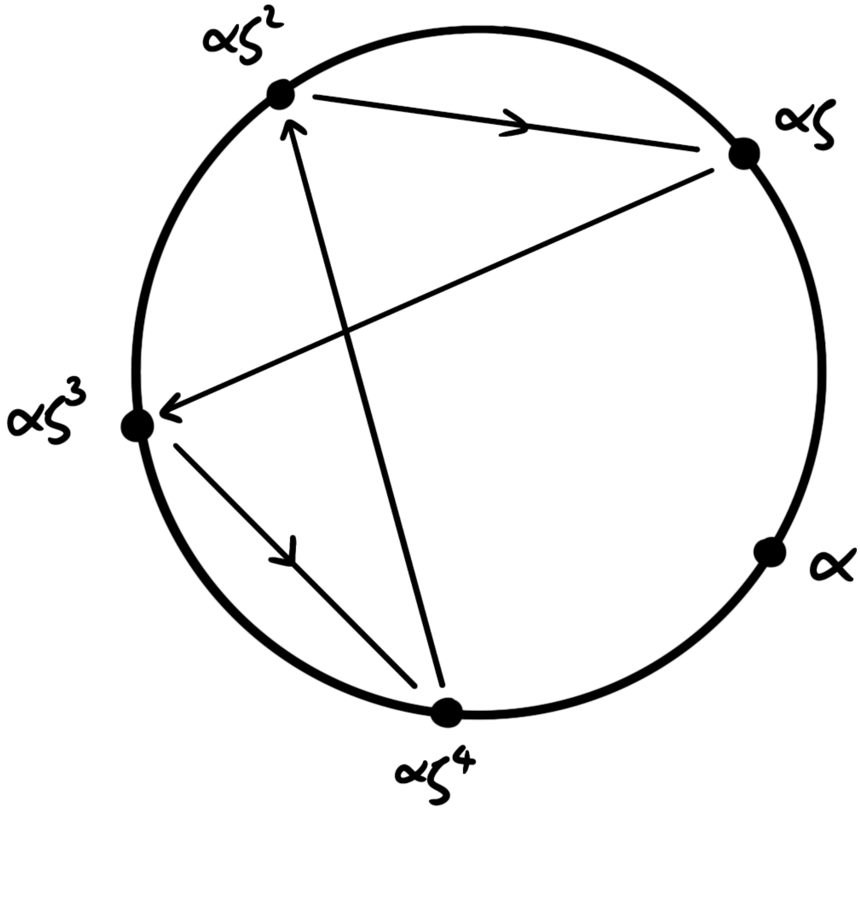
체론 복습노트

디멘(최정담)



1. 기초 개념

정의

환의 정의. R이 다음 세 조건을 만족할 때 환이라고 한다.

1. 덧셈에 대해 아벨군이다.
2. 곱셈에 대해 모노이드이다. (즉, 연산에 대해 닫혀 있고 결합법칙을 만족한다)
3. 분배법칙을 만족한다.

체의 정의. 환이 0을 제외한 곱셈에 대해 아벨군일 때 체라고 한다.

정의.

- $a \in R$에 대해 a가 곱셈에 대한 역원을 가질 때 **정원**$_{\textbf{unit}}$이라고 한다.
- $a \in R$에 대해 어떤 $b \in R$가 존재하여 $ab = 0$일 때 **영인자**$_{\textbf{divisor of zero}}$라고 한다.
- $a, b \in R$에 대해 어떤 정원 $u \in R$가 존재하여 $a = bu$일 때 a, b를 **동반원**$_{\textbf{associates}}$이라고 한다.
- $p \in R$에 대해 $p = ab \Rightarrow a = 1 \vee b = 1$일 때 p를 **기약원**$_{\textbf{irreducible}}$이라고 한다.

정역의 정의. 교환환 D의 0이 아닌 모든 원소들이 영인자가 아닐 때 D를 정역이라고 한다.

Note. D가 정역일 때, **소거법칙**이 성립함. 즉, $ab = ac \;\Rightarrow\; b = c$

Note. 환, 정역, 체는 각각 $M_n(\mathbb{R})$, $\mathbb{Z}$, $\mathbb{Q}$의 일반화임.

몫체의 정의. 정역 D에 형식적 나눗셈 구조를 추가하여 얻어진 체 $\mathrm{Frac}(D) = D/D^* \cong (D \times D^*)/\sim$을 몫체라고 한다. 여기서 $D^* = D \setminus \{0\}$이며 $a/b \sim c/d \;\Leftrightarrow\; ac = bd$이다.

정리. Frac(D)는 D를 포함하는 가장 작은 체이다. 즉, 체 F에 대해 포함 사상 $\iota: D \to F$가 존재한다면, 표준 사영 사상 $\pi: D \to \mathrm{Frac}(D)$에 대해 전사인 $\lambda: \mathrm{Frac}(D) \to F$가 유일하게 존재한다.

기초 정수론

정리. 다음이 성립한다.

1. 모든 체는 정역이다.
2. 모든 유한 정역은 체이다.

증명. 1은 자명. 2는 counting argument를 사용.

따름정리. $\mathbb{Z}_n$의 단원들로 이루어진 집합 $\mathbb{Z}_n^\times$는 곱셈에 대해 군을 이룬다.

오일러 정리. a와 n이 서로소일 때, $a^{\phi(n)} \equiv 1 \pmod n$

선형 모듈러 방정식의 풀이. $d = \gcd(a, n)$일 때, $ax \equiv b \pmod n$가 근을 가질 필요충분조건은 $d \mid b$인 것이며, 근의 개수는 d개이다.

정리. 체 F의 곱군 $F^\times$의 유한 부분군은 순환군이다.

증명 $G \leq F^\times$가 유한군이라고 하자. 유한생성 아벨군 정리에 의해 $G = \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_n^{k_n}\mathbb{Z}$ 이다. $r = \operatorname{lcm}(p_1^{k_1}, \ldots, p_n^{k_n})$이라고 하자. 방정식 $x^r = 1$은 $F[x]$에서 $|F^\times| = p_1^{k_1}, \ldots, p_n^{k_n}$개의 근을 가진다. 그런데 근의 개수는 r을 초과할 수 없으므로, $r = p_1^{k_1}, \ldots, p_n^{k_n}$이다. 따라서 $p_1, \ldots, p_n$은 서로 다른 소수이며, $G = \mathbb{Z}/r\mathbb{Z}$는 순환군이다.

아이디얼

아이디얼의 정의. I가 R의 덧셈에 대한 부분군이고, $\forall a \in R$ $aI, Ia \subset I$일 때 I를 R의 아이디얼이라고 한다.

Note. 정의에 의해 아이디얼은 R의 덧셈에 대한 부분군일 뿐 아니라 R의 부분환임.

Note. 준동형사상의 기본정리들은 정규부분군을 아이디얼로 바꿨을 때 동일하게 성립함.

환의 세계	**정수의 세계**
소 아이디얼: $ab \in I \Rightarrow (a \in I) \vee (b \in I)$	소수: $p \mid ab \Rightarrow (p \mid a) \vee (p \mid b)$
극대 아이디얼: $I \subset J \Rightarrow (J = I) \vee (J = R)$	기약원: $a \mid p \Rightarrow (a = 1) \vee (a = p)$

R이 정역일 때,

- p가 소수이다 ⇔ pR이 0이 아닌 소 아이디얼이다.
- c가 기약원이다 ⇔ cR이 $\{aR : a \in R \setminus R^\times, a \neq 0\}$ 중에서 극대이다.

따름정리. 정역에서 모든 소수는 기약원이다.

군의 세계	환의 세계
N이 G의 정규부분군일 때, G/N은 군이다.	I가 R의 아이디얼일 때, R/I는 환이다.
M이 G의 극대정규부분군일 때, G/M은 단순군이다.	M이 R의 극대 아이디얼일 때, R/M은 체이다.
n/a	M이 R의 소 아이디얼일 때, G/M은 정역이다.

따름정리.

1. 환에서 모든 극대 아이디얼은 소 아이디얼이다.
2. 유한환에서 모든 소 아이디얼은 극대 아이디얼이다.

2. 인수분해

ED ⇒ PID ⇒ UFD

ED의 정의. D가 정역이라고 하자. 다음을 만족하는 함수 $v: D \to \mathbb{Z}_{\geq 0}$ 가 존재할 때 D를 **유클리드 정역**이라고 한다. 또한, 아래를 만족하는 함수를 **유클리드 노름**이라고 한다.

1. $v(x) = 0 \Leftrightarrow x = 0$
2. 임의의 $a, b \in D$ $(b \neq 0)$에 대해 어떤 $q, r \in D$가 존재하여 $a = bq + r$이고 $v(b) > v(r)$이다.
3. 임의의 $a, b \in D$ $(b \neq 0)$에 대해 $v(a) \leq v(ab)$이다.

PID의 정의. 정역 D의 모든 아이디얼이 **주 아이디얼**임. 즉, $I \lhd D \Rightarrow I = \langle a \rangle$ for $a \in D$.

UFD의 정의. 정역 D가 다음 두 조건을 만족함.

1. 0과 정원이 아닌 D의 모든 원소는 기약원들의 유한곱으로 표현됨.
    - 주 아이디얼에 대해 ACC가 성립
2. $p_1 \dots p_r$과 $q_1 \dots q_s$가 같은 원소의 인수분해일 때, $r = s$이며 적절한 재배열 하에 p_i와 q_i는 동반원.
    - Prime ⇔ Irreducible

ED의 정원. D가 유클리드 정역일 때, $u \in D^\times \Leftrightarrow v(u) = v(1)$

ED ⇒ PID. D가 유클리드 정역이면 D는 PID이다.

증명. $I \lhd D$일 때, I의 0이 아닌 원소 중 가장 유클리드 노름이 작은 원소가 I를 생성한다.

PID satisfies ACC. PID의 모든 아이디얼 체인 $I_1 \subset I_2 \subset \dots$은 길이가 유한하다.

PID: Prime ⇔ Irreducible. PID의 소 아이디얼은 극대 아이디얼이다.

따름정리. PID ⇒ UFD

증명. ACC로부터 UFD의 1번 조건(분해의 유한성)이 충족되고, Prime ⇒ Irreducible로부터 UFD의 2번 조건(분해의 유일성)이 충족됨.

D: UFD ⇒ D[x]: UFD

정리. F가 체라면 F[x]는 ED이다.

증명. 나눗셈 알고리즘

따름정리. F[x]는 UFD이다.

정의. D가 UFD라고 하자.

1. $f(x) \in D[x]$에 대해, 계수의 최대공약수가 1인 f를 원시 다항식이라고 한다.
2. $f(x) \in D[x]$에 대해, 어떤 원시 다항식 $g(x) \in D[x]$가 존재하여 $f(x) = cg(x)$이다. 이 때, $c \in D$는 동반원에 한해 유일하며, f의 내용이라고 한다.

가우스 제1보조정리. D가 UFD라고 하자. $f, g \in D[x]$가 원시 다항식이라면 fg도 원시 다항식이다.

증명 어떤 기약원(= 소수) $c \in D$에 대해 $c \mid C(fg)$라고 가정하자. $\langle c \rangle$는 소 아이디얼이므로, $D/\langle c \rangle$는 정역이다. 표준적으로 정의된 사상 $\phi: D[x] \to (D/\langle c \rangle)[x]$를 생각하자. ϕ는 준동형 사상임을 쉽게 확인할 수 있으며, 이에 따라 $\phi(fg) = \phi(f)\phi(g)$이다. $c \mid C(fg)$이므로 $\phi(fg) = 0$이며, $D/\langle c \rangle$가 정역이므로, $\phi(f) = 0$ 또는 $\phi(g) = 0$이다. 이것은 f, g가 원시임에 모순되므로, $C(fg) = 1$이다.

가우스 제2보조정리. D가 UFD라고 하자. D*가 D의 몫체일 때, $f \in D[x]$에 대해 1과 2는 서로 필요충분조건이다.

1. f가 D[x]에서 기약이다.
2. f가 원시 다항식이고, f가 D*[x]에서 기약이다.

Remark) D*[x]는 D[x]보다 더 많은 정원을 가지므로, 기약원이 되기가 더 쉽다.

따름정리. D가 UFD라면 D[x]도 UFD이다.

증명 D의 몫체 D*에 대해 D*[x]는 ED이므로 UFD이다. 따라서 기약인 $f(x) \in D[x]$를 D*[x]의 원소로 생각하면 $f(x) = g_1(x) \dots g_n(x)$로 유일하게 소인수분해된다. 우변의 항이 유한하므로, 서로소 $n, m \in D$에 대해 $n f(x) = m h_1(x) \dots h_n(x)$ $(h_1, \dots h_n \in D[x])$ 이다. 양변에 C를 취하면 가우스 보조정리에 의해 $n = m C(h_1) \dots C(h_n)$이 되며, n, m이 서로소이므로 $C(h_1) = \dots = C(h_n) = 1$이다. 따라서 $n = m$이며 $f(x) = h_1(x) \dots h_n(x)$는 D[x]에서의 인수분해이다.

곱 노름

정의. 정역 D 위에서 정의된 곱 노름은 다음을 만족하는 함수 $N: D \to \mathbb{Z}$이다.

1. $N(x) = 0 \Leftrightarrow x = 0$
2. $N(ab) = N(a)N(b)$

정리. N이 D 위의 곱 노름일 때 다음이 성립한다.

1. u는 정원 $\Rightarrow$ $|N(u)| = 1$
2. 1의 역이 성립할 때, $|N(\pi)|$ = 소수 $\Rightarrow$ π는 기약원

<u>예시.</u> $\mathbb{Z}[i]$에서 $N(a + bi) = a^2 + b^2$은 곱 노름인 동시에 유클리드 노름임을 확인할 수 있음. 따라서 정리의 2번이 성립하여, $|N(\pi)|$가 소수일 때 π는 기약원임. 따라서 $5 = (1 + 2i)(1 - 2i)$이므로 5는 $\mathbb{Z}[i]$의 기약원이 아니지만, $N(1 \pm 2i) = 5$는 소수이므로 $1 \pm 2i$는 기약원이 맞음.

페르마 소수 정리. 소수 p가 $p = a^2 + b^2$ $(a, b \in \mathbb{Z})$로 표현될 필요충분조건은 $p \equiv 1 \pmod 4$인 것이다. 즉, 정수 소수가 가우스 정수 소수일 필요충분조건은 $p \equiv 1 \pmod 4$ 인 것이다.

증명. 필요조건은 자명. 충분조건임을 보인다.

$G = (\mathbb{Z}/p\mathbb{Z})^\times$라고 하자. $|G| = p - 1$이므로, $|G|$는 4로 나누어떨어진다. $|G|$가 짝수이므로 제곱했을 때 1이 되는, 1이 아닌 원소 -1이 G에 존재한다. 또한 $|G| / 2$가 짝수이므로 제곱했을 때 -1이 되는, -1이 아닌 원소 n이 존재한다. 따라서 $n^2 \equiv -1 \pmod p$이며, $p \mid n^2 + 1$이다.

이제 p를 $\mathbb{Z}[i]$의 원소로 보자. $p \mid (n + i)(n - i)$이다. 만약 p가 $\mathbb{Z}[i]$의 기약원(= 소수)라면, $p \mid n + i$ 또는 $p \mid n - i$인데 이는 불가능하다. 따라서 p는 기약원이 아니며, 이에 따라 $p = zw$ $(z, w \in \mathbb{Z}[i])$이다. 복소수의 상등에 의해 $w = \text{conj}(z)$이며, $p = a^2 + b^2$이다. ∎

3. 환론

뇌터 환

정리. 환 R에 대해, 다음은 동치이다.

1. R의 아이디얼이 모두 유한 생성된다.
2. $I_1 \subset I_2 \subset I_3 \subset \ldots$이 아이디얼의 체인일 때, $\cup I_k = I_n$인 자연수 n이 존재한다. (Ascending Chain Condition)
3. $\mathcal{S}$가 아이디얼의 집합일 때, $\mathcal{S}$는 극대(maximal) 아이디얼을 가진다.

증명. 초른 정리를 사용.

정의. 위 조건을 만족하는 환을 뇌터 환이라고 한다.

Remark) **PID ⇒ Not**

힐베르트 기저 정리. R이 뇌터 환이라면 R[x]도 뇌터 환이다.

증명. $I \lhd R[x]$가 유한하게 생성되지 않는 아이디얼이라고 하자. 선택 공리에 의해 다항식열 $(f_1, f_2, \ldots)$이 존재하여 f_{i+1}은 $I \setminus \langle f_1, \ldots, f_i \rangle$ 중 가장 차수가 작은 다항식이다. a_i가 f_i의 최고차항이라고 하자. R이 뇌터환이므로 충분히 큰 n에 대해 $\langle a_1, a_2, \ldots \rangle = \langle a_1, a_2, \ldots, a_n \rangle$이다. 그런데 이때 $\langle f_1, f_2, \ldots, f_n \rangle$의 원소로 f_{n+1}의 최고차항을 소거할 수 있어 모순이다.

4. 체의 확장

체의 확장

정리. $F \le E \le L$일 때, $[L : E][E : F] = [L : F]$이다.

정의. $F \le E$가 확장체라고 하자. 체 E의 부분집합 S에 대해,

- S에 의해 **생성된 체** $F(S)$는 F와 S를 포함하는 E의 가장 작은 부분체이다.
- S에 의해 **생성된 환** $F[S]$는 F와 S를 포함하는 E의 가장 작은 부분환이다.

정리. $S = \{\alpha_1, \dots, \alpha_n\}$이라고 하자.

$$F(S) = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} : f, g \in F[x_1, \dots, x_n], g \neq 0 \right\}$$

$$F[S] = \left\{ f(\alpha_1, \dots, \alpha_n) : f \in F[x_1, \dots, x_n] \right\}$$

정의. $F \le E$가 확장체라고 하자. $\alpha \in E$가 F에서 **대수적**이라는 것은, $f(\alpha) = 0$인 $f(x) \in F[x]$가 존재한다는 것이다.

크로네커 정리

대수적 수의 기본정리. $F \le E$가 확장체라고 하자. $\alpha \in E$가 F에서 대수적이라면, α를 근으로 가지면서 기약인 다항식 $p(x) \in F[x]$가 유일하게 존재한다.

따름정리. $p(x)$를 α의 **최소다항식**이라고 한다.

크로네커 정리. F가 체라고 하자. 기약다항식 $p(x) \in F[x]$에 대해, $F[x]/\langle p \rangle$를 표준적인 방식으로 F의 확장체로 생각할 수 있다. 이때, 다음이 성립한다.

1. $x + \langle p \rangle$는 $p(x)$의 근이다.
2. $F \le E$가 확장체이고 $\alpha \in E$가 $p(x)$를 최소다항식으로 가질 때, $F[\alpha] = F(\alpha) \cong F[x]/\langle p \rangle$이다.

대수적 폐포

대수적 수의 기본정리. $F \leq E$

5. 유한체

유한체

정리. F가 유한체라면 char F는 소수이다.

증명 분배공리와 소거법칙으로부터 따라 나온다.

정리. F가 유한체이고 $F \le E$가 유한 확장일 때, $|E| = |F|^{[E : F]}$ 이다.

따름정리. F가 유한체이면 $|F| = p^n$ (p는 소수)이다.

유한체의 분류. 임의의 소수 p와 자연수 n에 대해,

1. $\mathbb{Z}_p$의 대수적 폐포에서 $x^{p^n} = x$는 p^n개의 서로 다른 근을 가지며, 이들은 크기가 p^n인 체를 이룬다.
2. 크기가 p^n인 체는 1의 체와 동형이다.

증명

1. $x^{p^n} = x$가 중근을 가지지 않음을 보이기: 다음의 보조정리로부터 따라 나온다.
    1. **보조정리.** gcd(f, f') = 1이라면 f는 중근을 가지지 않는다.
2. $x^{p^n} = x$의 근들이 체를 이룸을 보이기: 이항정리로부터 따라 나온다. (cf. Freshman exponentiation)

정리. char F = p인 체 F에 대해, $\sigma: x \mapsto x^p$는 자기동형사상이다. σ를 **프로베니우스 사상**이라고 부른다.

6. 체의 자기동형사상

켤레

정의. $F \leq E$가 확장체라고 하자. $\alpha, \beta \in E$에 대해 α와 β의 최소다항식이 같을 때, 둘을 **켤레**라고 한다.

켤레동형사상 정리. $\alpha, \beta \in E$가 켤레일 때, $\psi: F(\alpha) \to F(\beta)$, $\alpha \mapsto \beta$인 동형사상이 존재한다.

갈루아 군

정의. $F \leq E$가 확장체라고 하자. 자기동형사상 $\sigma: E \to E$에 대해, $\sigma|_F = id_F$ 일 때 $\sigma \in Gal(E/F)$이다. $Gal(E/F)$는 합성 연산 하에서 군을 이루며, 이 군을 **갈루아 군**이라고 한다.

예시. $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$에 대해 $\sigma: \sqrt{2} \mapsto -\sqrt{2}$, $\tau: \sqrt{3} \mapsto -\sqrt{3}$은 $Gal(E/F)$의 원소이다.

정의. S가 $Aut(E)$의 부분집합이라고 하자. S에 의해 **고정된 체** E_S를 $\{ x \in E \mid \forall\sigma \in E : \sigma(x) = x \}$와 같이 정의한다. E_S는 자연스러운 방식으로 체를 이룬다.

Remark.

1. $F \leq E_{Gal(E/F)}$
2. F가 char $F = p$인 유한체일 때, 프로베니우스 사상 σ에 대해 $F_{<\sigma>} = \mathbb{Z}_p$이다.

7. 분해체

정의

PID의 정의. 정역 D의 모든 아이

8. 갈루아 이론

정의

PID의 정의. 정역 D의 모든 아이

9. 오차방정식의 비가해성

정의

PID의 정의. 정역 D의 모든 아이