Pierre de Fermat의 출생 연도

version 201213

문구 추가 201213

[II]의 표지에 등장하는 Pierre de Fermat의 출생 연도가 최근 1607년으로 수정되었다.

예전에 1601년이라고 했던 것은 Pierre의 이복형 Piere('r' 한 개)와 혼동했기 때문이라고 한다.[1]

따라서 Pierre de Fermat(1607–1665)는 57세에 사망하였으니, 그 당시의 기준으로도 장수했다고는 할 수 없을 것이다. 또 Blaise Pascal(1623–1662)과의 나이 차이도 줄어들었다.

[1] https://www.maa.org/press/periodicals/convergence/when-was-pierre-de-fermat-born 참조.

제 3 장 : Substructure

현재 제 3 장의 제목은 "Subobject" 이다. 그러나, 엄격하게 말하면, 이는 정확한 표현이 아니다.[2]

따라서 제 3 장의 제목을 "Substructure" 로 수정하는 것이 좋아 보인다. 한편, 제 4 장의 제목 "Quotient Object" 는 OK. ("Quotient Structure" 라고 해도 괜찮겠지만, 무언가 어색하게 느껴진다.)

[2] Category Theory 에서 subobject 는 homomorphism 의 kernel 이 될 수 있는 것들을 의미한다.

명제 5.3.5 의 증명

version 201112

명제 5.3.5. Maximal ideal 은 항상 prime ideal 이다.

명제 5.3.5 의 증명에서 "본능적으로 귀류법을 생각한다"라고 한 부분이 명확하지 않다.

우리는 물론 $ab \in \mathfrak{m}$ 이면 $a \in \mathfrak{m}$ 또는 $b \in \mathfrak{m}$ 임을 보여야 한다. 이 증명 '방법'은 다음 세 가지로 나누어 생각할 수 있을 것이다.

증명 방법 1 : $a \notin \mathfrak{m}$ 이고 $b \notin \mathfrak{m}$ 이라고 가정하자. 그러면, $a \notin \mathfrak{m}$ 이므로, 이러저러하여……, $b \in \mathfrak{m}$ 이 된다. 따라서 **모순**. □

증명 방법 2 : 두 가지 경우로 나누어 생각한다. 우선, 만약 $a \notin \mathfrak{m}$ 이라면, 이러저러하여……, $b \in \mathfrak{m}$ 이므로, 증명 끝. 다음, 만약 $b \notin \mathfrak{m}$ 이라면, 마찬가지로 $a \in \mathfrak{m}$ 이 된다. 증명 끝. □

증명 방법 3 : 두 가지 경우로 나누어 생각한다. 우선, 만약 $a \in \mathfrak{m}$ 이라면 더 증명할 것이 없다. 다음, 만약 $a \notin \mathfrak{m}$ 이라면, 이러저러하여……, $b \in \mathfrak{m}$ 이 된다. 증명 끝. □

물론 위 세 가지 증명 '방법'은 본질적으로 같은 내용이다. 이때 [증명 방법 1] 은 분명히 귀류법이라고 할 수 있을 것이다. 그렇지만, [증명 방법 2]와 [증명 방법 3]은 귀류법이라고 부르기가 망설여진다.

근본적인 문제는, 무엇보다도, 귀류법(Proof by Contradiction)의 명확한 정의가 불분명하다는 것인 듯하다……. (다시 생각해 보니, "귀류법" 부분은 삭제하고, 위의 [증명 방법 2]를 선택하는 것이 더 좋았을 것 같다.)

§5.4 : UFD 의 성질 추가

UFD 에서는, 물론, 정리 5.3.11 이 성립하지 않는다. 이를 분명히 하면, 다음과 같다.

즉, D 가 UFD 일 때, $0 \neq p \in D$ 라고 하면,

$$\begin{array}{ccc} p\text{는 prime element} & \Leftrightarrow & \text{p는 irreducible element} \\ \Updownarrow & & \not\Downarrow \ \Uparrow \\ (p)\text{는 prime ideal} & \begin{array}{c}\not\Rightarrow \\ \Leftarrow\end{array} & (p)\text{는 maximal ideal} \end{array}$$

이 된다. (이때 $\not\Rightarrow$, $\not\Downarrow$ 는 물론 일반적으로는 성립하지 않는다는 뜻이다. 반례는 $D = \mathbb{Z}[t]$ 인 경우. 보기 5.3.13 참조.)

참고 : 예를 들어, Eisenstein Criterion (명제 5.7.2) 에서 p 를 irreducible element 라고 하지 않고 prime element 라고 한 이유를 독자들은 짐작할 수 있을 것이다. (뭐 그리 심각한 얘기는 아니다……, 저자는 단지 "UFD 에서는 irreducible element 는 prime element 이다"라는 문장을 추가로 타자 치기 싫었을 뿐이다.)

정리 5.5.1. PID 는 UFD 이다.

이 명제와 그의 증명을 공부한 후, 적지 않은 독자들이 오해하는 사실이 하나 있어 분명히 언급해 둔다.

의외로 많은 독자들이 *"정수(또는 자연수)와 다항식의 소인수분해조차도 완전히 이해하기 위해서는 [PID 이면 UFD]라는 명제와 그 증명(maximal ideal, ACC, MC 등의 ideal language)이 필수적"*이라는 오해를 하는 것 같다.

그러나, 우리는 Euclidean Domain 에서 소인수분해의 존재성을 **수학적 귀납법**으로 — ideal language 없이 — 증명할 수 있다. 대부분의 대수학 교재에는 이 귀납법 증명에 관한 언급이 없는데, 그 이유는 대수학 교재들이 "가장 일반적인 명제(지금 경우에는 [PID 이면 UFD]라는 명제)를 (하나만) 증명한다"는 원칙을 따르기 때문이다.

참고: 이 홈페이지에 있는 article "Euclidean Domain"을 참고하기 바란다. 이 article 에서는 [Euclidean Domain 이면 UFD]라는 명제를 ideal language 와 Noetherian property 없이 증명하고 있다.

version

201213

수정 : Multiple root 의 정의

현재 정의 6.4.12 의 multiple root 와 multiplicity 의 정의는 주어진 다항식의 splitting field 의 선택에 depend 하는 것 같아 불안하게 느껴진다. 게다가, 아직 splitting field 의 (up to F-isomorphism) uniqueness 를 모르는 상황이므로, 수정이 필요해 보인다.

수정 : 정의 6.4.12. $f(t) \in F[t]$ 일 때, $f(\alpha) = 0$ 이라고 하자 (단, $\deg(f) \geq 1$). (Kronecker's Theorem 을 생각하면, α 가 살고 있는 곳은 F 의 어떤 extension field 일 것이다.) 그런데 인수정리(보기 1.7.15) 에 의해, $(t-\alpha) \mid f(t)$ in $F(\alpha)[t]$. 한편 $F(\alpha)[t]$ 는 UFD 이므로,

$$f(t) = (t-\alpha)^m g(t), \qquad g(\alpha) \neq 0$$

인 $g(t) \in F(\alpha)[t]$ 와 자연수 m 이 유일하게 존재할 것이다. 이때, 자연수 m 을 α 의 **multiplicity** 라고 부르고,[3] 만약 $m \geq 2$ 이면, α 를 [**multiple root** with multiplicity m] 이라고 부른다.

그러나, 사실 현재의 정의도 별문제는 없다. 왜냐하면, 이제 위 새로운 정의로부터 다음 관찰은 거의 자명하기 때문이다.

관찰 6.4.12 a $f(t) \in F[t]$ 라고 하자 (단, $\deg(f) \geq 1$). 이때 K 를 [splitting field of $f(t)$ over F] 라고 하면,

$$f(t) = a(t-\alpha_1)^{n_1}(t-\alpha_2)^{n_2}\cdots(t-\alpha_k)^{n_k}$$

로 쓸 수 있다 (단, $a \in F^\times$, $\alpha_i \in K$ 는 mutually distinct). 이때 n_i 는 α_i 의 multiplicity 이다.

증명 : 잉크를 아끼자. 거의 자명하므로 독자들에게 맡긴다. □

[3] 예전 정의에 따르면 1은 multiplicity 라고 부를 수 없었지만, 이제부터는 1도 multiplicity 가 될 수 있다.

보충 : 따름명제 6.5.17 의 증명

version 201213

명제 6.5.18. K 와 L 이 non-constant polynomial $f(t) \in F[t]$ 의 splitting field 이면, F-isomorphism $\tau : K \to L$ 이 존재.

노파심에서 증명에 한 줄을 추가한다.

증명은 — $n = \deg(f)$ 로 놓을 때 — F-isomorphism 을 $K = F(\alpha_1, \ldots, \alpha_n)$ 까지 확장하면 끝난다. 이때 $L = F(\beta_1, \ldots, \beta_n)$ 이다. (물론, 예를 들어, $\alpha_1 = \alpha_2$ 일 수 있고 $\alpha_2 \in F(\alpha_1)$ 일 수도 있다.)

version

201213

수정 : 명제 6.5.18

이 문서에서 multiple root의 정의를 약간 수정했으므로, 명제 6.5.18도 수정하는 것이 부드러워 보인다. (뭐, 현재의 statement도 잘못된 것은 없지만.)

수정 : 명제 6.5.18. $p(t) \in F[t]$가 irreducible polynomial이면, $p(t)$의 모든 root들의 multiplicity는 같다. 즉, K/F와 L/F가 field extension이고, $\alpha \in K$와 $\beta \in L$이 $p(t)$의 root이면, α와 β의 multiplicity는 같다.

즉, 이 명제에서는 splitting field를 생각할 필요가 없다는 뜻이다. 다시 말해, 이 명제는 Isomorphism Extension Theorem(명제 6.5.14)보다 앞에 등장할 수 있을 것이다.

따라서, 증명에도 약간의 보충 설명이 필요할 것이다.

증명 : 당연히, F-isomorphism $\psi_\beta^\alpha : F(\alpha) \to F(\beta)$를 생각한다. 그리고, ψ_β^α는 ring isomorphism $\psi_\beta^\alpha : F(\alpha)[t] \to F(\beta)[t]$를 induce한다. 물론

$$p(t) = (t-\alpha)^m g(t), \qquad g(\alpha) \neq 0$$

로 놓으면(단, $g(t) \in F(\alpha)[t]$), 자연수 m이 α의 multiplicity이다. 이제 간단히 $\psi_\beta^\alpha = \sigma$로 표기하면,

$$p^\sigma(t) = p(t), \qquad \big((t-\alpha)^m\big)^\sigma = (t-\beta)^m$$

이므로(표기법 6.5.13 참조),

$$p(t) = p^\sigma(t) = (t-\beta)^m g^\sigma(t)$$

가 된다. 이때

$$g^\sigma(\beta) = \sigma\big(g(\alpha)\big) \neq 0$$

이므로(왜 그런가?), β의 multiplicity도 m이다. 증명 끝. □

명제 13.4.9 의 더 간단한 증명

명제 13.4.9. $|G| = 15$ 이면, G 는 cyclic.

증명 : G 의 원소의 order 는 1, 3, 5 또는 15 이다. 그런데 — 373 쪽의 증명에서처럼 — Sylow 3-subgroup 과 Sylow 5-subgroup 은 각각 한 개뿐이다. 따라서 G 에는 order 가 3 인 원소가 2 개 있고, order 가 5 인 원소가 4 개 있다. 그러므로 G 에는 order 가 15 인 원소가 8 개 있을 것이다. 즉, G 는 cyclic. □

참고 : $\phi(15) = 8$ 이므로, additive cyclic group $\mathbb{Z}_{15}$ 에는 generator 가 8 개 있다.

보기 16.2.15 : $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\sqrt[3]{3})$

보기 16.2.15 의 설명에는 gap 이 있다. 정말로 $\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\sqrt[3]{3})$ 인지 보여야 한다! (이는 보기 6.2.20 에서 "m, n 이 서로 소가 아닌 경우에는 매우 어려우므로, 시간낭비하지 말 것"이라고 단언했던 문제 중 가장 간단한 것이라고 할 수 있다.)

이 문제는 꿈속에서조차 한번도 생각해 보지 않았던 것이었다. 한번도 의심하지 않았던 자명한 사실이었다고 하는 편이 더 정확한 표현일 것이다. 수강생(들)이 "$\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\sqrt[3]{3})$ 임을 '무식한 방법'을 사용하지 않고 설명할 수 있는가?"라고 질문했을 때 깜짝 놀랐다.[4]

이제 $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{3})$ 이라고 가정해 보자. 그러면, $\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ 인 유리수 a, b, c 가 존재할 것이다.[5] (질문을 받자마자 "norm map 을 이용하면 될 것 같다"라고 큰소리 쳤지만, 잘 되지 않았다. 오히려 연습문제 16.4.11 에서조차 괄시받은 trace map 이 큰 힘을 발휘한 것은 약간 의외였다.[6])

연습문제 16.4.11 에 추가: $x, y, z \in \mathbb{Q}$ 일 때,

$$\mathrm{tr}_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(x + y\sqrt[3]{2} + z\sqrt[3]{4}) = 3x = \mathrm{tr}_{\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}}(x + y\sqrt[3]{3} + z\sqrt[3]{9})$$

임을 보여라.

그런데, 우리는 $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{3})$ 이라고 가정하고 있으므로,

$$0 = \mathrm{tr}_{\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}}(\sqrt[3]{3}) = \mathrm{tr}_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = 3a$$

가 된다. 즉, $a = 0$. 이제 등식 $\sqrt[3]{3} = b\sqrt[3]{2} + c\sqrt[3]{4}$ 의 양변을 세제곱하는 것은 일도 아니다. 독자들에게 맡긴다.

---

[4] 질문을 이해하는 데 한참 걸렸을 정도였다. 이 질문을 던진 2018 년 2 학기 수강생(들)에게 박수를 보낸다.

[5] 이때 '무식한 방법'이란, 물론, 이 등식의 양변을 세제곱하는 방법이겠지만, 엄두가 나지 않아 시도해 보지도 않았다.

[6] Norm map 과 trace map 은 정의 16.4.7 참조.