大学数学への接続シリーズ２

多項式の因数分解と体の拡大

（♯ガロア理論への入り口）

松田 修　著

2023 年 8 月 16 日

はじめに

多項式の因数分解，これは高校 1 年生で学習する．たとえば，

$$3x^2 - 10x + 8 = (x-2)(3x-4), \quad x^3 - x^2 + x - 1 = (x-1)(x^2+1)$$

などがある．上の 2 つの因数分解には違いがある．それは，x の 2 次式 $3x^2-10x+8$ が x の 1 次式 $(x-2)$ と $(3x-4)$ の積で表されるのに対し，x の 3 次式 x^3-x^2+x-1 は x の 1 次式 $(x-1)$ と，これ以上因数分解できない 2 次式 (x^2+1) の積で表されるということである．

「これ以上因数分解できない」とはどういうことだろうか．

本書は，大学の数学科で学ぶ「代数学」という分野で扱う「体論」と「環論」いう視点から，多項式の因数分解の考え方を説明する．具体的には，3 次多項式と 4 次多項式の因数分解の考え方について説明する．

それらは，5 次以上の多項式の因数分解の理論，さらにはガロア理論にも結び付いている．

目次

第 1 章

有理数係数の多項式の因数分解

多項式の因数分解，これは高校 1 年生で学習する．たとえば，

$$3x^2-10x+8=(x-2)(3x-4),\quad x^3-x^2+x-1=(x-1)(x^2+1)$$

などがある．上の 2 つの因数分解には違いがある．それは，x の 2 次式 $3x^2-10x+8$ が x の 1 次式 $(x-2)$ と $(3x-4)$ の積で表されるのに対し，x の 3 次式 x^3-x^2+x-1 は x の 1 次式 $(x-1)$ と，これ以上因数分解できない 2 次式 (x^2+1) の積で表されるということである．

「これ以上因数分解できない」とはどういうことだろうか．

1.1 「これ以上因数分解できない」の意味

因数分解 $3x^2-10x+8=(x-2)(3x-4)$ でわかることは，2 次方程式 $3x^2-10x+8=0$ の解が，$x=2$ と $x=\dfrac{4}{3}$ であるということである．このように，因数分解を与えられた式の解を求めるという意味で捉えると，$x-2$ や $3x-4$ などの 1 次式は，式の性質上，これ以上因数分解できない式である．しかし，x^2+1 の解は，虚数単位 $\sqrt{-1}=i$ を使って $x=\pm i$ と表される．したがって，3 次式 x^3-x^2+x-1 の因数分解を

$$x^3-x^2+x-1=(x-1)(x-i)(x+i)$$

と，してはいけないのだろうか？

３次式を１次式の積に分解できるのだから，因数分解は必ず１次式の積に分解するものという考え方のほうが，分かりやすいようにも思える．

それでは，４次式 $x^4-x^3+x^2-1$ の因数分解を考えよう．$x=1$ は方程式 $x^4-x^3+x^2-1=0$ の解なので，因数定理を使うと，

$$x^4-x^3+x^2-1=(x-1)(x^3+x+1)$$

という分解まではわかる．問題は，３次式 x^3+x+1 を３つの１次式の積とするために，どのような数を用いて分解するかである．そのためには，３次方程式

$$x^3+x+1=0$$

を解けばよい．そしてこの３次方程式の３つの解 x_1,x_2,x_3 がわかると，

$$x^3+x+1=(x-x_1)(x-x_2)(x-x_3)$$

と因数分解できることになる．しかしこの方程式を解くことは，２次方程 $x^2+1=0$ を解くことに比べてはるかに難しい．

この３次方程式を解くことの難しさは，３つの解 x_1,x_2,x_3 が，明らかにどれも有理数でないという点にある．そうなると，x_1,x_2,x_3 は，２乗根の記号 $\sqrt{\ }$ や３乗根の記号 $\sqrt[3]{\ }$，さらには i を含んだ数になることが想像される．実際，３次方程式の解法にはカルダノの公式というものが知られており，それを用いると，$\sqrt{\ }$ や $\sqrt[3]{\ }$ や i を使って，x_1,x_2,x_3 を求めることができる．

実は，４次方程式の解法にもフェラーリの公式というものが知られており，４次方程式の解は，$\sqrt{\ }$，$\sqrt[3]{\ }$，$\sqrt[4]{\ }$ そして i を使って，解 x_1,x_2,x_3,x_4 を求めることができる．したがって，どんな４次式もフェラーリの公式を使って求めた解 x_1,x_2,x_3,x_4 から，$(x-x_1)(x-x_2)(x-x_3)(x-x_4)$ などのような形として１次式の因数分解が完成する．

しかし，５次方程式については，一般にその解を $\sqrt{\ }$，$\sqrt[3]{\ }$，$\sqrt[4]{\ }$，$\sqrt[5]{\ }$ そして i を使って，求めることができないことが，アーベルやガロアといった１９世紀の若き数学者たちによって証明されている．６次以上の方程式についても同様である．

話を元に戻す．高校の数学では，x^2+1 や x^3+x+1 などはこれ以上因数分解できない式であるとされている．それは，方程式 $x^2+1=0$ と $x^3+x+1=0$ は，どちらも方程式のすべての解が有理数でないからである．つまり，与えられた式のすべての解が有理数でないとき，その式はこれ以上因数分解できないとされているのである．

これ以上因数分解できない式は，**既約多項式**と呼ばれているのだが，x^2+1 や x^3+x+1 について正確に述べると，これらは，有理数体 $\mathbb{Q}$ 上の多項式環 $\mathbb{Q}[x]$ での既約多項式である．ここに，“体”，“環”などの言葉を使ったが，これらの概念の意味を，以下で説明していく．

1.2　有理数体 $\mathbb{Q}$

有理数体 $\mathbb{Q}$ とは，有理数全体の集合のことである．そして $\mathbb{Q}$ は，$\mathbb{Q}$ に属する任意の 2 つの数の演算結果が $\mathbb{Q}$ に属するという特徴をもつ．

ここで，体という言葉を用いたが，一般に**体**とは，簡単に言えば，四則演算が定義された集合のことである．

四則演算とは，和，差，積，商という演算のことであるが，a, b を有理数とすると，差 $a-b$ については，$a-b=a+(-b)$ とできるため，和の演算として扱うことができる．同様に，商 a/b についても $a/b=a\times\dfrac{1}{b}$ とできるため，積の演算として扱うことができる．

ここで，有理数 a に対して $-a$ を a の**反対元**という．反対元の正確な定義は，a に対して，$a+a'=0$ となる a' のことで，この a' を $-a$ と表すのである．

0 でない有理数 x に対して $\dfrac{1}{x}$ を x の**逆元**という．逆元の正確な定義は，0 でない x に対して，$x\times x'=1$ となる x' のことで，この x' を $\dfrac{1}{x}$ と表すのである．

体の正確な定義を述べよう．

定義（体）集合 F には 2 つの内部演算 $+$（加法）と $\cdot$（乗法）が定義されていて，F の任意の元 a, b, c に対して，以下の全ての性質が成り立つとき，F を**体**と呼ぶ．

(1) $a+b=b+a$，$a\cdot b=b\cdot a$

(2) $(a+b)+c=a+(b+c)$，$(a\cdot b)\cdot c=a\cdot(b\cdot c)$

(3) $a+0=0+a$ となる 0 という元（**零元**）が存在する．

(4) $a\cdot 1=1\cdot a$ となる 1 という元（**単位元**）が存在する．

(5) $a+a'=0$ となる a' という元（a の反対元）が存在する．

(6) $b\cdot b'=1$ となる b' という元（b の逆元）が存在する．

(7) $a\cdot(b+c)=ab+bc$，$(a+b)\cdot c=ac+bc$

実数全体の集合 $\mathbb{R}$ も，複素数全体の集合 $\mathbb{C}$ も体である．しかし，整数全体の集合 $\mathbb{Z}$ は体ではない．

問題 1.1. 整数全体の集合 $\mathbb{Z}$ は体でないを証明せよ．

1.3　有理数体 $\mathbb{Q}$ 上の多項式環 $\mathbb{Q}[x]$

次に，有理数体 $\mathbb{Q}$ 上の**多項式環** $\mathbb{Q}[x]$ について説明する．

$\mathbb{Q}[x]$ は，$\mathbb{Q}$ を係数とする x の多項式全体の集合を意味し，

$$\mathbb{Q}[x]=\{\ a_0+a_1x+a_2x^2+\cdots+a_nx^n \mid a_i\in\mathbb{Q}\ \}$$

のことである．

$f(x), g(x)\in\mathbb{Q}[x]$ とすると，$f(x)\pm g(x)\in\mathbb{Q}[x]$ であり，$f(x)g(x)\in\mathbb{Q}[x]$ であ

る．しかし，$f(x) \neq 0$ のとき，$\dfrac{1}{f(x)} \notin \mathbb{Q}[x]$ である．

環とは，和と差と積が定義された集合のことである．したがって，$\mathbb{Q}[x]$ は環である．このことから，$\mathbb{Q}[x]$ を有理数体 $\mathbb{Q}$ 上の多項式環と呼んでいる．

環の正確な定義を述べよう．

定義（環）集合 R には 2 つの内部演算 $+$（加法）と $\cdot$（乗法）が定義されていて，F の任意の元 a, b, c に対して，以下の全ての性質が成り立つとき，R を**環**と呼ぶ．

(1) $a + b = b + a$

(2) $(a + b) + c = a + (b + c)$，$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(3) $a + 0 = 0 + a$ となる 0 という元（**零元**）が存在する．

(4) $a + a' = 0$ となる a' という元（a の**反対元**）が存在する．

(5) $a \cdot (b + c) = ab + bc$，$(a + b) \cdot c = ac + bc$

環 R が，乗法において $ab = ba$ を満たすとき，R は**可換環**と呼ばれる．また，環 R が，$a \cdot 1 = 1 \cdot a$ となる 1 という元（**単位元**）が存在するとき，R は**単位的環**と呼ばれる．単位的環 R の元 a が乗法における逆元 a^{-1} を持つとき，a を**単元**という．

さて，R を単位的可換環とする．$a \in R$ に対して $ab = ba = 0$ となる 0 でない $b \in R$ が存在するとき，a を**零因子**という．そして，0 以外に零因子を持たない単位的可換環を**整域**という．

有理数体 $\mathbb{Q}$ 上の多項式環 $\mathbb{Q}[x]$ は，整域であり，さらに，$\mathbb{Q}[x]$ の単元は，有理数 $a \in \mathbb{Q}$ である．

問題 1.2. 整数全体の集合 $\mathbb{Z}$ は整域であること，さらに $\mathbb{Z}$ 上の多項式全体の集合 $\mathbb{Z}[x]$ も整域であることを証明せよ．

1.4　$\mathbb{Q}[x]$ の既約多項式

$\mathbb{Q}[x]$ の多項式 $f(x) = a_0 + a_1x + \cdots + a_nx^n$ （ただし $a_n \neq 0$, $a_j \in \mathbb{Q}$ ）を考える．このとき，n を f の**次数**と呼び，$\deg(f) = n$ で表す．次に，$\mathbb{Q}[x]$ の多項式 g の次数は $\deg(g) = m < n$ とする．g が f を割り切るとき，g を f の**因数**と呼ぶ．このとき，$f = gh$ で $\deg(h) = n - m$ となる f の因数 h が存在する．

$f \in \mathbb{Q}[x]$ は，$f = gh$ かつ $\deg(g), \deg(h) \geq 1$ となる多項式 g, h が $\mathbb{Q}[x]$ の中に存在しないとき，$\mathbb{Q}[x]$ の**既約多項式**と呼ばれる．明らかに，f が $\mathbb{Q}[x]$ の既約多項式ならば $-f$ も $\mathbb{Q}[x]$ の既約多項式である．

以下の定理は，次数に関する数学的帰納法で証明できる．

定理 1.1.　$f \in \mathbb{Q}[x]$ で $\deg(f) \geq 1$ とする．このとき，以下が成り立つ．
(1) f は $\mathbb{Q}[x]$ の既約多項式 $g_1, g_2, \cdots, g_r$ によって，

$$f = g_1g_2 \cdots g_r$$

と表される．
(2) f は $\mathbb{Q}[x]$ の既約多項式 $h_1, h_2, \cdots, h_s$ によって，

$$f = g_1g_2 \cdots g_r = h_1h_2 \cdots h_s$$

と表されたとする．このとき $r = s$ であり，適当に順番を変えれて $g_j = h_j$ または $g_j = -h_j$ とすることができる．

定理 1.1 は，$\mathbb{Q}[x]$ のどんな多項式も，既約多項式によって，順序と符号の差を除い

て一意的に因数分解されることを示している．

では，$f \in \mathbb{Q}[x]$ が既約多項式であるのか，そうでないか，このことを判定する方法はないのだろうか．

定理 1.2. $a_0, a_1, \cdots, a_n$ を整数，$a_n \neq 0$ とし，$f(x) = a_0 + a_1 x + \cdots + a_n x^n$ とする．このとき，p, q を互いに素な整数として $f(p/q) = 0$ となるならば，$f(x)$ は $\mathbb{Q}[x]$ の中で $(x - p/q)$ を因数にもち，さらに，p は a_0 の約数かつ q は a_n の約数である．

定理 1.2 は，高校 1 年生で学ぶ**因数定理**と呼ばれるものである．定理 1.2 は，$f(p/q) = 0$ となる互いに素な整数 p, q の候補が，p は a_0 の約数，q は a_n の約数であるといっているのであるから，どんな p, q の候補を考えても $f(p/q) \neq 0$ となるなら，$f(x)$ は $\mathbb{Q}[x]$ での既約多項式ということになる．

例 1.1. $f(x) = x^5 - 1$ を $\mathbb{Q}[x]$ で因数分解せよ．

解答．$f(1) = 0$ なので，因数定理より $f(x) = (x-1)(x^4 + x^3 + x^2 + x + 1)$ である．$g(x) = x^4 + x^3 + x^2 + x + 1$ と置く．定理 1.2 より，$g(x) = 0$ となる候補は $x \pm 1$ である．しかし，$g(1) \neq 0,\ g(-1) \neq 0$ である．よって，$g(x)$ は $\mathbb{Q}[x]$ の既約多項式である．したがって，$f(x)$ の因数分解は $f(x) = (x-1)(x^4 + x^3 + x^2 + x + 1)$ である．（解答終）

問題 1.3. $f(x) = x^4 - 2x^3 + 3x^2 - 5x - 2$ を $\mathbb{Q}[x]$ で因数分解せよ．

定理 1.2 において，a_0 や a_n が大きい数であると，$f(p/q) = 0$ となる互いに素な整数 p, q の候補も多くなる．つまり，$f(x)$ が $\mathbb{Q}[x]$ で既約多項式かどうかを判定するの

は大変である．次は，**アイゼンシュタインの既約判定法**と呼ばれているものである．

定理 1.3.　$f \in \mathbb{Q}[x]$ を $f(x) = a_0 + a_1x + \cdots + a_nx^n$ とする．このとき，ある素数 p が存在して，$a_0, a_1, \cdots, a_n$ が以下の (1),(2),(3) を全て満たすとき，f は $\mathbb{Q}[x]$ の既約多項式である．
(1) a_n 以外の a_j はすべて p の倍数である．
(2) a_n は p の倍数でない．
(3) a_0 は p^2 の倍数でない．

例 1.2. $f(x) = x^3 + 4x^2 + 10x + 12$ を $\mathbb{Q}[x]$ で因数分解せよ．

解答．$f(-2) = (-2)^3 + 4 \cdot (-2)^2 + 10 \cdot (-2) + 12 = 0$．よって，因数定理より $f(x) = (x+2)(x^2+2x+6)$ である．$g(x) = x^2 + 2x + 6$ と置くと，$a_0 = 6, a_1 = 2$ はどちらも $p = 2$ の倍数であり，$a_3 = 1$ は $p = 2$ の倍数でなく $a_0 = 6$ は $p^2 = 4$ の倍数でない．よって，定理 1.3 より，g は $\mathbb{Q}[x]$ の既約多項式である．よって，$f(x)$ の因数分解は $f(x) = (x+2)(x^2+2x+6)$ である．（解答終）

問題 1.4. $f(x) = 2x^4 + x^3 + 3x^2 - 6$ を $\mathbb{Q}[x]$ で因数分解せよ．

ところで，$f(x)$ に定理 1.3 が使えないときは，どうすればよいか？

一つの方法として，x を $x + c$ に置き換えた $f(x + c)$ に，定理 1.3 を使ってみるというアイディアがある．

その理由は，もし $f(x) = g(x)h(x)$ と分解されたとすると，

$$f(x + c) = g(x + c)h(x + c)$$

と分解されるし，逆に $f(x + c) = g'(x)h'(x)$ と分解されるならば，

$$f(x) = g'(x - c)h'(x - c)$$

と分解されるからである．このことを，定理としてまとめておく．

定理 1.4. $f \in \mathbb{Q}[x]$ を $f(x) = a_0 + a_1x + \cdots + a_nx^n$ とする．このとき，f が $\mathbb{Q}[x]$ であることと，ある有理数 c が存在して $f(x+c)$ が $\mathbb{Q}[x]$ で既約であることは同値である．

例 1.3. $f(x) = x^4 + x^3 + 12x^2 + 47x + 35$ を $\mathbb{Q}[x]$ で因数分解せよ．

解答．$f(-1) = 0$ なので，因数定理より $f(x) = (x+1)(x^3 + 12x + 35)$ である．$g(x) = x^3 + 12x + 35$ と置く．定理 1.3 は使えないので，$g(x-5) = (x-5)^3 + 12(x-5) + 35 = x^3 - 15x^2 + 87x - 150$ を考える．$a_0 = -150, a_1 = 87, a_2 = -15$ はどれも $p = 3$ の倍数であり，$a_3 = 1$ は $p = 3$ の倍数でなく $a_0 = -150$ は $p^2 = 9$ の倍数でない．よって，定理 1.4 より $g(x)$ は $\mathbb{Q}[x]$ の既約多項式である．したがって，$f(x)$ の因数分解は $f(x) = (x+1)(x^3 + 12x + 35)$ である．（解答終）

問題 1.5. $f(x) = x^4 - x^3 + 12x^2 + 13x - 25$ を $\mathbb{Q}[x]$ で因数分解せよ．

第 2 章

体 F 係数の多項式の因数分解

2.1 体 $\mathbb{Q}(\alpha)$ と環 $\mathbb{Q}(\alpha)[x]$ での因数分解

u を正の整数とし，x^2+ux+u^2 を因数分解することを考える．これは，環 $\mathbb{Q}[x]$ では因数分解できない．

そこで，$x^2+ux+u^2=0$ の解の一つを形式的に α として，因数定理を使って，左辺の多項式 x^2+ux+u^2 を無理やり因数分解してみる．結果は，

$$x^2+ux+u^2=(x-\alpha)\{x+(u+\alpha)\}$$

となる．確認のため，右辺を展開すると

$$(x-\alpha)\{x+(u+\alpha)\}=x^2+ux-(\alpha^2+\alpha u)$$

であるが，α は $x^2+ux+u^2=0$ の解なので，$\alpha^2+\alpha u=-u^2$ である．

明らかに，$\alpha\notin\mathbb{Q}$ である．そして，$u+\alpha$ は α の $\mathbb{Q}$ 係数の多項式である．したがって，多項式 x^2+ux+u^2 は，多項式環 $\mathbb{Q}[\alpha]$ の数 α と $u+\alpha$ を用いて因数分解することができたということになる．

ところで，多項式環 $\mathbb{Q}[\alpha]$ とは，

$$\mathbb{Q}[\alpha]=\{\ s+t\alpha\mid s,t\in\mathbb{Q}\}$$

のことである．α^n（$n \geq 2$）の項がないのは，α が $x^2 + ux + u^2 = 0$ の解であるため

$$\alpha^2 = -u\alpha - u^2,\ \ \alpha^3 = -u\alpha^2 - u^2\alpha = u^3,\ \ \alpha^4 = -u^4\alpha - u^5,\ \ \cdots$$

などとなるためである．

次に，$s + t\alpha \neq 0$ のとき，$\dfrac{1}{s + t\alpha}$ の分母の有理化が可能かどうかを考えよう．解と係数の関係式を使うと，$x^2 + ux + u^2 = 0$ の α 以外のもう一つの解は，$-u - \alpha$ である．したがって，$s + t\alpha$ に $s - t(u + \alpha)$ を掛けてみる．

$$\begin{aligned}\frac{1}{s + t\alpha} &= \frac{s - t(u + \alpha)}{(s + t\alpha)\{s - t(u + \alpha)\}} = \frac{s - t(u + \alpha)}{s^2 + ust + t^2(u\alpha + \alpha^2)} \\ &= \frac{(s - tu) - t\alpha}{s^2 + ust - t^2u^2} \in \mathbb{Q}[\alpha]\end{aligned}$$

となる．よって，$\mathbb{Q}[\alpha]$ は体である．

定義　多項式環 $\mathbb{Q}[\alpha]$ が体であるとき，$\mathbb{Q}[\alpha]$ は $\mathbb{Q}(\alpha)$ と書かれる．

以下の定理が知られている．

定理 2.1.　K を体とし，$\alpha \notin K$ はある K 係数の既約な n 次方程式の解であるとする．このとき，多項式環 $K[\alpha]$ は体，すなわち $K[\alpha] = K(\alpha)$ である．

例 2.1. $f(x) = x^3 - 7x + 7$ とし，$f(\alpha) = 0$ とする．以下の問いに答えよ．

(1) $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$ を示せ．

(2) $f(x)$ を $\mathbb{Q}(\alpha)[x]$ 上で因数分解せよ．

解答．(1) 定理 1.3 より $f(x)$ は $\mathbb{Q}[x]$ の既約多項式である．したがって，$\alpha \notin \mathbb{Q}$ で

ある．よって，定理 2.1 より $\mathbb{Q}[\alpha]=\mathbb{Q}(\alpha)$ である．

(2) $-\alpha(\alpha^2-7)=7$ より

$$f(x)=x^3-7x+7=(x-\alpha)\left(x^2+\alpha x+\alpha^2-7\right)$$

である．ここで，$s,t,u,s',t',u'\in\mathbb{Q}$ として

$$x^2+\alpha x+\alpha^2-7=\{x+(s\alpha^2+t\alpha+u)\}\{x+(s'\alpha^2+t'\alpha+u')\}$$

と置くと，

$$s+s'=0,\ t+t'=1,\ u+u'=0$$

であって，さらに計算を進めると

$$\begin{aligned}\alpha^2-7&=(s\alpha^2+t\alpha+u)(s'\alpha^2+t'\alpha+u')\\&=(s\alpha^2+t\alpha+u)(-s\alpha^2+(1-t)\alpha-u)\\&=-s^2\alpha^4+(s-2st)\alpha^3+(t-t^2-2su)\alpha^2+(u-2tu)\alpha-u^2\\&=-s^2(7\alpha^2-7\alpha)+(s-2st)(7\alpha-7)+(t-t^2-2su)\alpha^2+(u-2tu)\alpha-u^2\\&=(-7s^2+t-t^2-2su)\alpha^2+(7s^2+7s-14st+u-2tu)\alpha+14st-7s-u^2\end{aligned}$$

となる．よって，連立方程式

$$\begin{cases}-7s^2+t-t^2-2su=1\\7s^2+7s-14st+u-2tu=0\\14st-7s-u^2=-7\end{cases}$$

を得る．得られた連立方程式を手計算で解くことは面倒であるが，数学アプリなどを使うと，$s=-3,t=-4,u=14$ または $s=3,t=5,u=-14$ を得る．したがって，$f(x)$ の $K[x]$ 上での因数分解は

$$f(x)=(x-\alpha)(x-3\alpha^2-4\alpha+14)(x+3\alpha^2+5\alpha-14)$$

である．（解答終）

問題 2.1. $f(x)=x^3-3x+1$ とし，$f(\alpha)=0$ とする．以下の問いに答えよ．

(1) $\mathbb{Q}[\alpha]=\mathbb{Q}(\alpha)$ を示せ．

(2) $f(x)$ を $\mathbb{Q}(\alpha)[x]$ 上で因数分解せよ．

2.2　最小分解体

改めて，u を正の整数とし，多項式 x^2+ux+u^2 を考える．これは，環 $\mathbb{Q}[x]$ では因数分解できない．しかし，$x^2+ux+u^2=0$ の解の一つを形式的に α とすると，体 $\mathbb{Q}(\alpha)$ を考えることができ，環 $\mathbb{Q}(\alpha)[x]$ では，

$$x^2+ux+u^2=(x-\alpha)\{x+(u+\alpha)\}$$

と因数分解できた．

定義（拡大次数）

K を体とし，$\alpha\notin K$ はある K 係数の既約な n 次方程式の解であるとする．このとき，体 $K(\alpha)$ は K に α を**添加した体**と呼ばれ，さらに，$K(\alpha)$ は K の n **次拡大体**であるといい，このことを，$[K(\alpha):K]=n$ と表す．n は**拡大次数**と呼ばれる．

以下の定理が知られている．

定理 2.2.　K を体とし，$M=K(\alpha)$ を K の n 次拡大体，$L=M(\beta)$ を M の m 次拡大体とする．このとき，L は K の nm 次拡大体，すなわち

$$[L:M][M:K]=[L:K]=nm$$

となる．

定義（最小分解体）

$f(x) =\in \mathbb{Q}[x]$ の n 次多項式とし，M を $\mathbb{Q}$ の拡大体とし，$f(x)$ は $M[x]$ で重複も込めて 1 次式の積に因数分解されたとする．このとき，拡大次数 $[M:\mathbb{Q}]$ が最小となる体 M を，$f(x)$ の**最小分解体**という．

例 2.2. $f(x) = x^5 - 9x^3 + 7x^2 + 14x - 14$ の最小分解体を M とする．$[M:\mathbb{Q}]$ を求めよ．

解答．$f(x) = (x^2-2)(x^3-7x+7)$ と因数分解される．x^2-2 の最小分解体を M_1 と置く．x^2-2 の解は $\pm\sqrt{2}$ であり，x^2-2 は $\mathbb{Q}(\sqrt{2})[x]$ で 1 次方程式の積に分解されるので，$M_1 = \mathbb{Q}(\sqrt{2})$ である．よって，$[M_1:\mathbb{Q}] = 2$ である．また，x^3-7x+7 の最小分解体を M_2 と置とおく．$x^3-7x+7=0$ の解を α と置くと，例 2.1 より，x^3-7x+7 は $\mathbb{Q}(\alpha)[x]$ で 1 次方程式の積に分解されたので，$M_2 = \mathbb{Q}(\alpha)$ である．よって，$[M_2:\mathbb{Q}] = 3$ である．さらに，$M = M_1(\alpha)$ である．したがって，定理 2.2 より $[M:\mathbb{Q}] = [M_2:M_1][M_1:\mathbb{Q}] = 6$ である．（解答終）

問題 2.2. $f(x) = x^4 - 8x^2 + 15$ の最小分解体を M とする．$[M:\mathbb{Q}]$ を求めよ．

2.3　判別式と 3 次多項式の因数分解

この節では，3 次方程式の因数分解のあり方が，体の拡大でどのように変化していくのか詳細に見ていく．

そのために，まず，もう一度，例 2.1 の 3 次多項式 x^3-7x+7 を復習しながら考

えていこう．

$x^3-7x+7=0$ の解を α と置くと，3 次多項式 x^3-7x+7 は $\mathbb{Q}(\alpha)[x]$ 上で

$$x^3-7x+7=(x-\alpha)(x-3\alpha^2-4\alpha+14)(x+3\alpha^2+5\alpha-14) \qquad (2.1)$$

と 1 次式の積に因数分解された．このことから，x^3-7x+7 の最小分解体は $\mathbb{Q}(\alpha)$ であり，$[\mathbb{Q}(\alpha):\mathbb{Q}]=3$ となる．

しかし，一般に 3 次方程式 $f(x)=a_3x^3+a_2x^2+a_1x+a_0=0$ の解を α と置くと，$\mathbb{Q}(\alpha)[x]$ 上での $f(x)$ の因数分解は

$$f(x)=(x-\alpha)(b_2x^2+b_1x+b_0) \qquad (2.2)$$

で，$b_2x^2+b_1x+b_0$ は $\mathbb{Q}[x]$ 上で既約多項式となる場合が考えられる．この場合，$f(x)$ の最小分解を M と置くと，$[M:\mathbb{Q}]=[M:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]=2\times3=6$ となる．

このことを念頭に，今度は，x^3-7x+7 の定数項の 7 を 5 に変えた既約な 3 次多項式 x^3-7x+5 の因数分解について考えよう．

x^3-7x+5 の $\mathbb{Q}(\alpha)[x]$ 上での因数分解は，例 2.1 の計算とほぼ同じようになる．まず，$-\alpha(\alpha^2-7)=5$ より

$$f(x)=x^3-7x+5=(x-\alpha)\left(x^2+\alpha x+\alpha^2-7\right)$$

である．ここで，$s,t,u,s',t',u'\in\mathbb{Q}$ として

$$x^2+\alpha x+\alpha^2-7=\{x+(s\alpha^2+t\alpha+u)\}\{x+(s'\alpha^2+t'\alpha+u')\}$$

と置くと，

$$s+s'=0,\ t+t'=1,\ u+u'=0$$

であって，さらに計算を進めると

$$\begin{aligned}\alpha^2-7&=(s\alpha^2+t\alpha+u)(s'\alpha^2+t'\alpha+u')\\&=(s\alpha^2+t\alpha+u)(-s\alpha^2+(1-t)\alpha-u)\\&=-s^2\alpha^4+(s-2st)\alpha^3+(t-t^2-2su)\alpha^2+(u-2tu)\alpha-u^2\\&=-s^2(7\alpha^2-7\alpha)+(s-2st)(7\alpha-7)+(t-t^2-2su)\alpha^2+(u-2tu)\alpha-u^2\\&=(-7s^2+t-t^2-2su)\alpha^2+(7s^2+7s-14st+u-2tu)\alpha+14st-7s-u^2\end{aligned}$$

となる．よって，連立方程式

$$\begin{cases}-7s^2+t-t^2-2su=1\\7s^2+7s-14st+u-2tu=0\\14st-7s-u^2=-5\end{cases}$$

を得る．この連立方程式の解を求めるために数学アプリなどを使ってみると，有理数解が無いように見える．しかし判断はできない．

３次方程式の $\mathbb{Q}(\alpha)[x]$ 上での因数分解が，どのようになっているかを，上の方法で考えることは，高次連立方程式を解かなければならないこともあって，限界がある．別なアイディアが必要となる．

別なアイディアを考えるために，もう一度，x^3-7x+7 の $\mathbb{Q}(\alpha)[x]$ での因数分解を振り返る．

３次方程式 $x^3-7x+7=0$ の体 $\mathbb{Q}(\alpha)$ での解は，

$$x_1=\alpha,\quad x_2=3\alpha^2+4\alpha-14,\quad x_3=-3\alpha^2-5\alpha+14$$

であった．そこで，

$$\begin{aligned}x_1-x_2&=-3\alpha^2-3\alpha+14\\x_1-x_3&=3\alpha^2+6\alpha-14\\x_2-x_3&=6\alpha^2+9\alpha-28\end{aligned}$$

を考える．

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

と置く．$\alpha^3 - 7\alpha = -7$ を使いながら Δ を頑張って計算すると，$\Delta = 7$ となる．ただし，Δ は，解 x_1, x_2, x_3 が正確に分かっていたから計算できたのである．もし，そうでなかったら，Δ は計算できない．我々は，正確な解が分からなくても因数分解の構造を理解したいので，これでは進展が望めない．

実は，$D = \Delta^2$ が重要な武器となる．なぜならば，

$$\begin{aligned} D = &-4x_1x_2x_3(x_1 + x_2 + x_3)^3 + (x_1 + x_2 + x_3)^2(x_1x_2 + x_2x_3 + x_3x_1)^2 \\ &+18x_1x_2x_3(x_1 + x_2 + x_3)(x_1x_2 + x_2x_3 + x_3x_1) \\ &-4(x_1x_2 + x_2x_3 + x_3x_1)^3 - 27(x_1x_2x_3)^2 \end{aligned}$$

であることから，解の値が直接分かっていなくても，解と係数の関係式を使って D を計算できるからである．

3 次方程式 $x^3 - 7x + 7 = 0$ でいえば，

$$x_1 + x_2 + x_3 = 0, \quad x_1x_2 + x_2x_3 + x_3x_1 = -7, \quad x_1x_2x_3 = -7$$

なので，

$$D = -4 \cdot (-7)^3 - 27 \cdot (-7)^2 = 49$$

となるのである．

定義（判別式） n 次方程式 $f(x) = a_nx^n + a_{n-1}x^n + \cdots + a_1x + a_0 = 0$ の解を $x_1, x_2, \cdots, x_n$ とする．ただし，$a_j \in \mathbb{Q}$ とする．このとき，

$$D = (x_1 - x_2)^2(x_1 - x_3)^2 \cdots (x_2 - x_3)^2(x_2 - x_4)^2 \cdots (x_{n-1} - x_n)^2$$

を $f(x)$ の**判別式**という．

判別式 D の例をいくつか挙げる．

(1) x^2+bx+c のとき，$D=b^2-4c$

(2) x^3+bx^2+cx+d のとき，$D=-4b^3d+b^2c^2+18bcd-4c^3-27d^2$

(4) x^4+bx+c のとき，$D=256c^3-27b^4$

(5) x^5+bx+c のとき，$D=256b^5+3125c^4$

ガロア理論と呼ばれる代数方程式の理論より，以下の重要な定理が得られている．

定理 2.3.　$b,c,d\in\mathbb{Q}$ とし，$f(x)=x^3+bx^2+cx+d$ とする．さらに，M を $f(x)$ の最小分解体とする．このとき，$[M,\mathbb{Q}]=3$ であることの必要十分条件は $D\in\mathbb{Q}^2$ であることである．

例 2.3. $\mathbb{Q}[x]$ の既約な 3 次多項式 $f(x)=x^3-57x+19$ の最小分解体を M とする．$[M:\mathbb{Q}]$ を求めよ．さらに，$x^3-57x+19=0$ の解を α とするとき，$\mathbb{Q}(\alpha)[x]$ での $x^3-57x+19$ の因数分解は何次式の積で構成されるか述べよ．

解答．$f(x)=x^3-57x+19$ が $\mathbb{Q}[x]$ の既約多項式であることは明らかである．よって，$[M,\mathbb{Q}]=3,6$ である．$x^3-57x+19=0$ の解を $x_1,\ x_2,\ x_3$ とする．解と係数の関係式より

$$x_1+x_2+x_3=0,\quad x_1x_2+x_2x_3+x_3x_1=-57,\quad x_1x_2x_3=-19$$

である．

$$D=-4\cdot(-57)^3-27\cdot(-19)^2=731025=855^2$$

よって，定理 2.3 より $[M,\mathbb{Q}]=3$ である．このことから，$M=\mathbb{Q}(\alpha)$ もいえる．したがって，$\mathbb{Q}(\alpha)[x]$ での $x^3-57x+19$ の因数分解は 3 つの 1 次式の積で構成される．

（解答終）

問題 2.3. $\mathbb{Q}[x]$ の既約な 3 次多項式 $f(x) = x^3 - 7x + 9$ の最小分解体を M とする．$[M : \mathbb{Q}]$ を求めよ．さらに，$x^3 - 7x + 9 = 0$ の解を α とするとき，$\mathbb{Q}(\alpha)[x]$ での $x^3 - 7x + 9$ の因数は何次式の積で構成されるか述べよ．

2.4　4 次多項式の因数分解

$\mathbb{Q}[x]$ の既約な 4 次多項式

$$f(x) = x^4 + bx^3 + cx^2 + dx + e$$

の因数分解を，$\mathbb{Q}$ からの拡大体から説明する．そのために，$f(x) = 0$ の解を $x_1,\ x_2,\ x_3,\ x_4$ とし，

$$K_1 = \mathbb{Q}(x_1),\ K_2 = K_1(x_2),\ M = K_1(x_3)$$

と置く．M は $f(x)$ の最小分解体を意味する．$f(x)$ の因数分解は，以下の 4 つのタイプに分類される．

（タイプ 1）$[M, \mathbb{Q}] = 4$ ならば，$K_1 = M$ であり，$f(x)$ は $K_1[x]$ において 4 つの 1 次多項式で因数分解される．

（タイプ 2）$[M, \mathbb{Q}] = 8$ ならば，$K_1 \neq K_2,\ K_2 = M$ であり，$f(x)$ は $K_1[x]$ において，2 個の 1 次多項式と 1 個の既約な 2 次多項式で因数分解される．

（タイプ 3）$[M, \mathbb{Q}] = 12$ ならば，$K_1 \neq K_2,\ K_2 = M$ であり，$f(x)$ は $K_1[x]$ において，1 個の 1 次多項式と 1 個の既約な 3 次多項式で因数分解される．

（タイプ 4）$[M, \mathbb{Q}] = 24$ ならば，$K_1 \neq K_2,\ K_2 \neq M$ であり，$f(x)$ は $K_1[x]$ において，1 個の 1 次多項式と 1 個の既約な 3 次多項式で因数分解され，さらに，得られた 3 次多項式は $K_2[x]$ において，1 個の 1 次多項式と 1 個の既約な 2 次多項式で因数分解される．

残念ながら既約な 4 次多項式の因数分解が上のどのタイプであるのかについては，4 次方程式の判別式 D からだけでは判断できない．実は，4 次多項式の因数分解で

は，リゾルベントと呼ばれる 3 次多項式が威力を発揮する．以下，そのことについて説明する．

4 次方程式

$$x^4 + bx^3 + cx^2 + dx + e = 0 \tag{2.3}$$

の解を $x_1,\ x_2,\ x_3,\ x_4$ とする．そして，

$$\begin{aligned} t_1 &= x_1x_2 + x_3x_4 \\ t_2 &= x_1x_3 + x_2x_4 \\ t_3 &= x_1x_4 + x_2x_3 \end{aligned}$$

と置く．さらに，

$$R(x) = (x - t_1)(x - t_2)(x - t_3)$$

と置く．このとき，4 次方程式 (2.3) の解と係数の関係から，$\mathbb{Q}$ 係数の 3 次方程式

$$R(x) = x^3 - cx^2 + (bd - 4e)x + 4ce - b^2e - d^2$$

が得られる．

定義（4 次方程式のリゾルベント）　$\mathbb{Q}$ 係数の 3 次方程式

$$R(x) = x^3 - cx^2 + (bd - 4e)x + 4ce - b^2e - d^2$$

を 4 次方程式 $x^4 + bx^3 + cx^2 + dx + e = 0$ の**リゾルベント**と呼ぶ．

4 次方程式のリゾルベント $R_4(x)$ の重要性も，$R(x)$ の最小分解体 M_r にある．つまり，$R(x)$ は 3 次多項式なので，M_r の $\mathbb{Q}$ 上の拡大次数は，

$$[M_r : \mathbb{Q}] = 6,\ 3,\ 2,\ 1$$

のいずれかとなる．以下の重要な定理が証明されている．

定理 2.4.　M を $\mathbb{Q}[x]$ の既約な 4 次方程式 $f(x)$ の最小分解体，M_r を $R(x)$ の最小分解体，さらに，D を $f(x)$ の判別式と置く．このとき以下のことが成り立つ．

(1) $[M_r:\mathbb{Q}]=6 \iff [M:\mathbb{Q}]=24$
(2) $[M_r:\mathbb{Q}]=3 \iff [M:\mathbb{Q}]=12$
(3) $[M_r:\mathbb{Q}]=2 \iff [M:\mathbb{Q}]=8,\ 4$
(4) $[M_r:\mathbb{Q}]=1 \iff [M:\mathbb{Q}]=4$

例 2.4. 以下の既約な 4 次多項式 $f(x)$ の最小分解体を M とするとき，$[M:\mathbb{Q}]$ を求めよ．さらに，$f(x)=0$ の解を α とするとき，$\mathbb{Q}(\alpha)[x]$ での $f(x)$ の因数分解は何次式の積で構成されるか述べよ．

(1) x^4+1　　(2) $x^4-8x+12$　　(3) x^4+5x^2+5　　(3) x^4-x+1

解答．(1) $b=c=d=0,\ e=1$ より，$R(x)=x^3-4x=x(x-2)(x+2)$ である．よって，$[M_r:\mathbb{Q}]=1$ なので，$[M:\mathbb{Q}]=4$ である．したがって，$\mathbb{Q}(\alpha)[x]$ での x^4+1 の因数分解は 4 つの 1 次式の積で構成される．

(2) $b=c=0,\ d=-8, e=12$ より，$R(x)=x^3-48x-64$ で，これは既約である．$R(x)$ の判別式を求める．

$$D=-4\cdot(-48)^3-27*(64)^2=331776=576^2.$$

よって，$[M_r:\mathbb{Q}]=3$ なので，$[M:\mathbb{Q}]=12$ である．したがって，$\mathbb{Q}(\alpha)[x]$ での $x^4-8x+12$ の因数分解は 1 次式と 3 次式の積で構成される．

(3) $b=d=0,\ c=e=5$ より，$R(x)=x^3-5x^2-20x+100=(x-5)(x^2-20)$ である．よって，$[M_r:\mathbb{Q}]=2$ なので，$[M:\mathbb{Q}]=4,8$ である．したがって，$\mathbb{Q}(\alpha)[x]$ での x^4+5x^2+5 の因数分解は $[M:\mathbb{Q}]=4$ ならば 4 つの 1 次式の積で構成され，$[M:\mathbb{Q}]=8$ ならば 2 つの 2 次式の積で構成される．

(4) $b=c=0,\ d=-1, e=1$ より，$R(x)=x^3-4x-1$ で，これは既約である．$R(x)$ の判別式を求める．

$$D=-4\cdot(-4)^3-27*(1)^2=229=\sqrt{229}^2.$$

よって，$[M_r:\mathbb{Q}]=4$ なので，$[M:\mathbb{Q}]=24$ である．したがって，$\mathbb{Q}(\alpha)[x]$ での x^4-x+1 の因数分解は1次式と3次式の積で構成される．（解答終）

問題 2.4. 以下の既約な4次多項式 $f(x)$ の最小分解体を M とするとき，$[M:\mathbb{Q}]$ を求めよ．さらに，$f(x)=0$ の解を α とするとき，$\mathbb{Q}(\alpha)[x]$ での $f(x)$ の因数分解は何次式の積で構成されるか述べよ．

(1) x^4+2x+2　(2) x^4+5x^2+1　(3) x^4+5x^2+3　(3) x^4+4x^3+28

2.5　8次拡大の最小分解体をもつ4次多項式

定理 2.4 の (3) は $[M_r:\mathbb{Q}]=2 \iff [M:\mathbb{Q}]=8,\ 4$ であった．以下，$[M:\mathbb{Q}]=8,\ 4$ の違いの4次多項式について説明する．

既約な4次多項式 x^4+5x^2+5 について考える．そのために，$x^4+5x^2+5=0$ の一つの解を α と置く．環 $\mathbb{Q}(\alpha)[x]$ で因数分解すると，$\alpha^4+5\alpha^2+5=0$ と $\alpha^2+5=-\alpha^6-6\alpha^4-9\alpha^2=-(\alpha^3+3\alpha)^2$ より

$$\begin{aligned}x^4+5x^2+5&=(x-\alpha)(x^3+\alpha x^2+(\alpha^2+5)x+\alpha^3+5\alpha)\\&=(x-\alpha)(x+\alpha)(x^2+\alpha^2+5)\\&=(x-\alpha)(x+\alpha)(x-\alpha^3-3\alpha)(x+\alpha^3+3\alpha).\end{aligned}$$

よって，$[M:\mathbb{Q}]=4$ である．

一方, x^4+5x^2+5 のリゾルベントは $R(x)=(x-5)(x^2-20)$ であった．$x^2-20=0$ より $x=\pm 2\sqrt{5}$ であることから，$M_r=\mathbb{Q}(\sqrt{5})$ であることがわかる．この立場から，

x^4+5x^2+5 をみると，環 $M_r[x]$ で

$$x^4+5x^2+5=\left(x^2+\frac{5+\sqrt{5}}{2}\right)\left(x^2-\frac{5-\sqrt{5}}{2}\right)$$

と因数分解できる，すなわち x^4+5x^2+5 は $M_r[x]$ で可約であることがいえる．

以下の定理が知られている．

定理 2.5.　M を $\mathbb{Q}[x]$ の既約な 4 次方程式 $f(x)$ の最小分解体，M_r を $R(x)$ の最小分解体とし，$[M:\mathbb{Q}]=4,8$ とする．このとき，以下が成り立つ．

$$f(x) \text{ が } M_r[x] \text{ で可約} \iff [M:\mathbb{Q}]=4$$

例 2.5.　既約な 4 次多項式 $f(x)=x^4+3x+3$ の最小分解体を M とするとき，$[M:\mathbb{Q}]$ を求めよ．さらに，$x^4+3x+3=0$ の解を α とするとき，$\mathbb{Q}(\alpha)[x]$ での x^4+3x+3 の因数分解は何次式の積で構成されるか述べよ．

解答．リゾルベントは，$R(x)=(x+3)(x^2-3x-3)$ である．よって，$[M_r:\mathbb{Q}]=2$ なので，$[M:\mathbb{Q}]=4,8$ である．一方，$M_r=\mathbb{Q}(\sqrt{21})$ である．そこで，x^4+3x+3 の x^3 の係数と x^2 の係数はどちらも 0 であることから，$s,t\in M_r$ と考えて，

$$x^4+3x+3=\left(x^2-tx-s\right)\left(x^2+tx+(s+t^2)\right)$$

と因数分解してみる．これより

$$-t^3-2st=3,\quad -s^2-st^2=3$$

でなくてはならない．よって，

$$s^2+(t^2-2t)s-t^3=0$$

を得る．この方程式の判別式 D を求めると

$$D=(t^2-2t)^2+4t^3=t^4+4t^2.$$

$\sqrt{D} \in \mathbb{Q}(\sqrt{21})$ でなくてはならないので，$t = \sqrt{21}a,\ a \in \mathbb{Q}$ と置ける．
$D = 21a^2(21a^2+4)$ より，

$$s = \frac{-(21a^2 - 2\sqrt{21}a) \pm a\sqrt{21(21a^4+4)}}{2}$$

を得る．$-t^3 - 2st = 3$ より

$$-21\sqrt{21}a^3 - \sqrt{21}a\{-(21a^2 - 2\sqrt{21}a) \pm a\sqrt{21(21a^2+4)}\} = 3.$$

よって，

$$7a^2(-2 \pm \sqrt{21a^2+4}) = 1.$$

さらに整理して，

$$1029a^6 - 28a^2 - 1 = 0 \quad \rightarrow \quad (7a^2+1)(147a^4 - 21a^2 - 1) = 0$$

を得る．これは $a \in \mathbb{Q}$ に反する．したがって，$x^4 + 3x + 3$ は $M_r[x]$ の既約多項式である．よって，定理 2.5 より $[M : \mathbb{Q}] = 8$ である．このことから，$M \neq \mathbb{Q}(\alpha)$ もいえる．したがって，$\mathbb{Q}(\alpha)[x]$ での $x^4 + 3x + 3$ の因数分解は 2 つの 2 次式の積で構成される．（解答終）

問題 2.5. 以下の既約な 4 次多項式 $f(x)$ の最小分解体を M とするとき，$[M : \mathbb{Q}]$ を求めよ．さらに，$f(x) = 0$ の解を α とするとき，$\mathbb{Q}(\alpha)[x]$ での $f(x)$ の因数分解は何次式の積で構成されるか述べよ．

(1) $x^4 - 3$　　(2) $x^4 + 5x + 5$

問題の解答

問題 1.1　$a \in \mathbb{Z}$ で，$a \neq 0$ とする．このとき，体の定義 (6) の $a \cdot x = 1$ を満たす $x \in \mathbb{Z}$ が存在しない．よって，$\mathbb{Z}$ は体ではない．

問題 1.2　$\mathbb{Z}$ と $\mathbb{Z}[x]$ が，どちらも環の定義 (1) から (5) を満たすことは明らか．また，$a, b \in \mathbb{Z}$ に対し，$ab = ba$ も成り立ち．$1 \in \mathbb{Z}$ であることから，$\mathbb{Z}$ は単位的可換環である．さらに，0 以外に零因子がないことは明らかなので，$\mathbb{Z}$ は整域である．

$f, g \in \mathbb{Z}[x]$ に対し，$fg = gf$ も成り立ち．$1 \in \mathbb{Z}[x]$ であることから，$\mathbb{Z}[x]$ は単位的可換環である．さらに，0 以外に零因子がないことは明らかなので，$\mathbb{Z}[x]$ は整域である．

問題 1.3　$f(2) = 0$ なので，因数定理より $f(x) = (x-2)(x^3+3x+1)$ である．$g(x) = x^3+3x+1$ と置く．定理 1.2 より，$g(x) = 0$ となる候補は $x \pm 1$ である．しかし，$g(1) \neq 0,\ g(-1) \neq 0$ である．よって，$g(x)$ は $\mathbb{Q}[x]$ の既約多項式である．したがって，$f(x)$ の因数分解は $f(x) = (x-1)(x^3+3x+1)$ である．

問題 1.4　$f(-1) = 2 \cdot (1)^4 + (1)^3 + 3 \cdot (1) - 6 = 0$. よって，因数定理より $f(x) = (x-1)(2x^3+3x^2+6x+6)$ である．$g(x) = 2x^3+3x^2+6x+6$ と置くと，$a_0 = 6, a_1 = 6, a_2 = 3$ は $p = 3$ の倍数で，$a_3 = 2$ は $p = 3$ の倍数でなく $a_0 = 6$ は $p^2 = 9$ の倍数でない．よって，定理 1.3 より，g は $\mathbb{Q}[x]$ の既約多項式である．よって，$f(x)$ の因数分解は $f(x) = (x-1)(2x^3+3x^2+6x+6)$ である．

問題 1.5　$f(1) = 0$ なので，因数定理より $f(x) = (x-1)(x^3+12x+25)$ である．$g(x) = x^3+12x+25$ と置く．定理 1.3 は使えないので，$g(x-1) = (x-5)^3+12(x-5)+35 = x^3-3x^2+15x+12$ を考える．$a_0 = 12, a_1 = 15, a_2 = 3$ はどれも $p = 3$ の倍数であり，$a_3 = 1$ は $p = 3$ の倍数でなく $a_0 = 12$ は $p^2 = 9$ の倍数でない．よって，定理 1.4 より $g(x)$ は $\mathbb{Q}[x]$ の既約多項式である．したがって，$f(x)$ の因数分解は $f(x) = (x-1)(x^3+12x+25)$ である．

問題 2.1　(1) もし $x-\alpha$ が $P(x)$ の因数であれば，$\alpha = \pm 1$ であるはずだが，どれも $P(\alpha) \neq 0$ である．よって，$f(x)$ は $\mathbb{Q}[x]$ の既約多項式である．したがって，$\alpha \notin \mathbb{Q}$

である．よって，定理 2.1 より $\mathbb{Q}[\alpha]=\mathbb{Q}(\alpha)$ である．

(2) $-\alpha(\alpha^2-3)=1$ より

$$f(x)=x^3-3x+1=(x-\alpha)\left(x^2+\alpha x+\alpha^2-3\right)$$

である．ここで，$s,t,u,s',t',u'\in\mathbb{Q}$ として

$$x^2+\alpha x+\alpha^2-3=\{x+(s\alpha^2+t\alpha+u)\}\{x+(s'\alpha^2+t'\alpha+u')\}$$

と置くと，

$$s+s'=0,\ t+t'=1,\ u+u'=0$$

であって，

$$\begin{aligned}\alpha^2-3&=(s\alpha^2+t\alpha+u)(s'\alpha^2+t'\alpha+u')\\&=(s\alpha^2+t\alpha+u)(-s\alpha^2+(1-t)\alpha-u)\\&=-s^2\alpha^4+(s-2st)\alpha^3+(t-t^2-2su)\alpha^2+(u-2tu)\alpha-u^2\\&=-s^2(3\alpha^2-\alpha)+(s-2st)(3\alpha-1)+(t-t^2-2su)\alpha^2+(u-2tu)\alpha-u^2\\&=(-3s^2+t-t^2-2su)\alpha^2+(s^2+3s-6st+u-2tu)\alpha+2st-s-u^2\end{aligned}$$

である．よって，連立方程式

$$\begin{cases}-3s^2+t-t^2-2su=1\\ s^2+3s-6st+u-2tu=0\\ 2st-s-u^2=-3\end{cases}$$

を得る．これより $s=1,t=1,u=-2$ または $s=-1,t=0,u=2$ を得る．したがって，$f(x)$ の $K[x]$ 上での因数分解は

$$f(x)=(x-\alpha)(x+\alpha^2+\alpha-2)(x-\alpha^2+2)$$

である．

問題 2.2　$f(x)=(x^2-3)(x^2-5)$ と因数分解される．x^2-3 の最小分解体を M_1 と置く．x^2-3 の解は $\pm\sqrt{3}$ であり，x^2-3 は $\mathbb{Q}(\sqrt{3})[x]$ で 1 次方程式の積に分解されるので，$M_1=\mathbb{Q}(\sqrt{3})$ である．よって，$[M_1:\mathbb{Q}]=2$ である．また，x^2-5 の最小分解体を M_2 と置く．x^2-5 の解は $\pm\sqrt{5}$ であり，x^2-5 は $\mathbb{Q}(\sqrt{5})[x]$ で 1 次方程式の

積に分解されるので，$M_1 = \mathbb{Q}(\sqrt{5})$ である．よって，$[M_1 : \mathbb{Q}] = 2$ である．さらに，$M = M_1(\sqrt{5})$ である．したがって，定理 2.2 より $[M : \mathbb{Q}] = [M_2 : M_1][M_1 : \mathbb{Q}] = 4$ である．

問題 2.3　$f(x) = x^3 - 7x + 9$ が $\mathbb{Q}[x]$ の既約多項式であることは明らかである．よって，$[M, \mathbb{Q}] = 3, 6$ である．$x^3 - 7x + 9 = 0$ の解を $x_1,\ x_2,\ x_3$ とする．解と係数の関係式より

$$x_1 + x_2 + x_3 = 0,\quad x_1x_2 + x_2x_3 + x_3x_1 = -7,\quad x_1x_2x_3 = -9$$

である．

$$D = -4 \cdot (-7)^3 - 27 \cdot (-9)^2 = 731025 = -815$$

よって，定理 2.3 より $[M, \mathbb{Q}] = 3 \times 2 = 6$ である．このことから，$M \neq \mathbb{Q}(\alpha)$ である．したがって，$\mathbb{Q}(\alpha)[x]$ での $x^3 - 7x + 9$ の因数分解は 1 次式と 2 次式の積で構成される．

問題 2.4　(1) $b = c = 0,\ d = e = 2$ より，$R(x) = x^3 - 8x - 4$ で，これは既約である．$R(x)$ の判別式を求める．

$$D = -4 \cdot (-8)^3 - 27 * (4)^2 = 1616 = \sqrt{16162}.$$

よって，$[M_r : \mathbb{Q}] = 6$ なので，$[M : \mathbb{Q}] = 24$ である．したがって，$\mathbb{Q}(\alpha)[x]$ での $x^4 + 2x + 2$ の因数分解は 1 次式と 3 次式の積で構成される．

(2) $b = d = 0,\ c = 5,\ e = 1$ より，$R(x) = x^3 - 5x^2 - 4x + 20 = (x-5)(x-2)(x+2)$ である．よって，$[M_r : \mathbb{Q}] = 1$ なので，$[M : \mathbb{Q}] = 4$ である．したがって，$\mathbb{Q}(\alpha)[x]$ での $x^4 + 5x + 1$ の因数分解は 4 つの 1 次式の積で構成される．

(3) $b = d = 0,\ c = 5,\ e = 3$ より，$R(x) = x^3 - 5x^2 - 12x + 60 = (x-5)(x^2-12)$ である．よって，$[M_r : \mathbb{Q}] = 2$ なので，$[M : \mathbb{Q}] = 4, 8$ である．したがって，$\mathbb{Q}(\alpha)[x]$ での $x^4 + 5x^2 + 3$ の因数分解は $[M : \mathbb{Q}] = 4$ ならば 4 つの 1 次式の積で構成され，$[M : \mathbb{Q}] = 8$ ならば 2 つの 2 次式の積で構成される．

(4) $b = 4,\ c = d = 0,\ e = 28$ より，$R(x) = x^3 - 112x - 448$ で，これは既約であ

る．$R(x)$ の判別式を求める．

$$D = -4 \cdot (-112)^3 - 27 * (448)^2 = 200704 = 448^2.$$

よって，$[M_r : \mathbb{Q}] = 3$ なので，$[M : \mathbb{Q}] = 12$ である．したがって，$\mathbb{Q}(\alpha)[x]$ での $x^4 + 5x^2 + 3$ の因数分解は1次式と3次式の積で構成される．

問題 2.5　(1) $R(x) = x(x^2 + 12)$ である．よって，$[M_r : \mathbb{Q}] = 2$ なので，$[M : \mathbb{Q}] = 4, 8$ である．一方，$M = \mathbb{Q}(\sqrt{3}i)$ である．また，

$$x^4 - 3 = \left(x^2 - \sqrt{3}\right)\left(x^2 + \sqrt{3}\right)$$

である．しかしこれは，$x^4 - 3$ が $M_r[x]$ で因数分解できることに矛盾する．したがって，$x^4 - 3$ は $M_r[x]$ の既約多項式である．よって，定理 2.5 より $[M : \mathbb{Q}] = 8$ である．したがって，$\mathbb{Q}(\alpha)[x]$ での $x^4 - 3$ の因数分解は2つの2次式の積で構成される．

(2) $R(x) = (x - 5)(x^2 + 5x + 5)$ である．よって，$[M_r : \mathbb{Q}] = 2$ なので，$[M : \mathbb{Q}] = 4, 8$ である．一方，$M_r = \mathbb{Q}(\sqrt{5})$ である．そこで，$x^4 + 5x + 5$ の x^3 の係数と x^2 の係数はどちらも 0 であることから，$s, t \in M_r$ と考えて，

$$x^4 + 5x + 5 = \left(x^2 - tx - s\right)\left(x^2 + tx + (s + t^2)\right)$$

と因数分解してみる．これより

$$-t^3 - 2st = 5, \quad -s^2 - st^2 = 5$$

でなくてはならない．よって，

$$s^2 + (t^2 - 2t)s - t^3 = 0$$

を得る．この方程式の判別式 D を求めると

$$D = (t^2 - 2t)^2 + 4t^3 = t^4 + 4t^2.$$

$\sqrt{D} \in \mathbb{Q}(\sqrt{5})$ でなくてはならないので，$t = \sqrt{5}a,\ a \in \mathbb{Q}$ と置ける．
$D = 5a^2(5a^2 + 4)$ より，

$$s = \frac{-(5a^2 - 2\sqrt{5}a) \pm a\sqrt{5(5a^4 + 4)}}{2}$$

を得る．$-t^3 - 2st = 5$ より

$$-5\sqrt{5}a^3 - \sqrt{5}a\{-(5a^2 - 2\sqrt{5}a) \pm a\sqrt{5(5a^2+4)}\} = 5.$$

よって,

$$a^2(-2 \pm \sqrt{5a^2+4}) = 1.$$

さらに整理して,

$$5a^6 - 4a^2 - 1 = 0 \quad \rightarrow \quad (a^2-1)(5a^4+5a^2+1) = 0$$

を得る．よって，$a = \pm 1$ を得る．これより，x^4+5x+5 は $M_r[x]$ で可約である．したがって，定理 2.5 より $[M:\mathbb{Q}] = 4$ である．したがって，$\mathbb{Q}(\alpha)[x]$ での x^4+5x+5 の因数分解は 4 つの 1 次式の積で構成される．