Cisimler ve Galois Teorisi

Utkan Utkaner

May 8, 2020

1 Temel Tanımlar ve Sonuçlar

1.1 Simetri

1.2 Halkalar

1.3 Tamlık Bölegeleri ve Cisimler

1.4 Homomorfizmalar ve İdealler

1.5 Bölüm Halkaları

1.6 Cisimler Üzerinde Polinom Halkaları

1.7 Asal İdealler ve Maksimal İdealler

2 Cisimlerin Cebirsel Genişlemeleri

2.1 Polinomların Çarpanlara Ayrılması

Önerme 2.1 (Gauss Lemma (İlkellik))**.** *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. $\varphi : \mathbb{Z} \to \mathbb{Z}_p$ doğal homomorfizma olsun ve $\varphi^* : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ halka homomorfizmasını alalım.

$$\varphi^*(f(x)g(x)) = \varphi^*(f(x))\varphi^*(g(x)).$$

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

Önerme 2.2 (Gauss Lemma (İndirgenemezlik))**.** *Diyelim ki $f(x) \in \mathbb{Z}[x]$ olsun. Eğer $f(x)$ $\mathbb{Q}$ üzerinde indirgenebilir ise, o zaman $\mathbb{Z}$ üzerinde de indirgenebiliridir.*

İspat. 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 indirgenebilirdir. □

Önerme 2.3. *Diyelim ki $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$ 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

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

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

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

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. □

Önerme 2.4 (Eisenstein Kriteri)**.** *Diyelim ki $n \geq 1$ için $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ olsun. Eğer $p^2 \not| a_0$, $p|a_1, \ldots, p|a_{n-1}$, $p \not| a_n$ 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 $p^2 \not| a_0$ olduğundan ya $p|b_0$ ve $p \not| c_0$ ya da $p|c_0$ ve $p \not| b_0$ olur. Burada $p|c_0$ ve $p \not| b_0$ olduğu durumu alalım. Hipotezden $p \not| a_n$ olduğundan $p \not| b_r$ ve $p \not| c_s$ 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 $p \not| a_m$ ve buradan $m = n$ olduğu görülür. O halde $n = m \leq s < n$ olur ki bu imkansızdır. Benzer şekilde $p|b_0$ ve $p \not| c_0$ olması durumunda da çelişkiye varırız. xxx'ten $f(x)$ $\mathbb{Q}$ üzerinde indirgenemezdir. □

Uyarı 2.1. 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 elemanıyla yer değiştirir).

2.2 Köklerin Eklenmesi

Tanım 2.1. 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 2.2. 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.

Önerme 2.5. *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 $\{\alpha_1, \ldots, \alpha_n\}$ ve K/F cisim genişlemesinin bir bazı $\{\beta_1, \ldots, \beta_m\}$ 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. □

Önerme 2.6. *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 $F \to F' = \{a + I : a \in F\} \subset E$ 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. □

Uyarı 2.2. Bir F cisminden bir E cismine birebir homomorfizma varsa, E cismi F cisminin bir cisim genişlemesi olarak alınabilir.

Önerme 2.7 (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. □

Önerme 2.8. *Diyelim ki F bir cisim, $p(x)$ $F[x]$ polinomlar halkasında indirgenemez bir polinom ve α F cisminin bir E cisim genişlemesinde $p(x)$ polinomunun bir kökü olsun. O zaman*

(i) $F(\alpha)$, E cisminin F ve 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 $\{1, \alpha, \ldots, \alpha^{n-1}\}$ kümesi F üzerinde $F(\alpha)$ için bir baz olur. Öyleyse $F(\alpha)$ cisminin her elemanı $a_i \in F$ olmak üzere $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ 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 ve α ile üretilen alt cismini, yani E cisminin F cismini ve α elemanını içeren en küçük alt cismini $F(\alpha)$ ile gösterelim. Şimdi $\varphi : F[x] \to E$ dönüşümü $b_0+b_1x+\cdots+b_mx^m \in F[x]$ için

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

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

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

Birinci İzomorfizma Teoreminden

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

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

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

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

2.3 Cebirsel Genişlemeler

Tanım 2.3. 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 2.9. *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) şıkkından $f(x)|g(x)$ ve $g(x)|f(x)$ ve her ikisi de monik polinom olduğundan $f(x) = g(x)$ elde edilir.

□

Tanım 2.4. Bir F cismi üzerinde bir α elemanını kök kabul eden monik indirgenemez polinom α elemanının F üzerindeki minimal polinomu olarak adlandırılır.

Tanım 2.5. 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 2.10. *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

$$\sum_{i=0}^{n} a_i \alpha^i = 0$$

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. □

Uyarı 2.3. 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 2.6. 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 2.4. 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*

$$(a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m)^{-1}$$

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 2.11. *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 her α_i $i = 1, \dots, n$ için E_{i-1} üzerinde cebirsel ve $E_0 = F$ olur. Ayrıca $E_i = E_{i-1}(\alpha_i)$ olur. Öyleyse xxx'ten $[E_i : E_{i-1}]$ sonludur. Burada $[E_i : E_{i-1}] = d_i$ diyelim. xxx'ten

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

ve buradan

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

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

Önerme 2.12. *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 xxx'ten $F(\alpha, \beta)$ F cisminin bir cebirsel genişlemesidir.

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

2.4 Cebirsel Kapalı Cisimler

Tanım 2.7. Eğer bir F cisminin öz cebirsel genişlemesi yoksa, o zaman F cismi cebirsel kapalıdır.

Tanım 2.8. Eğer bir F cisminin bir E cisim genişlemesi cebirsel kapalı ve F üzerinde cebirsel ise, o zaman E F alt cisminin cebirsel kapanışıdır.

Önerme 2.13. *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

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

olacak şekilde $q_1, \ldots, q_n \in R$ ve $p_1, \ldots, p_n \in I$ polinomları olurdu. Fakat F cisminin her bir $p_1(x), \ldots, p_n(x)$ polinomunun bir $\alpha_1, \ldots, \alpha_n$ 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

$$F/F_1/F_2/\ldots$$

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 cismindedir 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 2.14. *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. xxx'ten 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. □

Lemma 2.15. *Diyelim ki F bir cisim ve $\varphi : F \to E$ F cisminden cebirsel kapalı bir E cismine birebir homomorfizma olsun. Ayrıca $K = F(\alpha)$ F cisminin bir cebirsel genişlemesi olsun. O zaman φ bir $\phi : K \to E$ birebir homomorfizmasına genişletilebilir ve bu genişlemelerin sayısı α elemanının minimal polinomunun farklı köklerinin sayısına eşittir.*

İspat. Diyelim ki $p(x) = a_0 + a_1 + \cdots + a_{n-1} + a_n$ α elemanının F üzerindeki minimal polinomu olsun. Ayrıca

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

diyelim. Burada $p^{\varphi}(x)$ polinomu için E cisminde bir kök β olsun. Eğer α 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 $\phi : F(\alpha) \to E$ 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. □

Önerme 2.16. *Diyelim ki K bir F cisminin bir cebirsel genişlemesi ve $\varphi : F \to E$ F cisminden cebirsel kapalı bir E cismine birebir homomorfizma olsun. O zaman φ bir $\phi : K \to E$ 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 kısıtlanışı Φ ise, o zaman $(L, \Phi) \leq (L', \Phi')$ olsun. Burada $(F, \varphi) \in S$ olduğundan $S \neq \varnothing$ 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 xxx'ten $\phi : L \to E$ birebir homomorfizmasının bir $\phi^* : L(\alpha) \to E$ genişlemesi olur ve bu (L, ϕ) ikilisinin maksimalliği ile çelişir. O halde $L = K$ olmalıdır ve ispat tamamlanır. □

Önerme 2.17. *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 $\varphi : F \to E$ her $a \in F$ için $\varphi(a) = a$ olacak şekilde birebir homomorfizma olsun. xxx'ten φ bir $\varphi^* : E' \to E$ birebir homomorfizmasına genişletilebilir. O zaman $E' \cong \varphi^*(E')$ olur. Öyleyse $\varphi^*(E')$ F cismini içeren cebirsel kapalı bir cisimdir. Burada E F cisminin bir cebirsel genişlemesi olduğundan aynı zamanda $\varphi^*(E')$ cisminin de cebirsel genişlemesidir ve F ile E arasında yer alır. O halde $\varphi^*(E') = E$ yani φ^* E' cisminden E cismine bir izomorfizma olur. □

3 Normal ve Ayrılabilir Genişlemeler

4 Galois Teorisi

References

[1]