Galois Teorisi

David Pierce

6 Temmuz 2018
Matematik Bölümü, MSGSÜ
mat.msgsu.edu.tr/~dpierce/

Bu notlar, bir lisans Galois kuramı dersinin asgari içeriği teklifidir. Her kanıtlanmamış teoremi kanıtlamak bir alıştırmadır.

İçindekiler

1 Halkalar

Tanım 1. Bu notlarda her **halka,** değişmeli ve birimli bir halkadır.

Postulat 2. ***Tamsayılar,*** *sıralı bir halkayı oluşturur. Bu sıralı halkanın pozitif elemanları, iyisıralıdır.*

Tanım 3. Tamsayılar halkası $\mathbb{Z}$'dir,

$$\{x \in \mathbb{Z} \colon x > 0\} = \mathbb{N}, \qquad \{x \in \mathbb{Z} \colon x \geqslant 0\} = \omega.$$

Teorem 4 (Bölme)**.** *$\mathbb{Z}$'de eğer $b \neq 0$ ise, o zaman her*

$$a = bx + y \ \ \& \ \ 0 \leqslant y < |b| \tag{1}$$

sistemi çözülebilir.

Kanıt. $\omega \cap \{a - bx \colon x \in \mathbb{Z}\} = A$ olsun. Bu küme ω iyisıralanmış kümesinin boş olmayan bir altkümesi olduğundan A'nın d en küçük elemanı vardır. O zaman bir c tamsayısı için $d = a - bc$, dolayısıyla

$$a = bc + d.$$

Ayrıca $d \geqslant 0$ (çünkü $d \in \omega$), dolayısıyla

$$0 \leqslant d < |b|\,,$$

çünkü değilse $d \geqslant |b|$, ve sonuç olarak

$$0 \leqslant d - |b| = a - bc - |b| = a - b(c \pm 1),$$

dolayısıyla $d - |b|$, A'nın d'den küçük olan bir elemanıdır, ki bu imkânsızdır. Böylece (c, d), verilen (1) sisteminin çözümüdür. □

Sonuç 5. *$\mathbb{Z}$'de en büyük ortak bölenler bulmak için* ***Öklid Algoritması*** *kullanılabilir ve $(a,b) \neq (0,0)$ ise*

$$ax + by = \text{ebob}(a,b)$$

Bézout Denklemi *çözülebilir.*

Tanım 6. R bir halka, $a \in R$ ve $b \in R$ olsun. O zaman

$$\begin{aligned} (a) &= \{ax \colon x \in R\}, && \textbf{(ideal)} \\ b + (a) &= \{b + x \colon x \in (a)\}, && \textbf{(eşküme)} \\ R/(a) &= \{x + (a) \colon x \in R\}. && \textbf{(bölüm)} \end{aligned}$$

Teorem 7. *$R/(a)$ iyitanımlanmış bir halkadır, ve*

$$x \mapsto x + (a)$$

göndermesi, R'den $R/(a)$ bölümüne giden bir homomorfizimdir.

Teorem 8. *Her n sayma sayısı için*

i) $\mathbb{Z}/(n)$'nin en çok n tane elemanı vardır, ve aslında $k \in \omega$ ise

$$\mathbb{Z}/(n) = \{x + (n) \colon k \leqslant x < k + n\};$$

ii) $\mathbb{Z}/(n)$'nin en az n tane elemanı vardır, ve aslında $k \in \omega$ ise

$$0 \leqslant i < j < n \implies k + i + (n) \neq k + j + (n).$$

Not 9. Teoremde normalde $k = 0$ veya

$$\begin{cases} n \text{ çift ise} & k = 1 - n/2, \\ n \text{ tek ise} & k = (1-n)/2. \end{cases}$$

Ayrıca $x + (n)$, x olarak yazılabilir. Örneğin

$$\mathbb{Z}/(4) = \{0, 1, 2, 4\} = \{-1, 0, 1, 2\},$$
$$\mathbb{Z}/(5) = \{0, 1, 2, 3, 4\} = \{-2, -1, 0, 1, 2\}.$$

Bunların $\mathbb{Z}$'nin althalkası olmadığı hatırlanmalı.

Tanım 10. Eğer bir R halkasında $ax = b$ denklemi çözülebilirse, o zaman a, b'yi **böler,** ve

$$a \mid b$$

yazılır. Ayrıca

$$R^\times = \{x \in R \colon x \mid 1\},$$

ve bunun elemanları, R'nin **birimleridir.** Eğer $R^\times = R \setminus \{0\}$ ise, o zaman R bir **cisimdir.**

Teorem 11. *$a \mid b$ ve $a \mid c$ ise $a \mid bx + cy$.*

Teorem 12. *$R^\times$, çarpmalı bir gruptur.*

Tanım 13. Bir halkanın 0 veya birim olmayan bir π elemanı için,

- eğer
$$\pi = ab \ \ \& \ \ a \nmid 1 \implies b \mid 1$$
gerektirmesi sağlanırsa, π **indirgenemezdir;**
- eğer
$$\pi \mid ab \ \ \& \ \ \pi \nmid a \implies \pi \mid b$$
gerektirmesi sağlanırsa, π **asaldır.**

Not 14. Öklid'in tanımına göre asal olan sayıları, pozitif indirgenemez tamsayılardır.

Teorem 15. *İndirgenemez tamsayılar asaldır.*

Kanıt. $\mathbb{Z}$'de π indirgenemez, $\pi \mid ab$, ama $\pi \nmid a$ olsun. O zaman $\text{ebob}(\pi, a) = 1$ olduğundan

$$\pi x + ay = 1$$

Bézout denklemi çözülebilir, ve bu durumda

$$\pi bx + aby = b.$$

Teorem 11 sayesinde $\pi \mid b$. □

2 Sonlu cisimler

Teorem 16. *n sayma sayısı olmak üzere*

$$n \text{ asaldır} \iff \mathbb{Z}/(n) \text{ bir cisimdir.}$$

Tanım 17. $\mathbb{Z}$'de her pozitif p asalı için $\mathbb{Z}/(p)$ cismi

$$\mathbb{F}_p$$

olarak yazılır.

Teorem 18. *Her cisim, altcisimlerinden her biri üzerinde bir vektör uzayıdır.*

Sonuç 19. *Her K sonlu cismine bir $\mathbb{F}_p$ cismi gömülebilir, ve bir n sayma sayısı için*

$$|K| = p^n.$$

Tanım 20. n sayma sayısı olmak üzere $\mathbb{Z}/(n)$ halkasının toplamalı grubu

$$\mathbb{Z}_n$$

olarak yazılsın.

Teorem 21. *$\mathbb{Z}$'de her pozitif p asalı için*

$$\mathbb{F}_p{}^{\times} \cong \mathbb{Z}_{p-1}.$$

Kanıt. Her asalın ilkel kökleri vardır. □

Tanım 22. Girdileri bir K cisminden gelen her $(a_0, \ldots, a_n)$ listesi için

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

veya

$$\sum_{k=0}^{n} a_kX^k$$

olarak yazılan bir **polinom** vardır. Verilen polinomun **değişkeni** X'tir, ve **katsayıları** a_k'lardır. Eğer verilen polinom f ve $a_n \neq 0$ ise, o zaman f'nin **başkatsayısı*** a_n olur, f'nin **derecesi** n'dir ve

$$\mathrm{der}(f) = n$$

yazılır. Ayrıca

$$\mathrm{der}(0) = -\infty,$$

ve $d \in \omega \cup \{-\infty\}$ ise

$$-\infty + d = -\infty = d - \infty.$$

Değişkeni X olan, katsayıları K'dan gelen polinomlar

$$K[X]$$

kümesini oluşturur.

* *Vikipedi*'de f'nin "en büyük katsayısı."

Teorem 23. *Her K cismi için $K[X]$ bir halkadır. Bu halkada*

$$\begin{gathered}\operatorname{der}(f+g) \leqslant \max(\operatorname{der}(f), \operatorname{der}(g)),\\ \operatorname{der}(fg) = \operatorname{der}(f) + \operatorname{der}(g)\end{gathered}$$

Teorem 24. *Her polinomlar halkasında eğer $g \neq 0$ ise, o zaman her*

$$f = gx + y \ \ \& \ \ \operatorname{der}(y) < \operatorname{der}(g)$$

sistemi çözülebilir.

Sonuç 25. *$f \in K[X]$ olmak üzere*

$$f \text{ indirgenemezdir} \iff K[X]/(f) \text{ bir cisimdir.}$$

Teorem 26. *Eğer bir K cismi, bir α elemanını içeren başka bir L cisminin altcismi ise, o zaman $K[X]$'ten L cismine giden bir ve tek bir homomorfizim*

1) K'da özdeşliktir ve

2) X'i α'ya gönderir.

Eğer bu homomorfizim birebir değilse, o zaman $K[X]$ halkasının, başkatsayısı 1 olan bir ve tek bir f indirgenemez elemanı için, homomorfizmin çekirdeği (f) idealidir.

Tanım 27. Teoremdeki homomorfizim altında, $K[X]$'in imgesi

$$K[\alpha]$$

olarak yazılır, ve her g polinomunun imgesi

$$g(\alpha)$$

olarak yazılır. Eğer $g(\alpha) = 0$ ise, o zaman α, g'nin bir **köküdür.** Homomorfizmin birebir olmadığı durumda f, α'nın **indirgenemez polinomudur,** ve bu durumda

i) α, K üzerinde **cebirseldir,**
ii) α'nın **derecesi** $\mathrm{der}(f)$ olur.
L cisminde f'nin başka bir kökü, α ile **eşleniktir.**

Örnek 28. Eğer $f \in K[X]$ ve indirgenemez ise, o zaman $K[X]/(f)$ cisminde f'nin $X+(f)$ kökü vardır. Eğer α da f'nin bir kökü ise, o zaman

$$K[X]/(f) \cong_K K[\alpha].$$

Sonuç olarak α ve β eşlenik ise

$$K[\alpha] \cong_K K[\beta].$$

Örnek 29. $\mathbb{C} = \mathbb{R}[\,\mathrm{i}\,]$, ve i'nin indirgenemez polinomu X^2+1 olur.

Teorem 30. *Bir K cismi üzerinde f, bir α'nın indirgenemez polinomu olsun, ve* $\mathrm{der}(f) = n$ *olsun. O zaman K üzerinde $(1, \alpha, \ldots, \alpha^{n-1})$ listesi, $K[\alpha]$ uzayının bir tabanıdır. Özel olarak K sonlu ise $K[\alpha]$ cisminin mertebesi $|K|^n$ olur.*

Örnek 31. $\mathbb{F}_3$ üzerinde X^2+1 indirgenemezdir. Eğer α bu polinomun bir kökü ise, o zaman

$$\mathbb{F}_3[\alpha] = \{\alpha x + y \colon (x, y) \in {\mathbb{F}_3}^2\}$$

ve $|\mathbb{F}_3[\alpha]| = 9$. Bu cisimde $\alpha^2 = -1$.

Teorem 32. *Bir cisimde, derecesi n olan bir polinomun en çok n tane kökü vardır.*

Teorem 33. *Her sonlu cismin birim grubu devirlidir.*

Kanıt. $K^\times$ grubunda mertebesi en büyük olan eleman a olsun. O zaman

$$|a| \leqslant \left|K^\times\right|, \qquad\qquad \langle a\rangle \leqslant K^\times.$$

Şimdi

- b, $K^\times$ grubunun rasgele bir elemanı;
- $\operatorname{ebob}(|a|, |b|) = d$

olsun. O zaman

$$\left|b^d\right| = \frac{|b|}{d}, \qquad \operatorname{ebob}(|a|, \left|b^d\right|) = 1, \qquad \langle a\rangle \cap \langle b^d\rangle = \langle 1\rangle,$$

dolayısıyla

$$\left|ab^d\right| = \operatorname{ekok}\left(|a|, \frac{|b|}{d}\right) = |a| \cdot \frac{|b|}{d}$$

olur. Bu mertebe $|a|$'dan büyük olamadığından $d = |b|$, dolayısıyla $|b|$, $|a|$'nın bir çarpanıdır. Bu şekilde $K^\times$ kümesinin her elemanı, $x^{|a|} - 1$ polinomunun bir köküdür, dolayısıyla $|K^\times| \leqslant |a|$. Bundan dolayı

$$|a| = \left|K^\times\right|, \qquad\qquad \langle a\rangle = K^\times.$$

Özel olarak $K^\times$ devirlidir. □

Teorem 34. *Mertebesi p^n olan bir K cismi varsa, o zaman K'nin altcisimleri, m'nin n'nin bir çarpanı olduğu*

$$\{x \in K \colon x^{p^m} = x\}$$

kümeleridir. Bu durumda $\mathbb{F}_p$ üzerinde $X^{p^n} - X$ polinomunun indirgenemez çarpanlarının dereceleri, n'nin çarpanlarıdır.

Örnek 35. $\mathbb{F}_3$ üzerinde

$$\begin{aligned} X^9 - X &= X(X-1)(X+1)(X^2+1)(X^4+1) \\ &= X(X-1)(X+1)(X^2+1)(X^2+X-1)(X^2-X-1). \end{aligned}$$

Şimdi α, X^2+1 polinomunun bir kökü olsun. O zaman $\mathbb{F}_3[\alpha]$ cisminde yukarıdaki çarpanların kökleri, aşağıdaki gibidir.

polinom	kökleri
X^2+1	$\pm\alpha$
X^2+X-1	$\pm\alpha+1$
X^2-X-1	$\pm\alpha-1$

Ayrıca $\alpha+1$'in kuvvetleri, aşağıdaki gibidir.

k	0	1	2	3	4	5	6	7
$(\alpha+1)^k$	1	$\alpha+1$	$-\alpha$	$-\alpha+1$	-1	$-\alpha-1$	α	$\alpha-1$

Böylece $\mathbb{F}_3[\alpha]^\times = \langle \alpha+1 \rangle$.

Alıştırma 36. Aşağıdaki durumlarda $\mathbb{F}_p$ üzerinde $X^{p^n} - X$ polinomunun indirgenemez çarpanlara ayrılışını bulun:

a) $p=2$ ve $n \in \{2,3,4\}$,
b) $p=3$ ve $n=3$,
c) $p=5$ ve $n=2$.

3 Cisim genişlemeleri

Tanım 37. Eğer K, bir L cisminin bir altcismi ise, o zaman (L,K) sıralı ikilisi, bir **cisim genişlemisidir** ve

$$L/K$$

olarak yazılabilir. K üzerinde vektör uzayı olarak L'nin boyutu

$$[L : K]$$

olarak yazılır. Bu boyutun sonlu olduğu durumda L/K genişlemesinin kendisine **sonlu** denir. Her durumda $f \in K[X]$ ve L'nin α_i elemanları için

$$f = \prod_{i=1}^{n} (X - \alpha_i)$$

ise, o zaman f, L'de **parçalanır.** Eğer ayrıca

$$L = K[\alpha_1, \ldots, \alpha_n]$$

ise, o zaman K üzerinde L, f'nin bir **parçalanış cismidir.** Eğer f'nin α_i kökleri birbirinden farklı ise, o zaman f **ayrılabilir.** Eğer K üzerinde her indirgenemez polinom ayrılabilirse, o zaman K **mükemmeldir.**

Örnek 38. Mertebesi p^n olan sonlu bir L cismi varsa, bu cisim $\mathbb{F}_p$ üzerinde $X^{p^n} - X$ polinomunun parçalanış cismidir, ve bu polinom ayrılabilir. Eğer $K \subseteq L$ ise, o zaman

$$p^n = |K|^{[L:K]}.$$

Tanım 39. Eğer $K \subseteq L$ ve $\alpha \in L$ ise, o zaman L'nin altcismi olan, K'yi kapsayan ve α'yı içeren cisimlerin en küçüğü

$$K(\alpha)$$

olarak yazılır.

Not 40. K üzerinde α

- cebirsel ise $K(\alpha) = K[\alpha]$,

- cebirsel değilse $K(\alpha)$, $K[\alpha]$'dan büyüktür.

Örnek 41. $\mathbb{F}_p \subseteq L$, $\alpha \in L$, $\beta = \alpha^p$ ve $K = \mathbb{F}_p(\beta)$ olsun. Eğer α, $\mathbb{F}_p$ üzerinde cebirsel değilse, o zaman K üzerinde
- $X^p - \beta$ polinomu indirgenemez, ve
- $K[\alpha]$, $X^p - \beta$ polinomunun bir parçalanış cismidir, ama
- $X^p - \beta$ ayrılamaz.

Teorem 42. *Her K cismi üzerinde*

- *her polinomun parçalanış cisimleri vardır,*
- *bunlar birbirine K üzerinde izormorftur.*

Teorem 43. *Bir $K[X]$ polinomlar halkasında bir ve tek bir $f \mapsto f'$ islemi için*

$$\begin{gathered} a \in K \implies a' = 0, \\ X' = 1, \\ (f+g)' = f' + g', \\ (fg)' = f'g + fg'. \end{gathered}$$

Teorem 44. *Bir f polinomu ayrılabilir ancak ve ancak*

$$\operatorname{ebob}(f, f') = 1.$$

Teorem 45. *Karakteristiği sıfır olan (yani $\mathbb{Q}$ cismini kapsayan) her cisim mükemmeldir.*

Teorem 46. *Karakteristiği p olan (yani $\mathbb{F}_p$ cismini kapsayan) bir K cismi mükemmeldir ancak ve ancak $K^p = K$ olur.*

Sonuç 47. *Her sonlu cisim mükemmeldir.*

Teorem 48. *Her p asalı için, her n sayma sayısı için, mertebesi p^n olan cisimler vardır, ve bunlar birbirine izomorftur.*

Tanım 49. Mertebesi p^n olan bir cisim

$$\mathbb{F}_{p^n}$$

olarak yazılır.

Sonuç 50. *$\mathbb{F}_p$ üzerinde $X^{p^n} - X$ polinomunun indirgenemez çarpanlarının dereceleri, n'nin çarpanlarıdır.*

4 Cisim otomorfizimleri

Tanım 51. Bir L cisminin otomorfizimleri

$$\mathrm{Otom}(L)$$

grubunu oluşturur. Eğer $\sigma \in \mathrm{Otom}(L)$ ve $x \in L$ ise, o zaman σ altında x'in imgesi

$$x^\sigma$$

olarak yazılsın. Tanıma göre

$$\bigcap_{x \in K} \{\sigma \in \mathrm{Otom}(L) \colon x^\sigma = x\} = \mathrm{Otom}(L/K).$$

Benzer şekilde $G \leqslant \mathrm{Otom}(L)$ ise, o zaman

$$\bigcap_{\sigma \in G} \{\sigma \in \mathrm{Otom}(L) \colon x^\sigma = x\} = \mathrm{Sab}(G).$$

Teorem 52. *Her L/K cisim genişlemesi için*

i) $\mathrm{Otom}(L/K)$, $\mathrm{Otom}(L)$*'nin bir altgrubudur,*

ii) $\mathrm{Sab}(G)$, *L cisminin bir altcismidir.*

Teorem 53. *Her L/K cisim genişlemesi için*

- $\mathrm{Otom}(L)$*'nin* $\mathrm{Otom}(L/K)$ *altgrupları ve*
- L*'nin* $\mathrm{Sab}(G)$ *altcisimleri,*

eşlenik kümeleri oluşturur. Bir eşleme, tersi $K \mapsto \mathrm{Otom}(L/K)$ olan $G \mapsto \mathrm{Sab}(G)$ göndermesidir.

Kanıt. $\mathrm{Otom}(L/K) = K'$ ve $\mathrm{Sab}(G) = G'$ olsun. O zaman

$$K \subseteq K'', \qquad G \subseteq G''.$$

Özel bir durum olarak

$$G' \subseteq G''', \qquad K' \subseteq K'''. \tag{2}$$

Eğer $K \subseteq F \subseteq L$ ve $G \leqslant H \leqslant \mathrm{Otom}(L)$ ise, o zaman

$$F' \subseteq K', \qquad H' \leqslant G'.$$

Özel bir durum olarak

$$K''' \subseteq K', \qquad G''' \subseteq G'.$$

(2) kapsamaları ile karşılaştırılarak

$$G' = G''', \qquad K' = K'''.$$

Öyleyse $\{K' \colon K \subseteq L\}$ ve $\{G' \colon G \leqslant \mathrm{Otom}(L)]\}$ eşleniktir, ve bir eşleme, tersi $K \mapsto K'$ olan $G \mapsto G'$ göndermesidir. □

Tanım 54. Bir G için $K = \mathrm{Sab}(G)$ ise L/K genişlemesi **Galoisdır.**

Lemma 55. *Eğer*

- L/K, *bir cisim genişlemesi,*
- $f \in K[X]$,
- L, K *üzerinde* f*'nin bir parçalanış cismi,*
- $\alpha \in L$ *ve* $\beta \in L$,
- α *ve* β, K *üzerinde eşlenik*

ise, o zaman $\mathrm{Otom}(L/K)$ *grubunun bir* σ *elemanı için*

$$\alpha^\sigma = \beta.$$

Lemma 56. *Eğer* $\alpha \in L$ *ve* K *üzerinde cebirsel ise, o zaman*

$$[K' : K(\alpha)'] \leqslant [K(\alpha) : K]. \tag{3}$$

Eğer ayrıca α*'nın indirgenemez polinomu ayrılabilirse ve* L*'de parçalanırsa, o zaman*

$$[K' : K(\alpha)'] = [K(\alpha) : K]. \tag{4}$$

Kanıt. α'nın indirgenemez polinomu f, $K' = G$, ve $K(\alpha)' = H$ olsun. Eğer G'nin elemanlarının ikisi σ ve τ ise, o zaman

$$\alpha^\sigma = \alpha^\tau \iff \alpha^{\sigma\tau^{-1}} = \alpha \iff \sigma\tau^{-1} \in H \iff H\sigma = H\tau.$$

Sonuç olarak $H\backslash G$ bölümünden $\{x \in L\colon f(x) = 0\}$ kümesine giden, iyitanımlanmış, birebir bir

$$H\sigma \mapsto \alpha^\sigma$$

göndermesi vardır. Böylece

$$|H\backslash G| \leqslant |\{x \in L\colon f(x) = 0\}|. \tag{5}$$

Tanıma göre

$$|H\backslash G| = [G : H].$$

Ayrıca

$$\begin{aligned} |\{x \in L\colon f(x) = 0\}| &\leqslant \operatorname{der}(f) && \text{[Teorem 32]} \quad (6)\\ &= [K(\alpha) : K] && \text{[Teorem 30].} \end{aligned}$$

Bunlardan dolayı (3) eşitsizliği çıkar. Eğer f, L'de parçalanırsa, o zaman son lemma sayesinde gönderme örtendir, dolayısıyla (5) eşitsizliği bir eşitliktir. Eğer aynı zamanda f ayrılabilirse, o zaman (6) eşitsizliği de bir eşitliktir, ve sonuç olarak (4) eşitliği çıkar. □

Lemma 57. *Eğer L/K sonlu ise, o zaman*

$$|\operatorname{Otom}(L/K)| \leqslant [L : K]. \quad (7)$$

Eğer L, K üzerinde ayrılabilir bir polinomun parçalanış cismi ise, o zaman

$$|\operatorname{Otom}(L/K)| = [L : K]. \quad (8)$$

Kanıt. $K \subseteq F \subseteq L$ ve F/K sonlu olsun. Son lemmadan ve $[F : K]$ üzerinde tümevarımdan

$$[K' : F'] \leqslant [F : K],$$

ve $F = L$ ise (7) eşitsizliği çıkar. Zira $\alpha \in F \smallsetminus K$ olsun, ve tümevarım hipotezi olarak

$$[K(\alpha)' : F'] \leqslant [F : K(\alpha)]$$

varsayılsın. O zaman

$$\begin{aligned} [K' : F'] &= [K' : K(\alpha)'][K(\alpha)' : F'] \\ &\leqslant [K(\alpha) : K][K(\alpha)' : F'] && \text{[Lemma 56]} \\ &\leqslant [K(\alpha) : K][F : K(\alpha)] && \text{[hipotez]} \\ &= [F : K]. \end{aligned}$$

Verilen özel durumda eşitsizlikler eşitliktir. □

Teorem 58. *L/K, sonlu bir cisim genişlemesi olsun. Aşağıdaki koşullar birbirine denktir.*

I. *L/K Galois'dır.*

II. *K üzerinde L'nin her elemanının indirgenemez polinomu, ayrılabilir ve L'de parçalanır.*

III. *K üzerinde L, ayrılabilir bir polinomun parçalanış cismidir.*

IV. $|\mathrm{Otom}(L/K)| = [L : K]$.

Kanıt. 1. L/K Galois ve $\alpha \in L$ olsun. $G = K'$ olsun. Bir n sayma sayısı için, L'nin bazı birbirinden farklı olan α_k elemanları için,

$$\{\alpha^\sigma : \sigma \in G\} = \{\alpha_1, \ldots, \alpha_n\}.$$

Şimdi

$$\prod_{k<n}(X - \alpha_k) = f$$

olsun. O zaman f ayrılabilir ve L'de parçalanır. Ayrıca G'nin her elemanı $\{\alpha_1, \ldots, \alpha_n\}$ kümesinin bir permütasyonu kurduğundan f'nin katsayıları G' cismindedir. Varsayıma göre bu cisim K'dir.

2. K üzerinde L'nin her elemanının indirgenemez polinomu, ayrılabilsin ve L'de parçalansın. L/K sonlu olduğundan

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = L,$$

öyle ki $\ell < s$ olmak üzere $K_{\ell+1}$ cisminin bir β_ℓ elemanının K üzerinde f_ℓ indirgenemez polinomu vardır, ve $K_{\ell+1}$, $f_0 \cdots f_\ell$ polinomunun parçlanış cismidir.

3. Eğer K üzerinde L, ayrılabilir bir polinomun parçalanış cismi ise, o zaman (8) eşitliği çıkar.

4. Tekrar $G = K'$ olsun. O zaman

$$\begin{aligned} |G| &= |\mathrm{Otom}(L/\mathrm{Sab}(G))| && [\text{Teorem 53}] \\ &\leqslant [L : \mathrm{Sab}(G)] && [\text{Lemma 57}] \\ &\leqslant [L : K]. && [K \subseteq \mathrm{Sab}(G)] \end{aligned}$$

Eğer (8) doğru ise, o zaman $\mathrm{Sab}(G) = K$. □

Alıştırma 59. $\mathbb{Q}$ üzerinde $f = X^3 - 3X + 1$ olsun.

A. $\mathbb{C}$ cisminde f'nin köklerini bulun.

B. f'nin Galois grubunu bulun.

Alıştırma 60. $\mathbb{Q}$ üzerinde $X^4 - 2$ polinomunun parçalanış cismini ve onun altcisimlerini bulun.

Teorem 61. *Eğer L/K Galois, $K \subseteq F \subseteq L$, ve F/K genişlemesi de Galois ise, o zaman*

$$\mathrm{Otom}(L/F) \trianglelefteqslant \mathrm{Otom}(L/K).$$

Kanıt. Hipoteze göre $\alpha \in F$ ise, o zaman K üzerinde α'nın her eşleniği F'dedir. Sonuç olarak $\sigma \in \mathrm{Otom}(L/K)$ ise $\alpha^\sigma \in F$. Bundan dolayı $\tau \in \mathrm{Otom}(L/F)$ ise τ F'yi sabitlediğinden

$$\alpha^{\sigma^{-1}\tau\sigma} = \alpha^{\sigma^{-1}\sigma} = \alpha.$$

Böylece $\sigma^{-1}\tau\sigma \in \mathrm{Otom}(L/F)$. □

Alıştırma 62. Eğer L/K Galois, $K \subseteq F \subseteq L$, ve

$$\mathrm{Otom}(L/F) \trianglelefteqslant \mathrm{Otom}(L/K)$$

ise, o zaman F/K genişlemesinin Galois olduğunu kanıtlayın.

5 İndirgenemezlik

Tanım 63. Eğer her a_k katsayısı bir tamsayı ve

$$\text{ebob}(a_0, a_1, \ldots, a_n) = 1$$

ise $a_0 + a_1X + \cdots + a_nX^n$ polinomuna **ilkel** denir.

Lemma 64 (Gauss)**.** *İki ilkel polinomun çarpımı da ilkeldir.*

Kanıt. Eğer f ilkel ama fg ilkel değilse, g'nin ilkel olmadığını göstereceğiz. Şimdi

$$f = \sum_{i=0}^{m} a_i X^i, \qquad\qquad g = \sum_{j=0}^{n} b_j X^j$$

olsun. Ayrıca $i > m$ ise $a_i = 0$ olsun, ve $j > n$ ise $b_j = 0$ olsun. O zaman

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

olmak üzere

$$fg = \sum_{k=0}^{m+n} c_k X^k.$$

Eğer bu polinom ilkel değilse, o zaman bir p asalı, her c_k katsayısını böler. O halde f ilkel ise, bir ℓ için $p \nmid a_\ell$, ama $i < \ell$ olduğunda $p \mid a_i$. Böylece

$$p \mid a_0 b_\ell + a_1 b_{\ell-1} + \cdots + a_{\ell-1} b_1,$$

dolayısıyla $p \mid a_\ell b_0$, çünkü

$$a_\ell b_0 = c_\ell - (a_0 b_\ell + a_1 b_{\ell-1} + \cdots + a_{\ell-1} b_1).$$

Şimdi Öklid Lemması'ndan $p \mid b_0$. Bundan dolayı

$$p \mid c_{\ell+1} - (a_0 b_{\ell+1} + a_1 b_\ell + \cdots + a_{\ell-1} b_2 + a_{\ell+1} b_0),$$

yani $p \mid a_\ell b_1$, ve sonuç olarak $p \mid b_1$. Bu şekilde her j için $p \mid b_j$, dolayısıyla g ilkel değildir. □

Teorem 65. *Katsayıları tamsayı olan bir polinom $\mathbb{Z}$ üzerinde indirgenemezse, o zaman $\mathbb{Q}$ üzerinde de indirgenemez.*

Kanıt. Katsayıları tamsayı olan bir h polinomu $\mathbb{Z}$ üzerinde indirgenemezse, o zaman ilkeldir. Şimdi a_i, c_i, b_j, ve d_j tamsayı olmak üzere

$$\begin{aligned} \operatorname{ebob}(a_i, c_i) &= 1, & \operatorname{ebob}(b_j, d_j) &= 1, \\ f &= \sum_i \frac{a_i}{c_i} X^i, & g &= \sum_j \frac{b_j}{d_j} X^j, \\ a &= \operatorname{ebob}_i a_i, & b &= \operatorname{ebob}_j b_j, \\ c &= \operatorname{ekok}_i c_i, & d &= \operatorname{ekok}_j d_j \end{aligned}$$

olsun. O zaman $(c/a)f$ ve $(d/b)g$, $\mathbb{Z}$ üzerinde ve ilkeldir. Gauss Lemma sayesinde $(cd/ab)fg$ de ilkeldir. Eğer fg'nin $\mathbb{Z}$ üzerinde olan ve ilkel bir h polinomuna eşit olduğunu bilirsek, o zaman $ab = cd$, dolayısıyla $h = (c/a)f(d/b)g$. Sonuç olarak h $\mathbb{Z}$ üzerinde indirgenemezse, $\mathbb{Q}$ üzerinde de indirgenemez. □

Teorem 66 (Eisenstein Kriteri)**.** *Eğer*

- *Her a_k tamsayı,*
- *bir p asalı için*
  - *$p^2 \nmid a_0$, ama*
  - *$0 \leqslant k < n$ olmak üzere $p \mid a_k$, ama*
  - *$p \nmid a_n$*

ise, o zaman

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + a_n X^n$$

polinomu $\mathbb{Q}$ *üzerinde indirgenemez.*

Kanıt. Verilen polinom f olsun. Bunun ilkel olduğunu varsayabiliriz. Bu durumda f'nin $\mathbb{Z}$ üzerinde indirgenemediğini kanıtlamak yeter. $\mathbb{Z}$ üzerinde

$$g = \sum_{i=0}^{n} b_i X^i, \qquad\qquad g = \sum_{j=0}^{n} c_j X^j$$

olmak üzere $f = gh$ olsun. O zaman f ve g de ilkeldir. Ayrıca $a_0 = b_0 c_0$ olduğundan $p \mid b_0$ ve $p \nmid c_0$ varsayabiliriz. Bir ℓ için $k < \ell$ ise $p \mid b_k$ olsun. Eğer $\ell = n$ ise, g ilkel olduğundan $p \nmid b_n$, dolayısıyla $\operatorname{der}(g) = n$, ve sonuç olarak $\operatorname{der}(h) = 0$ ve $h = \pm 1$. Diğer durumda $p \mid a_\ell$, ama

$$a_\ell = b_0 c_\ell + b_1 c_{\ell-1} + \cdots + b_\ell c_0,$$

dolayısıyla $p \mid b_\ell$. Tümevarımdan $k < n$ ise $p \mid b_k$, ve yukarıdaki gibi $h = \pm 1$. □

Örnek 67. $\mathbb{Z}$'de bir p asalı için $p \mid d$ ama $p^2 \nmid d$ olsun, ve

$$f = X^5 - d$$

olsun. O zaman Eistenstein Kriterinden dolayı $\mathbb{Q}$ üzerinde f indirgenemez. Şimdi $\mathbb{C}$'de ρ, f'nin bir kökü olsun ve

$$\zeta = \zeta_5 = \exp \frac{2\pi \mathrm{i}}{5}$$

olsun. O zaman f'nin kökleri, $\{\zeta^k \cdot \rho \colon 0 \leqslant k < 5\}$ kümesini oluşturur, dolayısıyla

$$\mathbb{Q}(\rho, \zeta)$$

cismi, $\mathbb{Q}$ üzerinde f'nin parçalanış cismidir. Ayrıca Eistenstein Kriterinden dolayı $\mathbb{Q}$ üzerinde $X^4+X^3+X^2+X+1$, ζ'nın indirgenemez polinomudur, çünkü

$$X^4+X^3+X^2+X+1=\frac{X^5-1}{X-1},$$
$$\frac{(X+1)^5-1}{(X+1)-1}=X^4+5X^3+10X^2+10X+5.$$

Şimdi

$$\begin{aligned}[\mathbb{Q}(\rho,\zeta):\mathbb{Q}] &= [\mathbb{Q}(\rho,\zeta):\mathbb{Q}(\zeta)][\mathbb{Q}(\zeta):\mathbb{Q}] \\ &= [\mathbb{Q}(\rho,\zeta):\mathbb{Q}(\rho)][\mathbb{Q}(\rho):\mathbb{Q}],\end{aligned}$$

ama

$$[\mathbb{Q}(\zeta):\mathbb{Q}]=4, \qquad [\mathbb{Q}(\rho):\mathbb{Q}]=5.$$

Ayrıca $\text{ebob}(4,5)=1$ ve

$$[\mathbb{Q}(\rho,\zeta):\mathbb{Q}(\rho)] \leqslant [\mathbb{Q}(\zeta):\mathbb{Q}], \quad [\mathbb{Q}(\rho,\zeta):\mathbb{Q}(\zeta)] \leqslant [\mathbb{Q}(\rho):\mathbb{Q}].$$

Bundan dolayı $[\mathbb{Q}(\rho,\zeta):\mathbb{Q}]=20$, dolayısıyla

$$\begin{aligned}|\text{Otom}(\mathbb{Q}(\rho,\zeta)/\mathbb{Q})| &= 20,\\ |\text{Otom}(\mathbb{Q}(\rho,\zeta)/\mathbb{Q}(\zeta))| &= 5,\\ |\text{Otom}(\mathbb{Q}(\rho,\zeta)/\mathbb{Q}(\rho))| &= 4.\end{aligned}$$

Sonuç olarak $\text{Otom}(\mathbb{Q}(\rho,\zeta)/\mathbb{Q}(\zeta))$ devirlidir, ve grubun aşikâr olmayan her elemanı bir üreteçtir. Özellikle

$$\rho^\tau=\zeta\cdot\rho \text{ olmak üzere } \text{Otom}(\mathbb{Q}(\rho,\zeta)/\mathbb{Q}(\zeta))=\langle\tau\rangle.$$

Ayrıca $\mathbb{Q}$ üzerinde ve $\mathbb{Q}(\rho)$ üzerinde, ζ'nın eşlenikleri ζ^2, ζ^4, ζ^8, ve ζ^{16} olur, dolayısıyla

$$\zeta^\sigma=\zeta^2 \text{ olmak üzere } \text{Otom}(\mathbb{Q}(\rho,\zeta)/\mathbb{Q}(\rho))=\langle\sigma\rangle.$$

x	ρ	ζ
x^σ	ρ	ζ^2
x^τ	$\zeta\cdot\rho$	ζ

Tablo 1: $\mathbb{Q}(\rho,\zeta)$'nın otomorfizmaları

Şimdi σ ve τ tablodaki gibidir, ve

$$\mathrm{Otom}(\mathbb{Q}(\rho,\zeta)/\mathbb{Q}) = \langle\sigma,\tau\rangle.$$

Teorem 61 ve Alıştırma 62 sayesinde

$$\langle\sigma\rangle \not\trianglelefteq \langle\sigma,\tau\rangle, \qquad\qquad \langle\tau\rangle \trianglelefteq \langle\sigma,\tau\rangle.$$

Aslında

$$\rho^{\sigma^{-1}\tau\sigma} = \rho^{\tau\sigma} = (\zeta\cdot\rho)^\sigma = \zeta^2\cdot\rho = \rho^{\tau^2}$$

olduğundan

$$\sigma^{-1}\tau\sigma = \tau^2, \qquad\qquad \tau\sigma = \sigma\tau^2,$$

dolayısıyla

$$\tau^{-k}\sigma\tau^k = \sigma\tau^{-k}.$$

Sylow Teoremleri sayesinde $\langle\sigma,\tau\rangle$ grubunun

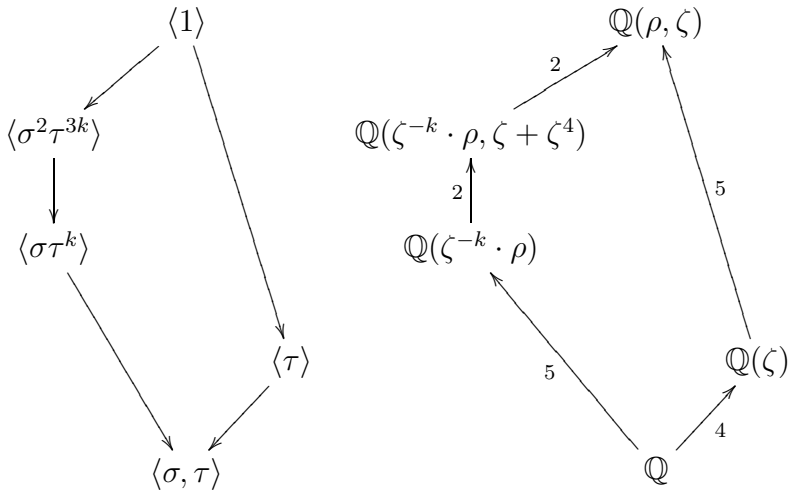
- tek Sylow 5-altgrubu $\langle\tau\rangle$'dur;
- Sylow 2-altgrubları, $0\leqslant k<5$ olmak üzere $\langle\sigma\tau^k\rangle$'dır.

Ayrıca

$$\sigma\tau^k\sigma\tau^k = \sigma^2\tau^{2k+k} = \sigma^2\tau^{3k}$$

olduğundan $\langle\sigma\tau^k\rangle$ grubunun tek mertebesi 2 olan altgrubu $\langle\sigma^2\tau^{3k}\rangle$ olur. Şimdi

$$(\zeta^\ell\cdot\rho)^{\sigma\tau^k} = (\zeta^{2\ell}\cdot\rho)^{\tau^k} = \zeta^{2\ell+k}\cdot\rho$$



Şekil 1: $X^5 - d$ için Galois eşlemesi

olduğundan

$$\mathrm{Sab}(\sigma\tau^k) = \mathbb{Q}(\zeta^{-k}\cdot\rho), \quad \mathrm{Sab}(\sigma^2\tau^{3k}) = \mathbb{Q}(\zeta^{-k}\cdot\rho, \zeta+\zeta^4).$$

$X^5 - d$ polinomu için Galois eşlemesi, şekildeki gibidir.

Alıştırma 68. $\mathbb{Q}$ üzerinde $X^6 - 2$ polinomunun parçalanış cisminin tüm altcismilerini bulun.