1강

Abstract Algebra Lec 1 OT

Review

<정의> 체 (field)

$(R, +, \times)$가 1을 갖는 가환환으로써

1) $(R, +)$는 아벨군 (abelian group)

2) $(R-\{0\}, \times)$ 역시 아벨군

3) 분배법칙

<정의> 확대체 (extension field)

$(R, +_R, \cdot_R)$가 체라 하자.

$R \subset E$ 이고 $(E, +_E, \cdot_E)$ 역시 체로써

$+_E|_R = +_R$ 이고 $\cdot_E|_R = \cdot_R$

를 만족한다면, E를 F의 확대체

(extension field)

라 하고, $F \leq E$ 라 쓴다.

부분군 ← 군
부분환 환
부분체 체

$n \cdot 1 \neq 0$ ($|1| = char R$)

주어진 R이 정역이면 1의 덧셈에 대한 위수가 Char R

* R이 정역일 때 Char R = 0 이거나

Char R = p (소수)

Characteristic ?

for $\forall r \in R$, $\exists n \in \mathbb{N}$ s.t $n \cdot r = 0$

└ r에 따라 n이 변하지 않는다. (r을 n번 더함)

[예제 1] $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$

Char이 p인 것 중에서 제일 작은 field는 $\mathbb{Z}_p$

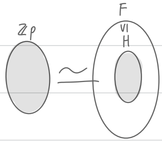
소체 (prime field)

1. char F = p 이면, $\mathbb{Z}_p \leq F$ 라 할 수 있다. 완전 같은 말은 아님.

char F = 0 이면, $\mathbb{Q} \leq F$ 라 할 수 있다.

Char이 0인 것 중에서 제일 작은 field는 $\mathbb{Q}$

$\mathbb{Z}_p$ 또는 $\mathbb{Q}$가 field 중 가장 작은 field 이다.



$\mathbb{Z}_p$가 F의 Subfield

H와 동형. $\mathbb{Z}_p \simeq H$

<정의> 대수적 (algebraic)

F가 field. $F \leq E$ (F의 확대체), $a \in E$ → a가 대수적

⇒ $\exists f(x) \in F[x]$ s.t $f(a) = 0$

a를 해로 갖는 다항식

· 초월적 (transdental) 대수적 아니다.

$f(a) \neq 0$ for $\forall f(x) \in F[x]$

<정의> 최소다항식 (minimal polynomial)

F(base field)가 field. $F \leq E$ (확대체) $a \in E$, a가 대수적

$\exists f \in F[x]$ s.t $\boxed{f(a) = 0}$

게다가 f가 기약 아니다.

a를 해로 갖는 이 다항식 몇 개 존재할까?

$x^n f = g$ 라 해도 a를 해로 갖는다.

→ 해를 갖는 다항식 여러 개 있을 수 있다.

$f = gh$ $0 = f(a) = g(a)h(a)$ 둘 중 하나는 0

∈ F (field에 들어가는 원소)

$g(a) = 0$ 이라 하게 되면 $\deg f = \deg gh$ degree 정의에 의해

$= \deg g + \deg h$

≥1 ≥1 (기약다항식 이라는 조건에 의해)

즉 $\deg f \neq \deg g$

→ 기약다항식이 되면 그 차수보다 ($\deg f$) 더 낮으면서도

a를 해로 갖는 다항식이 (g) 존재한다.

then, a를 해로 갖는 다항식 중에서 차수가 가장

작은 다항식은 몇 개 있을까?

무수히 많다! 앞에 $\times 2$ $\times 3$ ⋯ 무수히 많음.

(기약이라고 해도 ⋯)

→ 그럼 앞 계수가 1인 것

즉, a를 해로 갖는 최고차항의 계수가 1인 모닉다항식

기약인 다항식을 최소다항식, $\mu_{a,F}$ 해 base field.

<정의> 단순확대체

Note) 기호정리 F[x] 와 F(a). F[a]

F[x] $a \in$ F를 계수로 갖게 되는 유한차수

다항식들을 모아놓음.

$F \leq E \ni a$.

F(a) : F와 a를 포함하는 가장 작은 체

ⓚ E는 F와 a를 포함하는 체.

정의에 의해 $F(a) \subset E$

$F[a] = \{ f(a) \mid f \in F[x] \}$

$a_0 + a_1 a + a_2 a^2 + \cdots + a_n a^n \in F(a)$

($a_1 a \in F(a)$, $a_1 \in F(a)$, $a_2 \in F(a)$)

$a_0, a_1, \cdots, a_n \in F$

$F \subset E$ 이므로 $\in E$, $a \in E$ 이므로

$\subset F(a)$

즉 $F[a] \subset F(a) \geq F$

확대체인데 딱 한 개의 원소만 집어넣어서

만든 확대체라고 해서 '단순 확대체'

<정의> 차원, 유한확대

$F \leq E$ (확대체) F를 스칼라체로 갖는 벡터공간

으로 생각해보자.

(V, +, ·) F 다섯가지 조건 만족하면 V를 벡터공간 (E, 아벨군)

1) $a \in F$ 와 $b \in V$ 를 곱한 결과가 $ab \in V$

(즉 연산이 닫혀있다)

2) $a, b \in F$, $(a+b)v = av + bv$ 덧셈에 대해 분배법칙 만족

3) $u, v \in V$, $a(u+v) = au + av$ 곱셈에 대해 분배법칙 만족

4) 1은 F의 unity (단위원), $1 \cdot V = V$

5) $a, b \in F$, $(a \cdot b) \cdot u = a(b \cdot u)$

→ $F \leq E$ 이면 E는 위 조건을 다 만족하게 됨.

F상의 연산이므로.

$\dim_F E =: [E : F]$

F를 스칼라필드로 갖는다.

E가 코일 때는 이 기호를 좌잉여류의 갯수로 썼었는데, E가 Field일 때는 차원을 이렇게 씀.

$\dim_F E < \infty$ 유한차원

차원이 유한이면 E를 유한확대.

Abstract Algebra Lec 1 OT

[예제] $|\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}| + |\mathbb{C}:\mathbb{R}| = 5$ ($3 + 2$)

① $|\mathbb{C}:\mathbb{R}| = 2$

$\{a+bi \mid a,b \in \mathbb{R}\}$

기저 2개

$a①+bⓘ$ 일차결합 $\Rightarrow 2$

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

단순확대체

$\sqrt[3]{3}$ $\sqrt[3]{9}$ $\sqrt[3]{27} = 3$

$x = \sqrt[3]{3}$

$x^3 = 3 \Rightarrow x^3 - 3 = 0$

$\mu_{\sqrt[3]{3}/\mathbb{Q}} = 1 \cdot x^3 - 3 \Rightarrow \deg \mu = 3$

$x^3 - 3 = 0$ 기약다항식인지 어떻게 확인?

3가지 ① $\deg f \le 3$ 일 때

→ 해 가지면 가약, 해 없으면 기약.

② mod p test (criterion)

prime number p 가 존재해서

$a_1 \equiv \sim \pmod{p}$ 해서 만든게 $\bar{F}$

⋮

$\mathbb{Z}_p$ 상에서 기약이면, f는 기약

③ Eigenstein's thm $p = 3$

적당한 mod p 가 존재해서 p가 최고차항을 못나누고, 이외의 다른 항들의 계수들은 다 나누면서 특별히 p^2이 상수항을 못 나누는 그러한 p가 존재.

$|\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}|$ 구하기 위해 필요한

Thm 9.1.5) (단순확대의 기저)

F 상에서 대수적인 $\alpha \in E \supset F$ 에 대해

$\deg \mu_{\alpha/F} = n$ 이라 할 때.

(1) $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ 은

$F[\alpha]$ 의 F-기저이다.

(2) $|F[\alpha]:F| = n = \deg \mu_{\alpha/F}$

$F[\alpha] = F(\alpha)$

$\therefore |\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}| = 3$

(fraleigh)
Thm 29.3 (Kronecker's Thm)

Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$.

Then there exists an extension field E of F and $\alpha \in E$ s.t. $f(\alpha) = 0$.

F가 field. $f \in F[x] - F$

상수는 해 유무가 너무 자명하므로
제로다항식 : F의 모든 값이 해
영이 아니면 : 해가 없다

$x^2+1 \in \mathbb{R}[x] \subset \mathbb{C}[x]$

실수 상에서 해 안가짐. $\in \mathbb{C}$

$\mathbb{R} \le \exists \mathbb{C}$

* field를 계수로 가지는 다항식이 있으면 해를 갖게 되는 확대체가 존재.

$SF(f/F)$ 라 씀

가장 작은

<정의> 분해체 (splitting field)

Thm 20.1 체 이론의 기본정리 (Kronecker's Thm) 1887

F가 체이고 $f(x)$가 $F[x]$에서 상수가 아닌 다항식이라 하자. 그러면 f의 근을 포함하는 F의 확대체 E가 존재한다.

존재하는 체 중에서 제일 작은 체 — 분해체 $\cap E$, $F \le E$ = 체

f의 모든 해를 갖는체 └ 어떻게 구하나? 주어진 확대체 E 가져와서

F의 단순확대체 · K의 단순확대체

$$\begin{tikzcd} \alpha \in F[\alpha] \arrow[r, "\theta"] & K[\beta] \ni \beta \\ F \arrow[r, "\sigma"] & K \end{tikzcd}$$

$\cong$ 동형확대정리

p의 해계해: p · $\bar{p}$의 해: $\bar{p} = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n$

$F[\alpha]|_F = \sigma$

F, K는 field, 동형

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

f의 모든 해를 포함하는 체

f의 확대체

$f = (x-a_1)(x-a_2)\cdots(x-a_n)$ E_n

$f_2 \in E_2[x]$, $f = (x-a_1)(x-a_2)f_2$ E_2

$f_1 \in E_1[x]$, $f = (x-a_1)f_1$ E_1 확대체

$f \in F[x]$

$\therefore f \in F[x] - F$

$\exists E \ge F$ s.t f의 모든 해 $\subset E$

Corol 9.3.7 $f \in F[x]$에 대하여,

F 상의 f의 임의의 두 분해체는 F-동형이다.

Homework #1

1. $\mathrm{char}F = p$ 이면, $\mathbb{Z}_p \le F$ 라 할 수 있다.
$\mathrm{char}F = 0$ 이면, $\mathbb{Q} \le F$ 라 할 수 있다.

2. 따름정리 9.1.4
$\alpha \in E \supset F$에 대하여, α가 F 상에서 대수적일 때, $F[\alpha]$는 체이다.

$F[\alpha] = F(\alpha)$ $E \ge F$

조건
$F \le E \ni \alpha$ 대수적

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

onto 인 준동형사상

$\phi : F[x] \to F[\alpha] \subset E$

동형정리 $F[x]/\ker\phi \simeq \phi(F[x]) = F[\alpha]$ ① 체 ② 체가 된다. ③ 체가 된다.

$\ker\phi = \langle \mu_{\alpha/F} \rangle$ 기약 · $f(\alpha) = 0$ · α를 해로 갖는 다항식 모아놓은 집합.

* $\mu_{\alpha/F} \Rightarrow$ 기약이면, $\langle \mu_{\alpha/F} \rangle \Rightarrow$ 극대 아이디얼. 그럼 체가 된다 ①

$f(\alpha) = 0$, $f \in \langle \mu_{\alpha/F} \rangle$

α 대입 $f = \mu_{\alpha/F} \cdot q + r$

$r = 0$ or $\deg r < \deg \mu_{\alpha/F}$ (μ보다 작은 ($\rightarrow\leftarrow$)) $= 0$

$f(\alpha) = \mu_{\alpha/F}(\alpha) \cdot q(\alpha) + r(\alpha)$ — 0, 0, 0!

$F[\alpha] \subset F(\alpha)$

F, α 포함 체 ⊃ 얘가 제일 작으니까

$x \in F[x] \Rightarrow \alpha \in F[\alpha]$

$\therefore F[\alpha] = F(\alpha)$

단 α가 대수적일 때.

정리 9.1.5 (단순확대의 기저)
F 상에서 대수적인 $\alpha \in E \supset F$에 대하여 $\deg \mu_{\alpha/F} = n$이라고 할 때,
(1) $\{1, \alpha, \cdots, \alpha^{n-1}\}$ 은 $F[\alpha]$의 F-기저이다.
(2) $|F[\alpha]:F| = n$.