주의 및 추가

수정 1. 연습문제 1.4.16 (가) 항의 statement 는 true 가 아님. 예를 들어,

$$1 = (2t+1)^2 \in \mathbb{Z}_4[t].$$

주의 2. 연습문제 1.4.17 은 연습문제 2.1.15 를 모르는 상태에서 풀라는 뜻.

추가 3. 질문 4.3.9 를 다음 연습문제로 대체. (이 연습문제는 PID 위에서도 유효. 정리 5.3.11 참조.)

연습문제 4.3.9. $p \in \mathbb{Z}$ 가 irreducible number 일 때, p 가 prime number 임을 보이기 위해, $pc = ab$ 라고 하자 (단, $a, b, c \in \mathbb{Z}$). 이때, 다음을 보여라.

(가) $(p, a) = 1$ 이면, $p \,|\, b$.

(나) $(p, a) \neq 1$ 이면, $p \,|\, a$.

추가 4. p. 161 에 다음 연습문제 추가.

연습문제 5.3.23. Finite characteristic 을 갖는 infinite field 를 찾아라.

추가 5. 보기 6.2.21 (나) 항의 설명에 gap 이 있음. 즉, 3 이하 6 의 약수는 1 또는 2 또는 3. 그런데, 만약 $[\,\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha+\beta)\,] = 2$ 라면, $\operatorname{irr}\big(\alpha, \mathbb{Q}(\alpha+\beta)\big)$ divides $(t^3 - 2)$ in $\mathbb{Q}(\alpha+\beta)[t]$. 한편 $\mathbb{C}[t]$ 는 UFD 이고, (t^3-2) 는 $\mathbb{C}[t]$ 에서

$$t^3 - 2 = (t-\alpha)(t-\alpha\zeta)(t-\alpha\zeta^2), \qquad (\text{단, } \zeta^3 = 1,\ \zeta \neq 1)$$

로 소인수분해되므로,

$$\operatorname{irr}\big(\alpha, \mathbb{Q}(\alpha+\beta)\big) = (t-\alpha)(t-\alpha\zeta) \quad \text{또는} \quad (t-\alpha)(t-\alpha\zeta^2)$$

이어야 한다. 그러나 이 두 후보는 모두 실계수 다항식이 아니므로, $\mathbb{Q}(\alpha+\beta)[t]$ 의 원소가 될 수 없다. 모순. (연습문제 6.2.22 는 삭제.)

추가 6. 질문 6.2.24 앞에 다음 연습문제 추가. 이 연습문제는 명제 16.1.11 의 증명에 필요.

연습문제 $F \leq E, K \leq L$ 일 때, 다음을 보여라.

(가) E/F 가 finite extension 이면, EK/K 도 finite extension.

(나) E/F, K/F 가 모두 finite extension 이면, EK/K 도 finite extension.

수정 및 추가 7. 쑥스러운 얘기지만, 질문 6.2.25 의 답은 간단하다. [**증명**: $\sqrt{2} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$ 라고 가정하자. Tower $\mathbb{Q} < \mathbb{Q}(\sqrt{3}) < \mathbb{Q}(\sqrt{3}, \sqrt{5})$ 를 생각하면, $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})] = 2$ 이므로,

$$\sqrt{2} = a\sqrt{5} + b, \qquad (a, b \in \mathbb{Q}(\sqrt{3}))$$

꼴로 쓰여질 것이다. 양변 제곱하면,

$$2 = 5a^2 + b^2 + 2ab\sqrt{5}$$

이므로, 만약 $ab \neq 0$ 이라면 $\sqrt{5} \in \mathbb{Q}(\sqrt{3})$ 이므로 모순. 따라서 $ab = 0$ 이고, $a = 0$ 이면 $\cdots\cdots$, $b = 0$ 이면 $\cdots\cdots$.] (나) 항도 비슷. **보기 16.2.13 부터의 감동을 위해** 질문 6.2.25 는 다음 새 질문으로 대체.

새 질문 6.2.25 $d, m, n \in \mathbb{Z}$ 이고, $\zeta_n = \exp(2\pi\mathbf{i}/n)$ 일 때,
(가) $\sqrt{d} \in \mathbb{Q}(\zeta_5)$ 일 필요충분조건은? $\zeta_3 \notin \mathbb{Q}(\zeta_5)$?
(나) $\zeta_m \in \mathbb{Q}(\zeta_n)$ 일 필요충분조건은?

독자들은 **§ 16.2 (와 § 16.5) 를 공부한 후** 이 질문을 답해 보기 바란다.

추가 8. 연습문제 14.2.4 뒤에 다음 연습문제 추가. 이 연습문제는 연습문제 15.1.18 에 필요.

연습문제 $F \leq E, K \leq L$ 일 때, 다음을 보여라.
(가) E/F 가 algebraic extension 이면, EK/K 도 algebraic extension.
(나) E/F, K/F 가 algebraic extension 이면, EK/K 도 algebraic extension.

수정 9. 400–401 쪽의 순서를 다음과 같이 변경.

$$15.1.13 \longrightarrow 15.1.15 \longrightarrow 15.1.17 \longrightarrow 15.1.14 \longrightarrow 15.1.16$$

수정 10. 418 쪽 [Galois's Theorem (나) 항의 증명 (ii)] 는 귀류법을 사용하지 않는 것이 더 좋아 보인다. 즉, E/F 가 normal extension 임을 보이기 위해, $\sigma : E \to \overline{F}$ 를 임의의 F-embedding 이라고 하자. 이제 σ 를 K 로 확장하면, $\sigma \in \mathrm{Gal}(K/F)$ 인 것은 이제 익숙하다. 그런데 $\mathrm{Gal}(K/E)$ 는 $\mathrm{Gal}(K/F)$ 의 normal subgroup 이므로, 관찰 16.1.9 에 의해

$$\mathrm{Gal}(K/E) = \sigma \cdot \mathrm{Gal}(K/E) \cdot \sigma^{-1} = \mathrm{Gal}(K/\sigma E)$$

가 된다. 따라서, Galois's Theorem 의 (가) 항에 의해, $\sigma E = E$. 증명 끝.

version

201213

정오표

표지 ; Fermat (1601–1665) $\longrightarrow$ Fermat (1607–1665).

p. 5, 정의 1.1.10 ; R 의 곱셈과 M 의 덧셈도 서로 '다툴' 기회가 없다.

p. 50, 1 행 ; 이용하여) $\longrightarrow$ 이용하여, $1_{\mathcal{A}} \in \mathcal{A}$ 일 때).

p. 50, 9 행과 11 행 ; α 와 β 로 묘사하라 $\longrightarrow$ α 와 β 로 묘사하라 (단, $\varphi(1) = 1$).

p. 56, 15 행 ; [I, 연습문제 11.9.12] $\longrightarrow$ [I, 연습문제 11.9.11].

p. 57, 밑 4 행 ; linear $\longrightarrow$ F-linear.

p. 69, 명제 2.3.17 ; commutative ring $\longrightarrow$ commutative ring with 1.

p. 86, 밑 2 행 ; $S \longrightarrow \mathfrak{B}$.

p. 88, 연습문제 3.2.11 (가) ; $1_R = 1_S$ 로 가정.

p. 88, 연습문제 3.2.11 (나) ; $\varphi(1) = 1$ 로 가정.

p. 94, 註 ; submodle $\longrightarrow$ submodule.

p. 110, 註 ; Conuter $\longrightarrow$ Counter.

p. 113, 삼각형 그림 ; $X/Y \longrightarrow X/\ker\varphi$.

p. 118, 연습문제 4.3.4 ; $1 \leq k \in \mathbb{Z} \longrightarrow 1 < k \in \mathbb{Z}$.

p. 119, 2 행 ; 연습문제 1.3.9 (다) 항 $\longrightarrow$ 연습문제 1.3.10.

p. 122, 연습문제 4.3.19 ; $a, b \in \mathbb{Z}$, $b \neq 0$, $b \nmid a$ 일 때, $x = a^{\phi(b)-1}$, $y = \big(1 - a^{\phi(b)}\big)/b$ 는 방정식 $ax + by = 1$ 의 해가 됨을 보여라.

p. 125, 밑 4 행 ; $x - x'$ 는 □□ 가 group 일 때는 ${x'}^{-1}x$ 로 이해.

p. 128, 마지막 註 ; *말한디* $\longrightarrow$ *말한다*.

p. 132, 밑 1 행 ; convese $\longrightarrow$ converse.

p. 133, 연습문제 4.5.9 ; commutative ring $\longrightarrow$ commutative ring with 1.

p. 139, 1 행 ; 결코 한두 줄로 답할 수 없다 $\longrightarrow$ 한두 줄이면 충분하다. (아래 註 76 번은 삭제.)

p. 150, 4 행은 D 가 PID 일 때 성립.

p. 152, 10 행 ; [I, 정의 8,5,9] $\longrightarrow$ [I, 연습문제 8.5.10].

p. 153, Algebraic Proof ; 문자 r 이 두번 사용되었음.

p. 153, 밑 7 행 ; $|r-m| < 1/2$, $|s-n| < 1/2 \longrightarrow |r-m| \leq 1/2$, $|s-n| \leq 1/2$.

p. 157, 밑 2 행 ; $R \longrightarrow D$.

p. 159, 밑 2 행 ; 0 과 R 뿐 $\longrightarrow$ 0 과 $R/\mathfrak{m}$ 뿐.

p. 165, 밑 4 행 ; prime number $\longrightarrow$ positive prime number.

p. 167 의 모든 ideal 은 **left** ideal. 12 행의 (two-sided) 삭제.

p. 171, 14 행 ; $i > n$, $j > m$ 이면 $a_i = 0 = b_j$ 로 이해한다.

p. 193, 1 행 ; $\alpha \in F \longrightarrow \alpha \in E$.

p. 207, 연습문제 6.3.4 ; $0 < \alpha \in \mathbb{R}$.

p. 214, 따름정리 6.4.9 ; 편의상 $f(t)$ 가 monic 인 경우만 다루었다.

p. 215, 정의 6.4.12 ; "참고 및 추가" 참조. 추가-201213

p. 221, 11 행 ; $\widetilde{\sigma}|_F = \sigma \longrightarrow \widetilde{\sigma}|_E = \sigma$.

p. 223, 명제 6.5.18 ; "참고 및 추가" 참조. 추가-201213

p. 225, 따름명제 6.6.6 의 증명 ; $p(t)$ 가 monic 이라고 해도 괜찮다.

p. 231, 11 행 ; 'inseparable' polynomial $\longrightarrow$ 'inseparable' irreducible polynomial.

p. 232, 연습문제 7.2.8 (가) ; p 는 odd prime.

p. 247, 1 행 ; Pubic $\longrightarrow$ Public.

p. 285, 연습문제 9.3.2 (1) ; $M = \oplus_{i=1}^n N_i \longrightarrow M = \oplus_{i \in I} N_i$.

p. 286, 3 행 ; $x \in X \longrightarrow x \in N$.

p. 286, 밑 7 행 ; $M = \oplus_{i=1}^n N_i \longrightarrow M = \oplus_{i \in I} N_i$.

p. 309, 밑 5 행 ; § 4.5 에서 $\longrightarrow$ § 3.5 에서.

p. 326, 밑 7 행 ; § 5.4 $\longrightarrow$ § 5.5.

p. 332, 1 행 ; $M < N \longrightarrow M > N$.

p. 362, 註 ; $G \approx \mathbb{Z}_p$ or $\longrightarrow G \approx \mathbb{Z}_{p^2}$ or.

p. 364, 15 행 ; $\mathfrak{M}_{r,n-r}(F) \longrightarrow \mathfrak{M}_{r,n-r}(\mathbb{F}_q)$.

p. 365, 11 행 ; $\mathfrak{M}_{r,n-r}(F) \longrightarrow \mathfrak{M}_{r,n-r}(\mathbb{F}_q)$.

p. 393, 7 행 ; 로 놓는다 $\longrightarrow$ 로 놓는다(이때 $\mathfrak{X} \neq \emptyset$ 임은 자명).

p. 412, 註 (39 번) ; $K \longrightarrow E$ (두 곳).

p. 422, 밑 1 행 ; $\beta = -\alpha - b \longrightarrow \beta = -\alpha - a$.

p. 429, 밑 3 행 ; elementary symmetric polynomial $\longrightarrow$ elementary symmetric polynomial (in $x_1, \ldots, x_n$).

p. 437, 註 ; $K/F \longrightarrow E/F$.

p. 441, 3 행 ; $(\mathbb{F}_{q^m/q})^H \longrightarrow (\mathbb{F}_{q^m})^H$.

p. 446, 15 행 ; $\Phi_n(t) = \mathrm{irr}\left(\mathbb{Q}(\zeta)\right) \longrightarrow \Phi_n(t) = \mathrm{irr}\,(\zeta, \mathbb{Q})$.

p. 448, 밑 3 행 ; $=, \approx, \approx \longrightarrow \approx, =, \approx$.

p. 462, 14 행 ; $y_3 = x_1x_3 + x_2x_4 \longrightarrow y_3 = x_1x_4 + x_2x_3$.

p. 463, 5 행 ; $z^2 - y_1t + s_4 \longrightarrow z^2 - y_1z + s_4$.