代数学 2 環と体とガロア理論 初版
雪江 明彦 著
解答集

半沢鏡

前書き

第 3 章の問題のみ解答がそろっています。他の章についても現在製作中です。誤植・訂正・要望がある場合はグーグルフォーム https://forms.gle/mwtHVys6k6DpjkCA9 で連絡してください。各問題に [解答] と書いてますが、教科書の文言そのままの場合は [解答*] と書くことにしています。

目次

第 1 章

1.1.1（群環での計算）

$G=\mathfrak{S}_3,\quad \sigma_1=1,\quad \sigma_2=(12),\quad \sigma_3=(13),\quad \sigma_4=(23),\quad \sigma_5=(123),\quad \sigma_6=(132)$ とする.$g=1-2\sigma_2+3\sigma_5,\quad h=3\sigma_6-2\sigma_4+\sigma_2\in\mathbb{Z}[G]$ に対し，gh を計算せよ.

[解答]
$$\begin{aligned}
gh &= (1-2\sigma_2+3\sigma_5)(3\sigma_6-2\sigma_4+\sigma_2)\\
&= (3\sigma_6-2\sigma_4+\sigma_2)+(-6\sigma_2\sigma_6+4\sigma_2\sigma_4-2\sigma_2^2)+(9\sigma_5\sigma_6-6\sigma_5\sigma_4+3\sigma_5\sigma_2)\\
&= (3\sigma_6-2\sigma_4+\sigma_2)+(-6\sigma_3+4\sigma_5-2)+(9-6\sigma_2+3\sigma_3)\\
&= 7-5\sigma_2-3\sigma_3-2\sigma_4+4\sigma_5+3\sigma_6 \qquad \square
\end{aligned}$$

1.1.2（群環でのノルム元）

G を有限群，A を可換環，$N=\sum_{g\in G} g\in A[G]$ とおく. このとき，すべての $g\in G$ に対し，$gN=Ng=N$ であることを証明せよ.

[解答]　$gN=N$ を示そう. 計算が分かりやすいように Σ 内の変数を h に変えると，g を左から掛ける写像 $\phi: G\to G, h\mapsto gh$ は全単射であるので（難しく言っているが要は gh が G 内をくまなく，

かつ各点を一回だけ通過するということ)，$gh = h'$ とおくことで，$gN = \sum_{h\in G} gh = \sum_{h'\in G} h' = N$ となる. 同様に $Ng = N$ も示せるので，題意は示された. □

1.1.3

$A = \mathbb{Z}[\sqrt{-2}]$, $a = 1 + 3\sqrt{-2}$, $b = 2 - \sqrt{-2}$ とする.$2a + b, ab$ を計算せよ.

[解答]
$$2a + b = (2 + 6\sqrt{-2}) + (2 - \sqrt{-2}) = 4 + 5\sqrt{-2}$$
$$ab = (2 - \sqrt{-2}) + (6\sqrt{-2} + 6) = 8 + 5\sqrt{-2} \quad \square$$

1.2.1

(1) $g(x) = 3x^3 - x^2 + x - 1$ を $f(x) = x^2 - 3x + 1$ で ($\mathbb{Z}[x]$ において) 割り算せよ.
(2) $f(x, y) = x^2 + 3xy^3 - y^2 - 3$, $g(x, y) = x^3y^2 + 3xy^3 - 2x^2y + x - 3 \in \mathbb{Z}[x, y]$ とするとき，$g(x, y)$ を x の多項式とみなして，$f(x, y)$ で割り算せよ.

[解答] (1),(2) の $f(x), f(x, y)$ の最高次の係数は 1 で，命題 1.2.10（もしくはその命題の後の記述）により割り算ができることが保証されていることは頭に留めておくべきだろう.
(1)

$$\begin{array}{rl|l} & & 3x \quad +8 \\ \hline x^2-3x+1 & \big) & 3x^3 \quad -x^2 \quad +x-1 \\ & & \underline{3x^3-9x^2 \quad +3x} \\ & & \quad 8x^2 \quad -2x-1 \\ & & \quad \underline{8x^2-24x+8} \\ & & \quad\quad 22x-9 \end{array}$$

より，$g(x) = (3x + 8)f(x) + 22x - 9$.
(2) x の多項式として考えると，$f(x, y) = x^2 + 3y^3x + (-y^2 - 3)$, $g(x, y) = y^2x^3 - 2yx^2 + (3y^3 + 1)x - 3$ と書けるので,

$$\begin{array}{rl|llll} & & y^2x & -2y-3y^5 & & \\ \hline x^2+3y^3x-y^2-3 & \big) & y^2x^3 & -2yx^2 & +(3y^3+1)x & -3 \\ & & \underline{y^2x^3} & \underline{+3y^5x^2} & \underline{+(-y^4-3y^2)x} & \\ & & & (-2y-3y^5)x^2 & +(3y^3+1+y^4+3y^2)x & -3 \\ & & & \underline{(-2y-3y^5)x^2} & \underline{+(-6y^4-9y^8)x} & \underline{+2y^3+3y^7+6y+9y^5} \\ & & & & (3y^3+1+7y^4+3y^2+9y^8)x & -3-2y^3-3y^7-6y-9y^5 \end{array}$$

より，$g(x, y) = (y^2x - 3y^5 - 2y)f(x, y) + (9y^8 + 7y^4 + 3y^3 + 3y^2 + 1)x - 3y^7 - 9y^5 - 2y^3 - 6y - 3$
□

1.2.2

$f(x, y, z) = x^2 + yz$ に $x = t^2 + 1$, $y = 1 - t$, $z = 3t + 2$ を代入して整理せよ.

[解答]
$$\begin{aligned} f(x,y,z) &= (t^2+1)^2 + (1-t)(3t+2) \\ &= t^4 + 2t^2 + 1 + 3t + 2 - 3t^2 - 2t \\ &= t^4 - t^2 + t + 3 \end{aligned}$$ □

1.2.4

多項式 $f(x,y) = x^2 + y^2 + 2x + y + 1 \in \mathbb{C}[x,y]$ の定数項は何か？ また $f(x,y)$ を (a) $\mathbb{C}[x][y]$, (b) $\mathbb{C}[y][x]$ の元とみなしたときの定数項は何か？

[解答*] 1. (a) $f(x,y) = y^2+y+(x^2+2x+1)$ より x^2+2x+1. (b) $f(x,y) = x^2+2x+(y^2+y+1)$ より y^2+y+1. □

1.3.3

環 $\mathbb{Z}$ の自己同型は恒等写像だけであることを証明せよ.

[解答] 環 $\mathbb{Z}$ は生成系 $\{1\}$ を取ることで，$\mathbb{Z}$ 代数として有限生成である. 定義 1.3.13 の後の記述から環 $\mathbb{Z}$ 上の自己同型は $\mathbb{Z}$ 同型である. よって $\mathbb{Z}$ 上の自己同型は 1 の行き先によって決まる. しかし環の準同型性から，これは 1 になるしかなく，これは恒等写像における 1 の行き先と一致するので，$\mathbb{Z}$ 上の自己同型は恒等写像しかないことが分かる. □

1.3.4

写像 $\phi : \mathbb{Z} \to \mathbb{Z}$ で定義 1.1.7 (1) のはじめの 2 条件は満たすが，最後の条件は満たさないものはあるか？

[解答*] 恒等的に 0 であるような写像. □

※逆に恒等的に 0 であるような写像以外は存在しないことが次のようにして分かる.$\phi(n+m) = \phi(n) + \phi(m)\,(\forall n, m \in \mathbb{Z})$ より，$\phi(n) = \underbrace{\phi(1) + \cdots + \phi(1)}_{n\text{ 個}}$ (n は正の整数) となるので，ϕ を決めることは，$\phi(1)$ の値を決めることに対応する（n が正でない場合についても $\phi(0) = 0, \phi(n) = -\phi(-n)$ が成り立つことに注意すれば，$\phi(1)$ の値によって決まることが分かるので大丈夫). そこで $\phi(1) = k$ とおくと，$\phi(n) = n\phi(1) = nk\,(\forall n \in \mathbb{Z})$ となり，$\phi(nm) = \phi(n)\phi(m)$ から $\forall n, m \in \mathbb{Z}$ について，$nmk = nmk^2$ が成り立つ. 整理すると $nmk(k-1) = 0$ で，n, m は任意なので $k = 0, 1.k = 1$ のときは条件 $\phi(1) \neq 1$ を満たさないので不適.$k = 0$ のとき，$\phi(n) = 0$ となり，恒等的に 0 であるような写像に対応する. したがってこれのみとなる.

1.3.6

$A = \mathbb{C}[x,y]$ とする.$x^2 - x^5y$ がイデアル $I = (x^2 - y^3, x^5 - y^2)$ の元であることを証明せよ.

[解答] $x^2 - x^5y = (x^2 - y^3) - y(x^5 - y^2)$ より明らか. □

1.3.15

$A=\mathbb{C}[x,y]$, $I=(x^2+y+1, x+y^2)$, $J=(x,y)$ とするとき，$I+J$ は何か？

[解答]　$(x^2+y+1)-x\cdot x-y=1\in I+J$ となり，イデアルが 1 を含むことと，イデアルが環全体になることは同値なので $I+J=A$ となる．　□

1.4.1

(1) $\mathbb{Z}[\sqrt{2}]/(3+\sqrt{2})\cong\mathbb{F}_7$ であることを証明せよ．
(2) $\mathbb{Z}[\sqrt{5}]/(1+2\sqrt{5})$ は何か？

[解答]　(1) 例題 1.4.11 と同様に解く．まず例 1.4.10 より $\mathbb{Z}[\sqrt{2}]\cong\mathbb{Z}[x]/(x^2-2)$ という同型があり，この同型により $(3+\sqrt{2})\subset\mathbb{Z}[\sqrt{2}]$ というイデアルは $\mathbb{Z}[x]/(x^2-2)$ の中で $3+x$ により生成されるイデアル $\overline{(3+x)}$ に対応する (分かりやすいように剰余群内のイデアルは $\overline{I}$ のように上線をつけて表す). 定理 1.4.4（イデアルの対応）より $\overline{(3+x)}$ に対応する $\mathbb{Z}[x]$ のイデアルが存在することが分かっている．明らかにそれは $(3+x,x^2-2)\subset\mathbb{Z}[x]$（$x^2-2$ が出てきたのは，定理 1.4.4（イデアルの対応）では (x^2-2) を含むようなイデアルが対応するからである）で，対応から $\overline{(3+x)}=(3+x,x^2-2)/(x^2-2)$ となる．よって命題 1.4.5(第三同型定理) を 2 回使えば，

$$\mathbb{Z}[\sqrt{2}]/(3+\sqrt{2})\cong\frac{\mathbb{Z}[x]/(x^2-2)}{(3+x,x^2-2)/(x^2-2)}\cong\mathbb{Z}[x]/(3+x,x^2-2)\cong\frac{\mathbb{Z}[x]/(3+x)}{(x^2-2,3+x)/(3+x)}$$

となる．ここで $\mathbb{Z}[x]$ の元 x に -3 を代入する準同型を考えると，例 1.4.9 より $\mathbb{Z}[x]/(3+x)\cong\mathbb{Z}$ で，この同型でイデアル $(x^2-2,3+x)/(3+x)\subset\mathbb{Z}[x]/(3+x)$ は $(9^2-2)=(7)=7\mathbb{Z}\subset\mathbb{Z}$ に対応する．よって

$$\mathbb{Z}[\sqrt{2}]/(3+\sqrt{2})\cong\mathbb{Z}/7\mathbb{Z}\cong\mathbb{F}_7$$

となる．

(2) (1) と全く同様にして $\mathbb{Z}[\sqrt{5}]/(1+2\sqrt{5})\cong\dfrac{\mathbb{Z}[x]/(1+2x)}{(x^2-5,1+2x)/(1+2x)}$ までは導出できる．ここで $\mathbb{Z}[x]$ において $(x^2-5,2x+1)=(19,2x+1)$ であることを示す．まず $\subset$ について $4(x^2-5)=(2x-1)(2x+1)-19$ より（この式は x^2-5 を $2x+1$ で $\mathbb{Q}[x]$ の元として割り算した後，適当な整数をかけて $\mathbb{Z}[x]$ 上の等式になるように調整するという発想で得られる）$19=(2x-1)(2x+1)-4(x^2-5)\in(x^2-5,2x+1)$ となることから分かる．$\supset$ については再び先ほどの等式から $4(x^2-5)\in(19,2x+1)$ が分かる．また $19(x^2-5)\in(19,2x+1)$ も分かる．そこで $4,19$ は互いに素なので $4x+19y=1$ となる整数 x,y を取ってくると，$x^2-5=x\cdot4(x^2-5)+y\cdot19(x^2-5)\in(19,2x+1)$ となり $\supset$ が得られる．よって $(x^2-5,2x+1)=(19,2x+1)$ であることと，(1) と同様に剰余の順番を変えることで

$$\mathbb{Z}[\sqrt{5}]/(1+2\sqrt{5})\cong\frac{\mathbb{Z}[x]/(1+2x)}{(19,1+2x)/(1+2x)}\cong\frac{\mathbb{Z}[x]/(19)}{(19,1+2x)/(19)}$$

が得られる．命題 1.4.12 より $\mathbb{Z}[x]/(19)\cong\mathbb{F}_{19}[x]$ で，この同型により $(19,1+2x)/(19)\subset\mathbb{Z}[x]/(19)$ は $(1+2x)\subset\mathbb{F}_{19}[x]$ に対応する．さらに $\mathbb{F}_{19}$ の中では 2 の逆元 2^{-1} が存在するので $(1+2x)=$

$(x-2^{-1}) \in \mathbb{F}_{19}[x]$ で，$\mathbb{Z}[\sqrt{5}]/(x-2^{-1}) \cong \mathbb{F}_{19}[x]/(1+2x) \cong \mathbb{F}_{19}$ となる. ただし最後の同型は例 1.4.9 による． □

※ (2) の解法を用いて同様に (1) でも $(3+x, x^2-2) = (3+x, 7)$ のように生成元の次数を下げることで解答することもできる.

1.4.2

環 A とその部分環 B で，B が整域で A が整域ではないものの例を一組見つけよ.

[解答*]　$A = \mathbb{C}[x,y]/(y^2)$, $B = \mathbb{C}[x]$ が求める例の一つである. ただし B は次のようにして A の部分環とみなす. 自然な写像 $i : B \to A$ について，$f(x) \in \mathrm{Ker}(i)$ とすると，$f(x) = g(x,y)y^2$ $(g(x,y) \in A)$ と書ける.$y = 0$ を代入することで，$f(x) = 0$ が得られる. つまり $\mathrm{Ker}(i) = \{0\}$ で i は単射であるので，$B \cong \mathrm{Im}(i) \subset A$ となるので，$\mathrm{Im}(i)$ を B と同一視することで A の部分環とみなす. このとき A において $y \neq 0$ であるが，$y^2 = 0$ となるので A は確かに整域でないが，B は明らかに整域であるので，題意は示された.

[別解]　同様にして $A = \mathbb{C}[x]/(x^2)$, $B = \mathbb{C}$ という，もう少し簡単な例も挙げられる． □

1.8.2

$\mathbb{C}[t^{24}, t^{35}] \subset \mathbb{C}[t]$ の商体は $\mathbb{C}(t)$ であることを証明せよ.

[解答]　例 1.8.11 と同じ方針で示す.$\mathbb{C}[t^{24}, t^{35}]$ の商体を K とおく.$\mathbb{C}[t^{24}, t^{35}] \subset \mathbb{C}[t]$ で，商体においても包含関係は保たれるので (命題 1.8.10)，$K \subset \mathbb{C}(t)$ である. 逆の包含関係を示そう. そのためには $t \in K$ を示せば十分である.24 と 35 は互いに素なので，$24x + 35y = 1$ となるような整数 x, y が存在する. 故に $t^1 = (t^{24})^x \cdot (t^{35})^y \in K$ であることが言えたので，$K \supset \mathbb{C}(t)$ で，題意は示された． □

1.8.9

$I_1, \cdots, I_n$ が環 A のイデアルなら，$\sqrt{I_1 \cap \cdots \cap I_n} = \sqrt{I_1} \cap \cdots \cap \sqrt{I_n}$ であることを証明せよ.

[解答]　$\sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}$ を示せば十分である.

まず $\subset$ を示そう.$x \in \sqrt{I_1 \cap I_2}$ とすると，ある正の整数 n により $x^n \in I_1 \cap I_2 (\Leftrightarrow x^n \in I_1, I_2)$ となる. よって $x \in \sqrt{I_1}, \sqrt{I_2} (\Leftrightarrow x \in \sqrt{I_1} \cap \sqrt{I_2})$ となり，$\subset$ は示された.

次に $\supset$ を示す.$x \in \sqrt{I_1} \cap \sqrt{I_2} (\Leftrightarrow x \in \sqrt{I_1}, \sqrt{I_2})$ とすると，ある正の整数 n_1, n_2 が存在して $x^{n_1} \in I_1, x^{n_2} \in I_2$.$I_1, I_2$ はイデアルなので，$x^{n_1+n_2} \in I_1, I_2 (\Leftrightarrow x \in I_1 \cap I_2)$. よって $x \in \sqrt{I_1 \cap I_2}$ となり，$\supset$ は示された.

したがって題意は示された． □

第 2 章

2.7.12

K が整域で $|K| < \infty$ なら，K は体であることを証明せよ．（ヒント：$x \in K^\times$ なら x の乗法群 $K^\times$ での位数を考えよ.)

[解答]　$x \in K(x \neq 0)$ の逆元が存在することを言えば良い.K は環なので，積について閉じているので $x, x^2 \cdots, x^n, \cdots \in K$ であるが，$|K| < \infty$ より，ある正の整数 $i, j\,(i > j)$ が存在して $x^i = x^j$ となる. よって $x^j(x^{i-j} - 1) = 0$ となるが，K は整域なので

$$x^{i-j} = x \cdot x^{i-j-1} = x^{i-j-1} \cdot x = 1$$

が得られる. つまり $x^{i-j-1} \in K$ は x の逆元であることが示されたので，題意は示された.　□

※上の解答は K は可換整域であると仮定して作成した. 教科書の文脈的にも，おそらくこの問題では K の可換性を仮定して良いだろう. このような注意を残したのは K が非可換有限整域である場合でも K は斜体ではなく，体となることが示せるからである（ウェダーバーンの小定理）. ウェダーバーンの小定理の証明を見たい方は私のブログの記事を見ていただけると嬉しい.

今回の解答はできるだけ問題のヒントに従ったつもりだが，ヒントでは $x \in K(x \neq 0)$ ではなく，$x \in K^\times$ と書いているため，やや私の解答と筆者の想定している解答にズレがあるように感じる. より良い解答があれば前書きのグーグルフォームから教えていただけると嬉しい.

第 3 章

3.1.1

次の素数 p に対し，$(x+y)^p = x^p + y^p + pf(x,y)$ となる $f(x,y) \in \mathbb{Z}$ を求めよ.

(1) $p = 2$　(2) $p = 3$　(3) $p = 5$　(4) $p = 7$

[解答]　二項展開を用いて計算するだけである.

(1)

$$(x+y)^2 = x^2 + y^2 + 2xy$$

より $f(x,y) = xy$.

(2)

$$(x+y)^3 = x^3 + y^3 + 3(x^2y + 3xy^2)$$

より $f(x,y) = x^2y + xy^2$.

(3)

$$\begin{aligned}(x+y)^5 &= x^5 + y^5 + {}_5\mathrm{C}_1 x^4 y + {}_5\mathrm{C}_2 x^3 y^2 + {}_5\mathrm{C}_3 x^2 y^3 + {}_5\mathrm{C}_4 x y^5 \\ &= x^5 + y^5 + 5(x^4y + 2x^3y^2 + 2x^2y^3 + xy^4)\end{aligned}$$

より $f(x,y)=x^4y+2x^3y^2+2x^2y^3+xy^4$.

(4)

$$\begin{aligned}(x+y)^7 &= x^7+y^7+{}_7\mathrm{C}_1x^6y+{}_7\mathrm{C}_2x^5y^2+{}_7\mathrm{C}_3x^4y^3+{}_7\mathrm{C}_4x^3y^4+{}_7\mathrm{C}_5x^2y^5+{}_7\mathrm{C}_6xy^6\\ &= x^7+y^7+7(x^6y+3x^5y^2+5x^4y^3+5x^3y^4+3x^2y^5+xy^6)\end{aligned}$$

より $f(x,y)=x^6y+3x^5y^2+5x^4y^3+5x^3y^4+3x^2y^5+xy^6$. □

3.1.2

p を素数とするとき，$x,y\in\mathbb{Z}$ で $x\equiv y \mod p$ なら，
すべての $n>0$ に対し，$x^{p^n}\equiv y^{p^n} \mod p^{n+1}$ であることを証明せよ.

[解答] n (ただし $n=0$ も加えた $n\geq 0$ で考える) に関する数学的帰納法で示す.

[1] $n=0$ のとき 仮定より成り立つことは明らか.

[2] $n=k$ $(k\in\mathbb{Z},k\geq 0)$ のとき仮定が成り立つとして，$n=k+1$ のときを考える.$n=k$ のときの仮定から $x^{p^k}\equiv y^{p^k} \mod p^{k+1}$ より $x^{p^k}-y^{p^k}=p^{k+1}m$ $(m\in\mathbb{Z})$ とおける. つまり $x^{p^k}=y^{p^k}+p^{k+1}m$ となる.

よって $n=k+1$ のとき

$$\begin{aligned}x^{p^{k+1}}-y^{p^{k+1}} &= (x^{p^k})^p-y^{p^{k+1}}\\ &= (y^{p^k}+p^{k+1}m)^p-y^{p^{k+1}}\\ &= \sum_{i=1}^{p}{}_p\mathrm{C}_i(y^{p^k})^{p-i}(p^{k+1}m)^i \quad \because \text{二項展開}\end{aligned}$$

$2\leq i\leq p$ のとき $(p^{k+1}m)^i$ は p^{k+2} で割り切れる.$i=1$ のとき ${}_p\mathrm{C}_1$ は p で割り切れるので，${}_p\mathrm{C}_1p^{k+1}m$ は p^{k+2} で割り切れる. よって $x^{p^{k+1}}-y^{p^{k+1}}$ は p^{k+2} で割り切れるので，$n=k+1$ のときも主張は成り立つ.

[1],[2] より題意は示された. □

3.1.3

素体の自己同型は恒等写像だけであることを証明せよ.

[解答] まず $\mathbb{Q}$ について考える.φ を体 $\mathbb{Q}$ の自己同型とすると $\varphi(1)=1$, $\varphi(0)=0$ である.$n\in\mathbb{N}$ について

$$\begin{aligned}\varphi(n) &= \varphi(\underbrace{1+\cdots+1}_{n\text{ 個}})\\ &= \underbrace{\varphi(1)+\cdots+\varphi(1)}_{n\text{ 個}}\\ &= n\end{aligned}$$

また $-n<0$ についても $\varphi(-n)=-\varphi(n)=-n$ となる. つまり $\varphi(n)=n$ $(n\in\mathbb{Z})$ が示された.

次に $\mathbb{Q}$ の元 $\frac{n}{m}$ $(m \neq 0,\ n, m \in \mathbb{Z})$ についても

$$\begin{aligned}\varphi(\tfrac{n}{m}) &= \varphi(nm^{-1}) \\ &= n\varphi(m)^{-1} \\ &= \tfrac{n}{m}\end{aligned}$$

となるので，$\varphi = \mathrm{id}_{\mathbb{Q}}$ であることが示された.
次に $\mathbb{F}_p$ 上の自己同型 ψ について考える. 上の $\mathbb{Q}$ の場合と同様に $\psi(\overline{n}) = \overline{n}$ $(\forall \overline{n} \in \mathbb{F}_p)$ を示せる. これは $\psi = \mathrm{id}_{\mathbb{F}_p}$ を意味するので，題意は示された. □
※この証明で単射・全射性を用いていないため，問題の条件を“自己同型”ではなく“自己準同型”に緩めても OK.

3.1.4

$L = K(x_1, x_2)$ を体 K 上の 2 変数有理関数体，$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ とするとき，$\phi(x_1) = ax_1 + cx_2,\ \phi(x_2) = bx_1 + dx_2$ となる $\phi \in \mathrm{Aut}_K^{\mathrm{al}} L$ があることを証明せよ.

[解答] 命題 1.3.14 より $\tilde{\phi} \in \mathrm{Hom}_K^{\mathrm{al}}(K[x_1, x_2], K[x_1, x_2])$ で $\tilde{\phi}(x_1) = ax_1 + cx_2,\ \tilde{\phi}(x_2) = bx_1 + dx_2$ が存在する. 行列で書けば

$$\begin{pmatrix} \tilde{\phi}(x_1) & \tilde{\phi}(x_2) \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \end{pmatrix} A$$

$A \in \mathrm{GL}_2(K)$ より A^{-1} が取れるので，両辺にかければ

$$\begin{pmatrix} x_1 & x_2 \end{pmatrix} = \begin{pmatrix} \tilde{\phi}(x_1) & \tilde{\phi}(x_2) \end{pmatrix} A^{-1}$$

となる. これは A^{-1} に対しても $\tilde{\phi}$ と同様に定めた写像が $\tilde{\phi}$ の逆写像になることを意味する. よって $\tilde{\phi} \in \mathrm{Aut}_K^{\mathrm{al}}(K[x_1, x_2])$. 局所化の普遍性 (命題 1.8.6) より $\tilde{\phi}$ を問題の $\phi \in \mathrm{Aut}_K^{\mathrm{al}} L$ に拡張することができる. したがって題意は示された. □

3.1.5

$L = K(x)$ を体 K 上の 1 変数有理関数体，$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ とするとき，$\phi(x) = (ax + c)/(bx + d)$ となる $\phi \in \mathrm{Aut}_K^{\mathrm{al}} L$ があることを証明せよ.

[解答] 命題 1.3.14 より $\tilde{\phi} \in \mathrm{Hom}_K^{\mathrm{al}}(K[x], L)$ で $\tilde{\phi}(x) = (ax+c)/(bx+d)$ が存在する. さらに $\tilde{\phi}$ は局所化の普遍性 (命題 1.8.6) より $\tilde{\phi}$ を問題の $\phi \in \mathrm{Hom}_K^{\mathrm{al}}(L, L)$ に拡張することができる ※. ここで ϕ の逆写像を推測するために $\tilde{\phi}(x) = (ax + c)/(bx + d)$ を x について解くと，$x = (-d\phi(x) + c)/(b\phi(x) - a)$ となることがわかる. そこで $\begin{pmatrix} -d & b \\ c & -a \end{pmatrix} \in \mathrm{GL}_2(K)$ から同様に定められた写像 $\phi' \in \mathrm{Hom}_K^{\mathrm{al}}(L, L)$ を構成すると，$\phi'(x) = (-dx + c)/(bx - a)$ で先ほどの関係式を満たすように定めたので明らかに ϕ の逆写像になる. したがって $\phi \in \mathrm{Aut}_K^{\mathrm{al}} L$ となり題意は示された. □

※局所化の普遍性のときに $A \in GL_2(K)$ という条件を用いている.$\tilde{\phi}$ は $K[x]$ の元を L の単元に移す必要がある.L は商体なので，このことは $\tilde{\phi}(f(x))$，つまり $f(\tilde{\phi}(x))$ $(\forall f(x) \in K[x])$ が 0 でないこと

と同値. さらにこれは $\phi(x)$ が K 上超越的であることに同値. そこで $\phi(x)$ が超越的である条件を調べる. もし $\phi(x)$ が超越的でないとすると $\exists f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x] \quad f(\phi(x)) = 0.$ よって

$$\begin{aligned}\left(\frac{ax+c}{bx+d}\right)^n + a_{n-1}\left(\frac{ax+c}{bx+d}\right)^{n-1} + \cdots + a_0 &= 0\\ (ax+c)^n + a_{n-1}(ax+c)^{n-1}(bx+d) + \cdots + a_0(bx+d)^n &= 0\\ a_0(bx+d)^n &\equiv 0 \mod (ax+c)\end{aligned}$$

$a_0 = 0$ なら $f(x)$ を x で割ることで $a_0 \neq 0$ となるように $f(x)$ を取り換えることができる. 故に $a_0 \neq 0$ としても良いので，$(bx+d)^n$ は $ax+c$ で割り切れる.$ax+c$ は素元なので，これは $bx+d$ は $ax+c$ で割り切れることと同値. さらにこれは $(\ a \quad c\ ), (\ b \quad d\ )$ が線形従属である，つまり $A \notin GL_2(K)$ であることと同値. まとめると「$\phi(x)$ が K 上超越的でない $\Rightarrow A \notin GL_2(K)$」が示された. 逆に $A \notin GL_2(K)$ とすると，$ad - bc = 0$ より

$$\phi(x) = \frac{adx + cd}{d(bx+d)} = \frac{c(bx+d)}{d(bx+d)} = \frac{c}{d}$$

となるので $\phi(x)$ は超越的でない. つまり「$\phi(x)$ が K 上超越的 $\Leftrightarrow A \in GL_2(K)$」なので，$A \in GL_2(K)$ という条件を課しているのである.

3.1.6

$n, d > 0$ を整数，$p_1, \cdots, p_t$ は相異なる素数，$a_1, \cdots, a_t > 0$ は整数，$d = p_1^{a_1} \cdots p_t^{a_t}$，$K = \mathbb{Q}(\sqrt[n]{d})$ とする。

(1) a_1 が n と互いに素なら，$d' = p_1 p_2^{b_2} \cdots p_t^{b_t}$ ($b_2, \cdots, b_t \geq 0$ は整数) という形の整数で $\sqrt[n]{d'} \in K$ となるものがあることを証明せよ。

(2) (1) の状況で $[K : \mathbb{Q}] = n$ であることを証明せよ。

[解答]　(1) a_1 と n が互いに素より $a_1 x + ny = 1$ となるような整数 x, y が存在する (さらに後のために x は自然数とする)。このとき $p_1^y(\sqrt[n]{d})^x \in K$ について考えると

$$\begin{aligned}p_1^y(\sqrt[n]{d})^x &= \sqrt[n]{p_1^{a_1 x + ny} p_2^{a_2 x} \cdots p_t^{a_t x}}\\ &= \sqrt[n]{p_1 p_2^{a_2 x} \cdots p_t^{a_t x}}\end{aligned}$$

となるので，$d' = p_1 p_2^{a_2 x} \cdots p_t^{a_t x}$ と取ればよい (x を自然数としたため $a_i x \geq 0$ は満たす)。

(2) (1) の d' について $K' = \mathbb{Q}(\sqrt[n]{d'})$ とおくと $K \supset K'$ である。$\sqrt[n]{d}$ は $x^n - d$ の根なので $[K : \mathbb{Q}] \leq n$。また $\sqrt[n]{d'}$ は $x^n - d'$ の根で，$x^n - d'$ はアイゼンシュタインの判定法 (定理 1.12.11) で $p = p_1$ として考えれば $\mathbb{Q}$ 上既約であることが分かる。よって $[K' : \mathbb{Q}] = n$ である。これまでのことを合わせて $[K : K'] = 1 \Leftrightarrow K = K'$ となり，$[K : \mathbb{Q}] = n$ が導かれる.　□

3.1.7

K を体，L, F を K の拡大体とするとき，$[L : K] = 3, [F : K] = 4$ なら，L は F に含まれることはないことを証明せよ.

[解答]　例題 3.1.22 と同じ方針で示す. もし $K \supset L \supset F$ なら，$4 = [F : K] = [F : L][L : K] = 3[F : L]$ となり，4 が 3 で割り切れてしまうので矛盾である.　□

3.1.8

$\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[4]{2})$ であることを証明せよ.

[解答]　$x^4 - 2, x^3 - 2$ はアイゼンシュタインの判定法 (定理 1.12.11) より $\mathbb{Q}$ 上既約で，さらにモニックなのでそれぞれ $\sqrt[4]{2}, \sqrt[3]{2}$ の最小多項式となる (系 3.1.25). よって $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4, [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ となる. ここで仮に $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[4]{2})$ とすると $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ となり，問題 3.1.7 よりこれは矛盾. したがって題意は示された.　□

3.1.9

L/K を体の拡大で $[L : K] = 2$ とする.$f(x) \in K[x]$ が 3 次の既約多項式なら，$f(x)$ は L 上でも既約であることを証明せよ.

[解答]　$f(x)$ は L 上で既約でないとすると，3 次なので $\exists \alpha \in L,\ f(\alpha) = 0.f(x)$ は K 上 3 次の多項式より $[K(\alpha) : K] = 3.\alpha \in L$ より $L \supset K(\alpha) \in K$ であるので，$[L : K] = [L : K(\alpha)][K(\alpha) : K]$ より $2 = [L : K(\alpha)]3$. これは明らかに矛盾するので，題意は示された.　□

3.1.10

L/K は体の拡大で $L = K(\alpha), [L : K] = 3$ とするとき，$L = K(\alpha^2)$ であることを証明せよ.

[解答]　$K(\alpha)$ は体なので $\alpha^2 \in K(\alpha)$ であるから $L \supset K(\alpha^2) \supset K$. よって $3 = [L : K(\alpha^2)][K(\alpha^2) : K]$ が成り立つ.$\alpha^2 \in K$ とすると $\exists c \in K,\ \alpha^2 - c = 0$ となる. これは α の K 上の最小多項式が 2 次以下であることを表し，$[L : K] = 3$ に矛盾. よって $\alpha^2 \in K$，すなわち $[K(\alpha^2) : K] > 1$. このとき先程の等式から $[L : K(\alpha^2)] = 1$ となるしかなく，これは $L = K(\alpha^2)$ を意味するので，題意は示された.
□

3.1.11

K を体，$f(x) \in K[x]$ を 2 次の既約多項式，$f(\alpha) = f(\beta) = 0$ とする. このとき，$K(\alpha) = K(\beta)$ であることを証明せよ.

[解答*]　$f(x) = x^2 + a_1 x + a_2$ とする.$\alpha = \beta$ なら明らかである.$\alpha \neq \beta$ なら解と係数の関係から $\alpha + \beta = -a_1 \Leftrightarrow \beta = -\alpha - a_1 \in K(\alpha)$ となるので，$K(\beta) \subset K(\alpha)$. 同様にして $K(\alpha) \subset K(\beta)$ となるので，$K(\alpha) = K(\beta)$ は示される. 補足として標数が 2 でなければ，2 次方程式の解の公式が使えるので明らかであるが，この証明なら標数が 2 でも良いというメリットがある.　□

3.1.12

次の元の $\mathbb{Q}$ 上最小多項式と $\mathbb{Q}$ 上の共役をすべて求めよ.
(1) $\sqrt{3} + \sqrt{5}$　(2) $\sqrt[3]{4}$　(3) $\sqrt{-1}\sqrt[3]{2}$　(4) $\sqrt{1 + \sqrt{2}}$

[解答] (1)

$$\begin{aligned}\alpha &= \sqrt{3}+\sqrt{5}\\ \alpha-\sqrt{3} &= \sqrt{5}\\ \alpha^2-2\sqrt{3}\alpha+3 &= 5\\ \alpha^2-2 &= 2\sqrt{3}\alpha\\ \alpha^4-4\alpha^2+4 &= 12\alpha^2\\ \alpha^4-16\alpha^2+4 &= 0\end{aligned}$$

よって x^4-16x^2+4 が求める最小多項式であることを示す. 上の式変形より $\sqrt{3}=\frac{\alpha^2-2}{2\alpha}, \sqrt{5}=\alpha-\sqrt{3}$ で $\sqrt{3},\sqrt{5}\in\mathbb{Q}(\alpha)$ となるので, $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{3},\sqrt{5})$. 例題 3.1.34(1),(2) と同様に $\sqrt{5}\notin\mathbb{Q}(\sqrt{3})$ を示せば $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$ を示せるので, $\sqrt{5}\notin\mathbb{Q}(\sqrt{3})$ を示す. 仮に $\sqrt{5}\in\mathbb{Q}(\sqrt{3})$ とすると明らかに $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2$ より $\exists a,b\in\mathbb{Q},\ \sqrt{5}=a+b\sqrt{3}$ となる. 両辺を 2 乗して $a^2+3b^2+2\sqrt{3}ab=5$ が得られる.$\sqrt{3}$ は無理数なので, この式が成り立つには $ab=0$ となる必要がある.$b=0$ のなら $\sqrt{5}=a\in\mathbb{Q}$ となり矛盾. よって $a=0$ であり, b を $b=\frac{c}{d}$ $(c,d\in\mathbb{Z},d\neq0)$ と書くと $3c^2=5d^2$ となる. 両辺の素因数 5 の個数を考えると $c^2,d^2(\neq0)$ は平方数で, 両辺の偶奇が一致しないので矛盾. よって $\sqrt{5}\notin\mathbb{Q}(\sqrt{3})$ は示されたので, $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$ となり, これは x^4-16^2+4 が求める最小多項式であることを意味する. また上の式変形を逆に辿ることで, 共役は $\pm\sqrt{3}\pm\sqrt{5}$ と求まる.

(2) 明らかに $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$ であるので, 問題 3.1.10 より $\mathbb{Q}(\sqrt[3]{4})=\mathbb{Q}(\sqrt[3]{2})$ であり, $[\mathbb{Q}(\sqrt[3]{4}):\mathbb{Q}]=3$ となる. つまり求める最小多項式は 3 次であるが, $(\sqrt[3]{4})^3-4=0$ よりそれは x^3-4 だとわかる. また共役はその最小多項式の根を求めることで, 1 の原始 3 乗根 ω を用いて $\sqrt[3]{4},\sqrt[3]{4}\omega,\sqrt[3]{4}\omega^2$ となる.

(3) $(\sqrt{-1}\sqrt[3]{2})^6+4=0$ なので, x^6+4 が求める最小多項式であることを示す.$\frac{(\sqrt{-1}\sqrt[3]{2})^4}{2}=\sqrt[3]{2}, \sqrt{-1}=\frac{\sqrt{-1}\sqrt[3]{2}}{\sqrt[3]{2}}$ より $\sqrt[3]{2},\sqrt{-1}\in\mathbb{Q}(\sqrt{-1}\sqrt[3]{2})$ が分かる.$\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式が x^3-2 であることから, $[\mathbb{Q}(\sqrt{-1}\sqrt[3]{2})\sqrt[3]{2}):\mathbb{Q}]$ は 3 の倍数だと言える. また明らかに $[\mathbb{Q}(\sqrt{-1}):\mathbb{Q}]=2$ であることから $[\mathbb{Q}(\sqrt{-1}\sqrt[3]{2}):\mathbb{Q}]$ は 6 の倍数だと言える. よって x^6+4 が求める最小多項式だと分かる. また共役は方程式 $x^6+4=0$ を解くことで 1 の原始 3 乗根 ω を用いて $\sqrt{-1}\sqrt[3]{2},\sqrt{-1}\omega\sqrt[3]{2},\sqrt{-1}\omega^2\sqrt[3]{2},-\sqrt{-1}\sqrt[3]{2},-\sqrt{-1}\omega\sqrt[3]{2},-\sqrt{-1}\omega^2\sqrt[3]{2}$ と書ける.

(4)

$$\begin{aligned}\alpha &= \sqrt{1+\sqrt{2}}\\ \alpha^2 &= 1+\sqrt{2}\\ \alpha^2-1 &= \sqrt{2}\\ \alpha^4-2\alpha^2+1 &= 2\\ \alpha^4-2\alpha^2-1 &= 0\end{aligned}$$

x^4-2x^2-1 はアイゼンシュタインの判定法 (定理 1.12.11) より既約であるので, これが求める最小多項式である. また共役な元は上の式変形を逆に辿ることで, $\pm\sqrt{1\pm\sqrt{2}}$ であることが分かる. □

3.1.13

(1) $\sqrt{3}+\sqrt{5}$ の $\mathbb{Q}(\sqrt{3})$ 上の多項式を求めよ.
(2) $\sqrt[4]{2}$ の $\mathbb{Q}(\sqrt{2})$ 上の最小多項式を求めよ.
(3) $\sqrt{-1}\sqrt[3]{2}$ の $\mathbb{Q}(\sqrt{-1})$ 上の最小多項式を求めよ.

[解答] (1) 問題 3.1.12(1) より $\sqrt{3}+\sqrt{5}$ の $\mathbb{Q}$ 上の最小多項式は 4 次なので，$[\mathbb{Q}(\sqrt{3}+\sqrt{5}):\mathbb{Q}]=4$ だと分かる. ここで明らかに $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2$ であることから，$[\mathbb{Q}(\sqrt{3}+\sqrt{5}):\mathbb{Q}]=2$，つまり求める最小多項式は 2 次だと分かる. ここで問題 3.1.12(1) の解答から $(\sqrt{3}+\sqrt{5})^2-2\sqrt{3}(\sqrt{3}+\sqrt{5})-2=0$ であるので，$x^2-2\sqrt{2}x-2$ が求める最小多項式だと分かる.
(2) $\sqrt[4]{2}$ の $\mathbb{Q}$ 上の最小多項式 x^4-2 の次数が 4 であることから $\sqrt[4]{2}\notin\mathbb{Q}(\sqrt{2})$ と言える. よって $[\mathbb{Q}(\sqrt{2})(\sqrt[4]{2}):\mathbb{Q}(\sqrt{2})]\geq 2$，つまり求める最小多項式は 2 次以上. ここで $(\sqrt[4]{2})^2-\sqrt{2}=0$ であるので，$x^2-\sqrt{2}$ が求める最小多項式だと分かる.
(3) $\frac{(\sqrt{-1}\sqrt[3]{2})^4}{2}=\sqrt[3]{2}$ より $\sqrt[3]{2}\in\mathbb{Q}(\sqrt{-1})(\sqrt{-1}\sqrt[3]{2})$ が分かる.$\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式が x^3-2 であることから，$[\mathbb{Q}(\sqrt{-1})(\sqrt{-1}\sqrt[3]{2}):\mathbb{Q}]$ は 3 の倍数だと言える. また明らかに $[\mathbb{Q}(\sqrt{-1}):\mathbb{Q}]=2$ で 2 と 3 は互いに素であることから $[\mathbb{Q}(\sqrt{-1})(\sqrt{-1}\sqrt[3]{2}):\mathbb{Q}(\sqrt{-1})]$ は 3 の倍数だと言える. つまり $[\mathbb{Q}(\sqrt{-1})(\sqrt{-1}\sqrt[3]{2}):\mathbb{Q}(\sqrt{-1})]\geq 3$ で，求める最小多項式は 3 次以上となる. ここで $(\sqrt{-1}\sqrt[3]{2})^3+2\sqrt{-1}=0$ であるので，$x^3+2\sqrt{-1}$ が求める最小多項式だと分かる. □

3.1.14

$L/\mathbb{Q}$ は体の拡大で $\alpha\in L$ は x^3-x-1 の根とする. 次の元を $a\alpha^2+b\alpha+c\,(a,b,c\in\mathbb{Q})$ という形に表せ.
(1) $(\alpha^2+1)^2$　　(2) $(\alpha^2+\alpha+2)(\alpha^2-2\alpha+3)$

[解答*] α は $\alpha^3-\alpha-1\Leftrightarrow\alpha^3=\alpha+1$ という関係式を満たすので，それを用いて α の次数を下げていけばよい.
(1)

$$(\alpha^2+1)^2=\alpha^4+2\alpha^2+1=(\alpha+1)\alpha+2\alpha^2+1=3\alpha^2+\alpha+1$$

(2) (1) の式を利用して

$$\begin{aligned}(\alpha^2+\alpha+2)(\alpha^2-2\alpha+3)&=[(\alpha^2+1)+(\alpha+1)][(\alpha^2+1)-2(\alpha-1)]\\&=(\alpha^2+1)^2+(-\alpha+3)(\alpha^2+1)-2(\alpha^2-1)\\&=3\alpha^2+\alpha+1-\alpha^3-\alpha+3\alpha^2+3-2\alpha^2+2\\&=4\alpha^2+6-(\alpha+1)\\&=4\alpha^2-\alpha+5\quad\square\end{aligned}$$

3.1.15

(1) $\alpha=\sqrt[3]{3}-\sqrt[3]{9}$ の $\mathbb{Q}$ 上の最小多項式を求めよ.
(2) α^{-1} を $a\sqrt[3]{9}+b\sqrt[3]{3}+c\,(a,b,c\in\mathbb{Q})$ という形に表せ.

[解答]　(1) 例題 2.7.3 と同様に解く.$\mathbb{Q}(\sqrt[3]{3})$ の $\mathbb{Q}$ 上の基底 $\{1, \sqrt[3]{3}, \sqrt[3]{9}\}$ に対し,

$$\begin{cases} \alpha \cdot 1 = \quad 0 + 1\sqrt[3]{3} - 1\sqrt[3]{9} \\ \alpha \cdot \sqrt[3]{3} = -3 + 0\sqrt[3]{3} + 1\sqrt[3]{9} \\ \alpha \cdot \sqrt[3]{9} = \quad 3 - 3\sqrt[3]{3} + 0\sqrt[3]{9} \end{cases} \implies P = \begin{pmatrix} 0 & 1 & -1 \\ -3 & 0 & 1 \\ 3 & -3 & 0 \end{pmatrix}$$

なので, α は $\det(xI - P) = x^3 + 9x + 6$ の根.$\alpha \notin \mathbb{Q}$ で $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ は素数なので, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{3})$. したがって $x^3 + 9x + 6$ が α の最小多項式.

[別解]　例題 3.1.33(1) と同様に解く (※解答の流れが分かりやすいように節 3.1 以降の知識も用いることにする).α の最小多項式について, 上の解答と同様にして $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ より 3 次となることがわかり, 定理 3.3.21 より $\mathrm{Hom}^{\mathrm{al}}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \overline{\mathbb{Q}}) = \{\mathrm{id}, \phi_1, \phi_2\}$ と書け, 問題 3.3.5 より求める最小多項式は $(x-\alpha)(x-\phi_1(\alpha))(x-\phi_2(\alpha))$ と書ける. ここで命題 3.1.32(2) より $\mathrm{Hom}^{\mathrm{al}}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{3}), \overline{\mathbb{Q}})$ の 2 つの元で $\sqrt[3]{3}$ をそれぞれその共役 $\omega\sqrt[3]{3}, \omega^2\sqrt[3]{3}$ (ωは 1 の原始 3 乗根) に移すものが存在する. それらを $\mathbb{Q}(\alpha)$ 上に制限したものが ϕ_1, ϕ_2 となり, これらの作用によって $\alpha \mapsto \omega\sqrt[3]{3} - \omega^2\sqrt[3]{9},\ \alpha \mapsto \omega^2\sqrt[3]{3} - \omega\sqrt[3]{9}$ となる. よって求める最小多項式は $(x - \sqrt[3]{3} + \sqrt[3]{9})(x - \omega\sqrt[3]{3} + \omega^2\sqrt[3]{9})(x - \omega^2\sqrt[3]{3} + \omega\sqrt[3]{9})$ となる. 後は以下のように関係式 $\omega^2 + \omega + 1 = 0$ を利用すると, この多項式の係数が求められる.

$$\begin{aligned} &\alpha + \phi_1(\alpha) + \phi_2(\alpha) \\ &= \sqrt[3]{3} - \sqrt[3]{9} + \omega\sqrt[3]{3} - \omega^2\sqrt[3]{9} + \omega^2\sqrt[3]{3} - \omega\sqrt[3]{9} \\ &= 0 \end{aligned}$$

$$\begin{aligned} &\alpha\phi_1(\alpha) + \phi_1(\alpha)\phi_2(\alpha) + \phi_2(\alpha)\alpha \\ &= (\omega\sqrt[3]{9} - 3\omega^2 - 3\omega + 3\omega^2\sqrt[3]{3}) + (\sqrt[3]{9} - 3\omega^2 - 3\omega + 3\sqrt[3]{3}) + (\omega^2\sqrt[3]{9} - 3\omega^2 - 3\omega + 3\omega\sqrt[3]{3}) \\ &= \sqrt[3]{9}(\omega^2 + \omega + 1) + 3\sqrt[3]{3}(\omega^2 + \omega + 1) - 9(\omega^2 + \omega) \\ &= 9 \end{aligned}$$

$$\begin{aligned} &\alpha\phi_1(\alpha)\phi_2(\alpha) \\ &= 3 - 3\omega^2\sqrt[3]{3} - 3\omega + 3\sqrt[3]{9} - 3\sqrt[3]{3} + 3\omega^2\sqrt[3]{9} + 3\omega\sqrt[3]{9} - 9 \\ &= -6 + 3\sqrt[3]{9}(\omega^2 + \omega + 1) - 3\sqrt[3]{3}(\omega^2 + \omega + 1) \\ &= -6 \end{aligned}$$

したがって求める最小多項式は $x^3 + 9x - 6$ となる.

(2) (1) より

$$\begin{aligned} \alpha^3 + 9\alpha + 6 &= 0 \\ \alpha^{-1} &= -\frac{1}{6}(\alpha^2 + 9) \\ &= -\frac{1}{2} - \frac{1}{2}\sqrt[3]{3} - \frac{1}{6}\sqrt[3]{9} \quad \square \end{aligned}$$

3.1.16

(1) 多項式 $f(x)=x^3-x+1$ は $\mathbb{Q}$ 上既約であることを証明せよ.
(2) $L/\mathbb{Q}$ は体の拡大で $\alpha\in L$ は $f(x)$ の根とする. このとき，$\beta=\alpha^2+\alpha+1$ の $\mathbb{Q}$ 上の最小多項式を求めよ.
(3) β^{-1} を $a\alpha^2+b\alpha+c$ $(a,b,c\in\mathbb{Q})$ という形に表せ.

[解答]　(1) $\deg f(x)=3$ なので，$\mathbb{Q}$ 上既約でないとすると $f(x)$ は $\mathbb{Q}$ 上で根をもつ. 命題 1.12.4 より根の候補は ±1 のみである. しかし $f(\pm1)=1\neq0$ よりこれは矛盾. よって $f(x)$ は既約.
(2) 例題 2.7.3 と同様に解く.$\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ 上の基底 $\{1,\alpha,\alpha^2\}$ に対し，関係式 $\alpha^3-\alpha+1=0$ を利用すると

$$\begin{cases}\beta\cdot1 &= +1\cdot1+1\alpha+1\alpha^2\\ \beta\cdot\alpha &= -1\cdot1+2\alpha+1\alpha^2\\ \beta\cdot\alpha^2&= -1\cdot1-0\alpha+2\alpha^2\end{cases}\quad\Longrightarrow\quad P=\begin{pmatrix}1&1&1\\-1&2&1\\-1&0&2\end{pmatrix}$$

なので，β は $\det(xI-P)=x^3-5x^2+10x-7$ の根.$\beta\notin\mathbb{Q}$ で $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$ は素数なので，$\mathbb{Q}(\beta)=\mathbb{Q}(\alpha)$. したがって $x^3-5x^2+10x-7$ が β の最小多項式.
※ α の共役が分からないため，問題 3.1.15 の別解のようには解けない.
(3) (2) より

$$\begin{aligned}\beta^3-5\beta^2+10\beta-7&=0\\ \beta^{-1}&=-\frac{1}{7}(\beta^2-5\beta+10)\\ &=-\frac{1}{7}\alpha^2-\frac{2}{7}\alpha+\frac{4}{7}\end{aligned}\quad\square$$

3.1.17

$\mathrm{Aut}^{\mathrm{al}}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))=\{1\}$ であることを証明せよ.

[解答]　$\phi\in\mathrm{Aut}^{\mathrm{al}}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$ とする. 命題 3.1.13(1) より $\mathbb{Q}$ 準同型は生成元の値により定まるので，$\phi(\sqrt[3]{2})$ により ϕ は定まる. よって $\phi(\sqrt[3]{2})$ を調べよう. 例 3.1.30 より $\sqrt[3]{2}$ の共役は 1 の原始 3 乗根 ω を用いて $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ であるので，命題 3.1.31 より共役に移るので $\phi(\sqrt[3]{2})=\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$. しかし $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2\notin\mathbb{R}$ より $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2\notin\mathbb{Q}(\sqrt[3]{2})$ であるので，$\phi(\sqrt[3]{2})=\sqrt[3]{2}$ しかあり得ない. 命題 3.1.13(1) よりこれは $\phi=1$ であることを意味するので，題意は示された.　$\square$

3.1.18

$\alpha=\sqrt{2}+\sqrt{-1}$ とする.$\alpha-\sqrt{2}$ を考えることなどにより，α の $\mathbb{Q}$ 上の最小多項式を求めよ.

[解答]

$$\begin{aligned}\alpha-\sqrt{2}&=\sqrt{-1}\\ \alpha^2-2\sqrt{2}\alpha+2&=-1\\ \alpha^2+3&=2\sqrt{2}\alpha\\ \alpha^4+6\alpha^2+9&=8\alpha^2\\ \alpha-2\alpha^2+9&=0\end{aligned}$$

よって x^4-2x^2+9 が α の $\mathbb{Q}$ 上の最小多項式であることを示す. 上の式変形から $\sqrt{2}=\frac{\alpha^2+3}{2\alpha}$ より $\sqrt{2}\in\mathbb{Q}(\alpha)$. つまり $\mathbb{Q}(\alpha)\supset\mathbb{Q}(\sqrt{2})$. また α は実数でないので $\alpha\notin\mathbb{Q}(\sqrt{2})$ で $[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})]\geq 2$.$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ を利用すれば

$$[\mathbb{Q}(\alpha):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]\geq 4$$

これは α の $\mathbb{Q}$ 上の最小多項式の次数は 4 次以上であることを意味するので，x^4-2x^2+9 が求める最小多項式であることが示された. □

3.1.19

$\alpha=\sqrt[3]{2}+\sqrt{2}$ とする.$\alpha-\sqrt{2}$ を考えることなどにより，α の $\mathbb{Q}$ 上の最小多項式を求めよ.

[解答]

$$\begin{aligned}\alpha-\sqrt{2}&=\sqrt[3]{2}\\ \alpha^3-3\sqrt{2}\alpha^2+6\alpha-2\sqrt{2}&=2\\ \alpha^3+6\alpha-2&=\sqrt{2}(3\alpha^2+2)\\ \alpha^6+36\alpha^2+4+12\alpha^4-24\alpha-4\alpha^3&=2(9\alpha^4+12\alpha^2+4)\\ \alpha^6-6\alpha^4-4\alpha^3+12\alpha^2-24\alpha-4&=0\end{aligned}$$

よって $x^6-6x^4-4x^3+12x^2-24x-4$ が α の $\mathbb{Q}$ 上の最小多項式であることを示す. 上の式変形から $\sqrt{2}=\frac{\alpha^3+6\alpha-2}{3\alpha^2+2}$ より $\sqrt{2}\in\mathbb{Q}(\alpha)$. また $\sqrt[3]{2}=\alpha-\sqrt{2}$ より $\sqrt[3]{2}\in\mathbb{Q}(\alpha)$. つまり $\mathbb{Q}(\alpha)\supset\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt[3]{2})$. これは $[\mathbb{Q}(\alpha):\mathbb{Q}]$ が $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2,[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$ の倍数であることを意味する. よって $[\mathbb{Q}(\alpha):\mathbb{Q}]\geq 6$ である. つまり α の $\mathbb{Q}$ 上の最小多項式の次数は 6 次以上であるので，$x^6-6x^4-4x^3+12x^2-24x-4$ が求める最小多項式であることが示された. □

3.2.1

$[\overline{\mathbb{Q}}:\mathbb{Q}]=\infty$ であることを証明せよ.

[解答] $[\overline{\mathbb{Q}}:\mathbb{Q}]\neq\infty$ と仮定すると，$\exists n\in\mathbb{N}$, $[\overline{\mathbb{Q}}:\mathbb{Q}]=n$ となる. このとき $\sqrt[n+1]{2}\in\overline{\mathbb{Q}}$ について $(\sqrt[n+1]{2})^{n+1}-2=0$ で，アイゼンシュタインの判定法 (定理 1.12.11) より $\sqrt[n+1]{2}$ の $\mathbb{Q}$ 上の最小多項式は $x^{n+1}-2$ であることが分かる. よって $[\mathbb{Q}(\sqrt[n+1]{2}):\mathbb{Q}]=n+1$ であるが，$\overline{\mathbb{Q}}\supset\mathbb{Q}(\sqrt[n+1]{2})$ より

$$n=[\overline{\mathbb{Q}}:\mathbb{Q}]=[\overline{\mathbb{Q}}:\mathbb{Q}(\sqrt[n+1]{2})][\mathbb{Q}(\sqrt[n+1]{2}):\mathbb{Q}]\geq n+1$$

となり矛盾する. したがって背理法により題意は示された. □

3.2.2

$K=\mathbb{C}(x)$ を 1 変数有理関数体とする.$[\overline{K}:K]=\infty$ であることを証明せよ.

[解答]　前問 3.2.1 と同様に示す.$[\overline{K}:K]\neq\infty$ と仮定すると，$\exists n\in\mathbb{N},\ [\overline{K}:K]=n$ となる. このとき $\sqrt[n+1]{x}\in\overline{K}$ について $(\sqrt[n+1]{x})^{n+1}-x=0$ である. さらに $\mathbb{C}[t]$ は一意分解環 (命題 1.11.22) より，アイゼンシュタインの判定法 (定理 1.12.11) が使えるので，$\sqrt[n+1]{x}$ の K 上の最小多項式は $t^{n+1}-x$ であることが分かる (※例題 1.7.14(2) より x は $\mathbb{C}[x]$ の素元). よって $[K(\sqrt[n+1]{x}):K]=n+1$ であるが，$\overline{K}\supset K(\sqrt[n+1]{x})$ より

$$n=[\overline{K}:K]=[\overline{K}:K(\sqrt[n+1]{x})][K(\sqrt[n+1]{x}):K]\geq n+1$$

となり矛盾する. したがって背理法により題意は示された.　□

3.3.1

次の $\mathbb{F}_p$ 上の多項式が重根を持つ p をすべて求めよ.

(1) $f(x)=x^3+3x^2+5$　　(2) $f(x)=x^4+4x+6$

[解答]　例題 3.3.7 のユークリッドの互除法を用いた方法で解く.

(1) $f'(x)=3x^2+6x$ なので，$p=3$ のとき (※後のユークリッドの互除法の途中で分母に 3 が出現するため個別に調べる必要がある)$f'(x)=0$ となり重根を持つ.$p=2$ のとき $f(x)=f'(x)\left(\frac{1}{3}x+\frac{1}{3}\right)-2x+5=1$ となり重根を持たない.$p\neq 2,3$ のとき，さらに互除法を続けて $f'(x)=(-2x+5)\left(-\frac{3}{2}x-\frac{27}{4}\right)-\frac{135}{4}$. そのため $f(x)$ が重根を持つ $\Leftrightarrow\frac{135}{4}=0$ より $p=5$ のときのみ重根をもつ. よって求める p は $p=3,5$.

(2) $f'(x)=4x^3+4$ なので，$p=2$ のとき $f'(x)=0$ となり重根を持つ.$p=3$ のとき $f(x)=f'(x)\cdot\frac{1}{4}x+3x+6=f'(x)\cdot\frac{1}{4}x$ となり重根を持つ (系 3.3.4).$p\neq 2,3$ のとき，さらに互除法を続けて $f'(x)=(x+2)(4x^2-8x+16)-28$(※単元倍は最大公約数への影響を無視できるので $3x+6$ の代わりに $x+2$ を考えた). そのため $f(x)$ が重根を持つ $\Leftrightarrow 28=0$ より $p=7$ のときのみ重根をもつ. よって求める p は $p=2,3,7$.　□

3.3.2

K を標数 2 の体，$f(x)=x^2+ax+b\in K[x]$ を K 上既約な分離多項式とする.$\alpha_1,\alpha_2\in\overline{K}$ が $f(x)$ の根なら，(1) $a,\alpha_1\neq 0$, (2) $\alpha_2/\alpha_1\notin K$ を証明せよ.

[解答]　(1) $\mathrm{ch}K=2$ より $f'(x)=2x+a=a$ となる. そのため $a=0$ とすると $f'(x)=0$ となり，これは命題 3.3.3 より $f(x)$ が重根を持つことを意味し $f(x)$ の分離性に矛盾. よって $a\neq 0$ である. またもし $\alpha_1=0$ とすると $\alpha\in K$ より $f(x)$ は K 上で根をもつので既約性に矛盾. よって $\alpha_1\neq 0$ となる.

(2) (1) より $\alpha_1\neq 0$ なので解と係数の関係から $\alpha_1\alpha_2=b\Leftrightarrow\alpha_2/\alpha_1=b/\alpha_1^2$. よって $\alpha_2/\alpha_1\in K$ とすると $\alpha_1^2\in K$ となる. つまり α_1 の K 上の最小多項式として $x^2-\alpha_1^2$ が取れる.$f(x)$ も α_1 の最小多項式であり，最小多項式の一意性から $a=0$ となる必要がある. これは (1) の $a\neq 0$ に矛盾する. したがって題意は示された.　□

3.3.3

K を体，$f(x)=x^2+ax+b,\ g(x)=x^2+cx+d\in K[x]$ を 2 次の K 上既約な分離多項式，$\alpha_1,\alpha_2\in\overline{K}$ を $f(x)$ の根，$\beta_1,\beta_2\in\overline{K}$ を $g(x)$ の根，$K(\alpha_1)(=K(\alpha_2))\neq K(\beta_1)$

(1) $\gamma_1=\alpha_1\beta_1+\alpha_2\beta_2,\ \gamma_2=\alpha_1\beta_2+\alpha_2\beta_1$ とするとき，$\gamma_1\neq\gamma_2$ であることを証明せよ.

(2) K 上の 2 次多項式 $h(x)$ で根が γ_1,γ_2 であるものを求めよ.

(3) $K(\gamma_1)$ は $K(\alpha_1,\beta_1)$ に含まれる K の 2 次拡大で，$K(\gamma_1)\neq K(\alpha_1),K(\beta_1)$ であることを証明せよ.

[解答] (1) $\gamma_1=\gamma_2$ とすると，分離性から $\beta_1\neq\beta_2$ なので

$$\begin{aligned}\alpha_1\beta_1+\alpha_2\beta_2&=\alpha_1\beta_2+\alpha_2\beta_1\\ \alpha_1(\beta_1-\beta_2)&=\alpha_2(\beta_1-\beta_2)\\ \alpha_1&=\alpha_2\end{aligned}$$

これは分離性から $\alpha_1\neq\alpha_2$ となることに矛盾するので，$\gamma_1=\gamma_2$ となる.

(2) γ_1,γ_2 が根である K 上の 2 次多項式 $h(x)=x^2+ex+f$ があるとすると，解と係数の関係から $-e=\gamma_1+\gamma_2,\ f=\gamma_1\gamma_2$ となる必要がある. そこで $f(x),g(x)$ についての解と係数の関係から $\alpha_1+\alpha_2=-a,\ \alpha_1\alpha_2=b,\ \beta_1+\beta_2=-c,\ \beta_1\beta_2=d$ であることを利用すると

$$\begin{aligned}&\gamma_1+\gamma_2\\ &=(\beta_1+\beta_2)\alpha_1+(\beta_2+\beta_1)\alpha_2\\ &=(\alpha_1+\alpha_2)(\beta_1+\beta_2)\\ &=ac\end{aligned}$$

$$\begin{aligned}&\gamma_1\gamma_2\\ &=\alpha_1^2\beta_1\beta_2+\alpha_1\alpha_2\beta_1^2+\alpha_1\alpha_2\beta_2^2+\alpha_2^2\beta_1\beta_2\\ &=\alpha_1\alpha_2(\beta_1^2+\beta_2^2)+\beta_1\beta_2(\alpha_1^2+\alpha_2^2)\\ &=\alpha_1\alpha_2[(\beta_1+\beta_2)^2-2\beta_1\beta_2]+\beta_1\beta_2[(\alpha_1+\alpha_2)^2-2\alpha_1\alpha_2]\\ &=b(c^2-2d)+d(a^2-2b)\\ &=a^2d+bc^2-4bd\end{aligned}$$

となる必要がある. 逆に係数をこのように定めればその解は γ_1,γ_2 となるので，求める多項式は $h(x)=x^2-acx+a^2d+bc^2-4bd$ となる.

※問題によって天下り的に γ_1,γ_2 を根にもつ 2 次多項式 $h(x)$ の存在が分かっているから，この解法が通じるようにみえる. しかし $\gamma_1\in K(\alpha,\beta)$ は $\mathrm{Hom}_K^{\mathrm{al}}(K(\alpha,\beta),\overline{K})$ の元を作用させても γ_1,γ_2 のどちらかにしか移らないことが言える. これは命題 3.3.15 から γ_1 の共役が γ_1,γ_2 のみだと言えるので，γ_1 の最小多項式として 2 次多項式 $h(x)$ の存在が天下り的ではなくあらかじめ分かっているのである.

(3) $K(\alpha_1,\beta_1)\supset K(\gamma_1)$ は明らかなので，K の 2 次拡大であることと $K(\gamma_1)\neq K(\alpha_1),K(\beta_1)$ を示せばよい. しかし $K(\gamma_1)\neq K(\alpha_1)$ を示せば $\gamma_1\notin K(\alpha_1)$ より $\gamma_1\notin K$ で，これは $K(\gamma_1)$ が 1 次より大きい拡大であることを意味する. さらに (2) より γ_1 を根とする K 上の 2 次多項式 $h(x)$ が存在するので $K(\gamma_1)$ は K の 2 次拡大であることが言える. また α_1,β_1 は対称的なので，$K(\gamma_1)\neq K(\alpha_1)$ が示さ

れれば $K(\gamma_1) \neq K(\beta_1)$ も言える. よって $K(\gamma_1) \neq K(\alpha_1)$ を示せば十分.
背理法により示すため $K(\gamma_1) = K(\alpha_1)$ とする. このとき $\gamma_1, \gamma_2 = ac - \gamma_1 \in K(\alpha)$ であることに注意.
ch$K \neq 2$ のとき　解と係数の関係から

$$\gamma_1 - \gamma_2 = \alpha_1(\beta_1 - \beta_2) - \alpha_2(\beta_1 - \beta_2) = (\alpha_1 - \alpha_2)(\beta_1 - \beta_2)$$

分離性より $\alpha_1 - \alpha_2 \neq 0$ であるので $\beta_1 - \beta_2 = \beta_1 - (-c - \beta_1) = 2\beta_1 + c$ は $K(\alpha)$ の元. つまり $2\beta_1 \in K(\alpha).2 \neq 0$ であるので $\beta_1 \in K(\alpha_1)$ となり，これは $K(\alpha_1) \neq K(\beta_1)$ に矛盾.
ch$K = 2$ のとき　同様に解と係数の関係から

$$\alpha_1\gamma_1 - \alpha_2\gamma_2 = \alpha_1^2\beta_1 + b\beta_2 - b\beta_2 - \alpha_2^2\beta_1 = -a(\alpha_1 - \alpha_2)\beta_1$$

より $-a(\alpha_1 - \alpha_2)\beta_1 \in K(\alpha_1)$ となる. 分離性より $\alpha_1 - \alpha_2 \neq 0$. また問題 3.3.2(1) より $a \neq 0$ であるので $\beta_1 \in K(\alpha_1)$ となる. これは $K(\alpha_1) \neq K(\beta_1)$ に矛盾. したがって背理法により題意は示された.
□

3.3.4

$K = \mathbb{F}_2(t)$ を $\mathbb{F}_2$ 上の 1 変数有理関数体とする.
(1) $f(x) = x^2 + x + t,\ g(x) = x^2 + x + t + 1$ は $\mathbb{F}_2(t)$ 上の既約な分離多項式であることを証明せよ.
(2) $\alpha, \beta \in \overline{K}$ をそれぞれ $f(x), g(x)$ の根とするとき，$K(\alpha) \neq K(\beta)$ であることを証明せよ.
(3) (1) の $f(x), g(x)$ に対して，前問 (2) の $h(x)$ を求めよ.

[解答]　(1) 命題 1.11.22 より $\mathbb{F}_2[t]$ は一意分解環であるので，命題 1.11.34 より $\mathbb{F}_2(t)$ 上の既約性は $\mathbb{F}_2[t]$ 上の既約性と考えてもよい. さらに $f(x), g(x)$ は 2 次多項式なので $\mathbb{F}_2[t]$ 上既約であることと，$\mathbb{F}_2[t]$ 上で根をもつことは同値. よって $f(x), g(x)$ が既約でないとすると，$f(x), g(x)$ は $\mathbb{F}_2[t]$ 上で根をもつ. 命題 1.12.4 よりそれぞれの根の候補は t の約元 $\pm 1, \pm t$，$t + 1$ の約元 $\pm 1, \pm(t + 1)$ となる. 実際に代入して計算すると $f(x), g(x)$ は 0 となることはないので矛盾する. よって $f(x), g(x)$ は既約. また $f'(x) = g'(x) = 1 \neq 0$ なので命題 3.3.5 より $f(x), g(x)$ は分離多項式である. よって題意は示された.
(2) ※ 4.15　アルティン-シュライアー理論での定理 4.15.4(2) の証明と同様.
$K(\alpha) = K(\beta)$ とすると $\exists c_0, c_1 \in K,\ \beta = c_0 + c_1\alpha$ と書ける. よって

$$\begin{aligned}
\beta^2 + \beta + t + 1 &= 0 \\
c_0^2 + c_1^2\alpha^2 + c_0 + c_1\alpha + t + 1 &= 0 \\
c_0^2 + c_1^2(-\alpha - t) + c_0 + c_1\alpha + t + 1 &= 0 \\
(-c_1^2 + c_1)\alpha + (c_0^2 - c_1^2 t + c_0 + t + 1) &= 0
\end{aligned}$$

$\alpha, 1$ の線形独立性から $c_1^2 - c_1 = 0 \Leftrightarrow c_1(c_1 - 1) = 0 \Leftrightarrow c_1 = 0, 1$ となる.$c_1 = 0$ とすると $\beta = c_0 \in K$ となり $g(x)$ の K 上既約性に矛盾. よって $c_1 = 1$ となり先ほどの式変形を続けると

$$c_0^2 + c_0 + 1 = 0$$

となる. つまり多項式 $x^2 + x + 1$ は K 上で根をもつ，すなわち可約である.(1) の既約性の議論と同様にして $x^2 + x + 1$ は既約であることが分かるので矛盾. したがって $K(\alpha) \neq K(\beta)$ となる.

(3) 問題 3.3.2(2) の解答で $a=c=1$, $b=t$, $d=t+1$ とおけばよいので,

$$h(x)=x^2-x+t+t+1=x^2+x+1$$

と求まる. □

3.3.5

K は体、L/K は分離代数拡大、$\alpha\in L$, $\{\phi(\alpha)\,|\,\phi\in \mathrm{Hom}_K^{\mathrm{al}}(L,\overline{K})\}=\{\alpha_1,\cdots,\alpha_n\}$ とする (ただし、左辺の重複を除いたものが右辺)。このとき、α の K 上の最小多項式は $(x-\alpha_1)\cdots(x-\alpha_n)$ であることを証明せよ。

[解答] α の最小多項式を $f(x)$ とおくと、L/K は分離代数拡大なので互いに異なる $\beta_1,\cdots,\beta_m\in\overline{K}$ $(m=\deg f(x))$ を用いて、

$$f(x)=(x-\beta_1)\cdots(x-\beta_m)$$

と書ける。よって $n=m$ かつ $\{\alpha_1,\cdots,\alpha_n\}=\{\beta_1,\cdots,\beta_m\}$ を示せばよい。しかし $\alpha_1,\cdots,\alpha_n,\beta_1,\cdots,\beta_m$ は重複を除いているので $\{\alpha_1,\cdots,\alpha_n\}=\{\beta_1,\cdots,\beta_m\}$ を示せば十分。
$\{\alpha_1,\cdots,\alpha_n\}\supset\{\beta_1,\cdots,\beta_m\}$ について示す。 β_i $(i=1,\cdots,m)$ について、命題 3.3.15 より $\exists\phi\in\mathrm{Hom}_K^{\mathrm{al}}(L,\overline{K})$ $\phi(\alpha)=\beta_i$ となる。したがって $\beta_i\in\{\phi(\alpha)\,|\,\phi\in\mathrm{Hom}_K^{\mathrm{al}}(L,\overline{K})\}=\{\alpha_1,\cdots,\alpha_n\}$。よって $\supset$ は示された。
次に $\{\alpha_1,\cdots,\alpha_n\}\subset\{\beta_1,\cdots,\beta_m\}$ を示す。こちらも命題 3.3.15 より各 α_i $(i=1,\cdots,n)$ は α の共役になるので $\beta_1,\cdots,\beta_m$ のどれかに一致するので、$\alpha_i\in\{\beta_1,\cdots,\beta_m\}$ となり $\subset$ は示された。
以上より題意は示された。 □

3.4.1

$L/M, M/K$ が体の正規拡大で L/K が正規拡大でない例を見つけよ.

[解答] $L=\mathbb{Q}(\sqrt[4]{2}), M=\mathbb{Q}(\sqrt{2}), K=\mathbb{Q}$ が例になっていることを示す. アイゼンシュタインの判定法 (定理 1.12.11) より $\sqrt[4]{2},\sqrt{2}$ の $\mathbb{Q}$ 上の最小多項式は x^4-2, x^2-2 であることが分かる. よって $\sqrt{2}$ の $\mathbb{Q}$ 上の共役は $\pm\sqrt{2}$ なので $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ は正規拡大, 一方 $\sqrt[4]{2}$ の $\mathbb{Q}$ 上の共役は $\pm\sqrt[4]{2},\pm\sqrt[4]{2}i$ で特に $\pm\sqrt[4]{2}i\notin\mathbb{Q}$ より $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ は正規拡大でない. また $(\sqrt[4]{2})^2=\sqrt{2}$ より $\mathbb{Q}(\sqrt[4]{2})\supset\mathbb{Q}(\sqrt{2})$ であり, $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=4, [\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ なので $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{2})]=2$ である. つまり $\sqrt[4]{2}$ の $\mathbb{Q}(\sqrt{2})$ 上の最小多項式は 2 次となるので, それは $x^2-\sqrt{2}$ である. これより $\sqrt[4]{2}$ の $\mathbb{Q}(\sqrt{2})$ 上の共役は $\pm\sqrt[4]{2}$ なので $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ は正規拡大. したがって題意は示された. □

3.4.2

$L, M\subset\overline{K}$ が K の拡大体で L/K が正規拡大なら, $L\cdot M$ は M の正規拡大であることを証明せよ.

[解答] 定理 3.4.2 の同値条件 (2) を使う (※初版では定理 3.4.2 の前提で“L/K が有限次拡大”となっているが, 第 2 版では削除されているように無限次でも成り立つ. よって無限次の場合の議論も含む). そこで $N=L\cdot M$ とおいて $\phi\in\mathrm{Hom}_M^{al}(N,\overline{K})$ について考える.$\alpha\in N$ とおくと $N=L\cdot M$

より

$$\alpha = \frac{f(l_1, \cdots, l_s, m_1, \cdots, m_t)}{g(l_1, \cdots, l_s, m_1, \cdots, m_t)}$$

$$l_1, \cdots, l_s \in L$$

$$m_1, \cdots, m_t \in M$$

$$s, t \in \mathbb{N} \cup \{0\},\ \frac{f}{g} \text{ は係数が } K \text{ の素体の元である } s+t \text{ 変数有理式}$$

と書ける. このとき ϕ の準同型性と M の元を不変に保つことから

$$\phi(\alpha) = \frac{f(\phi(l_1), \cdots, \phi(l_s), m_1, \cdots, m_t)}{g(\phi(l_1), \cdots, \phi(l_s), m_1, \cdots, m_t)}$$

ここで $\phi|_L \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{K})$ で L/K が正規拡大より $\phi(L) \subset L$. よって $\phi(l_i) = l_i' \in L$ $(i = 1, \ldots, s)$ とおけるので

$$\phi(\alpha) = \frac{f(l_1', \cdots, l_s', m_1, \cdots, m_t)}{g(l_1', \cdots, l_s', m_1, \cdots, m_t)}$$

となり，$\phi(\alpha) \in N$ となる. 定理 3.4.2(2) より $L \cdot M$ が M の正規拡大であることを意味するので，題意は示された. □

3.5.1

(a) $p = 3$ (b) $p = 5$ に対し，次の問に答えよ ((1) は $p = 3$ については，演習問題 1.12.2 に含まれる).

(1) $\mathbb{F}_p$ 上既約な 1 変数 x の 2 次多項式 $f_p(x)$ を一つみつけよ.

(2) $\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(f_p(x))$ において，α を x の剰余類とする.$\mathbb{F}_{p^2}^{\times}$ の生成元をみつけよ.

[解答] ※命題 1.11.38 より $\mathbb{F}_{p^2}^{\times}$ は巡回群となるので，確かに生成元が生成元が存在することに注意.

(a) $p = 3$ のとき (1) 演習問題 1.12.2 より $f_p(x)$ として $x^2 + 1$ がとれる.

(2) $|\mathbb{F}_9^{\times}| = 8$ より，位数 8 の元を探せばよい. 手を動かして探すと,

$$(\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha$$

$$(\alpha + 1)^4 = (2\alpha)^2 = 4\alpha^2 = -4 = -1$$

よって $\alpha + 1$ が生成元の一つとして取れる.

(b) $p = 5$ のとき (1) $\mathbb{F}_5$ のどの元を代入しても根を持たないことから $f_p(x)$ として $x^2 + 2$ がとれる.

※代入して確かめなくても $\mathbb{F}_5$ ではフェルマーの小定理より $x \neq 0 \Rightarrow x^4 - 1 = 0 \Leftrightarrow (x^2 - 1)(x^2 + 1) = 0 \Leftrightarrow x^2 = \pm 1$ となることから既約性はわかる.

(2) $|\mathbb{F}_{25}^{\times}| = 24$ より，位数 24 の元を探せばよい. 手を動かして探すと,

$$(\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha - 1$$

$$(\alpha + 1)^3 = (2\alpha - 1)(\alpha + 1) = 2\alpha^2 + \alpha - 1 = \alpha$$

$$(\alpha + 1)^{12} = [(\alpha + 1)^3]^4 = \alpha^4 = 4$$

$$(\alpha + 1)^8 = (\alpha + 1)^{3 \cdot 2 + 2} = \alpha^2(2\alpha - 1) = -4\alpha + 2 = \alpha + 2$$

※位数 $4, 6$ の場合がないのは，それらは 12 の約数なので計算が簡単な 12 の場合に 1 にならないことが言えれば，位数 $4, 6$ ともならないことが言えるため.

よって $\alpha + 1$ が生成元の一つとして取れる. □

3.7.1

次の体の拡大 L/K に対し，$L = K(\alpha)$ となる $\alpha \in L$ をそれぞれ一つみつけよ. なお，(4) では K は 1 変数有理関数体である.

(1) $K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$

(2) $K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$

(3) $K = \mathbb{Q},\ L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$

(4) $K = \mathbb{F}_3(t),\ L = K(\sqrt{t}, \sqrt{t+1})$

[解答]　定理 3.7.1 の条件を満たすような元を α とすればよい.

(1) 例題 3.1.34(1)(もしくは問題 3.1.12(1)) と同様にして $[L : K] = 4$ は示される.$\mathrm{ch}\, K = 0$ より L/K は分離拡大であるので，$|\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{\mathbb{Q}})| = [L : K] = 4$. また $\sqrt{2}, \sqrt{5}$ の $\mathbb{Q}$ 上の共役はそれぞれ $\pm\sqrt{2}, \pm\sqrt{5}$ であり $\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{\mathbb{Q}})$ の元は生成元 $\sqrt{2}, \sqrt{5}$ の行き先で決定される. 故に

$$\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{5}) = \sqrt{5}, \qquad \tau(\sqrt{2}) = \sqrt{2}, \quad \tau(\sqrt{5}) = -\sqrt{5}$$

となる $\sigma, \tau \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{\mathbb{Q}})$ が存在して $\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{\mathbb{Q}}) = \{\mathrm{id}_L, \sigma, \tau, \sigma\tau\}$ となるしかない. このとき

$$\mathrm{id}_L(\sqrt{2}+\sqrt{5}) = \sqrt{2}+\sqrt{5} \qquad \sigma(\sqrt{2}+\sqrt{5}) = -\sqrt{2}+\sqrt{5}$$
$$\tau(\sqrt{2}+\sqrt{5}) = \sqrt{2}-\sqrt{5} \qquad \sigma\tau(\sqrt{2}+\sqrt{5}) = -\sqrt{2}-\sqrt{5}$$

となるので，定理 3.7.1 より $\alpha = \sqrt{2}+\sqrt{5}$ と取れる.

(2) アイゼンシュタインの判定法 (定理 1.12.11) より $x^2 - 2, x^3 - 3$ がそれぞれ $\sqrt{2}, \sqrt[3]{3}$ の K 上の最小多項式. ここで問題 3.1.9 より $[K(\sqrt{2}) : K] = 2, [L : K(\sqrt{2})] = 3$ であるので $[L : K] = 6$ となる.L/K は明らかに分離拡大なので $|\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{\mathbb{Q}})| = [L : K] = 6$ となり，$\sqrt{2}, \sqrt[3]{3}$ の K 上の共役はそれぞれ $\pm\sqrt{2},\ \sqrt[3]{3}, \omega\sqrt[3]{3}, \omega^2\sqrt[3]{3}$ (ω は 1 の原始 3 乗根) なので,

$$\sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(\sqrt[3]{3}) = \sqrt[3]{3}, \quad \tau(\sqrt{2}) = \sqrt{2}, \quad \tau(\sqrt[3]{3}) = \omega\sqrt[3]{3}$$

となる $\sigma, \tau \in \mathrm{Hom}_K^{\mathrm{al}}(L, \overline{\mathbb{Q}})$ が存在して $\mathrm{Hom}_K^{\mathrm{al}}(L, \overline{\mathbb{Q}}) = \{\mathrm{id}_L, \tau, \tau^2, \sigma, \sigma\tau, \sigma\tau^2\}$ となるしかない. このとき

$$\mathrm{id}_L(\sqrt{2}+\sqrt[3]{3}) = \sqrt{2}+\sqrt[3]{3} \qquad \sigma(\sqrt{2}+\sqrt[3]{3}) = -\sqrt{2}+\sqrt[3]{3}$$
$$\tau(\sqrt{2}+\sqrt[3]{3}) = \sqrt{2}+\omega\sqrt[3]{3} \qquad \sigma\tau(\sqrt{2}+\sqrt[3]{3}) = -\sqrt{2}+\omega\sqrt[3]{3}$$
$$\tau^2(\sqrt{2}+\sqrt[3]{3}) = \sqrt{2}+\omega^2\sqrt[3]{3} \qquad \sigma\tau^2(\sqrt{2}+\sqrt[3]{3}) = -\sqrt{2}+\omega^2\sqrt[3]{3}$$

となるので，$\alpha = \sqrt{2}+\sqrt[3]{3}$ と取れる.

(3) ※ 4.9 クンマー理論を用いないと $[L : K] = 8$ の議論が大変なので，4.9 までの知識を仮定する. 1 の原始 2 乗根 -1 を $\mathbb{Q}$ は含むので $n = 2$ の場合の定理 4.9.7 が使える.$\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ 内で $\{2, 3, 5\}$ が生成する部分群を $R/(\mathbb{Q}^\times)^2$ と書く. 定理 4.9.7 から L/K はガロア拡大で $\mathrm{Gal}(L/K) \cong R/(\mathbb{Q}^\times)^2$ である. そこで $R/(\mathbb{Q}^\times)^2$ を調べる. 例 4.9.8 と同様に準同型

$$\mathbb{Z}^3 \ni (a, b, c) \mapsto 2^a 3^b 5^c \in R/(\mathbb{Q}^\times)^2$$

を考える. 素因数分解の一意性から $2^a 3^b 5^b \in (Q^\times)^2 \Leftrightarrow a, b, c \in (2\mathbb{Z})^3$ が成り立つので，準同型定理から $R/(\mathbb{Q}^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$ となる. よって $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/2\mathbb{Z})^3$ となり，$|\mathrm{Gal}(L/K)| = 8$ が得られる.

また $\sqrt{2},\sqrt{3},\sqrt{5}$ の K 上の共役は明らかに $\pm\sqrt{2},\pm\sqrt{3},\pm\sqrt{5}$ なので，

$$\begin{aligned}
&\sigma(\sqrt{2})=-\sqrt{2}, && \sigma(\sqrt{3})=\sqrt{3}, && \sigma(\sqrt{5})=\sqrt{5},\\
&\tau(\sqrt{2})=\sqrt{2}, && \tau(\sqrt{3})=-\sqrt{3}, && \tau(\sqrt{5})=\sqrt{5},\\
&\upsilon(\sqrt{2})=\sqrt{2}, && \upsilon(\sqrt{3})=\sqrt{3}, && \upsilon(\sqrt{5})=-\sqrt{5}
\end{aligned}$$

となる.$\sigma,\tau,\upsilon\in\mathrm{Gal}(L/K)$ が存在して $\mathrm{Gal}(L/K)=\langle\sigma,\tau,\upsilon\rangle$ となるしかない. このとき

$$\begin{aligned}
&\mathrm{id}_L(\sqrt{2}+\sqrt{3}+\sqrt{5})=\sqrt{2}+\sqrt{3}+\sqrt{5} && \sigma(\sqrt{2}+\sqrt{3}+\sqrt{5})=-\sqrt{2}+\sqrt{3}+\sqrt{5}\\
&\tau(\sqrt{2}+\sqrt{3}+\sqrt{5})=\sqrt{2}-\sqrt{3}+\sqrt{5} && \sigma\tau(\sqrt{2}+\sqrt{3}+\sqrt{5})=-\sqrt{2}-\sqrt{3}+\sqrt{5}\\
&\upsilon(\sqrt{2}+\sqrt{3}+\sqrt{5})=\sqrt{2}+\sqrt{3}-\sqrt{5} && \sigma\upsilon(\sqrt{2}+\sqrt{3}+\sqrt{5})=-\sqrt{2}+\sqrt{3}-\sqrt{5}\\
&\tau\upsilon(\sqrt{2}+\sqrt{3}+\sqrt{5})=\sqrt{2}-\sqrt{3}-\sqrt{5} && \sigma\tau\upsilon(\sqrt{2}+\sqrt{3}+\sqrt{5})=-\sqrt{2}-\sqrt{3}-\sqrt{5}
\end{aligned}$$

となるので，$\alpha=\sqrt{2}+\sqrt{3}+\sqrt{5}$ と取れる.

(4) $\sqrt{t}$ の K 上の最小多項式はアイゼンシュタインの判定法 (定理 1.12.11) より x^2-t である ($\mathbb{F}_3[t]$ は一意分解環 (例 1.11.36) なので判定法は使える). よって $[K(\sqrt{t}):K]=2$ となる. また $\sqrt{t+1}\in K(\sqrt{t})$ とすると，$\exists a,b\in K$ $\sqrt{t+1}=a+b\sqrt{t}$ となる. 両辺を 2 乗して整理すれば $t+1=(a^2+b^2t)+2ab\sqrt{t}$ となり $\sqrt{t},1$ は線形独立なので $a^2+b^2t=t+1, ab=0$ となる.$ab=0$ より $a=0$ または $b=0$ であるが，$a=0$ なら $b^2t=t+1$ となる.$b=\frac{f}{g}\in K$ とおくと $tf^2=(t+1)g^2$ が $\mathbb{F}_3[t]$ で成り立つが，$\mathbb{F}_3[t]$ は一意分解環で両辺の素元 t の個数の偶奇が異なるので矛盾. 一方 $b=0$ としても $a^2=t+1$ となり，これは $x^2-(t+1)=0$ はアイゼンシュタインの判定法 (定理 1.12.11) より K 上既約であることに矛盾. よって $\sqrt{t+1}\notin K$ となるので，$x^2-(t+1)$ が $K(\sqrt{t})$ 上の $\sqrt{t+1}$ の最小多項式となる. このことから $[L:K]=4$ が分かる. また $\sqrt{t},\sqrt{t+1}$ の共役は $\pm\sqrt{t},\pm\sqrt{t+1}$ であることから，$\sqrt{t},\sqrt{t+1}$ は K 上分離的なので L/K は分離拡大. よって $\mathrm{Hom}_K^{\mathrm{al}}(L,\overline{K})=[L:K]=4$ である. よって

$$\sigma(\sqrt{t})=-\sqrt{t},\quad \sigma(\sqrt{t+1})=\sqrt{t+1},\quad \tau(\sqrt{t})=\sqrt{t},\quad \tau(\sqrt{t+1})=-\sqrt{t+1}$$

となる $\sigma,\tau\in\mathrm{Hom}_K^{\mathrm{al}}(L,\overline{K})$ が存在して $\mathrm{Hom}_K^{\mathrm{al}}(L,\overline{K})=\{\mathrm{id}_L,\sigma,\tau,\sigma\tau\}$ となるしかない. このとき

$$\begin{aligned}
&\mathrm{id}_L(\sqrt{t}+\sqrt{t+1})=\sqrt{t}+\sqrt{t+1} && \sigma(\sqrt{t}+\sqrt{t+1})=-\sqrt{t}+\sqrt{t+1}\\
&\tau(\sqrt{t}+\sqrt{t+1})=\sqrt{t}-\sqrt{t+1} && \sigma\tau(\sqrt{t}+\sqrt{t+1})=-\sqrt{t}-\sqrt{t+1}
\end{aligned}$$

となるので，$\alpha=\sqrt{t}+\sqrt{t+1}$ と取れる. □

3.7.2

$p>0$ を素数，$L=\mathbb{F}_p(x,y)$ を $\mathbb{F}_p$ 上の 2 変数有理関数体，$K=\mathbb{F}_p(x^p,y^p)$ とする.

(1) L/K は単拡大ではないことを証明せよ.

(2) L/K には中間体が無限個存在することを証明せよ.

[解答] (1) まず $[L:K]=p^2$ を示す.$x\in L$ の K 上の最小多項式はアイゼンシュタインの判定法 (定理 1.12.11) より t^p-x^p である. また $y\in L$ の $K(x)$ 上の多項式もアイゼンシュタインの判定法 (定理 1.12.11) より t^p-y^p となる. よって $[L:K(x)]=[K(x):K]=p$ なので $[L:K]=p^2$ となる. 次に $x\in L\Rightarrow x^p\in K$ を示す.$f(x,y)\in\mathbb{F}_p[x,y]$ とおくと補題 3.1.4 より $f(x,y)^p=f(x^p,y^p)$ となるので

(係数はフェルマーの小定理 (系 I-2.6.24) より不変であることに注意)，$f(x,y)^p \in L$ となる. よって $\mathbb{F}_p[x,y]$ の商体 L 上において $x \in L \Rightarrow x^p \in K$ となることがわかる. 故に L/K が単拡大であるとすると，$\alpha \in K$ を用いて $L = K(\alpha)$ となるが，$[L:K] = p^2$ より，その K 上の最小多項式は p^2 次. しかしこれは $x \in L \Rightarrow x^p \in K$ より $\alpha^p \in K$ であることに矛盾. したがって示された.

※ $t^p - x^p$ が K 上の最小多項式であることの別証として次のようなものもある ([1] より).ch$K = p$ より $t^p - x^p = (t-x)^p$ であるので，x の最小多項式は $(t-x)^d$ $(d \leq p)$ という形をしている. もし $d < p$ ならこの多項式の定数項は K に属することから，$x^d \in K$ となり明らかに矛盾するからである (もう少し厳密に示すなら，$x^d \in K$ とすると $x = \frac{f}{g} \in K$ とおけて，$x^d g = f$ より $\deg g + d = \deg f$ が成り立つが $\deg f, \deg g$ が p の倍数であることより矛盾を示せる). よって $x \in L$ の K 上の最小多項式は $t^p - x^p$ となる. 同様にして $t^p - y^p$ が $K(x)$ 上の最小多項式となることも示せる.

(2) ※ [1] を参考にした.

$L \setminus K \neq \emptyset$ より，適当な $z \in L \setminus K$ を取ってきて中間体 $K(z)$ を考えられる. このとき (1) の議論から $[K(z):K] = p$ である.$K(z) \neq L$ より $z' \in L \setminus K(z)$ となる z' が取れる. このとき各 $c \in K$ に対して定まる中間体 $M_c = K(z + cz')$ について考える. 仮に中間体が無限個存在しないとすると，K は無限体なので $c \neq c'$ で $M_c = M_{c'} =: M$ となる $c, c' \in K$ が存在することになる.$z + cz', z + c'z' \in M$ であるので $\frac{(z+cz')-(z+c'z')}{c-c'} = z' \in M$ となる. さらに $(z + cz') - cz' = z \in M$ ともなる. つまり $K(z) \subset M$ で $z' \notin K(z), z' \in M$ である.$[L:K] = p^2$ の約数は $1, p, p^2$ のみで $[M:K(z)] > 1$ より $[M:K] = p^2$ となる. これは $L = M = K(z + cz')$ となることを意味し，(1) の L が単拡大ではないことに矛盾. したがって題意は示された. □

3.7.3

(1) L/K が無限次代数拡大なら，L/K は単拡大ではないことを証明せよ.

(2) 分離代数拡大で単拡大でない例を一つみつけよ.

[解答] (1) 対偶「L/K が単拡大 $\Rightarrow$ L/K は無限次代数拡大でない」を示せばよい.

L/K を単拡大とする.L/K が代数拡大であるとすると明らかに主張は成り立つので，代数拡大としてもよい. このとき系 3.1.18(3) から L/K は有限次拡大となるため，無限次拡大ではなくなる. よって示された.

(2) $\overline{\mathbb{Q}}/\mathbb{Q}$ が求める例の一つとなっていることを示す. 問題 3.2.1 より $\overline{\mathbb{Q}}/\mathbb{Q}$ は無限次拡大なので，(1) より単拡大でない. また系 3.3.12 より $\mathbb{Q}$ は完全体なので，$\overline{\mathbb{Q}}/\mathbb{Q}$ は分離拡大となる. したがって $\overline{\mathbb{Q}}/\mathbb{Q}$ が求める例の一つである. □

第 4 章

参考文献

[1] 数学ちゃん. 雪江代数演習問題 3.7.2. https://note.com/shiny_broom989/n/nea5113cc22f9.