Abstract Algebra 1-2 Re

m차원 $\left(L \atop E\right)$ 기저 $\lambda_1, \lambda_2, \cdots, \lambda_m$ — λ_i 가 될 수 있는게 m개

mn차원

n차원 $\left(E \atop F\right)$ $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$ 기저 — ε_j 가 될 수 있는게 n개

전체 mn개

Thm 9.2.1 증명 과정에서 이 정리가 99% 쓰임.

체 $L \supset E \supset F$ 에 대해, $|L:E| = m$,

$|E:F| = n$ 이라 하자.

$\{\lambda_1, \lambda_2, \cdots, \lambda_m\}$ 이 L의 E-기저이고,

$\{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n\}$ 이 E의 F-기저일 때,

$\{\lambda_i \varepsilon_j \mid 1 \le i \le m,\ 1 \le j \le n\}$

은 L의 F-기저이다.

Claim)
① Linear indpt
② span

(pf)

① $\sum_{i,j} a_{ij} \lambda_i \varepsilon_j = 0$ 라 하자.

$\sum_i \sum_j \underbrace{a_{ij}}_{\in F \subset E} \lambda_i \underbrace{\varepsilon_j}_{\in E} = \sum_i \Big(\underbrace{\sum_j a_{ij}\varepsilon_j}_{\in E}\Big) \lambda_i$ — E에 들어가는 원소의 곱

field 이므로 곱셈에서 교환 law 만족

$\Rightarrow \lambda_1, \cdots, \lambda_n$ 기저이므로 $\sum_j \underbrace{a_{ij}}_{\in F} \underbrace{\varepsilon_j}_{기저} = 0$ — 기저 일차결합해서 0 만드려면 계수들 0 될수밖에.

그런데 ε_j 역시 기저.

$\Rightarrow \varepsilon_1, \cdots, \varepsilon_n$ 이 기저이므로 $\forall i, j\ \ a_{ij} = 0$

② span 함을 보이자. $\alpha \in L$ 고려

$\lambda_1, \cdots, \lambda_m$ 이 기저이므로

$\alpha = a_1 \lambda_1 + \cdots + a_m \lambda_m$ 으로 표현 가능. (기저)

$a_1 = b_{11}\varepsilon_1 + b_{12}\varepsilon_2 + \cdots + b_{1n}\varepsilon_n$, $a_i \in E$ 이므로, $a_m = b_{m1}\varepsilon_1 + b_{m2}\varepsilon_2 + \cdots + b_{mn}\varepsilon_n$

$= (b_{11}\varepsilon_1 + b_{12}\varepsilon_2 + \cdots + b_{1n}\varepsilon_n)\lambda_1 + \cdots + (b_{m1}\varepsilon_1 + \cdots + b_{mn}\varepsilon_n)\lambda_m$

기저 형태.

$= b_{11}\varepsilon_1\lambda_1 + \cdots + b_{1n}\varepsilon_n\lambda_1 + \cdots + b_{m1}\varepsilon_1\lambda_m + \cdots + b_{mn}\varepsilon_n\lambda_m$

따라서 span. ∎

$mn \left(L \overset{m}{|} E \overset{n}{|} F\right)$ $|L:E| = m$, $|E:F| = n$

$\Rightarrow |L:F| = mn = |L:E||E:F|$

* ii) 유한이다! $\left(L \overset{i)\ 유한}{|} E \overset{유한}{|} F\right)$ 이면, then, i) 유한 이면 $\left(L \overset{ii)\ 유한일까?}{|} E \overset{iii)\ 유한}{|} F\right)$ O O

[따름정리] 체의 확대 $F \le E \le L$ 에 대하여,

$F \le L$ 이 유한확대라면, $F \le E$, $E \le L$ 역시

유한확대이다.

90% 확률로 무조건 씀.

Corol 9.2.2

체의 확대 $L \supset E$, $E \supset F$ 가 유한 확대일 때,

$L \supset F$ 도 유한 확대이고,

$|L:F| = |L:E||E:F|$

[Ex]

$|\mathbb{Z}_3(\sqrt{2}) : \mathbb{Z}_3| + \boxed{|\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \sqrt[3]{3}) : \mathbb{Q}|} = ?$ (단순확대)

$x = \sqrt{2}$, $x^2 - 2 = 0$ ↓ $\mathbb{Z}_3$, $x^2 + 1 = 0$ 이므로 2

$|F(\alpha) : F| = \deg \mu_{\alpha/F}$, $\in F[x]$

$= |\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})||\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}|$ — $x^3 - 3 = 0$: 3

$= 3 \cdot |\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})||\mathbb{Q}(\sqrt{2}) : \mathbb{Q}|$ — $x = \sqrt{3}$, $x^2 - 3 = 0$: 2; $x = \sqrt{2}$, $x^2 = 2$: 2

$= 2 + (3 \times 2 \times 2) = 14.$

↓ **이렇게 풀 수 있는 이유**

앞에서는 $\mathbb{Q}(\sqrt{2}) \to \sqrt{2}$ 하나만 포함하는 가장 작은 체

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$? $\sqrt{2}$와 $\sqrt{3}$, $\mathbb{Q}$ 를 포함하는 가장 작은 체 (동시에 포함.)

$\cup \| \cap$

$(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$? $\sqrt{2}$와 $\sqrt{3}$을 포함하는 가장 작은 체

즉 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$

$(\cap)$ $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 은 $\sqrt{2}$와 $\sqrt{3}$을 포함하는 가장 작은 field 이고,

$(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$ 은 $\sqrt{2}$와 $\sqrt{3}$을 포함하는 field 이므로

최소성에 의해 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \cap (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$

$(\cup)$ $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$ 는 $\sqrt{2}$를 포함하고 $\sqrt{3}$을 포함하는

가장 작은 field.

$\mathbb{Q}(\sqrt{3}, \sqrt{2}) \supset \mathbb{Q}(\sqrt{2})$

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 은 $\mathbb{Q}(\sqrt{2})$랑 $\sqrt{3}$을 포함하는 체

$\therefore \mathbb{Q}(\sqrt{2}, \sqrt{3}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$

$|\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})|$

$\| \ (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$

Thm 9.2.3

$F \subset E$ 가 유한확대일 때,

(1) $F \subset E$ 는 대수적 확대이다.

(2) $\alpha_1, \alpha_2, \cdots, \alpha_n \in E$ 가 있어서

$E = F[\alpha_1, \alpha_2, \cdots, \alpha_n]$ 이다.

(pf) $n \left(E \ni \alpha \overset{유한}{|} F[x]\right)$ $\{\lambda_1, \cdots, \lambda_n\}$ 기저

기저이므로 span 하는 것보다 많으면 종속, 적은거 가져오면 생성 못함.

$1, \alpha, \alpha^2, \cdots, \alpha^n \in E$

E에 들어가는 원소 $n+1$개, 차원보다 1개 많음.

차원보다 많은 개수 벡터 갖고 오면 $\boxed{일차종속}$

$\exists\ a_0, a_1, \cdots, a_n \in F$ s.t

$1 \cdot a_0 + a_1\alpha + a_2\alpha + \cdots + a_n\alpha^n = 0$

$(a_0, a_1, \cdots, a_n) \ne 0$

$f = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$

└ α를 해로 갖고 계수가 $a \in F$인 다항식

그러므로 유한확대 ⇒ 대수적 확대.

(2) pf) $n \left(E \ni \alpha \ |\ F\right)$ $\alpha_1, \cdots, \alpha_n$: 기저 — 어떤 α도 기저들의 일차결합으로

$F\alpha_i = \{f\alpha_i \mid f \in F\}$ 라 하면

$E \subset F\alpha_1 + \cdots + F\alpha_n$ — E 원소가 $\alpha_1, \cdots, \alpha_n$ 으로 생성되므로 (기저)

얘들 다 포함한 집합이자 field

$\cap$

$F(\alpha_1, \cdots, \alpha_n)$ — $\alpha_1, \alpha_2, \cdots, \alpha_n$ 포함하는 '가장 작은' field

$\cap$

E

E는 F의 확대체, $\alpha_1, \cdots, \alpha_n \in E$ (기저), $F \subset E$ — 둘다 포함하는 field

결론

따라서 $E = F\alpha_1 + \cdots + F\alpha_n = F[\alpha_1, \cdots, \alpha_n] = E$

($\underbrace{F\alpha_1 + \cdots + F\alpha_n}_{E}$, $\underbrace{F[\alpha_1, \cdots, \alpha_n]}_{E}$)

(앞에서 $E \ni \alpha$, F: α: 대수적이면 $F[\alpha] = F(\alpha)$ ⇒ 지금 $\alpha_1, \cdots, \alpha_n$ 은 $\forall$ 대수적이므로, $F(\alpha_1, \cdots, \alpha_n) = F[\alpha_1, \cdots, \alpha_n]$) ∎

앞에서, 유한이다 (L — E 유한, E — F 유한) 이면 (L — E — F) 유한이고 유한이다.

then. Q) 대수적이겠는가? Yes. (L — E 대수적이고, E — F 대수적이면)

Thm 9.2.4

$F \subset E$, $E \subset L$ 이 대수적 확대일 때,

$F \subset L$ 도 대수적 확대이다.

(pf) $L \ni \alpha$ 인 $\alpha \in L$ 을 가져와서,

F를 계수로 갖는, α를 해로 갖는

다항식이 존재함을 보이면 됨.

α가 대수적이므로,

$\exists f \in E[x]$, $f(\alpha) = 0$ — E가 대수적 확대이므로 e_i 들은 대수적인 수가 된다.

$e_0 + e_1 x + \cdots + e_n x^n$, $e_i \in E$

$K = F(e_1, \cdots, e_n)$

$\Rightarrow |K:F| = \underbrace{|K : F(e_1, \cdots, e_n)|}_{\text{유한}} \, |F(e_1, \cdots, e_n) : F|$

$|F(e_1, \cdots, e_{n-1}, e_n) : F(e_1, \cdots, e_{n-1})|$ $< \infty$ 이므로

$(F(e_1, \cdots, e_{n-1}))(e_n)$

e_i 들 중 하나

$e_n \in E$, $g \in F[x]$ s.t $g(e_n) = 0$

그러므로 대수적

$F(e_1, \cdots, e_{n-1})$ 임을 고려하면, 관계이다. $\subset$

F — $(F(e_1, \cdots, e_{n-1}))[x]$

⇒ 그러면 g는 $F(e_1, \cdots, e_{n-1})$ 을 계수로 가지는

다항식으로써, e_n을 해로 가지는 다항식으로

생각할 수 있음. 게다가 g는 유한차원 다항식.

애 정의: $F(e_1, \cdots, e_{n-1})$ 을 계수로 가지면서,

e_n 을 해로 가지는 다항식 중에서 차원이 젤 낮은,

즉 기약 다항식의 차수!

$= |F(e_1, \cdots, e_{n-1}) : F(e_1, \cdots, e_{n-2})| \cdot |F(e_1, \cdots, e_{n-2}) : F|$

각 하면 앞에서와 같이, 유한됨. 계속 반복 ⋯

⇒ $|K:F| < \infty$ 가 나옴.

그런데 또 $f = e_0 + e_1 x + \cdots + e_n x^n$

$\in (F(e_0, \cdots, e_n))[x] = K[x]$

즉 f는 $K[x]$에 들어가는 다항식으로써

$f(\alpha) = 0$ 이 되는 다항식인 것

Then $|K(\alpha) : K|$ 고려 $< \infty$

K를 계수로 가지는 다항식 중에서
α를 해로 갖는 다항식 중에서
차수가 '제일 작은 것' 즉 유한값

$\therefore |K(\alpha) : F| < \infty$

$= \underbrace{|K(\alpha) : K|}_{\text{유한}} \underbrace{|K : F|}_{\text{유한}}$

따라서 α가 대수적인 수

$\alpha \in K(\alpha)$ — K 유한, K — F 유한 이므로, 유한이다.

⇒ L 에 들어가는 어떤 α 갖고 오던 간에

F를 계수로 갖는 다항식이 있어서 α가 대수적.

(= α를 해로 갖는 다항식이 존재)

* 요약

유한이다. (L — E 유한, E — F 유한) 이면 / 유한이면 (L — E — F) 유한이고 유한이다. / 대수적이다. (L — E 대수적이고, E — F 대수적이면)

Then. Q) 대수적이면 (L — E 대수적, $E \ni \alpha$, E — F 대수적) 일까?

$F \le E \le L$ 일 때 $F \le L$ 이 대수적이면

$F \le E$ ∧ $E \le L$ 대수적일까? (보였고 / 아닌거지!)

⇒ $\alpha \in E$ 인 α를 가져와서 F를 계수로 갖고

α를 해로 갖는 다항식이 존재하겠는가?

$\alpha \in$ $E \le L$ 이기 때문에, $\alpha \in L$ 라고 생각할 수도 있다.

근데 L이 F 상에서 대수적임을 이야기해 줬기 때문에

F를 계수로 가지면서 α를 해로 가지는 다항식 존재!

$\alpha \in L$ 인 α를 가져와서 E를 계수로 갖고 해가 α인 다항식

$\exists g \in F[x]$ s.t $g(\alpha) = 0$

$\subset E[x]$ 이므로

g가 E를 계수로 갖는 다항식이라 생각해도 상관 없다.

그러므로 L에 들어가는 원소를 가지고 오면,

그 원소가 E를 계수로 & α를 해로 갖는

다항식이 존재한다.

$\therefore F \le E$ 는 대수적이다.