大学数学への接続シリーズ１

分母の有理化と体

松田 修　著

2023 年 5 月 1 日

はじめに

例えば，$\dfrac{2}{\sqrt{3}}$ の分母を有理化すると，$\dfrac{2\sqrt{3}}{3}$ となる．分母の有理化ができると，

$$\sqrt{3}+\frac{2}{\sqrt{3}}=\sqrt{3}+\frac{2\sqrt{3}}{3}=\frac{5\sqrt{3}}{3}$$

というように，足し算ができる．

分母の有理化は，中学や高校の数学で学習する．これは一体何を意味しているのだろうか．

もう少し発展させて，$\dfrac{1}{\sqrt{3}+\sqrt{2}}$ の分母の有理化を考えてみる．

$$\frac{1}{\sqrt{3}+\sqrt{2}}=\frac{\sqrt{3}-\sqrt{2}}{(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2})}=\frac{\sqrt{3}-\sqrt{2}}{3-2}=\sqrt{3}-\sqrt{2}$$

となる．これによって，例えば

$$\sqrt{3}+\sqrt{2}+\frac{1}{\sqrt{3}+\sqrt{2}}=\sqrt{3}+\sqrt{2}+\sqrt{3}-\sqrt{2}=2\sqrt{3}$$

というように，足し算が可能となる．

さらに発展させると，「$\dfrac{1}{\sqrt{3}+\sqrt[3]{2}}$ の分母の有理化は？」という問題などが考えられる．

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」という視点から，分母の有理化の意味を説明する．その中で，$\dfrac{1}{\sqrt{3}+\sqrt[3]{2}}$ の分母の有理化や，より発展させた分母の有理化についても説明する．

目次

第 1 章

分母の有理化の意味

例えば，$\dfrac{2}{\sqrt{3}} = \dfrac{2\sqrt{3}}{3}$ というように，分母が有理数でない分数の分母を有理数に変えることを**分母の有理化**という．この意味について考える．

1.1　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．$\mathbb{Q}$ 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．

1.2　分母の有理化と体 $\mathbb{Q}[\sqrt{x}]$

日本の中学や高校では，分母の有理化を学習する．しかし，分母を有理化することは，どんな意味があるのだろうか．

例えば，$\dfrac{1}{\sqrt{2}}$ の分母を有理化すると $\dfrac{\sqrt{2}}{2}$ となる．このことを

$$\frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2} = \frac{1}{2} \cdot \sqrt{2}$$

としておく．他の数についても分母の有理化をいくつか考えると，たとえば

$$\frac{3+\sqrt{2}}{\sqrt{2}} = \frac{3\sqrt{2}+2}{2} = 1 + \frac{3}{2} \cdot \sqrt{2}$$

$$\frac{1}{3+\sqrt{2}} = \frac{3-\sqrt{2}}{7} = \frac{3}{7} - \frac{1}{7} \cdot \sqrt{2}$$

などとなる．上で考えた分母の有理化を一般化して整理すると，a, b, c, d を $\mathbb{Q}$ の元とし，$c + d\sqrt{2} \neq 0$ のとき

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = x + y\sqrt{2}$$

という形で，x, y も $\mathbb{Q}$ の元とすることができるといえる．

さて，$x = \sqrt{2}$ として，x の $\mathbb{Q}$ 係数の多項式を考えると，

$$a + bx + cx^2 = (a + 2c) + bx = (a + 2c) + b\sqrt{2}$$

となる．そこで，集合 $\mathbb{Q}[\sqrt{2}]$ を $\sqrt{2}$ の**多項式全体**として

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q},\ b \neq 0\}$$

と定義する．

これまで説明してきたことから，$\mathbb{Q}[\sqrt{2}]$ は体であることがわかる．つまり，$\mathbb{Q}[\sqrt{2}]$ の任意の元 x, y について，

$$x + y \in \mathbb{Q}[\sqrt{2}],\quad x - y \in \mathbb{Q}[\sqrt{2}],\quad xy \in \mathbb{Q}[\sqrt{2}]$$

が成り立ち，さらに，$y \neq 0$ ならば

$$\frac{x}{y} \in \mathbb{Q}[\sqrt{2}]$$

が成り立つからである．

同様な理由から，$\sqrt{3}$ の $\mathbb{Q}$ 係数の多項式全体である

$$\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q},\ b \neq 0\}$$

も体である．一般に，次の定理が成り立つ．

定理 1.1.　x を平方数でない正の整数とする．このとき，$\sqrt{x}$ の $\mathbb{Q}$ 係数の多項式全体

$$\mathbb{Q}[\sqrt{x}] = \{a + b\sqrt{x} \mid a, b \in \mathbb{Q},\ b \neq 0\}$$

は，体である．

分母の有理化は，集合 $\mathbb{Q}[\sqrt{x}]$ が体であることが前提になっていて，その計算できることを意味していたのである．

問題 1.2. 以下の集合は体となることを証明せよ．

(1) $\mathbb{Q}[\sqrt{3}]$　　(2) $\mathbb{Q}[\sqrt{-1}]$

1.3　分母の有理化と体 $\mathbb{Q}[\sqrt[3]{2}]$

集合 $\mathbb{Q}[\sqrt[3]{2}]$ について考えよう．これは，$\sqrt[3]{2}$ の多項式全体

$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\ \}$$

というものである．そして，$\mathbb{Q}[\sqrt[3]{2}]$ は体である．

$\mathbb{Q}[\sqrt[3]{2}]$ が体であることを示そう．$\mathbb{Q}[\sqrt[3]{2}]$ の任意の元 x, y について，

$$x + y \in \mathbb{Q}[\sqrt[3]{2}],\quad x - y \in \mathbb{Q}[\sqrt[3]{2}],\quad xy \in \mathbb{Q}(\sqrt[3]{2})$$

が成り立つことは明らかであるが，問題は，$y \neq 0$ ならば

$$\frac{x}{y} \in \mathbb{Q}[\sqrt[3]{2}]$$

が成り立つのかである．つまり，a, b, c, d, e, f を $\mathbb{Q}$ の元で，$d + e\sqrt[3]{2} + f\sqrt[3]{4} \neq 0$ のとき，

$$\frac{a + b\sqrt[3]{2} + c\sqrt[3]{4}}{d + e\sqrt[3]{2} + f\sqrt[3]{4}} = x + y\sqrt[3]{2} + z\sqrt[3]{4} \tag{1.1}$$

で，$x, y, z \in \mathbb{Q}$ とすることができるかである．そして，上の式 (1.1) を示すためには，a, b, c を $\mathbb{Q}$ の元で，$a + b\sqrt[3]{2} + e\sqrt[3]{4} \neq 0$ のとき，

$$\frac{1}{a + b\sqrt[3]{2} + c\sqrt[3]{4}} = x + y\sqrt[3]{2} + z\sqrt[3]{4} \tag{1.2}$$

で，$x, y, z \in \mathbb{Q}$ とすることを示せば十分であるので，(1.2) を示そう．

$f(x) = x^3 - 2$ と $g(x) = a + bx + cx^2$, $(c \neq 0)$ を考える．このとき，$f(x)$ の $g(x)$ による除算から

$$f(x) = \left(\frac{1}{c}x - \frac{b}{c^2}\right) g(x) + \frac{1}{c^2}\left\{(b^2 - ac)x + ab - 2c^2\right\} \tag{1.3}$$

得る．ここで，

$$Q(x) = \frac{1}{c}x - \frac{b}{c^2}, \quad h(x) = \frac{1}{c^2}\left\{(b^2 - ac)x + ab - 2c^2\right\}$$

と置くと，(1.3) は

$$f(x) = Q(x)g(x) + h(x) \tag{1.4}$$

となる．

ところで，$f(x)$ は $\mathbb{Q}$ 係数の多項式を使って因数分解できないので，$f(x)$ と $g(x)$ の最大公約数は 1 であり，さらに，(1.4) より，$g(x)$ と $h(x)$ の最大公約数も 1 であることに注意する．

同様に，$g(x)$ の $h(x)$ による除算から

$$g(x) = Q'(x)h(x) + R \tag{1.5}$$

という等式が得られる．ここで，$Q'(x)$ は x の $\mathbb{Q}$ 係数の 1 次式で，$R \in \mathbb{Q}$ である．そして，$g(x)$ と $h(x)$ の最大公約数が 1 であることから，$h(x)$ と R の最大公約数が 1，すなわち $R = 1$ を得る．したがって，$\alpha(x) = -Q'(x)$，$\beta(x) = Q(x)Q'(x) + 1$ と置くと，$\beta(x)$ は $\mathbb{Q}$ 係数の 2 次式であり，(1.4) と (1.5) より

$$\alpha(x)f(x) + \beta(x)g(x) = 1 \tag{1.6}$$

を得る．したがって，x に $\sqrt[3]{2}$ を代入することで，

$$\frac{1}{a + b\sqrt[3]{2} + c\sqrt[3]{4}} = \beta(\sqrt[3]{2}) \tag{1.7}$$

が得られる．これは等式 (1.2) が示されたことを意味する．$c = 0$, $b \neq 0$ の場合も同様にして，(1.2) が示される．

定理 1.2.　$\mathbb{Q}[\sqrt[3]{2}]$ は体である．

問題 1.3. $\mathbb{Q}[\sqrt[3]{3}]$ は体となることを証明せよ．

第 2 章

ユークリッドの互除法

有理化を理解するためには，多項式に関するユークリッドの互除法の理解が必要である．

2.1　整数に関するユークリッドの互除法

２つの正の整数 a と b の最大公約数 d を求めるための方法として，**ユークリッドの互除法**と呼ばれるものがある．それを以下に説明する．

（ステップ１）$a > b$ とする．a の b による除算から

$$a = q_1 b + r_1 \tag{2.1}$$

を得る．ここで，$b > r_1 \geq 0$ である．(2.1) より b と r_1 の最大公約数も d となる．もし，$r_1 = 0$ なら $d = b$ である．

（ステップ２）$r_1 > 0$ のとき，b の r_1 による除算から

$$b = q_2 r_1 + r_2 \tag{2.2}$$

を得る．ここで，$r_1 > r_2 \geq 0$ である．(2.2) より r_1 と r_2 の最大公約数も d となる．もし，$r_2 = 0$ なら $d = r_1$ である．

このステップをくり返すと，ステップ $n + 1$ において余りは 0 となる．すなわち，以下を得る．

（ステップ $n+1$）$r_{n-1} > 0$ のとき，r_{n-1} の r_n による除算から

$$r_{n-1} = q_n r_n \tag{2.3}$$

を得る．よって $d = r_n$ となる．

これが，ユークリッドの互除法である．そして，ユークリッドの互除法を逆に辿っていくことで，以下の定理が得られる．

定理 2.1.　2 つの正の整数 a と b の最大公約数を d とする．このとき，

$$ax + by = d$$

となる整数 x, y が存在する．

例 2.1. $a = 2652$, $b = 455$ の最大公約数 d を求めよ．

解答.（ステップ 1）$2652 = 5 \cdot 455 + 377$,（ステップ 2）$455 = 1 \cdot 377 + 78$,
（ステップ 3）$377 = 4 \cdot 78 + 65$,（ステップ 4）$78 = 1 \cdot 65 + 13$,
（ステップ 5）$65 = 5 \cdot 13$．よって，$d = 13$ （解答終）

例 2.2. $a = 819$, $b = 2205$ の最大公約数 d とする．このとき，$ax + by = d$ となる整数 x, y を 1 組だけ求めよ．

解答．$a = 3^2 \cdot 7 \cdot 13$, $b = 3^2 \cdot 5 \cdot 7^2$ より $d = 63$ である．$819x + 2205y = 63$ より $13x + 35y = 1$ を得る．よって，両辺を 13 で割った余りで考えると，

$$9y \equiv 1 \mod 13.$$

これより，$y = 3$，$y = -8$ を得る．（解答終）

問題 2.1. $a = 49911$, $b = 18923$ の最大公約数 d を求めよ．

問題 2.2. $a = 2275,\ b = 245$ の最大公約数 d とする．このとき，$ax + by = d$ となる整数 x, y を 1 組だけ求めよ．

2.2　多項式に関するユークリッドの互除法

$\mathbb{Q}$ 係数の 2 つの多項式 $f(x)$ と $g(x)$ の最大公約式 $d(x)$ を求めるためのユークリッドの互除法を説明する．以下で扱う記号 $\deg(f)$ は $f(x)$ の次数のことである．

（ステップ 1）$\deg(f) > \deg(g)$ とする．$f(x)$ の $g(x)$ による除算から

$$f(x) = q_1(x)g(x) + r_1(x) \tag{2.4}$$

を得る．ここで，$\deg(g) > \deg(r_1)$ である．(2.4) より $g(x)$ と $r_1(x)$ の最大公約式も $d(x)$ となる．もし，$r_1(x) = 0$ なら $d(x) = g(x)$ である．

（ステップ 2）$r_1(x) > 0$ のとき，$g(x)$ の $r_1(x)$ による除算から

$$g(x) = q_2(x)r_1(x) + r_2(x) \tag{2.5}$$

を得る．ここで，$\deg(r_1) > \deg(r_2)$ である．(2.5) より $r_1(x)$ と $r_2(x)$ の最大公約式も $d(x)$ となる．もし，$r_2 = 0$ なら $d = r_1$ である．

このステップをくり返すと，ステップ $n + 1$ において余りは 0 となる．すなわち，以下を得る．

（ステップ $n + 1$）$r_{n-1}(x) > 0$ のとき，$r_{n-1}(x)$ の $r_n(x)$ による除算から

$$r_{n-1}(x) = q_n(x)r_n(x) \tag{2.6}$$

を得る．よって $d(x) = r_n(x)$ となる．

これが，多項式に関するユークリッドの互除法である．そして，多項式に関するユークリッドの互除法を逆に辿っていくことで，以下の定理が得られる．

定理 2.2.　$\mathbb{Q}$ 係数の 2 つの多項式 $f(x)$ と $g(x)$ の最大公約式を $d(x)$ とする．このとき，

$$a(x)f(x)+b(x)g(x)=d(x)$$

となる $\mathbb{Q}$ 係数の多項式 $a(x), b(x)$ が存在する．

例 2.3. $f(x)=x(x+2)$, $g(x)=3(x-1)(x+2)$, $d(x)$ を $f(x)$ と $g(x)$ の最大公約式とする．このとき，$a(x)f(x)+b(x)g(x)=d(x)$ を満たす $\mathbb{Q}$ 係数の多項式 $a(x)$ と $b(x)$ をそれぞれ一つずつ求めよ．

解答．$d(x)=(x+2)$ である．$a(x)f(x)+b(x)g(x)=d(x)$ より

$$xa(x)+3(x-1)b(x)=1$$

である．両辺を x で割った余りを考えると，$-3b(x)\equiv 1 \mod x$ となるので，$b(x)=-\dfrac{1}{3}$ がとれる．よって，

$$a(x)=\frac{1-3(x-1)\left(-\frac{1}{3}\right)}{x}=1$$

である．実際

$$a(x)f(x)+b(x)g(x)=x(x+2)+3\left(-\frac{1}{3}\right)(x-1)(x+2)=x+2=d(x)$$

である．（解答終）

問題 2.3. $f(x)=(x-1)(2x-1)$, $g(x)=-(x+1)(2x-1)(2x+1)$, $d(x)$ を $f(x)$ と $g(x)$ の最大公約式とする．このとき，$a(x)f(x)+b(x)g(x)=d(x)$ を満たす $\mathbb{Q}$ 係数の多項式 $a(x)$ と $b(x)$ をそれぞれ一つずつ求めよ．

第 3 章

代数拡大

3.1 単純拡大体

$\mathbb{Q}[\sqrt{2}]$ や $\mathbb{Q}[\sqrt[3]{2}]$ は体であったが，体 $\mathbb{Q}$ はこれらの部分集合である．このように，体の部分集合で体となるものがある．

定義（拡大体） L を体，K を L の部分集合でかつ体であるとき，K を L の**部分体**，L を K の**拡大体**と呼ぶ．

定義（添加して得られる体） L を体，K を L の部分体，$x \in L$ とする．K の元を係数とする x の多項式全体 $K[x]$ が体であるとき，$K[x]$ を K に x を**添加して得られる体**と呼び，$K(x)$ と書く．すなわち，

$$K(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], g(x) \neq 0 \right\}.$$

定義（単純拡大体） K の拡大体 L が $L = K(x)$ であるとき，L は K の**単純拡大体**であるという．

定義（代数拡大体） L を体 K の拡大体とする．L の元 x に対して，0 でない K 係数の多項式 $f(X)$ が存在して，$f(x) = 0$ となるとき，x は K 上**代数的**であるという．そうでないとき，x は K 上**超越的**であるという．

L のすべての元が K 上代数的であるとき，L は K の**代数拡大体**であるという．そうでないとき，L は K の**超越拡大体**であるという．

$\mathbb{Q}[\sqrt{2}]$ も，$\mathbb{Q}[\sqrt[3]{2}]$ も体 $\mathbb{Q}$ の単純拡大体であり，代数拡大体である．一般に定理 1.1 を拡張した次の定理が知られている．証明には，前の節の多項式に関するユークリッド互徐法で述べた定理 2.2 が用いられる．

定理 3.1.　x を体 $\mathbb{Q}$ の代数的な元とする．このとき，$\mathbb{Q}[x] = \mathbb{Q}(x)$ である．

（証明）$f(x) = 0$ となる $\mathbb{Q}$ 係数の多項式 $f(X)$ は，$\mathbb{Q}$ 上既約（因数分解できない）で，次数が最小なものとする．このとき，最高次の係数は 1 としておく．$\mathbb{Q}$ 係数の多項式 $g(X) \in \mathbb{Q}[X]$ で $g(x) \neq 0$ であるもの考える．このとき，$g(x) \in \mathbb{Q}[x]$ である．一方，$g(X)$ は $f(X)$ を因数に持たないので，$f(X)$ と $g(X)$ の最大公約数は 1 である．定理 2.2 より，$\mathbb{Q}$ 係数の多項式 $a(X), b(X) \in \mathbb{Q}[X]$ が存在して，

$$a(X)f(X) + b(X)g(X) = 1$$

とすることができる．よって，$a(x)f(x) + b(x)g(x) = 1$ で $f(x) = 0$ より

$$b(x)g(x) = 1$$

である．これは $g(x)$ に逆数 $b(x)$ があることを意味する．よって，$\mathbb{Q}[x]$ は体であり，$\mathbb{Q}[x] = \mathbb{Q}(x)$ が成り立つ．（証明終）

定理 3.1 が有理化の一般的な意味となる．すなわち，$\mathbb{Q}(x)$ の元は x の**有理式**（$\mathbb{Q}$ 係数の多項式の比で表された式）であるが，それは $\mathbb{Q}[x]$ の元であるといっている．すなわち，$\mathbb{Q}(x)$ の元はすべて分母の有理化ができることを示している．

実は定理 2.2 は体 K 係数の多項式においても成立することから，定理 3.1 は，以下のように一般化される．

定理 3.2. x を体 K 上代数的な元とする．このとき，$K[x] = K(x)$ である．

例 3.1. $x = \sqrt{2} + \sqrt{3}$ とする．このとき，$2\sqrt{6} \in \mathbb{Q}[x]$ と $(2\sqrt{6})^{-1} \in \mathbb{Q}[x]$ をそれぞれ示せ．

解答．$x^2 = (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$ より

$$2\sqrt{6} = (\sqrt{2} + \sqrt{3})^2 - 5 = x^2 - 5 \in \mathbb{Q}[x]$$

である．これより

$$\frac{(x^2-5)^2}{24} = 1 \quad \rightarrow \quad \frac{x^2-5}{24} = \frac{1}{x^2-5}.$$

したがって，

$$(2\sqrt{6})^{-1} = \frac{1}{x^2-5} = \frac{1}{24}x^2 - \frac{5}{24} \in \mathbb{Q}[x]$$

である．（解答終）

問題 3.1. $x = \sqrt{2} + \sqrt{3}$ とする．このとき，$\sqrt{2} \in \mathbb{Q}[x]$ と $(\sqrt{2})^{-1} \in \mathbb{Q}[x]$ をそれぞれ示せ．

3.2　有限生成の代数拡大体

定義（添加して得られる体） L を体，K を L の部分体，$x_1, \cdots, x_n \in L$ とし．K の元を係数とする $x_1, \cdots, x_n$ の多項式全体 $K[x_1, \cdots, x_n]$ が体であるとき，$K[x_1, \cdots, x_n]$ を $x_1, \cdots, x_n$ を**添加して得られる体**と呼び，$K(x_1, \cdots, x_n)$ と書く．

例 3.2.　$\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ を考える．このとき，

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$$

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

解答．$(\sqrt{2})^2 = 2$, $(\sqrt{3})^2 = 3$, $(\sqrt{2})(\sqrt{3}) = \sqrt{6}$ より，$f(\sqrt{2}, \sqrt{3}) \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ ならば, $f(\sqrt{2}, \sqrt{3}) = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ $(a, b, c, d \in \mathbb{Q})$ と書ける．次に $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ を示す．定理 3.1 より，$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$ である．$K = \mathbb{Q}(\sqrt{2})$ と置くと，$f(\sqrt{2}, \sqrt{3}) = (a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3}$ $(a, b, c, d \in \mathbb{Q})$ は，$f(\sqrt{3}) = a + b\sqrt{3}$ $(a, b \in K)$ とできるので，$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = K[\sqrt{3}]$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = K(\sqrt{3})$ である．$\sqrt{3}$ は $\mathbb{Q}$ 上代数的で，$\mathbb{Q} \subset K$ より $\sqrt{3}$ は K 上代数的でもある．よって，定理 3.2 より，$K(\sqrt{3}) = K[\sqrt{3}]$ である．したがって，$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ である．（解答終）

問題 3.2. $\mathbb{Q}[\sqrt{2}, \omega]$ を考える．ここで，$\omega^3 = 1$ である．このとき，

$$\mathbb{Q}[\sqrt{2}, \omega] = \{a + b\sqrt{2} + c\omega + d\sqrt{2}\omega \mid a, b, c, d \in \mathbb{Q}\}$$

であり，$\mathbb{Q}[\sqrt{2}, \omega] = \mathbb{Q}(\sqrt{2}, \omega)$ であることを証明せよ．

定義（有限生成の体）$L = K(x_1, \cdots, x_n)$ であるとき，L を K 上**有限生成の体**という．

定理 3.2 は，さらに以下のように一般化される．

定理 3.3.　$x_1, \cdots, x_n$ を体 K 上代数的な元とする．このとき, $K[x_1, \cdots, x_n] = K(x_1, \cdots, x_n)$ である．

（証明）n に関する数学的帰納法を用いる．$n = 1$ のときは，定理 3.2 より成り立つ．$n-1$ まで $K[x_1, \cdots, x_{n-1}] = K(x_1, \cdots, x_{n-1})$ が成立していると仮定する．$M = K(x_1, \cdots, x_{n-1})$ と置くと, $K[x_1, \cdots, x_n] = M[x_n], K(x_1, \cdots, x_n) = M(x_n)$ である．x_n は K 上代数的で, $K \subset M$ でもあるので, x_n は M 上代数的である．よって，定理 3.2 より $M[x_n] = M(x_n)$ である．したがって，$K[x_1, \cdots, x_n] = M(x_n) = K(x_1, \cdots, x_n)$ である．（証明終）

例 3.3.　$x = \dfrac{1}{1+\sqrt{2}+\sqrt{6}} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ を示すことにより，x の分母の有理化を行え．

解答.
$$\begin{aligned} x &= \frac{1}{1+\sqrt{2}+\sqrt{6}} = \frac{1+\sqrt{2}-\sqrt{6}}{(1+\sqrt{2}+\sqrt{6})(1+\sqrt{2}-\sqrt{6})} \\ &= \frac{1+\sqrt{2}-\sqrt{6}}{2\sqrt{2}-3} = \frac{(1+\sqrt{2}-\sqrt{6})(2\sqrt{2}+3)}{(2\sqrt{2}-3)(2\sqrt{2}+3)} \\ &= -7-5\sqrt{2}+4\sqrt{3}+3\sqrt{6} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]. \end{aligned}$$

（解答終）

問題 3.3. $x = \dfrac{1}{1+\sqrt{2}+\sqrt{3}} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ を示すことにより，x の分母の有理化を行え．

第 4 章

単純拡大に関する定理

4.1　拡大次数

体 $\mathbb{Q}(\sqrt{2})$ を考えよう．

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

であったが，このとき $1, \sqrt{2}$ は $\mathbb{Q}(\sqrt{2})$ の生成元と呼ばれる．

次に，体 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ を考えよう．これは，

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\ \}$$

であった．そして，$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ の生成元は，$1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ である．

生成元の定義は以下である．

定義（有限生成の体の生成元） K を体，$L = K(x_1, \cdots, x_n)$ とする．

$$L = \{a_0 + a_1 y_1 + \cdots + a_m y_m \mid y_i \in L, a_i \in K\}$$

であるとき，$1,\ y_1,\ \cdots,\ y_m$ を L の**生成元**という．

さらに，$\mathbb{Q}(\sqrt{2},\sqrt{3})$ において $1,\sqrt{2},\sqrt{3},\sqrt{6}$ は $\mathbb{Q}$ 上 1 次独立である．1 次独立の定義を確認しよう．

定義（1 次独立） L を体，K を L の部分体とし，$x_1,x_2,\cdots,x_r \in L$ とする．$c_1,c_2,\cdots,c_r \in K$ で

$$c_1x_1+c_2x_2+\cdots+c_rx_r=0$$

をみたすものが，$c_1=c_2=\cdots=c_r=0$ のみであるとき，$x_1,x_2,\cdots,x_r$ は K 上**1 次独立**であるという．

$\mathbb{Q}(\sqrt{2},\sqrt{3})$ において $1,\sqrt{2},\sqrt{3},\sqrt{6}$ は $\mathbb{Q}$ 上 1 次独立であることを証明しよう．

まず，$1,\sqrt{2}$ が $\mathbb{Q}$ 上 1 次独立であることを示す．$c_1+c_2\sqrt{2}=0$ とする．もし $c_2\neq 0$ なら

$$\sqrt{2}=-\frac{c_1}{c_2}\in\mathbb{Q}$$

となり，$\sqrt{2}$ が無理数であることに矛盾する．よって，$c_2=0$，これより $c_1=0$ が得られる．したがって，1 と $\sqrt{2}$ は $\mathbb{Q}$ 上 1 次独立である．次に，

$$c_1+c_2\sqrt{2}+c_3\sqrt{3}+c_4\sqrt{6}=0$$

とする．これを

$$c_1+c_2\sqrt{2}+(c_3+c_4\sqrt{2})\sqrt{3}=0$$

と考える．$c_3\neq 0$ または $c_4\neq 0$ と仮定すると，

$$\sqrt{3}=-\frac{c_1+c_2\sqrt{2}}{c_3+c_4\sqrt{2}}$$

となる．これは，$\sqrt{3}=a+b\sqrt{2}$ となる $a,b\in\mathbb{Q}$ が存在することを意味する．両辺を 2 乗して，$-3+a^2+2b^2+2ab\sqrt{2}=0$ となるが，$1,\sqrt{2}$ は $\mathbb{Q}$ 上 1 次独立なので，

$a=b=0$ である．これは，$c_3\neq 0$ または $c_4\neq 0$ であるという仮定に矛盾する．よって，$c_3=c_4=0$ であり，再び，$1,\sqrt{2}$ は $\mathbb{Q}$ 上 1 次独立であることから，$c_1=c_2=0$ が得られる．したがって，$1,\sqrt{2},\sqrt{3},\sqrt{6}$ は $\mathbb{Q}$ 上 1 次独立である．

例 4.1. $1,\sqrt{3},\sqrt[3]{2},\sqrt[3]{4},\sqrt{3}\sqrt[3]{2},\sqrt{3}\sqrt[3]{4}$ は $\mathbb{Q}$ 上 1 次独立であることを利用して，

$$\frac{1}{\sqrt{3}+\sqrt[3]{2}}=a+b\sqrt{3}+c\sqrt[3]{2}+d\sqrt[3]{4}+e\sqrt{3}\sqrt[3]{2}+f\sqrt{3}\sqrt[3]{4}$$

となる $a,b,c,d,e,f\in\mathbb{Q}$ を求めよ．すなわち，$\dfrac{1}{\sqrt{3}+\sqrt[3]{2}}$ の分母を有理化せよ．

解答．$(a+b\sqrt{3}+c\sqrt[3]{2}+d\sqrt[3]{4}+e\sqrt{3}\sqrt[3]{2}+f\sqrt{3}\sqrt[3]{4})(\sqrt{3}+\sqrt[3]{2})=1$ であり，左辺を展開して，

$$(3b+2d)+(a+2f)\sqrt{3}+(a+3e)\sqrt[3]{2}+(c+3f)\sqrt[3]{4}+(b+c)\sqrt{3}\sqrt[3]{2}+(d+e)\sqrt{3}\sqrt[3]{4}=1$$

を得る．$1,\sqrt{3},\sqrt[3]{2},\sqrt[3]{4},\sqrt{3}\sqrt[3]{2},\sqrt{3}\sqrt[3]{4}$ は $\mathbb{Q}$ 上 1 次独立であるので，連立方程式

$$3b+2d=1,\ a+2f=0,\ a+3e=0,\ c+3f=0,\ b+c=0,\ d+e=0$$

を得る．これより，

$$a=-\frac{6}{23},\ b=\frac{9}{23},\ c=-\frac{9}{23},\ d=-\frac{2}{23},\ e=\frac{2}{23},\ f=\frac{3}{23}$$

を得る．（解答終）

問題 4.1. $\dfrac{1}{\sqrt{3}+\sqrt[3]{4}}$ の分母を有理化せよ．

一般的に，5 次以上の代数方程式の解はべき根（$\sqrt{x},\sqrt[3]{x},\sqrt[4]{x},\cdots$）を用いて表すことができないことが，証明されている（ガロア理論）．

例 4.2. $\mathbb{Q}$ 上既約な 5 次多項式 $f(X) = X^5 + 2X + 1 \in \mathbb{Q}[X]$ で，$f(\alpha) = 0$ となる α を考える．このとき，$1, \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4$ は $\mathbb{Q}$ 上 1 次独立であることを利用して，

$$\frac{1}{1+\alpha} = a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4$$

となる $a, b, c, d, e \in \mathbb{Q}$ を求めよ．すなわち，$\dfrac{1}{1+\alpha}$ の分母を有理化せよ．

解答．$(a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4)(1 + \alpha) = 1$ であり，$\alpha^5 = -2\alpha - 1$ に注意して，左辺を展開すると，

$$(a - e) + (a + b - 2e)\alpha + (b + c)\alpha^2 + (c + d)\alpha^3 + (d + e)\alpha^4 = 1$$

を得る．$1, \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4$ は $\mathbb{Q}$ 上 1 次独立であるので，連立方程式

$$a - e = 1,\ a + 2b - 2e = 0,\ b + c = 0,\ c + d = 0,\ d + e = 0$$

を得る．これより，

$$a = \frac{2}{3},\ b = -\frac{1}{3},\ c = \frac{1}{3},\ d = -\frac{1}{3},\ e = \frac{1}{3}$$

を得る．（解答終）

問題 4.2. $\mathbb{Q}$ 上既約な 5 次多項式 $f(X) = X^5 - X + 3 \in \mathbb{Q}[X]$ で，$f(\alpha) = 0$ となる α を考える．このとき，$\dfrac{1}{1+\alpha^2}$ の分母を有理化せよ．

定義（拡大次数） L を体，K を L の部分体とし，$x_1, x_2, \cdots, x_{n-1} \in L$ で，$M = \{a_0 + a_1x_1 + \cdots + a_{n-1}x_{n-1} \mid x_i \in L, a_i \in K\}$ は体であるとする．もし，$1, x_1, x_2, \cdots, x_{n-1}$ が K 上 1 次独立であるとき，M は K の n **次拡大体**であるといい，n を**拡大次数**と呼ぶ．そして，このことを

$$[M : K] = n$$

と表す．

上の定義から，$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ である．すなわち，$\mathbb{Q}(\sqrt{2})$ は $\mathbb{Q}$ の 2 次拡大体となっている．また，$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ である．すなわち，$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ は $\mathbb{Q}$ の 4 次拡大体となっている．さらに，$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ は

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

とみることもできる．このとき，$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ である．すなわち，$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ は $\mathbb{Q}(\sqrt{2})$ の 2 次拡大体となっている．

以下の定理が知られている．

定理 4.1. K, M, L をそれぞれ体とし，$L \supset M \supset K$ とする．このとき，$[L : M] = m$, $[M : K] = n$ ならば，$[L : K] = mn$ である．

例 4.3. $K = \mathbb{Q}$, $M = K(\sqrt{2})$, $L = M(\sqrt[3]{2})$ とする．$[M : K] = 2$ である．また，

$$M(\sqrt[3]{2}) = \{\ a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} \mid a_0, a_1, a_2 \in M\}$$

で，1, $\sqrt[3]{2}$, $\sqrt[3]{4}$ は M 上 1 次独立なので，$[L : M] = 3$ である．よって，定理 4.1 より，$[L : K] = 6$ である．

問題 4.3.　$K=\mathbb{Q},\ M=K(\sqrt{2}),\ L=M(\sqrt{3},\sqrt[3]{3})$ とする．このとき，$[L:M],\ [M:K],\ [L:K]$ をそれぞれ求めよ．

4.2　最小多項式

定義（最小多項式） L を体 K の拡大体，$x\in L$ を K 上代数的な元とする．$f(x)=0$ となる次数が最小な K 係数の K 上既約な多項式 $f(X)$ を，x の K 上の**最小多項式**という．

定理 4.2.　L を体 K の拡大体，$x\in L$ を K 上代数的な元とする．$f(X)$ を x の K 上の最小多項式とする．このとき，K 係数の多項式 $g(X)$ が $g(x)=0$ を満たすなら，$f(X)|g(X)$，すなわち $g(X)$ は $f(X)$ を因数にもつ．

（証明）$g(X)=f(X)q(X)+r(X)$ と置く．ここで，$q(X),r(X)$ は K 係数の多項式で，$r(X)$ については，その次数 $\deg\ r$ は $\deg\ r<\deg\ f$ を満たすか，または $r(X)=0$ であるとする．$f(x)=0,\ g(x)=0$ より $r(x)=0$ である．$f(X)$ は $f(x)=0$ となる多項式の中で次数が最小なものであったので，$r(X)=0$ である．したがって，$g(X)=f(X)q(X)$ であり，$f(X)|g(X)$ が示された．（証明終）

例 4.4. $f(X)=X^4-10X^2+1$ とし，$f(\alpha_i)=0$（$i=1,2,3,4$）とする．さらに，$g(X)$ を $\mathbb{Q}$ 係数の 5 次多項式で，$g(\sqrt{2}+\sqrt{3})=0$ とする．このとき，$g(\alpha_i)=0$（$i=1,2,3,4$）であることを示せ．

解答．$(\sqrt{2}+\sqrt{3})^4=49+20\sqrt{6},\ (\sqrt{2}+\sqrt{3})^2=5+2\sqrt{6}$ より，

$$(\sqrt{2}+\sqrt{3})^4-10(\sqrt{2}+\sqrt{3})^2+1=0.$$

$\alpha_1 = \sqrt{2} + \sqrt{3}$ と置き，$\mathbb{Q}$ の拡大体 $L = \mathbb{Q}(\alpha_1)$ を考えると，$f(X)$ は α_1 の最小多項式である．定理 4.2 より，$g(X) = f(X)(aX + b),\ a, b \in \mathbb{Q},\ a \neq 0$ である．したがって，$g(\alpha_i) = f(\alpha_i)(a\alpha_i + b) = 0$（$i = 1, 2, 3, 4$）となる．（解答終）

問題 4.4. $\sqrt{2} + \sqrt{3}$ の最小多項式 $f(X)$ を求め，$f(X) = 0$ の解を全て求めよ．

証明はしないが，以下の定理は重要である．

定理 4.3. L を体 K の拡大体，$x \in L$ を K 上代数的な元，$f(X)$ を x の K 上の最小多項式とする．このとき，

$$[K(x) \colon K] = \deg\ f$$

が成り立つ．

例 4.5. $f(X) = X^5 + 3X^2 + X^2 + 2X + 1$ とし，$f(\alpha) = 0$ となる α を考える．このとき，$[\mathbb{Q}(\alpha), \mathbb{Q}]$ を求めよ．

解答．$f(X)$ を体 $\mathbb{Q}$ 上で因数分解すると，

$$f(X) = (X^3 + 2X + 1)(X^2 + 1)$$

である．$g(X) = X^3 + 2X + 1$, $h(X) = x^2 + 1$ とする．$g(\alpha) = 0$ ならば, $[\mathbb{Q}(\alpha), \mathbb{Q}] = 3$，$h(\alpha) = 0$ ならば，$[\mathbb{Q}(\alpha), \mathbb{Q}] = 2$ である．（解答終）

問題 4.5. $f(X) = X^6 + 5X^4 + 8X^2 + 6$ とし，$f(\alpha) = 0$ となる α を考える．このとき，$[\mathbb{Q}(\alpha), \mathbb{Q}]$ を求めよ．

4.3　単純拡大に関する定理

体 $\mathbb{Q}$ 上有限生成の体 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ を考えよう．これは，

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}\}$$

であった．

次に，体 $\mathbb{Q}$ の単純拡大体 $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ を考えよう．

$$(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$$

であることから，

$$\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \{a+b(\sqrt{2}+\sqrt{3})+c\sqrt{6} \mid a,b,c \in \mathbb{Q}\}$$

このことから，明らかに $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3})$ である．

実は，$\mathbb{Q}(\sqrt{2},\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$ である．このことを証明しよう．

そのためには，$\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$，$\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ を示せばよい．

$$\sqrt{2} = (\sqrt{2}+\sqrt{3})(-2+\sqrt{6}) \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$
$$\sqrt{3} = (\sqrt{2}+\sqrt{3})(3-\sqrt{6}) \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

したがって，$\mathbb{Q}(\sqrt{2},\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$ である．よって，$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$，つまり，$\mathbb{Q}$ 有限生成の体 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ は $\mathbb{Q}$ の単純拡大体 $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ であることがわかったである．

一般に，以下の定理が知られており，本書が紹介したかった定理である．

定理 4.4.　$\mathbb{Q}$ 上有限生成の体 L は，代数拡大であり，さらに $\mathbb{Q}$ の単純拡大体である．すなわち，$L = \mathbb{Q}(x_1,\cdots,x_n) = \mathbb{Q}(x)$ となる代数的な元 $x \in L$ が存在する．

例 4.6. $f(X)=X^2+5,\ g(X)=X^3+X+2$ とし，$f(s)=0,\ g(t)=0$ とする．このとき，$\mathbb{Q}(s,t)=\mathbb{Q}(s+kt)$ となる $k\in\mathbb{Q}$ が存在することを証明せよ．

解答. $s^2=-5,\ t^3=-t-2$ であり，$s+kt\in Q(s,t)$ より，$\mathbb{Q}(s+kt)\subset\mathbb{Q}(s,t)$ である．したがって，$\mathbb{Q}(s,t)\subset\mathbb{Q}(s+kt)$ となる $k\in\mathbb{Q}$ の存在を示せばよい．そのためには，$s\in\mathbb{Q}(s+kt),\ t\in\mathbb{Q}(s+kt)$ となる $k\in\mathbb{Q}$ の存在を示せばよい．

$w=s+kt\ (k\neq 0)$ と置く．$f(w-kt)=0$ である．ここで，$F(X)=f(w-kX)$ と置くと，$F(X)$ は $\mathbb{Q}(w)[X]$ の元となる．勿論，$g(X)$ も $\mathbb{Q}(w)[X]$ の元とみることができる．そして t は $g(X)=0$ と $F(X)=0$ の共通解である．一方，$f(X)=0$ のもう一つの解を s'，$g(X)=0$ の残りの 2 つの解を $t_1,\ t_2$ とすると，

$$g(X)=(X-t)(X-t_1)(X-t_2)$$

$$\begin{aligned}F(X)&=(w-kX-s)(w-kX-s')\\&=k^2\left(X-\frac{w-s}{k}\right)\left(X-\frac{w-s'}{k}\right)\\&=k^2\left(X-\frac{(s+kt)-s}{k}\right)\left(X-\frac{(s+kt)-s'}{k}\right)\\&=k^2\,(X-t)\left(X-t-\frac{s-s'}{k}\right)\end{aligned}$$

となる．ここで，$t_1\neq t+\dfrac{s-s'}{k}$ と $t_2\neq t+\dfrac{s-s'}{k}$ のいずれも満たす k を考えると，$X-t$ は $\mathbb{Q}(w)$ 係数の $g(X)$ と $F(X)$ の最大公約式となる．定理 2.2 より，$\mathbb{Q}(w)$ 係数の多項式 $a(X),b(X)$ が存在して

$$X-t=a(X)g(X)+b(x)F(X)$$

となる．よって, $X-t\in\mathbb{Q}(w)[X]$, これより, $t\in\mathbb{Q}(w)$ であり, $s=w-kt\in\mathbb{Q}(w)$ である．ゆえに, この k により, $\mathbb{Q}(s,t)\subset\mathbb{Q}(s+kt)$ となる．よって, $\mathbb{Q}(s,t)=\mathbb{Q}(s+kt)$ となる $k\in\mathbb{Q}$ が存在することが示された．（解答終）

問題 4.6. $f(X)=X^2-X-1,\ g(X)=2X^2-X-4$ とし，$f(s)=0,\ g(t)=0$ とする．このとき，$\mathbb{Q}(s,t)=\mathbb{Q}(s+2t)$ となることを証明せよ．

問題の解答

問題 1.1　$a \in Z$ 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 $x \in Z$ が存在しない．よって，Z は体ではない．

問題 1.2　(1)　体の定義 (1), (2), (3),(4),(5) と (7) は明らかに成り立つので，体の定義 (6) の $(a + b\sqrt{3})$ の逆元 x の存在を示す．$(a + b\sqrt{3})x = 1$ となるものなので，

$$x = \frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{(a + b\sqrt{3})(a - b\sqrt{3})} = \frac{a}{a^2 - 3b^2} + \frac{-b}{a^2 - 3b^2}\sqrt{3} \in \mathbb{Q}(\sqrt{3}).$$

よって，$\mathbb{Q}[\sqrt{3}]$ は体である．

(2)　$i = \sqrt{-1}$ とする．体の定義 (1), (2), (3),(4),(5) と (7) は明らかに成り立つので，体の定義 (6) の $(a + bi)$ の逆元 x の存在を示す．$(a + bi)x = 1$ となるものなので，

$$x = \frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i \in G.$$

よって，$\mathbb{Q}[\sqrt{-1}]$ は体である．

問題 1.3　(1), (2), (3),(4),(5) と (7) は明らかに成り立つので，(6) の $(a + b\sqrt[3]{3} + c\sqrt[3]{9})$ の逆元 x の存在を示す．$(a + b\sqrt{3} + c\sqrt[3]{9})x = 1$ となるものなので，

$$x = \frac{1}{a + b\sqrt{3} + c\sqrt[3]{9}} \in \mathbb{Q}(\sqrt[3]{3})$$

を示せばよい．$f(x) = x^3 - 3$ と $g(x) = a + bx + cx^2$, $(c \neq 0)$ を考える．$f(x)$ と $g(x)$ の最大公約数が 1 より

$$\alpha(x)f(x) + \beta(x)g(x) = 1$$

を得る．ここで，$\alpha(x)$ も $\beta(x)$ も $\mathbb{Q}$ 係数の多項式である．したがって，x に $\sqrt[3]{3}$ を代入することで，

$$\frac{1}{a + b\sqrt[3]{3} + c\sqrt[3]{9}} = \beta(\sqrt[3]{3}) \in \mathbb{Q}(\sqrt[3]{3})$$

が得られる．$c = 0$, $b \neq 0$ の場合も同様にして示される．よって，$\mathbb{Q}(\sqrt[3]{3})$ は体である．

問題 2.1　$49911 = 2\cdot 18923 + 12065$, $18923 = 12065 + 6858$, $12065 = 6858 + 5207$, $6858 = 5207 + 1651$, $5207 = 3\cdot 1651 + 254$, $1651 = 6\cdot 254 + 127$, $254 = 2\cdot 127 + 0$ よって，$d = 127$

問題 2.2　$a = 5^2\cdot 7\cdot 13$, $b = 5\cdot 7^2$ より $d = 35$ である．$2275x + 245y = 35$ より $65x + 7y = 1$ を得る．よって，両辺を 7 で割った余りで考えると，$2x \equiv 1 \mod 7$. これより，$x = 4$, $y = -37$ を得る．

問題 2.3　$d(x) = (2x-1)$ である．$a(x)f(x) + b(x)g(x) = d(x)$ より

$$(x-1)a(x) - (x+1)(2x+1)b(x) = 1$$

である．両辺を $x-1$ で割った余りを考えると，$-6b(x) \equiv 1 \mod x-1$ となるので，$b(x) = -\dfrac{1}{6}$ がとれる．よって，

$$a(x) = \frac{1 + (x+1)(2x+1)\left(-\frac{1}{6}\right)}{x-1} = -\frac{1}{3}x - \frac{5}{6}$$

を得る．

問題 3.1　$\sqrt{2} = (\sqrt{2}+\sqrt{3})(-\sqrt{2}+\sqrt{6})$ であり，$\sqrt{6} = \dfrac{1}{2}(x^2-5)$ であったので，

$$\sqrt{2} = x\left(-2 + \frac{1}{2}(x^2-5)\right) = \frac{1}{2}x^3 - \frac{9}{2}x \in \mathbb{Q}[x].$$

さらに，$\dfrac{1}{2}\cdot\left(\dfrac{1}{2}x^3 - \dfrac{9}{2}x\right)^2 = 1$ より，$(\sqrt{2})^{-1} = \dfrac{1}{4}x^3 - \dfrac{9}{4}x \in \mathbb{Q}[x]$.

問題 3.2　$(\sqrt{2})^2 = 2$, $\omega^2 = -1-\omega$ より，$f(\sqrt{2},\omega) \in \mathbb{Q}[\sqrt{2},\omega]$ ならば，$f(\sqrt{2},\omega) = a + b\sqrt{2} + c\omega + d\sqrt{2}\omega$ （$a,b,c,d \in \mathbb{Q}$）と書ける．次に $\mathbb{Q}[\sqrt{2},\omega] = \mathbb{Q}(\sqrt{2},\omega)$ を示す．定理 3.1 より，$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$ である．$K = \mathbb{Q}(\sqrt{2})$ と置くと，$f(\sqrt{2},\omega) = (a + b\sqrt{2}) + (c + d\sqrt{2})\omega$ （$a,b,c,d \in \mathbb{Q}$）は，$f(\omega) = a + b\omega$ （$a,b \in K$）とできるので，$\mathbb{Q}[\sqrt{2},\sqrt{3}] = K[\omega]$，$\mathbb{Q}(\sqrt{2},\omega) = K(\omega)$ である．ω は $\mathbb{Q}$ 上代数的で，$\mathbb{Q} \subset K$ より ω は K 上代数的でもある．よって，定理 3.2 より，$K(\omega) = K[\omega]$ である．したがって，$\mathbb{Q}(\sqrt{2},\omega) = \mathbb{Q}[\sqrt{2},\omega]$ である．

問題 3.3

$$\begin{aligned} x &= \frac{1}{1+\sqrt{2}+\sqrt{3}} = \frac{1+\sqrt{2}-\sqrt{3}}{(1+\sqrt{2}+\sqrt{3})(1+\sqrt{2}-\sqrt{3})} \\ &= \frac{1+\sqrt{2}-\sqrt{3}}{2\sqrt{2}} = \frac{(1+\sqrt{2}-\sqrt{3})\sqrt{2}}{(2\sqrt{2})\sqrt{2}} \\ &= \frac{2+\sqrt{2}-\sqrt{6}}{4} \in \mathbb{Q}[\sqrt{2},\sqrt{3}]. \end{aligned}$$

問題 4.1 $\dfrac{1}{\sqrt{3}+\sqrt[3]{4}} = a+b\sqrt{3}+c\sqrt[3]{2}+d\sqrt[3]{4}+e\sqrt{3}\sqrt[3]{2}+f\sqrt{3}\sqrt[3]{4}$ と置く．

$$(a+b\sqrt{3}+c\sqrt[3]{2}+d\sqrt[3]{4}+e\sqrt{3}\sqrt[3]{2}+f\sqrt{3}\sqrt[3]{4})(\sqrt[3]{2}+\sqrt[3]{4}) = 1$$

であり，左辺を展開して，

$$(3b+2c)+(a+2e)\sqrt{3}+(2d+3e)\sqrt[3]{2}+(a+3f)\sqrt[3]{4}+(c+2f)\sqrt{3}\sqrt[3]{2}+(b+d)\sqrt{3}\sqrt[3]{4} = 1$$

を得る．$1, \sqrt{3}, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{3}\sqrt[3]{2}, \sqrt{3}\sqrt[3]{4}$ は $\mathbb{Q}$ 上 1 次独立であるので，連立方程式

$$3b+2c=1,\ a+2e=0,\ 2d+3e=0,\ a+3f=0,\ c+2f=0,\ b+d=0$$

を得る．これより，

$$a=-\frac{12}{11},\ b=\frac{9}{11},\ c=-\frac{8}{11},\ d=-\frac{9}{11},\ e=\frac{6}{11},\ f=\frac{4}{11}$$

を得る．よって，

$$\frac{1}{\sqrt{3}+\sqrt[3]{4}} = \frac{-12+9\sqrt{3}-8\sqrt[3]{2}-9\sqrt[3]{4}+6\sqrt{3}\sqrt[3]{2}+4\sqrt{3}\sqrt[3]{4}}{11}$$

である．

問題 4.2 $\dfrac{1}{1+\alpha} = a+b\alpha+c\alpha^2+d\alpha^3+e\alpha^4$ と置く．

$$(a+b\alpha+c\alpha^2+d\alpha^3+e\alpha^4)(1+\alpha^2) = 1$$

であり，$\alpha^5 = \alpha - 3$ に注意して，左辺を展開すると，

$$(a-e) + (a+b-2e)\alpha + (b+c)\alpha^2 + (c+d)\alpha^3 + (d+e)\alpha^4 = 1$$

を得る．$1, \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4$ は $\mathbb{Q}$ 上 1 次独立であるので，連立方程式

$$a - 3d = 1,\ b + d - 3e = 0,\ a + c + e = 0,\ b + d = 0,\ c + e = 0$$

を得る．これより，

$$a = 0,\ b = \frac{1}{3},\ c = 0,\ d = -\frac{1}{3},\ e = 0$$

を得る．よって，

$$\frac{1}{1+\alpha^2} = \frac{\alpha - \alpha^3}{3}$$

である．

問題 4.3 $[M : K] = 2$．また，
$M(\sqrt{3}, \sqrt[3]{3}) = \{a + b\sqrt{3} + c\sqrt[3]{3} + d\sqrt[3]{9} + e\sqrt[3]{3}\sqrt{3} + f\sqrt[3]{9}\sqrt{3} \mid a, b, c, d, e, f \in M\}$ で，$1, \sqrt{3}, \sqrt[3]{3}, \sqrt[3]{9}, \sqrt[3]{3}\sqrt{3}, \sqrt[3]{9}\sqrt{3}$ は M 上 1 次独立なので，$[L : M] = 6$．定理 4.1 より，$[L : K] = 12$.

問題 4.4 $X = \pm\sqrt{2} \pm \sqrt{3}$ と置く．$(X \mp \sqrt{2})^2 = 3$ より，$X^2 - 1 = \pm 2\sqrt{2}X$ である．よって，$(X^2 - 1)^2 = 8X^2$．これより，$X^4 - 10X + 1 = 0$ したがって，$X = \sqrt{2} + \sqrt{3}$ の最小多項式 $f(X)$ は $f(X) = X^4 - 10X + 1$ であり，$f(X) = 0$ の解は，$X = \sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} + \sqrt{3}, -\sqrt{2} - \sqrt{3}$ である．

問題 4.5 $f(X)$ を体 $\mathbb{Q}$ 上で因数分解すると，

$$f(X) = (X^4 + 2X^2 + 8x^2 + 6)(X^2 + 3)$$

である．$g(X) = X^4 + 2X^2 + 8x^2 + 6$，$h(X) = X^2 + 3$ とする．$g(\alpha) = 0$ ならば，$[\mathbb{Q}(\alpha), \mathbb{Q}] = 4$，$h(\alpha) = 0$ ならば，$[\mathbb{Q}(\alpha), \mathbb{Q}] = 2$ である．

問題 4.6 $s^2 = s+1, 2t^2 = t+4$ であり，$s+2t \in \mathbb{Q}(s,t)$ より，$\mathbb{Q}(s+2t) \subset \mathbb{Q}(s,t)$ である．したがって，$\mathbb{Q}(s,t) \subset \mathbb{Q}(s+2t)$ を示せばよい．そのためには，$s \in \mathbb{Q}(s+2t)$，$t \in \mathbb{Q}(s+2t)$ を示せばよい．

$w = s + 2t$ と置く．$f(w - 2t) = 0$ である．ここで，$F(X) = f(w - 2X)$ と置くと，$F(X)$ は $\mathbb{Q}(w)[X]$ の元となる．勿論，$g(X)$ も $\mathbb{Q}(w)[X]$ の元とみることができる．そして t は $g(X) = 0$ と $F(X) = 0$ の共通解である．一方，$f(X) = 0$ のもう一つの解を s'，$g(X) = 0$ のもう一つの解を t' とすると，

$$g(X) = (X - t)(X - t')$$

$$\begin{aligned} F(X) &= (w - 2X - s)(w - 2X - s') \\ &= 4\left(X - \frac{w - s}{2}\right)\left(X - \frac{w - s'}{2}\right) \\ &= 4\left(X - \frac{(s + 2t) - s}{2}\right)\left(X - \frac{(s + 2t) - s'}{2}\right) \\ &= 4\,(X - t)\left(X - t - \frac{s - s'}{2}\right) \end{aligned}$$

となる．ここで，$(s - s')^2 = (s + s')^2 - 4ss' = \dfrac{1}{4} + 8 = \dfrac{33}{4}$ より $(s - s') = \pm\dfrac{\sqrt{33}}{2}$ である．$t' = t + \dfrac{s - s'}{2}$ を仮定すると，$t' - t = \dfrac{s - s'}{2} = \pm\dfrac{\sqrt{33}}{4}$ である．しかし，$(t' - t)^2 = (t' + t)^2 - 4tt' = 1 + 4 = 5$ より $(t' - t) = \pm\sqrt{5}$ となり，仮定に矛盾する．

したがって，$X - t$ は $\mathbb{Q}(w)$ 係数の $g(X)$ と $F(X)$ の最大公約式となる．定理 2.2 より，$\mathbb{Q}(w)$ 係数の多項式 $a(X), b(X)$ が存在して

$$X - t = a(X)g(X) + b(x)F(X)$$

となる．よって，$X - t \in \mathbb{Q}(w)[X]$，これより，$t \in \mathbb{Q}(w)$ であり，$s = w - 2t \in \mathbb{Q}(w)$ である．ゆえに，$\mathbb{Q}(s, t) \subset \mathbb{Q}(s + 2t)$ が得られた．よって，$\mathbb{Q}(s, t) = \mathbb{Q}(s + 2t)$ が示された．