminin bir Galois genişlemesidir. Diyelim ki $G = G(E/\mathbb{R})$ ve H G grubunun bir Sylow 2-alt grubu olsun.

Diyelim ki $K = E^H$ ve $\alpha \in K$ olsun. O zaman K cisminin \mathbb{R} üzerindeki derecesi $(G : H)$ tek doğal sayısına eşit olur ve Önerme 2.5 ile $\alpha \in K$ elemanının \mathbb{R} üzerindeki minimal polinomunun derecesi tektir. O halde $\alpha \in K$ elemanının \mathbb{R} üzerindeki minimal polinomunun bir reel kökü vardır ve derecesi 1 olur. Böylece $\alpha \in \mathbb{R}$ olmak üzere $K = \mathbb{R}$ ve $G = H$ elde edilir.

Buradan $G(E/\mathbb{C})$ bir Sylow 2-grup olur. Böylece $G(E/\mathbb{C})$ grubunun indeksi 2 olan bir N alt grubu vardır ve $[E^N : \mathbb{C}] = 2$ olur. O halde E^N \mathbb{C} cisminin bir elemanının kareköküyle üretilir. Fakat \mathbb{C} cisminin bir elemanının karekökü \mathbb{C} cisminde olduğundan $E^N = \mathbb{C}$ çelişmesine varılır. Öyleyse $G(E/\mathbb{C}) = 1$ ve $E = \mathbb{C}$ olur. \square

References

[1]