$\mathrm{M_L}^3$

"$\mathrm{M_L}^3$" is the name of project
Mathematics of the Learners,
for the Learners, by the Learners,
or group of the project members.
And it has another name:
Mathematical Love Letter,
too Late, to you.
We believe Mathematics must be, like GNU in soft-ware, hacked freely. Euler, Gauss and Galois now should be the BEST-HACKERs.

# 作図不可能問題と2次体

## — 現代代数学的観点から —

***The Famous Impossibilities and Quadratic Fields***

***— From a Modern Algebraic Point of View. —***


**山下弘一郎**

**YAMASHITA, Koichiro**



This Document is $\mathrm{M_L}^3$-doc No. `kymst-alg0001`. Version `2007/08/25(Sat)`



Category: Algebra, Number Field, Geometry.


We hope your Exciting Math, Happy Hack and Whole Lotta Love.

Group $\mathrm{M_L}^3$. 2007. :-)

## Document Log

- `2007/08/25(Sat)`: The Last Alpha Version with Figures.
- `2006/04/14(Fri)`: The Last Alpha Version without Figures. `^^;`
- Originarily early draft of this doc. is written in manuscript for the material of meeting named AOM `1996/09/29(Sun)`.

# Contents

**Abstract**

この章では，立方体倍積問題と角の 3 等分問題の不可能性，つまり定木と compass による作図の不可能性を，現代代数学的観点から考察し証明する．残る円積問題は，残念ながら『解析学的要素』を多く含むために，示唆するに止める．

問題の成立はギリシア数学の自立とほぼ時を同じくするが，これらの問題が否定的に解かれる，つまり不可能性が証明される，のは，1837 年のことである．紀元前 5 世紀から 19 世紀まで，2400 年の時が流れる．そして，フランスの「ヤク中」(アヘン中毒患者)

Pierre Wantzel (1814-1848)

によって解決されることになる．ヨーロッパ数学 (それは，筆者の観点からする唯一の数学である．その理由は別に論を立てることを必要とするが，概略，世界理解としての数学足りうるのは，ヨーロッパのそれのみであることによる) が，不可能性をめぐって巡って現代にまで至った好例である．

この，

幾何学的問題が代数学によって解決される

というのが重要な点なのである．

以下，慣用に従い

$\mathbb{N}$: 非負整数の集合，　$\mathbb{Z}$: 整数の集合，　$\mathbb{Z}^+$: 正整数の集合
$\mathbb{Q}$: 有理数の集合，　$\mathbb{R}$: 実数の集合，　$\mathbb{C}$: 複素数の集合

とする．

# *Lecture* 1

# 不可能性証明 — 代数学的観点から

## § 1–1. いくつかの定義と準備

### 1.1.1 体

加減乗除 (0 による除法は除く) に関して閉じている集合を**体** (「タイ」と読む. ) と言う] (**Eng. *field*, Deu. *Körper***). 例えば有理数の集合 $\mathbb{Q}$, 実数の集合 $\mathbb{R}$, 複素数の集合 $\mathbb{C}$ は体であるが, 整数の集合 $\mathbb{Z}$ は除法について閉じていないから体ではない.

$\mathbb{F}$ が体であるとする. $\mathbb{F}$ の部分集合 $\mathbb{E}$ が, $\mathbb{F}$ と同じ演算 (加減乗除) でやはり体となることがある. このとき,

$\mathbb{E}$ は $\mathbb{F}$ の**部分体** (*subfield*) である,
$\mathbb{F}$ は $\mathbb{E}$ の**拡大体** (*extension field*) である

などとヌカス. 例えば $\mathbb{Q}$ は $\mathbb{R}$ の部分体, $\mathbb{Q}, \mathbb{R}$ は $\mathbb{C}$ の部分体である. 逆に, $\mathbb{R}$ や $\mathbb{C}$ は $\mathbb{Q}$ の拡大体, $\mathbb{C}$ は $\mathbb{R}$ の拡大体である.

### 1.1.2 Vector 空間

Vector と呼ばれる要素からなる集合 $V$ と体 $\mathbb{F}$ について,

$V$ が $\mathbb{F}$ 上の vector 空間 (***vector space***) である

とは, 次の (i) から (vi) がみたされることである :

(i) $V$ は加法 $+$ について閉じていて, 交換法則が成り立つ.
(ii) $\lambda \in \mathbb{F}$, $\boldsymbol{v} \in V$ ならば $\lambda \boldsymbol{v} \in V$.
(iii) $\lambda_1, \lambda_2 \in \mathbb{F}$, $\boldsymbol{v} \in V$ ならば $(\lambda_1 + \lambda_2)\,\boldsymbol{v} = \lambda_1 \boldsymbol{v} + \lambda_2 \boldsymbol{v}$.
(iv) $\lambda \in \mathbb{F}$, $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ ならば $\lambda\,(\boldsymbol{v}_1 + \boldsymbol{v}_2) = \lambda \boldsymbol{v}_1 + \lambda \boldsymbol{v}_2$.
(v) $1$ が $\mathbb{F}$ の乗法単位元ならば, 任意の $\boldsymbol{v} \in V$ について $1 \cdot \boldsymbol{v} = \boldsymbol{v}$.
(vi) $\lambda_1, \lambda_2 \in \mathbb{F}$, $\boldsymbol{v} \in V$ ならば, $\lambda_1\,(\lambda_2 \boldsymbol{v}) = (\lambda_1 \lambda_2)\,\boldsymbol{v}$.

幾何学的な (平面)vector $\boldsymbol{a}, \boldsymbol{b}$ で考えれば, 体 $\mathbb{F}$ が実数体 $\mathbb{R}$ として, オナジミの平面 vector の集合が $V$ となる. ところが, $1$ と $\sqrt{2}$ を 2 つの異なる vector と考えて, $a, b \in \mathbb{Q}$ について $a + b\sqrt{2}$ で表される数すべてからなる集合を作ると, この集合

$$V = \left\{ a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Q} \right\}$$

は $\mathbb{Q}$ 上の vector 空間と見なすことができる.

Vector 空間の定義の (i) から (vi) までを，この集合 $V$ がみたすことを確かめておくこと．

体 $\mathbb{F}$ 上の vector 空間 $V$ に含まれる vector $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n$ について，任意の vector $\boldsymbol{v} \in V$ が

$$\boldsymbol{v} = \lambda_1 \boldsymbol{v}_1 + \lambda_2 \boldsymbol{v}_2 + \cdots + \lambda_n \boldsymbol{v}_n \quad (\lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbb{F})$$

で表されるとき，

$$\text{集合 } \{\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n\} \text{ は } \mathbb{F} \text{ 上で vector 空間 } V \text{ を張る } (\textbf{spans } V \textbf{ over } \mathbb{F})$$

と言う．Vector 空間が有限次元であるとは，その vector 空間を張る vector の集合 $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n\}$ が有限集合であることである．例えば，平面 vector の集合は，平行でない 2 つの vector によって張られるから，有限次元である．

また，上で触れた集合 $V = \left\{a + b\sqrt{2} \,\middle|\, a, b \in \mathbb{Q}\right\}$ も集合 $\left\{1, \sqrt{2}\right\}$ で張られるから，有限次元である．

Vector 空間 $V$ の加法単位元を $\boldsymbol{o}$ とする (いわゆる zero vector)．Vector の集合 $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n\} \subset V$ が

$$\mathbb{F} \text{ 上で線形独立 (1 次独立) である } (\textbf{linearly-independent over } \mathbb{F})$$

とは，zero vector $\boldsymbol{o}$ が $\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n$ の自明な線形結合のみによって表されることである．つまり，

$$\boldsymbol{o} = \lambda_1 \boldsymbol{v}_1 + \lambda_2 \boldsymbol{v}_2 + \cdots + \lambda_n \boldsymbol{v}_n \quad (\lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbb{F})$$

ならば

$$\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$$

が成り立つことである．

集合 $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n\}$ が $\mathbb{F}$ 上の $V$ の基底 (**basis**) である，とは，この集合が $\mathbb{F}$ 上で $V$ を張り，かつ $\mathbb{F}$ 上で線形独立であることである．

有限次元の vector 空間の基底の選び方はいくらでもあるが，どのように基底を選んでもそれに含まれる vector の個数は一定である (**これを「基底定理」*basis theorem* と言う．**)．その個数を，その vector 空間の次元 (**dimension**) と言う．$n$ 次元 vector 空間で，$n$ 個より多くの vector をとるとき，それらは線形独立ではなく，どの vector をとっても他の vector の線形結合で表すことができる．このようなとき，それらの vector は線形従属 (**linearly dependent**) である，と言われる．

### 1.1.3 体と vector 空間

体 $\mathbb{F}$ とその部分体 $\mathbb{E}$ が与えられたとき，$\mathbb{F}$ を $\mathbb{E}$ 上の vector 空間と考えることができる．例えば $\mathbb{F}$ として $\mathbb{C}$，$\mathbb{E}$ として $\mathbb{R}$ をとれば，$\mathbb{C}$ の要素はすべて $a + b\boldsymbol{i} = a \cdot 1 + b \cdot \boldsymbol{i}$ $(a, b \in \mathbb{R},\ \boldsymbol{i}^2 = -1)$ と表されるから，$\mathbb{C}$ は $\mathbb{R}$ 上の vector 空間で，その基底は $\{1, \boldsymbol{i}\}$ である．

また，$\mathbb{Q}$ は $\mathbb{R}$ の部分体であるから，$\mathbb{R}$ も $\mathbb{Q}$ 上の vector 空間である．その基底は無限個あるから，$\mathbb{R}$ は $\mathbb{Q}$ 上の無限次元 vector 空間になる．

そこで，次のように定義する：

> 体 $\mathbb{F}$ とその部分体 $\mathbb{E}$ について，$\mathbb{F}$ が $\mathbb{E}$ の有限次元 vector 空間であるとき，その次元を $[\mathbb{F} : \mathbb{E}]$ で表し，これを
>
> $$\mathbb{F} \text{ の } \mathbb{E} \text{ 上の次数 } (\textbf{degree of } \mathbb{F} \textbf{ over } \mathbb{E})$$
>
> と言う．$[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{R}] = 1$ であることは明らかであろう．

### 1.1.4 多項式 Polynomials

$\mathbb{F}$ を体とする．ある「ナンダカワカランモノ」,「ワカランからそれ以上考エナイコトにしたもの」$X$ を定めて，$a_0,\ a_1,\ a_2,\ \cdots,\ a_n \in \mathbb{F}$ について

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \qquad \cdots(\#)$$

という「形式」を考え，それを多項式 (**形式的多項式　polynomial form**) と言う．

$X$ は，ある値をとったり，変化したりしない．つまり変数ではない．従って，多項式は関数ではない．

このように，多項式を形式的に考えるとき，文字 $X$ を不定元 (**indeterminate**) と言う．多項式で重要なのは不定元ではなく，その係数 $a_0,\ a_1,\ a_2,\ \cdots,\ a_n$ である．

$a_0,\ a_1,\ a_2,\ \cdots,\ a_n \in \mathbb{F}$ のとき，その多項式を体 $\mathbb{F}$ 上の多項式 (**polynomial over** $\mathbb{F}$) と言う．

2 つの多項式が等しいことを，それらの係数がそれぞれのべきに関して等しいことと定義する．

多項式 $(\#)$ で $a_n$ が 0 でないとき，この多項式の次数は $n$ であると言う．係数 $a_0,\ a_1,\ a_2,\ \cdots,\ a_n$ がすべて 0 であるとき，その多項式を zero 多項式と言い，その次数は考えない (マイナス無限大である，とする流儀もある)．

不定元 $X$ についての多項式を $f(X),\ g(X)$ などで表すのはいつも通りである．多項式 $f(X)$ の次数を $\deg f(X)$，あるいは $\deg f$ で表す．$\deg f(X) = n$ であるとき，$a_nX^n$ を多項式 $f(X)$ の主項 (**leading term，principal term**)，また係数 $a_n$ を主係数 (**leading coefficient，principal coefficient**) と言う．

体 $\mathbb{F}$ 上の多項式すべての集合を $\mathbb{F}[X]$ で表す．$\mathbb{F}[X]$ は多項式の加・減・乗法について閉じている．このように,「加・減・乗法について閉じている集合」を環 (**ring**) と言う．そこで $\mathbb{F}[X]$ を体 $\mathbb{F}$ 上の多項式環 (**polynomial ring over** $\mathbb{F}$) と言うことがある．

実際には $\mathbb{F}$ が体である必要はない．$\mathbb{F}$ そのものが環であれば，$\mathbb{F}[X]$ も環になる (確かめられたい)．

### 1.1.5 有理数解の TEST

多項式 $f(X)$ のゼロ点 (**zero point**) とは，$f(\alpha) = 0$ となる $\alpha$ のことである．次の判定法は，$\mathbb{Q}[X]$ に含まれるある多項式 $f(X)$ の，$\mathbb{Q}$ に含まれるゼロ点を見出すのに用いられる．

まず，$\mathbb{Q}[X]$ の多項式は $\mathbb{Z}[X]$ の多項式に書き換えられる．各係数の分母の最小公倍数 $l$ を求めて，$\frac{1}{l}$ でくくれば，$\mathbb{Z}$ 上の多項式が得られる．従って $\mathbb{Q}[X]$ の多項式のゼロ点を見出すことは，$\mathbb{Z}[X]$ の多項式のゼロ点を見出すことと同値である．次が成り立つ：

**THEOREM 1.1.1 (ヘタナテッポウ定理)**

$f(X) \in \mathbb{Z}[X]$ を $n$ 次の多項式とする：

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n, \quad a_i \in \mathbb{Z},\ a_n \neq 0.$$

有理数，特に既約分数 $\beta = \frac{r}{s}$ が $f(X)$ のゼロ点であるとき，

(i) $r \,\big|\, a_0$.　(ii) $s \,\big|\, a_n$.

---

*Proof.*

$f(\beta) = 0$ より

$$\begin{aligned} & a_0 + a_1\left(\frac{r}{s}\right) + a_2\left(\frac{r}{s}\right)^2 + \cdots + a_n\left(\frac{r}{s}\right)^n = 0 \\ \iff & a_0s^n + a_1rs^{n-1} + a_2r^2s^{n-2} + \cdots + a_nr^n = 0 \\ \iff & a_0s^n = -r\left(a_1s^{n-1} + a_2rs^{n-2} + \cdots + a_nr^{n-1}\right). \end{aligned}$$

よって $r$ は $a_0 s^n$ の約数である．ところが $r$ と $s$ は互いに素であるから，$r \mid a_0$.
　同様に

$$a_n r^n = -s\left(a_0 s^{n-1} + a_1 r s^{n-2} + \cdots + a_{n-1} r^{n-1}\right)$$

が成り立つから，$s$ は $a_n r^n$ の約数で，結局 $s \mid a_n$. ■

因数定理と組立て除法により高次方程式を解くときに，この定理 Theorem 1.1.1 (p.3) はしばしば乱用・悪用されるが，本来は次のような用い方をするべき定理である．

**Example 1.1.2**

2 の実数 5 乗根 $\sqrt[5]{2}$ は無理数である．

---

*Proof.*

$\sqrt[5]{2}$ は多項式 $f(X) = 2 - X^5$ のゼロ点である．もちろん $f(X) \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$ であるから，ヘタナテッポウ定理が使える．
　いま，$\frac{r}{s}$(既約分数) が $f(X)$ のゼロ点であるとすると，定理より

　　$r$ は 2 の約数，かつ $s$ は $-1$ の約数

であるから，$r = \pm 1,\ \pm 2,\quad s = \pm 1$ である．よって $\frac{r}{s} = \pm 1,\ \pm 2$ に限られる．
　ところがこれらは $f(X) = 2 - X^5$ のゼロ点ではないことが，代入すれば直ちにわかる．従って，$f(X) = 2 - X^5$ は $\mathbb{Q}$ にゼロ点をもたず，$\sqrt[5]{2} \notin \mathbb{Q}$. ■

# § 1–2. 代数的数とその多項式

## 1.2.1 代数的数

**Definition 1.2.1 (代数的数)**

　$\alpha \in \mathbb{C}$ が $\mathbb{C}$ の部分体 $\mathbb{F}$ 上で代数的である (**algebraic over a field** $\mathbb{F} \subset \mathbb{C}$) とは，$\alpha$ を zero 点とするような多項式 $f(X) \in \mathbb{F}$ が存在することである．ただし $f(X)$ は zero 多項式ではないとする．
　つまり，$a_0,\ a_1,\ a_2,\ \cdots,\ a_n \in \mathbb{F}$ を係数とするような多項式

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in \mathbb{F}[X]$$

が存在して，$a_0,\ a_1,\ a_2,\ \cdots,\ a_n$ のうちの少なくとも 1 つは $\neq 0$ であり，かつ $f(\alpha) = 0$ が成り立つとき，$\alpha$ は $\mathbb{F}$ 上代数的である．

---

それぞれの体 $\mathbb{F}$ について，$\alpha \in \mathbb{F}$ は代数的であると言える．$\alpha$ は $X - \alpha \in \mathbb{F}[X]$ の zero 点となるからである．

**Example 1.2.2**

- $\sqrt{2},\ \boldsymbol{i}, \omega$ は $\mathbb{Q}$ 上代数的である．
- $\sqrt[4]{2}\sqrt[6]{3}$ は $\mathbb{Q}$ 上代数的である．
- $1 + \sqrt{2}$ は $\mathbb{Q}$ 上代数的である．

　*Proof.*
　$\alpha = 1 + \sqrt{2} \iff \alpha - 1 = \sqrt{2}$ とすれば，

$$\alpha^2 - 2\alpha + 1 = 2 \iff \alpha^2 - 2\alpha - 1 = 0.$$

　よって $\alpha$ は $X^2 - 2X - 1 \in \mathbb{Q}[X]$ の zero 点であるから，$\mathbb{Q}$ 上代数的である． ■

---

$\alpha \in \mathbb{C}$ が $\mathbb{C}$ の部分体 $\mathbb{F}$ で代数的であることを，別の観点から考えるとオイシイ．$\alpha$ が代数的であれば，$\mathbb{F}[X]$ の多項式 $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ が存在して $a_n \neq 0$ である．つまり

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$$

が成り立つ．ここで，$a_0,\ a_1,\ a_2,\ \cdots,\ a_n \in \mathbb{F},\ \alpha,\ \alpha^2, \cdots \alpha^n \in \mathbb{C}$ で，$\mathbb{F}$ は $\mathbb{C}$ の部分体であるから，$\mathbb{C}$ を $\mathbb{F}$ の vector 空間と見なすことができる．

そこで，$\alpha,\ \alpha^2, \cdots, \alpha^n$ を vector と見なし，$a_0,\ a_1,\ a_2,\ \cdots,\ a_n$ を scalar と見なすことにすれば，次のように言える：

**Proposition 1.2.3 (代数的数と vector)**

$\alpha \in \mathbb{C}$ が $\mathbb{C}$ の部分体 $\mathbb{F}$ 上代数的であるとは，ある $n \in \mathbb{Z}^+$ が存在して，$\left\{1,\ \alpha,\ \alpha^2, \cdots,\ \alpha^n\right\}$ が $\mathbb{F}$ 上線形従属であることである．

---

*Proof.*

$a_n\alpha^n = -\left(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}\right)$ であるから，両辺 $a_n$ で割って

$$\alpha^n = -\frac{a_0}{a_n} - \frac{a_1}{a_n}\alpha - \frac{a_2}{a_n}\alpha^2 - \cdots - \frac{a_{n-1}}{a_n}\alpha^{n-1}$$

となる．これは，vector $\alpha^n$ は $n-1$ 個の vector $1,\ \alpha,\ \alpha^2, \cdots,\ \alpha^{n-1}$ の線形結合で表されることを意味するから，従属性が言えた． ■

### 1.2.2 モニック多項式

**Definition 1.2.4 (モニック多項式)**

多項式 $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{F}[X]$ がモニックである (**monic**) とは，主係数 $a_n = 1$ であることである．

---

**Lemma 1.2.5**

$\alpha \in \mathbb{C}$ が zero 多項式でない多項式 $f(X) \in \mathbb{F}[X]$ の zero 点であるならば，$\alpha$ はやはり zero 多項式でない **monic な多項式** $g(X) \in \mathbb{F}[X]$ の zero 点であり，$\deg f = \deg g$ が成り立つ．

---

### 1.2.3 最小多項式

**Lemma 1.2.6**

$\alpha \in \mathbb{C}$ が $\mathbb{F}(\subset \mathbb{C})$ 上代数的ならば，$\alpha$ を zero 点とする monic 多項式 $f(X) \in \mathbb{F}[X]$ の内で最低次数のものが一意的に定まる．

---

*Proof.*

存在することは明らかであるから，一意性を示す．最低次数を $n$ として，どちらも次数 $n$ の monic な多項式が 2 つあったとし，それらを

$$f_1(X) = a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} + X^n,$$
$$f_2(X) = b_0 + b_1X + b_2X^2 + \cdots + b_{n-1}X^{n-1} + X^n$$

とする．
$f(X)$ を，$c_i = a_i - b_i$ として

$$f(X) = f_1(X) - f_2(X) = c_0 + c_1X + c_2X^2 + \cdots + c_{n-1}X^{n-1}$$

と定めれば，$f(X) \in \mathbb{F}[X]$ であり，また $f(\alpha) = f_1(\alpha) - f_2(\alpha) = 0$ である．
このとき，$f(X)$ は zero 多項式であることを示す．$f(X)$ が zero 多項式でないとすると，$f(X)$ と同じ次数をもつ monic な多項式 $g(X)$ が存在して，$g(X)$ は $\alpha$ を zero 点にもつ (Lemma 1.2.5 (p.5) より)．これは $n$ の次数最小性に反するから $f(X) \equiv 0_{\mathrm{P}}$ が言える．よって $f_1(X) = f_2(X)$ である． ■

この Lemma 1.2.6 によって，任意の代数的数 $\alpha$ に対して，それぞれ一意的に monic な多項式を対応させることができる．$\alpha$ そのものの正体は解らなくても，それを zero 点にもつ多項式を考えることによって，$\alpha$ のもつ性質を探ろう，というのが，以下の考察におけるイデーである．

**Definition 1.2.7 (既約多項式，最小多項式)**

$\alpha \in \mathbb{C}$ が体 $\mathbb{F} \subset \mathbb{C}$ 上で代数的であるとする．多項式 $f(X) \in \mathbb{F}[X]$ のうちで，条件

(i) $f(\alpha) = 0$, (ii) $f(X)$ は monic, (iii) $\deg f$ が最小

であるようなものを

$\mathbb{F}$ 上の $\alpha$ の既約多項式 (**irreducible polynomial**)，または最小多項式 (**minimal polynomial**)

と言い，これを

$$\mathrm{irr}(\alpha, \mathbb{F})$$

と表す．また，その次数 $\deg \mathrm{irr}(\alpha, \mathbb{F})$ を

$\alpha$ の $\mathbb{F}$ 上の次数 (**degree of $\alpha$ over $\mathbb{F}$**)

と言い，それを $\deg(\alpha, \mathbb{F})$ で表す．

---

**Example 1.2.8**

$\sqrt{2}$ について，その $\mathbb{Q}$ 上の多項式は $\mathrm{irr}(\alpha, \mathbb{Q}) = X^2 - 2$ である．

---

*Proof.*

$X^2 - 2$ が $\sqrt{2}$ を zero 点とすることは明らかである．また，その係数は $\mathbb{Q}$ に含まれ，また monic である．残っているのは，この次数 2 が最小であることを示すだけである．もしさらに低い次数の多項式が存在したとすれば，それは $a \in \mathbb{Q}$ として

$$X + a$$

であるはずであるが，このとき $\sqrt{2} + a = 0$ となる．これは矛盾．よって

$$\mathrm{irr}\left(\sqrt{2}, \mathbb{Q}\right) = X^2 - 2, \quad \deg\left(\sqrt{2}, \mathbb{Q}\right) = 2.$$

■

$\mathrm{irr}\left(\sqrt{2}, \mathbb{R}\right)$ は $X^2 - 2$ ではなく，$X - \sqrt{2}$ であることに注意．

**Example 1.2.9**

$\alpha = \sqrt{2}\omega$ とするとき，

$$\mathrm{irr}(\alpha, \mathbb{C}) = X - \alpha, \quad \mathrm{irr}(\alpha, \mathbb{R}) = X^3 - 2\sqrt{2}, \quad \mathrm{irr}(\alpha, \mathbb{Q}) = X^6 - 8.$$

---

# § 1–3. 体の拡大

**不可能性証明 §1.3.**

### 1.3.1 $\mathbb{Q}\left(\sqrt{2}\right)$

**Definition 1.3.1 ($\mathbb{Q}$ に $\sqrt{2}$ を付け加える．)**

$\mathbb{C}$ の部分集合 $\mathbb{Q}(\sqrt{2})$ を

$$\mathbb{Q}(\sqrt{2}) \stackrel{\text{def}}{=} \left\{ a + b\sqrt{2} \,\middle|\, a, b \in \mathbb{Q} \right\}$$

と定義する．

---

つまり，$\mathbb{Q}(\sqrt{2})$ は $\left\{1, \sqrt{2}\right\}$ によって張られる vector 空間であり，$\mathbb{Q}$ 上の $\mathbb{C}$ の部分 vector 空間である．

**Lemma 1.3.2**

$B = \left\{1, \sqrt{2}\right\}$ は，$\mathbb{Q}$ 上の vector 空間 $\mathbb{Q}(\sqrt{2})$ の基底をなす．

---

*Proof.*

$\mathbb{Q}(\sqrt{2})$ の要素はその定義により 1 と $\sqrt{2}$ の線形結合で表されるから，確かに集合 $B$ は $\mathbb{Q}(\sqrt{2})$ を張る．
次に $B$ の要素が $\mathbb{Q}$ 上線形独立であることを示 $\cdots\cdots$ と思ったが，実は中学生が知っていることであったのでヤメル．(キガツイテナイデショウ?!) ■

Vector 空間 $\mathbb{Q}(\sqrt{2})$ の性質を考察する前に，環という概念をキチッと定義しておこう．

**Definition 1.3.3 (環)**

集合 $R$ が環 (**ring**) であるとは，$R$ 上に加法 $+$ と乗法 $\cdot$ が定義されていて，次がみたされることである：

(i) 加法 $+$ は $R$ 上で結合法則をみたし，単位元が存在する．また任意の $x \in \mathbb{R}$ も $+$ に関する逆元をもつ (これを反元と言う)．さらに交換法則が成り立つ．

(ii) $R$ は乗法について閉じている： $r_1, r_2 \in R \Rightarrow r_1 \cdot r_2 \in R$.

(iii) 乗法が結合的である： $r_1, r_2, r_3 \in R \Rightarrow r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$.

(iv) 乗法は加法に対して分配的である：

$$r_1, r_2, r_3 \in R \Rightarrow r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3.$$

加法の単位元は 0 で表される．

特に $r_1, r_2 \in R$ について，乗法の交換法則 $r_1 \cdot r_2 = r_2 \cdot r_1$ が成り立つとき，$R$ は可換環 (**commutative ring**) と言われる．

$R$ が乗法に関する単位元 1 をもつとき，単位元をもつ環 (**ring with unity**) と言われる．

---

**Lemma 1.3.4**

$\mathbb{Q}(\sqrt{2})$ は単位元をもつ可換環である．

---

*Proof.*

ヨクアル問題. ■

**Lemma 1.3.5**

$\mathbb{Q}(\sqrt{2})$ は体である．

---

*Proof.*

Lemma 1.3.4 で環であることが判っているから，除法について閉じていることを示せば十分であるが，それは 0 以外の $\mathbb{Q}(\sqrt{2})$ の要素が乗法の逆元をもつことと同値である．人はそれを有理化という．
■

**Lemma 1.3.6**

$\mathbb{Q}(\sqrt{2})$ は $\mathbb{Q}$ と $\sqrt{2}$ を含む最小の体である．

---

*Proof.*

$\mathbb{F}$ を，$\mathbb{Q}$ と $\sqrt{2}$ を含む任意の体として，$\mathbb{Q}(\sqrt{2}) \subset \mathbb{F}$ を示せば十分，つまり

$$\forall x\ ;\ x \in \mathbb{Q}(\sqrt{2}) \Rightarrow x \in \mathbb{F}$$

を示す．

$x \in \mathbb{Q}(\sqrt{2})$ とすれば，$a, b \in \mathbb{Q}$ として $x = a + b\sqrt{2}$ と表される．仮定より $\sqrt{2} \in \mathbb{F}$，また $a, b \in \mathbb{Q} \subset \mathbb{F}$ より $a, b \in \mathbb{F}$ である．$\mathbb{F}$ が体であることから $x = a + b\sqrt{2} \in \mathbb{F}$. ■

$\mathbb{Q}(\sqrt{2})$ が体であり，かつ $\mathbb{C}$ の部分体であることから，Section 1.2 (p.4) で導かれた様々な性質を $\mathbb{Q}(\sqrt{2})$ でそのまま考えることができる．つまり，体 $\mathbb{F}$ をそのまま $\mathbb{Q}(\sqrt{2})$ に読みかえれば，すべてそのまま成立する．

**Example 1.3.7**

$\sqrt{3}$ は $\mathbb{Q}(\sqrt{2})$ で代数的であり，その次数は 2 である．

---

*Proof.*

多項式 $X^2 - 3$ は $\mathbb{Q}$ 上の，従って $\mathbb{Q}(\sqrt{2})$ 上の多項式である：$X^2 - 3 \in \mathbb{Q}(\sqrt{2})$.

それは monic で，$\sqrt{3}$ を zero 点にもつから，$\sqrt{3}$ は $\mathbb{Q}(\sqrt{2})$ 上で代数的である．

次に $X^2 - 3$ が $\mathbb{Q}(\sqrt{2})$ 上で既約であることを示す．もし既約でないとすれば，$a \in \mathbb{Q}(\sqrt{2})$ として，monic な 1 次の多項式 $X + a$ が存在して，その zero 点が $\sqrt{3}$ である．$a \in \mathbb{Q}(\sqrt{2})$ より，$a = p + q\sqrt{2}$ と書けて，$p, q \in \mathbb{Q}$ である．$\sqrt{3}$ が $X + a$ の zero 点であることから，

$$\sqrt{3} + p + q\sqrt{2} = 0$$

が成り立つ．よって

$$\sqrt{3} = -\left(p + q\sqrt{2}\right), \quad \therefore\ 3 = p^2 + 2pq\sqrt{2} + 2q^2.$$

$p, q$ のいずれが $= 0$ としても矛盾するから $pq \neq 0$ であるが，このとき，

$$\sqrt{2} = \frac{3 - p^2 - 2q^2}{2pq} \in \mathbb{Q}$$

よりやはり矛盾．よって多項式 $X^2 - 3$ は $\mathbb{Q}(\sqrt{2})$ 上既約である．

以上より，

$$\mathrm{irr}\left(\sqrt{3}, \mathbb{Q}(\sqrt{2})\right) = X^2 - 3, \quad \deg\left(\sqrt{3}, \mathbb{Q}(\sqrt{2})\right) = 2.$$

■

### 1.3.2 体 $\mathbb{F}(\alpha)$ の構成

以上で $\mathbb{Q}(\sqrt{2})$ を構成した．これを一般化してみよう．つまり，$\mathbb{F}$ を $\mathbb{C}$ のある部分体とし，$\mathbb{F}$ 上で代数的な $\alpha \in \mathbb{C}$ について，

$$\mathbb{F}(\alpha) = \left\{a + b\alpha \,\middle|\, a, b \in \mathbb{F}\right\}$$

を考えると，これを $\mathbb{C}$ の部分 vector 空間と見なすことができて，また $\mathbb{C}$ の部分体でもある．さらにこの $\mathbb{F}(\alpha)$ は，$\alpha$ と $\mathbb{F}$ を含むような，$\mathbb{C}$ の最小の部分体であることが示される．

以下，$\alpha$ は $\mathbb{F}$ 上代数的であると仮定する．

**Definition 1.3.8 (代数拡大)**

$\mathbb{F}$ を $\mathbb{C}$ の部分体，$\alpha$ は $\mathbb{F}$ 上代数的で，$\deg(\alpha, \mathbb{F}) = n$ とする．$\mathbb{F}$ の $\alpha$ による代数拡大 (**algebraic extension of $\mathbb{F}$ by $\alpha$**) とは，次のような集合 $\mathbb{F}(\alpha)$ である：

$$\mathbb{F}(\alpha) \stackrel{\text{def}}{=} \left\{ b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1} \,\middle|\, b_0,\ b_1,\ b_2,\ \cdots,\ b_{n-1} \in \mathbb{F} \right\}.$$

---

つまり $\mathbb{F}(\alpha)$ とは，$\alpha$ のべき $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ の $\mathbb{F}$ 上の線形結合の集合であり，$\left\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\right\}$ が $\mathbb{F}$ 上に張る vector 空間 ($\mathbb{C}$ の部分 vector 空間) である．

**Lemma 1.3.9**

$\alpha$ の $n$ 次以上のべきは $\mathbb{F}(\alpha)$ の要素である：

$$\alpha^n,\ \alpha^{n+1},\ \alpha^{n+2},\ \cdots \in \mathbb{F}(\alpha).$$

---

*Proof.*

$\deg(\alpha, \mathbb{F}) = n$ であるから，$\alpha$ は多項式環 $\mathbb{F}[X]$ に含まれる monic な多項式の zero 点である．よってある $c_0,\ c_1,\ c_2,\ \cdots,\ c_{n-1} \in \mathbb{F}$ が存在して

$$\begin{aligned} & c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} + \alpha^n = 0 \\ \iff\ & \alpha^n = -\left(c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}\right) \end{aligned} \tag{1.1}$$

が成り立つ．定義より $\alpha, \alpha^2, \cdots, \alpha^{n-1} \in \mathbb{F}(\alpha)$ であるから，$\alpha^n$ はこれらの $\mathbb{F}$ 上の線形結合となり，$\alpha^n \in \mathbb{F}(\alpha)$.

(1.1) の両辺に $\alpha$ をかけて

$$\alpha^{n+1} = -\left(c_0\alpha + c_1\alpha^2 + \cdots + c_{n-1}\alpha^n\right)$$

を得るが，$\alpha, \alpha^2, \cdots, \alpha^{n-1} \in \mathbb{F}(\alpha)$ であり，かつ $\alpha^n \in \mathbb{F}(\alpha)$ より，$\alpha^{n+1} \in \mathbb{F}(\alpha)$.

以下同様にして $\alpha^{n+2},\ \alpha^{n+3},\ \cdots \in \mathbb{F}(\alpha)$. ■

**Lemma 1.3.10**

$\deg(\alpha, \mathbb{F}) = n$ とすれば，$\left\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\right\}$ は $\mathbb{F}$ 上線形独立である．

---

*Proof.*

$\left\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\right\}$ が線形従属であるとする．このとき，$c_0,\ c_1,\ c_2,\ \cdots,\ c_{n-1} \in \mathbb{F}$ について

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} = 0$$

が成り立ち，かつ少なくとも 1 つの $c_i$ は $\neq 0$ である．そのような $c_i$ のうちで番号 $i$ が最大のものを $c_k$ とする．両辺を $c_k$ で割って

$$\frac{c_0}{c_k} + \frac{c_1}{c_k}\alpha + \frac{c_2}{c_k}\alpha^2 + \cdots + \frac{c_{k-1}}{c_k}\alpha^{k-1} + \alpha^k = 0.$$

このとき，係数 $\frac{c_0}{c_k}, \frac{c_1}{c_k}, \cdots, \frac{c_{k-1}}{c_k} \in \mathbb{F}$ であるから，$\alpha$ は $k$ 次の多項式の zero 点であることになる．ところが $i \leq n-1$ であるから，これは $\deg(\alpha, \mathbb{F}) = n$ に反する．

よってこの Lemma が成り立つ. ■

**THEOREM 1.3.11 ($\mathbb{F}(\alpha)$ の基底定理)**

$\mathbb{F}$ を $\mathbb{C}$ の部分体，$\alpha \in \mathbb{C}$ が $\mathbb{F}$ 上代数的，かつ $\deg(\alpha, \mathbb{F}) = n$ とする．このとき，$\left\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\right\}$ は $\mathbb{F}$ 上の vector 空間 $\mathbb{F}(\alpha)$ の 1 つの基底をなす．

さらに，$\dim \mathbb{F}(\alpha) = \deg(\alpha, \mathbb{F}) = n$ である．つまり，vector 空間 $\mathbb{F}(\alpha)$ の次元と $\alpha$ の $\mathbb{F}$ 上の次数は一致する．

---

*Proof.*

Definition 1.3.8 (p.9) より $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ は $\mathbb{F}$ 上で vector 空間 $\mathbb{F}(\alpha)$ を張る．Lemma 1.3.10 (p.9) より $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ は線形独立であるから，$\mathbb{F}(\alpha)$ の基底をなす．その個数は $n$ であるから，$\dim \mathbb{F}(\alpha) = n = \deg(\alpha, \mathbb{F})$．■

**Lemma 1.3.12**

$\mathbb{F}(\alpha)$ は環をなす．

---

*Proof.*

$\mathbb{F}(\alpha) \in \mathbb{C}$ であるから，$\mathbb{F}(\alpha)$ が加法と乗法について閉じていることを示せば十分である．加法については自明．

乗法についても，$\alpha$ のべきがすべて $\mathbb{F}(\alpha)$ に含まれ，係数も $\mathbb{F}$ に含まれるから明らか．■

**THEOREM 1.3.13 (体 $\mathbb{F}(\alpha)$)**

$\mathbb{F}$ を $\mathbb{C}$ の部分体，$\alpha \in \mathbb{C}$ が $\mathbb{F}$ 上代数的であるとする．このとき，$\mathbb{F}(\alpha)$ は体をなす．

---

*Proof.*

Lemma 1.3.12 より，残るは $\mathbb{F}(\alpha)$ の要素 $\beta(\neq 0)$ が $\mathbb{F}(\alpha)$ の中に乗法逆元 $\beta^{-1}$ をもつことだけである．

集合 $\{1, \beta, \beta^2, \cdots, \beta^n\}$ は，$\mathbb{F}(\alpha)$ の $n+1$ 個の要素からなる集合であるから，$\dim \mathbb{F}(\alpha) = n$ より線形従属である．よって，「すべて 0」であることはない $d_0, d_1, d_2, \cdots, d_k$ $(k \leq n)$ が $\mathbb{F}$ の要素として存在して

$$d_0 + d_1\beta + d_2\beta^2 + \cdots + d_k\beta^k = 0 \tag{1.2}$$

が成り立つ．$d_0 = 0$ ならば両辺を $\beta$ で割って (1.2) の項の数を減らすことができる．

これを必要なだけ繰り返して，$\neq 0$ なる $d_i$ が第 1 項に現れるようにできる．従って，必要ならば番号をつけかえて，(1.2) で $d_0$ は $\neq 0$ としてよい．

両辺に $\dfrac{-1}{d_0}$ をかけて，$e_i = -\dfrac{d_i}{d_0} \in \mathbb{F}$ として

$$-1 + e_1\beta + e_2\beta^2 + \cdots + e_k\beta^k = 0.$$

従って

$$1 = e_1\beta + e_2\beta^2 + \cdots + e_k\beta^k = \beta\left(e_1 + e_2\beta + \cdots + e_k\beta^{k-1}\right)$$

であるから，$\beta$ は逆数 $\beta^{-1} = e_1 + e_2\beta + \cdots + e_k\beta^{k-1}$ をもつ．ここで $e_i, \beta^i \in \mathbb{F}(\alpha)$ であり，$\mathbb{F}(\alpha)$ が環をなすことから $\beta^{-1} \in \mathbb{F}(\alpha)$ である．従って確かに $\mathbb{F}(\alpha)$ は体をなす．■

**Example 1.3.14**

$\beta = \sqrt[3]{2} - 3$ とする．$\mathbb{Q}(\sqrt[3]{2})$ における $\beta$ の逆数をオテガルに求めてみよう．

$\beta + 3 = \sqrt[3]{2}$ の両辺を 3 乗して $\beta^3 + 9\beta^2 + 27\beta + 27 = 2$ であるから，

$$\beta\left(\beta^2 + 9\beta + 27\right) = -25 \iff \beta \cdot \frac{\beta^2 + 9\beta + 27}{-25} = 1$$

を得る．よって $\beta$ の逆数は $\beta^{-1} = \dfrac{\beta^2 + 9\beta + 27}{-25}$ である．

---

**THEOREM 1.3.15 (最小体定理)**

$\mathbb{F}$ を $\mathbb{C}$ の部分体，$\alpha \in \mathbb{C}$ が $\mathbb{F}$ 上代数的であるとする．このとき，$\mathbb{F}(\alpha)$ は $\mathbb{F}$ と $\alpha$ を含む最小の体である．

---

*Proof.*

$\mathbb{K}$ を $\mathbb{F}$ と $\alpha$ を含む任意の体とする．$\mathbb{F}(\alpha) \subset \mathbb{K}$ を示せば十分である．$\deg(\alpha, \mathbb{F}) = n$ とする．任意の $\gamma \in \mathbb{F}(\alpha)$ について

$$\gamma = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}$$

と表され，仮定より $\alpha \in \mathbb{K}$ でかつ $\mathbb{K}$ が体であるから，$\alpha^2, \alpha^3, \cdots, \alpha^{n-1} \in \mathbb{K}$．また，$\mathbb{F} \subset \mathbb{K}$ であるから，$b_0, b_1, b_2, \cdots, b_{n-1} \in \mathbb{K}$．再び $\mathbb{K}$ が体であることから $\gamma = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1} \in \mathbb{K}$．

以上より $\gamma \in \mathbb{F}(\alpha) \Rightarrow \gamma \in \mathbb{K}$ が示されたから

$$\mathbb{F}(\alpha) \subset \mathbb{K}.$$

■

**Example 1.3.16**

$\alpha \in \mathbb{C}$ とし，$\mathbb{F}$ を $\mathbb{C}$ の部分体とする．このとき，

$$\mathbb{F}(\alpha^2) \subset \mathbb{F}(\alpha).$$

---

*Proof.*

最小体定理 (Theorem 1.3.15 (p.10)) より $\mathbb{F}(\alpha)$ は $\alpha$ と $\mathbb{F}$ を含む．よって $\mathbb{F}(\alpha)$ は $\alpha^2 = \alpha \cdot \alpha$ を含むから，$\mathbb{F}(\alpha)$ は $\alpha^2$ と $\mathbb{F}$ を含む体である．

$\mathbb{F}(\alpha^2)$ はそのような体の内で最小だから，$\mathbb{F}(\alpha^2) \subset \mathbb{F}(\alpha)$ となる． ■

### 1.3.3 体の逐次的構成

Theorem 1.3.15 (p.10) で，$\mathbb{C}$ の部分体 $\mathbb{F}$ に $\alpha \in \mathbb{C}$ を添加して $\mathbb{F}(\alpha)$ を構成したとき，$\mathbb{F}(\alpha)$ は $\alpha$ と $\mathbb{F}$ を含む最小の体であることを見た．ここでは，さらに $\mathbb{F}(\alpha)$ に，$\mathbb{F}(\alpha)$ 上で代数的な $\beta(\in \mathbb{C})$ を添加して $(\mathbb{F}(\alpha))(\beta)$ を作り，さらにこの体上で代数的な $\gamma(\in \mathbb{C})$ を添加して $((\mathbb{F}(\alpha))(\beta))(\gamma)$ を作り，$\cdots$ という，体の逐次的拡大・逐次的構成を考えよう．

**Example 1.3.17**

$(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$ は $\{1, \sqrt{3}\}$ ををを基底 vector とする $\mathbb{Q}(\sqrt{2})$ 上に張られた vector 空間である．

---

*Proof.*

Example 1.3.7 (p.8) より，$\mathrm{irr}(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = X^2 - 3$ であるから，$\deg(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = 2$ である．
Definition 1.3.8 (p.9) より

$$(\mathbb{Q}(\sqrt{2}))(\sqrt{3}) = \left\{ x + y\sqrt{3} \,|\, x, y \in \mathbb{Q}(\sqrt{2}) \right\}$$

であるから，これは $\mathbb{Q}(\sqrt{2})$ 上で，$\{1, \sqrt{3}\}$ が張る vector 空間である．この基底が $\{1, \sqrt{3}\}$ であることは，Theorem 1.3.11 (p.9) から解る． ■

Example 1.3.17 から，順次拡大されていく体の列

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset (\mathbb{Q}(\sqrt{2}))(\sqrt{3})$$

が得られる．このような拡大体の系列を「体の昇鎖」(**tower of fields**) と呼ぶ．

$((\mathbb{F})(\alpha))(\beta)$ を単に $\mathbb{F}(\alpha)(\beta)$ と書く．

この昇鎖において，$\mathbb{Q}(\sqrt{2})(\sqrt{3})$ を $\mathbb{Q}$ 上の vector 空間と考えることもできる．つまり

**Example 1.3.18**

$\mathbb{Q}(\sqrt{2})(\sqrt{3})$ は，vector の集合 $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ が張る $\mathbb{Q}$ 上の vector 空間である．

---

### 1.3.4 体の昇鎖

$\mathbb{C}$ の部分体 $\mathbb{E},\mathbb{F},\mathbb{K}$ が $\mathbb{E}\subset\mathbb{F}\subset\mathbb{K}$ であり，かつどれも集合として異なるとき，3 個の vector 空間を考えることができる．つまり

- $\mathbb{E}$ 上の vector 空間としての $\mathbb{F}$,
- $\mathbb{F}$ 上の vector 空間としての $\mathbb{K}$,
- $\mathbb{E}$ 上の vector 空間としての $\mathbb{K}$

である．

**THEOREM 1.3.19 (昇鎖の基底)**

$\mathbb{C}$ の部分体 $\mathbb{E}\subset\mathbb{F}\subset\mathbb{K}$ について，

- vector 空間 $\mathbb{F}$ の $\mathbb{E}$ 上の基底が $\{\alpha_1,\,\alpha_2,\,\ldots,\,\alpha_m\}$ であり，
- vector 空間 $\mathbb{K}$ の $\mathbb{F}$ 上の基底が $\{\beta_1,\,\beta_2,\,\ldots,\,\beta_n\}$ である

とき，vector 空間 $\mathbb{K}$ の $\mathbb{E}$ 上の基底は

$$\alpha_i\beta_j\quad(1\le i\le n,\,1\le j\le m)$$

である．

---

*Proof.*

$k\in\mathbb{K}$ とする．$\mathbb{K}$ は $\mathbb{F}$ 上の vector 空間であるから，scaler $f_1,\,f_2,\,\ldots,\,f_n\in\mathbb{F}$ が存在して

$$k=f_1\beta_1+f_2\beta_2+\cdots+f_n\beta_n=\sum_{i=1}^{n}f_i\beta_i \tag{1.3}$$

と書ける．$f_i\in\mathbb{F}$ で，$\mathbb{F}$ は $\mathbb{E}$ 上の vector 空間であり，その基底が $\{\alpha_1,\,\alpha_2,\,\ldots,\,\alpha_m\}$ であるから，どの $f_i$ についても scaler $e_{i1},\,e_{i2},\,\cdots,\,e_{im}$ が存在して

$$f_i=e_{i1}\alpha_1+e_{i2}\alpha_2+\cdots+e_{im}\alpha_m=\sum_{j=1}^{m}e_{ij}\alpha_j \tag{1.4}$$

と書ける．

(1.6) に (1.7) を代入すれば

$$k=\sum_{i=1}^{n}\left(\sum_{j=1}^{m}e_{ij}\alpha_j\right)\beta_i=\sum_{i=1}^{n}\sum_{j=1}^{m}e_{ij}\left(\alpha_j\beta_i\right).$$

これで，$k\in\mathbb{K}$ は $\alpha_j\beta_i$ $(1\le j\le m,\,1\le i\le n)$ の線形結合であるから，$\alpha_j\beta_i$ は $\mathbb{E}$ 上で vector 空間 $\mathbb{K}$ を張ることが示された．

次に，vector の集合 $\left\{\alpha_j\beta_i\,\middle|\,1\le j\le m,\,1\le i\le n\right\}$ が $\mathbb{E}$ 上で線形独立であることを示す．そのためには，$\mathbb{E}$ の要素 $e_{ij}$ $(1\le i\le n,\,1\le j\le m)$ が

$$\sum_{i=1}^{n}\sum_{j=1}^{m}e_{ij}\alpha_j\beta_i=0 \tag{1.5}$$

をみたすとき，どの $e_{ij}$ も 0 であることを示せば十分である．

式 (1.8) を

$$\sum_{i=1}^{n}\left(\sum_{j=1}^{m}e_{ij}\alpha_j\right)\beta_i=0$$

と書き換える．このとき，それぞれの $\beta_i$ の係数 $\sum_{j=1}^{m} e_{ij}\alpha_j$ は $\mathbb{F}$ の要素で，また $\beta_i$ $(1 \leq i \leq n)$ は $\mathbb{F}$ 上で線形独立であるから，$1 \leq i \leq n$ なる任意の $i$ について

$$\sum_{j=1}^{m} e_{ij}\alpha_j = 0$$

が成り立つ．

ところが $\alpha_j$ $(1 \leq j \leq m)$ は $\mathbb{E}$ 上で線形独立であるから，$1 \leq j \leq m$ なる任意の $j$ について

$$e_{ij} = 0$$

となる．以上より，$\alpha_j\beta_i$ は $\mathbb{E}$ 上で線形独立であることが示された．よって，$mn$ 個の vector $\alpha_j\beta_i$ は $\mathbb{E}$ 上の vector 空間 $\mathbb{K}$ の基底をなす． ■

**THEOREM 1.3.20 (昇鎖の次元)**

$\mathbb{C}$ の部分体の昇鎖 $\mathbb{E} \subset \mathbb{F} \subset \mathbb{K}$ について，$\mathbb{E}$ 上の vector 空間 $\mathbb{F}$，$\mathbb{F}$ 上の vector 空間 $\mathbb{K}$ が有限次元ならば，vector 空間 $\mathbb{K}$ も $\mathbb{E}$ 上有限次元であり，

$$[\mathbb{K} : \mathbb{E}] = [\mathbb{K} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{E}]$$

が成り立つ．

これを

$$\dim_{\mathbb{E}} \mathbb{K} = \dim_{\mathbb{F}} \mathbb{K} \cdot \dim_{\mathbb{E}} \mathbb{F}$$

とも書く．

---

*Proof.*

Theorem 1.3.23 (p.14) より明らか． ■

**Corollary 1.3.21**

Theorem 1.3.24 (p.15) の仮定が成り立つとき，$[\mathbb{K} : \mathbb{F}]$ は $[\mathbb{K} : \mathbb{E}]$ の約数であり，$[\mathbb{F} : \mathbb{E}]$ も $[\mathbb{K} : \mathbb{E}]$ の約数である．

*Proof.*

**アタリマエ．** ■

**Example 1.3.22**

Vector 空間 $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ の $\mathbb{Q}$ 上の基底は $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ であり，この次元は 4 である．

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ であるから，確かに

$$\left[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}\right] = \left[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})\right] \cdot \left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2 \cdot 2 = 4$$

が成り立つ．Corrolary 1.3.25 から，$\mathbb{Q} \subset \mathbb{F} \subset \mathbb{Q}(\sqrt{2})(\sqrt{3})$ をみたす体 $\mathbb{F}$ で，$[\mathbb{F} : \mathbb{Q}] = 3$ であるようなものは存在しないことが言える．3 は 4 の約数ではないからである．

---

### 1.3.5 体の昇鎖

$\mathbb{C}$ の部分体 $\mathbb{E}, \mathbb{F}, \mathbb{K}$ が $\mathbb{E} \subset \mathbb{F} \subset \mathbb{K}$ であり，かつどれも集合として異なるとき，3 個の vector 空間を考えることができる．つまり

- $\mathbb{E}$ 上の vector 空間としての $\mathbb{F}$,
- $\mathbb{F}$ 上の vector 空間としての $\mathbb{K}$,
- $\mathbb{E}$ 上の vector 空間としての $\mathbb{K}$

である．

**THEOREM 1.3.23 (昇鎖の基底)**

$\mathbb{C}$ の部分体 $\mathbb{E} \subset \mathbb{F} \subset \mathbb{K}$ について，

- vector 空間 $\mathbb{F}$ の $\mathbb{E}$ 上の基底が $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ であり，
- vector 空間 $\mathbb{K}$ の $\mathbb{F}$ 上の基底が $\{\beta_1, \beta_2, \ldots, \beta_n\}$ である

とき，vector 空間 $\mathbb{K}$ の $\mathbb{E}$ 上の基底は

$$\alpha_i \beta_j \quad (1 \leq j \leq m,\ 1 \leq i \leq n)$$

である．

---

*Proof.*

$k \in \mathbb{K}$ とする．$\mathbb{K}$ は $\mathbb{F}$ 上の vector 空間であるから，scaler $f_1, f_2, \ldots, f_n \in \mathbb{F}$ が存在して

$$k = f_1\beta_1 + f_2\beta_2 + \cdots + f_n\beta_n = \sum_{i=1}^{n} f_i\beta_i \tag{1.6}$$

と書ける．$f_i \in \mathbb{F}$ で，$\mathbb{F}$ は $\mathbb{E}$ 上の vector 空間であり，その基底が $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ であるから，どの $f_i$ についても scaler $e_{i1}, e_{i2}, \cdots, e_{im}$ が存在して

$$f_i = e_{i1}\alpha_1 + e_{i2}\alpha_2 + \cdots + e_{im}\alpha_m = \sum_{j=1}^{m} e_{ij}\alpha_j \tag{1.7}$$

と書ける．

(1.6) に (1.7) を代入すれば

$$k = \sum_{i=1}^{n} \left( \sum_{j=1}^{m} e_{ij}\alpha_j \right) \beta_i = \sum_{i=1}^{n} \sum_{j=1}^{m} e_{ij} \left(\alpha_j \beta_i\right).$$

これで，$k \in \mathbb{K}$ は $\alpha_j\beta_i$ $(1 \leq j \leq m,\ 1 \leq i \leq n)$ の線形結合であるから，$\alpha_j\beta_i$ は $\mathbb{E}$ 上で vector 空間 $\mathbb{K}$ を張る．

次に，vector の集合 $\left\{\alpha_j\beta_i \,\middle|\, 1 \leq j \leq m,\ 1 \leq i \leq n\right\}$ が $\mathbb{E}$ 上で線形独立であることを示す．そのためには，$\mathbb{E}$ の要素 $e_{ij}$ $(1 \leq i \leq n,\ 1 \leq j \leq m)$ が

$$\sum_{i=1}^{n} \sum_{j=1}^{m} e_{ij}\alpha_j\beta_i = 0 \tag{1.8}$$

をみたすとき，どの $e_{ij}$ も 0 であることを示せば十分である．

式 (1.8) を

$$\sum_{i=1}^{n} \left( \sum_{j=1}^{m} e_{ij}\alpha_j \right) \beta_i = 0$$

と書き換える．このとき，それぞれの $\beta_i$ の係数 $\sum_{j=1}^{m} e_{ij}\alpha_j$ は $\mathbb{F}$ の要素で，また $\beta_i$ $(1 \leq i \leq n)$ は $\mathbb{F}$ 上で線形独立であるから，$1 \leq i \leq n$ なる任意の $i$ について

$$\sum_{j=1}^{m} e_{ij}\alpha_j = 0$$

が成り立つ．

ところが $\alpha_j$ $(1 \leq j \leq m)$ は $\mathbb{E}$ 上で線形独立であるから，$1 \leq j \leq m$ なる任意の $j$ について

$$e_{ij} = 0$$

となる．以上より，$\alpha_j\beta_i$ は $\mathbb{E}$ 上で線形独立であることが示された．よって，$mn$ 個の vector $\alpha_j\beta_i$ は $\mathbb{E}$ 上の vector 空間 $\mathbb{K}$ の基底をなす． ■

**THEOREM 1.3.24 (昇鎖の次元)**

$\mathbb{C}$ の部分体の昇鎖 $\mathbb{E} \subset \mathbb{F} \subset \mathbb{K}$ について，$\mathbb{E}$ 上の vector 空間 $\mathbb{F}$，$\mathbb{F}$ 上の vector 空間 $\mathbb{K}$ が有限次元ならば，vector 空間 $\mathbb{K}$ も $\mathbb{E}$ 上有限次元であり，

$$[\mathbb{K} : \mathbb{E}] = [\mathbb{K} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{E}]$$

が成り立つ．

これを

$$\dim_{\mathbb{E}} \mathbb{K} = \dim_{\mathbb{F}} \mathbb{K} \cdot \dim_{\mathbb{E}} \mathbb{F}$$

とも書く．

---

*Proof.*

Theorem 1.3.23 (p.14) より明らか． ■

**Corollary 1.3.25**

Theorem 1.3.24 (p.15) の仮定が成り立つとき，$[\mathbb{K} : \mathbb{F}]$ は $[\mathbb{K} : \mathbb{E}]$ の約数であり，$[\mathbb{F} : \mathbb{E}]$ も $[\mathbb{K} : \mathbb{E}]$ の約数である．

*Proof.*

**アタリマエ．** ■

**Example 1.3.26**

Vector 空間 $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ の $\mathbb{Q}$ 上の基底は $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ であり，この次元は 4 である．

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ であるから，確かに

$$\left[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}\right] = \left[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})\right] \cdot \left[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\right] = 2 \cdot 2 = 4$$

が成り立つ．Corrolary 1.3.25 から，$\mathbb{Q} \subset \mathbb{F} \subset \mathbb{Q}(\sqrt{2})(\sqrt{3})$ をみたす体 $\mathbb{F}$ で，$[\mathbb{F} : \mathbb{Q}] = 3$ であるようなものは存在しないことが言える．3 は 4 の約数ではないからである．

---

## § 1–4. 既約多項式

### 1.4.1 既約多項式

Definition 1.2.7 (p.6) で

$\mathbb{F}$ 上の $\alpha$ の既約 (最小) 多項式　$\mathrm{irr}\,(\alpha, \mathbb{F})$

を定義した．以下では,「$\mathbb{F}$ 上の既約多項式」という概念が定義される．この 2 つの間の関係は，後に明らかになるが，さし当たっては別個のものと考えておく方がよい.

**Definition 1.4.1 ($\mathbb{F}$ 上可約な多項式)**

$\mathbb{F}$ を体とする．多項式 $f(X) \in \mathbb{F}[X]$ が $\mathbb{F}$ 上で可約である (**reducible over** $\mathbb{F}$) とは，次の (i), (ii) をみたすような多項式 $g(X), h(X)$ が存在することである：

(i) $g(X), h(X)$ の次数はどちらも $f(X)$ よりも小さい.

(ii) $f(X) = g(X)\,h(X)$.

---

**Definition 1.4.2 ($\mathbb{F}$ 上既約な多項式)**

$\mathbb{F}$ を体とする．多項式 $f(X) \in \mathbb{F}[X]$ が $\mathbb{F}$ 上で既約である (**irreducible over** $\mathbb{F}$) とは，$f(X)$ が $\mathbb{F}$ 上で可約でなく，かつ定数でもないことである.

---

**Note 1.4.3**

ある多項式がある体上で既約であれば，その体のどんな部分体上でも既約である．つまり，$\mathbb{E}$ が体 $\mathbb{F}$ の部分体で，$f(X) \in \mathbb{E}[X]$ が $\mathbb{F}$ 上で既約であれば，$f(X)$ は $\mathbb{E}$ 上でも既約である.

### 1.4.2 可約多項式とその zero 点

**Definition 1.4.4 (1 次の因数)**

$\mathbb{F}$ を体とする．$f(X) \in \mathbb{F}[X]$ が $\mathbb{F}[X]$ の中に 1 次の因数をもつとは

$$f(X) = (aX + b)\,g(X)$$

と書けることである．ただし $a, b \in \mathbb{F},\ a \neq 0,\ g(X) \in \mathbb{F}[X]$ とする.

---

**THEOREM 1.4.5 (因数定理　Factor Theorem)**

$\mathbb{F}$ を体，$f(X) \in \mathbb{F}[X]$ とすると，次は同値である：

- $f(X)$ が $\mathbb{F}[X]$ に 1 次の因数をもつ.
- $f(X)$ は $\mathbb{F}$ に zero 点をもつ.

---

**THEOREM 1.4.6 (2 次，3 次多項式の既約性)**

$\mathbb{F}$ を体とする．$f(X) \in \mathbb{F}[X]$ について，$\deg f(X) = 2,\ 3$ ならば，次は同値である：

- $f(X)$ が $\mathbb{F}$ 上可約である.
- $f(X)$ が $\mathbb{F}$ に zero 点をもつ.

---

*Proof.*

**不可能性証明 §1.4.**

⇒) $f(X)$ が $\mathbb{F}$ 上可約ならば，$f(X) = g(X)\,h(X)$ となる多項式 $g(X)$, $h(X) \in \mathbb{F}[X]$ が存在する．$\deg g(X) + \deg h(X) = 2$ または 3 であるから，少なくともどちらか一方の次数は 1 である．よって因数定理 Theorem 1.4.5 により，それは $\mathbb{F}$ に zero 点をもつから，$f(X)$ も $\mathbb{F}$ に zero 点をもつ．

⇐) $f(X)$ が $\mathbb{F}$ に zero 点をもつとすれば，Theorem 1.4.5 により明らか．

■

**Example 1.4.7**

多項式 $2X^3 - 5$ は $\mathbb{Q}$ 上既約である．

---

### 1.4.3 既約性と irr $(\alpha, \mathbb{Q})$

**THEOREM 1.4.8 (既約多項式)**

$\mathbb{F} \subset \mathbb{C}$ を体，$\alpha \in \mathbb{C}$ が $\mathbb{F}$ 上代数的であるとする．このとき，次の (i), (ii) は同値である：

(i) $f(X) = \mathrm{irr}(\alpha, \mathbb{F})$.

(ii) $f(\alpha) = 0$，かつ $f(X)$ は $\mathbb{F}$ 上の monic な既約多項式である．

---

この定理によって，代数的数 $\alpha$ のもつ既約多項式と，体 $\mathbb{F}$ 上の既約性が結びつく．証明に入る前に，例を挙げておく：

**Example 1.4.9**

- $\mathrm{irr}\left(\sqrt{2}, \mathbb{Q}\right) = X^2 - 2$.

  $\mathbb{Q}$ 上で zero 点となりうるのは $\pm 1$, $\pm 2$ のみであるから，代入してみれば zero 点ではない．この多項式の次数は 2 であるから，Theorem 1.4.6 によって $\mathbb{Q}$ 上既約である．従って Theorem 1.4.8 により $\sqrt{2}$ の $\mathbb{Q}$ 上の既約多項式は $X^2 - 2$ であることが解る．

- $\mathrm{irr}\left(\sqrt[3]{2}, \mathbb{Q}\right) = X^3 - 2$.

  明らかに $\sqrt[3]{2}$ は $X^3 - 2$ の zero 点であり，同様にして示せる．

---

Theorem 1.4.8 (p.17) の証明に移る．

*Proof.*

いま，多項式の集合 $P$ を次のように定める：

$$P \overset{\text{def}}{=} \left\{ p(X) \in \mathbb{F}[X] \;\middle|\; p(\alpha) = 0,\ p(X) : \text{monic} \right\}.$$

- $(i) \Rightarrow (ii)$ を示す．(i) を仮定すれば，Definition 1.2.7 (p.6) ($\alpha$ の既約多項式の定義) より

  $f(X)$ は $P$ のうち最小次数の多項式である

  ことが言える．あとは，$f(X)$ が $\mathbb{F}$ 上で既約であることを示せば十分である．

  $f(X)$ が $\mathbb{F}$ 上で既約でないとする．$f(X)$ は定数ではないから $\mathbb{F}$ 上で既約であり，$\mathbb{F}[X]$ の多項式 $g(X)$, $h(X)$ が存在して

  $$f(X) = g(X)\,h(X)$$

  が成り立ち，かつ $g, h$ の次数は，いずれも $f$ の次数よりも低い．$g$ と $h$ はいずれも monic であるとして，一般性を失わない．$X$ に $\alpha$ を代入して

  $$0 = f(\alpha) = g(\alpha)\,h(\alpha)$$

  であるから，$g(\alpha) = 0$ または $h(\alpha) = 0$ のいずれかが成り立つ．

  従って $g(X)$ と $h(X)$ のいずれかが $P$ の要素であることになるが，これは $f(X)$ が $P$ の最小次数の多項式であることに矛盾する．

  以上から，$f(X)$ は既約であることが示された．

- $(ii) \Rightarrow (i)$ を示す．(ii) を仮定すれば，$f(X) \in P$ であるから，

$$\deg f(X) \geq \deg \operatorname{irr}(\alpha, \mathbb{F}).$$

$f(X)$ を $\operatorname{irr}(\alpha, \mathbb{F})$ で割れば，除法の原理によって，$q(X)$，$r(X) \in \mathbb{F}[X]$ なる $\deg r(X) < \deg \operatorname{irr}(\alpha, \mathbb{F})$ または $r(X) = 0_{\mathrm{P}}$ をみたす $q(X), r(X)$ が存在して

$$f(X) = \operatorname{irr}(\alpha, \mathbb{F})\, q(X) + r(X) \tag{1.9}$$

が成り立つ．

(1.9) の両辺に $X = \alpha$ を代入すれば

$$0 = 0 \cdot q(\alpha) + r(\alpha), \quad \therefore\ r(\alpha) = 0$$

となる．

もし $r(X) \neq 0_{\mathrm{P}}$ ならば，$r(X)$ の主係数で $r(X)$ を割って monic な多項式を得るが，それは集合 $P$ に含まれる．このとき $P$ は $\operatorname{irr}(\alpha, \mathbb{F})$ より低い次数の多項式を含むことになり，矛盾する．

よって $r(X) = 0_{\mathrm{P}}$ となり，(1.9) より

$$f(X) = \operatorname{irr}(\alpha, \mathbb{F})\, q(X).$$

ところが $f(X)$ は $\mathbb{F}$ 上で既約だから，$q(X)$ は定数でなければならず，更に $f(X)$ も $\operatorname{irr}(\alpha, \mathbb{F})$ もいずれも monic であることから $q(X) \equiv 1$ となり，$f(X) = \operatorname{irr}(\alpha, \mathbb{F})$ が言えた．

■

### 1.4.4 体の有限次拡大

$\mathbb{K}$ が体 $\mathbb{F}$ の拡大体であるとする．$\mathbb{F}$ 上の vector 空間としての $\mathbb{K}$ が有限次元であるとき，$\mathbb{K}$ の要素は $\mathbb{F}$ 上代数的であることを示す．

**THEOREM 1.4.10 (拡大体の次数)**

$\mathbb{F}$ を $\mathbb{K}$ の部分体とし，$[\mathbb{K} : \mathbb{F}] = n$ とする．

このとき，$\mathbb{K}$ に属する数 $\alpha$ はすべて $\mathbb{F}$ 上代数的であり，$\operatorname{irr}(\alpha, \mathbb{F}) \leq n$ が成り立つ．

---

*Proof.*

$\alpha \in \mathbb{K}$ とする．$[\mathbb{K} : \mathbb{F}] = n$ であるから，$\mathbb{K}$ の要素 $(n+1)$ 個からなる任意の集合は $\mathbb{F}$ 上で線形従属である．いま，集合

$$\left\{1, \alpha, \alpha^2, \cdots, \alpha^n\right\}$$

を考えれば，これはそうような集合の例となり，「すべて 0」であることはない $c_0, c_1, c_2, \cdots, {}_n \in \mathbb{F}$ が存在して

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0$$

が成り立つ．

いま，多項式 $p(X) \in \mathbb{F}[X]$ を

$$p(X) \stackrel{\text{def}}{=} c_0 + c_1X + c_2X^2 + \cdots + c_nX^n$$

と定めれば，$p(X)$ は $\mathbb{F}$ 上に zero 点 $\alpha$ をもつから，$\alpha$ は $\mathbb{F}$ 上代数的である．

$p(X)$ の次数は $n$ 次以下であるから，やはり $n$ 次以下の monic な多項式が存在して (∵ Lemma 1.2.5 (p.5))

$$\operatorname{irr}(\alpha, \mathbb{F}) \leq n$$

が成り立つ．■

**Corollary 1.4.11**

$\mathbb{F}$ を $\mathbb{C}$ の部分体，$\alpha \in \mathbb{C}$ を $\mathbb{F}$ 上の次数 $n$ をもつ代数的数とする．このとき，$\mathbb{F}\big(\alpha\big)$ に含まれる数はすべて $\mathbb{F}$ 上代数的で，その次数は $n$ を越えない．

**THEOREM 1.4.12 (代数的数体)**
$\mathbb{F}$ を体 $\mathbb{E}$ の部分体とする．$\mathbb{F}$ 上代数的であるような $\mathbb{E}$ の要素の全体は体をなす.

---

*Proof.*

$\alpha, \beta \in \mathbb{E}$ が $\mathbb{F}$ 上代数的であるとする．このとき，$\alpha \pm \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ (ただし $\beta \neq 0$) がすべて $\mathbb{F}$ 上代数的であることを示す.

体の昇鎖 $\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{F}(\alpha)(\beta)$ を考える．仮定より $\alpha$ は $\mathbb{F}$ 上代数的であるから，$\mathbb{F}(\alpha)$ は $\mathbb{F}$ の有限次拡大である．また，$\beta$ も $\mathbb{F}$ 上代数的であるから，$\mathbb{F}(\alpha)$ 上でも代数的で，従って $\mathbb{F}(\alpha)(\beta)$ は $\mathbb{F}(\alpha)$ の有限次拡大である．Theorem 1.3.24 (p.15) (昇鎖の次元) によって，$\mathbb{F}(\alpha)(\beta)$ は $\mathbb{F}$ の有限次拡大であり，Theorem 1.4.10 (p.18) によって，$\mathbb{F}(\alpha)(\beta)$ のすべての要素は，$\mathbb{F}$ 上代数的であることが言える.

$\alpha \pm \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ は $\mathbb{F}(\alpha)(\beta)$ の要素であるから，定理は証明された. ■

有理数体 $\mathbb{Q}$ 上の多項式の zero 点，つまり $\mathbb{Q}$ に係数をもつ方程式の解，を「代数的数」(**algebraic number**) と言う．Theorem 1.4.12 から，次が成り立つ：

**Corollary 1.4.13**
代数的数の集合は $\mathbb{C}$ の部分体である.

# §1–5. SC-作図

## 1.5.1 SC-作図とは?

定**木** (**straight-edge**) とコンパス (**compass**) のみを用いる作図を **SC 作図** (**straight-edge-and-compass construction**) と言うことにしよう.

次の section §1.6 (p.22) での「作図不可能性証明」のために，この section では，いくつかの要点を整理し，

**SC 作図可能数** (**SC-constructible number**)

という概念を定義しよう．まずは，SC 作図を厳密に定義することから始める.

「SC 作図問題」とは,

> 点集合 $\{P_1, P_2, \ldots, P_m\}$ が与えられたとき，それらから定木と compass のみを用いて，点の有限系列
>
> $$P_{m+1}, P_{m+2}, \cdots, P_{m+n}$$
>
> を作り，求める結果を得る

という問題である．もちろん点集合 $\{P_1, P_2, \ldots, P_m\}$ 以外に直線や円が与えられることもある．しかし，直線が与えられることは，その上にある 2 点が与えられることと同値であり，また円が与えられることは，中心と円周上の 1 点が与えられることと同値であるから，一般性を失うことなくこのようにして定めることができる.

与えられる点集合 $\{P_1, P_2, \ldots, P_m\}$ を**初期集合** (**initial set**) と言う．また，加えられていく点 $P_{m+1}, P_{m+2}, \cdots$ は，初期集合の要素で定まる直線または円の交点であるか，そうでなければ作図の過程で得られた点で定まる直線または円の交点である.

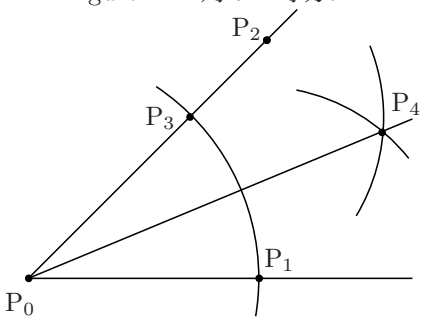
例として，任意に与えられた角の 2 等分線の SC 作図を見よう.

**Example 1.5.1**

任意角の 2 等分．Figure 1.1 (p. 20)

- 初期集合 $\{P_0,\ P_1,\ P_2\}$.
- 加えられる点列 $P_3,\ P_4$.

Figure 1.1: 角の 2 等分.




---

SC 作図の厳密な定義は，次の Definition 1.5.2 で与えられる：

**Definition 1.5.2 (SC-作図)**

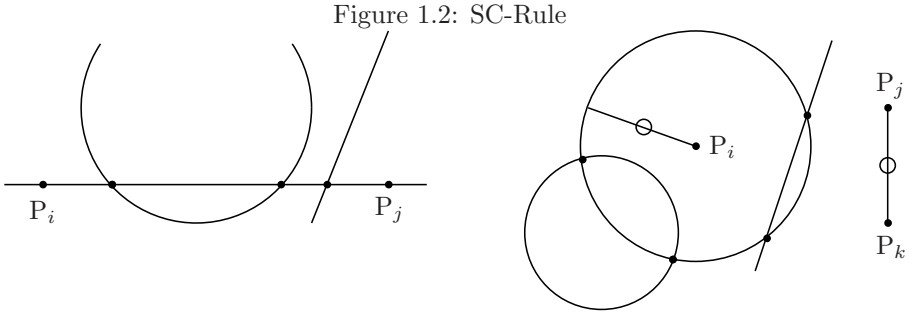
作図のどの段階であっても，既に存在している点に，次の **SC-Rule** のいずれかの手順で得られる点のみを新たな点として加えることができる：

**SC-Rule** (Figure 1.2 (p. 20) を参照のこと．)

(i) 既に得られている点 $P_i$ と $P_j$ とを結ぶ直線を引き，必要ならば延長して，既に得られている他の直線または円との交点を得ること．

(ii) 既に得られている点 $P_i$ を中心にして，既に得られている 2 点 $P_j, P_k$ の間の距離を半径とする円を描き，既に得られている直線または円との交点を得ること．

Figure 1.2: SC-Rule




---

このように SC-Rule を定めると，3 つの作図不可能性問題は次のようにまとめられる：

(I) **立方体倍積問題 Doubling the Cube**

初期集合 $\{P_0,\ P_1\}$ が与えられたとする．SC-Rule のみを用いて点の系列を作り，2 点 $P_0, P_1$ の距離 $d$ の $\sqrt[3]{2}$ 倍の距離をもつ 2 点 $P_i, P_j$ を得ることは可能か.

(II) **円積問題 Squaring the Circle**

初期集合 $\{\mathrm{P}_0,\, \mathrm{P}_1\}$ が与えられたとき，SC-Rule のみを用いて点の系列を作り，線分 $\mathrm{P}_0\mathrm{P}_1$ の $\sqrt{\pi}$ 倍の距離をもつ 2 点 $\mathrm{P}_i, \mathrm{P}_j$ を得ることは可能か.

(III) **角の 3 等分問題 Trisecting an Angle**

初期集合 $\{\mathrm{P}_0,\, \mathrm{P}_1,\, \mathrm{P}_2\}$ が与えられたとき，SC-Rule のみを用いて点の系列を作り，$\angle \mathrm{P}_i\mathrm{P}_0\mathrm{P}_1$ が $\angle \mathrm{P}_2\mathrm{P}_0\mathrm{P}_1$ の $\dfrac{1}{3}$ に等しくなるような点 $\mathrm{P}_i$ を得ることは可能か.

### 1.5.2 SC-作図可能数

「SC-作図可能である実数」(**SC-constructible real number**) という概念を定義しよう.

**Definition 1.5.3 (RC-作図可能数)**

$\gamma \in \mathbb{R}$ が **SC-作図可能な数である**，または単に**作図可能な数であるとは**，$\left|\mathrm{P}_0\mathrm{P}_1\right| = 1$ であるような初期集合 $\{\mathrm{P}_0,\, \mathrm{P}_1\}$ から始めて，SC-Rule のみを用いて，$\left|\mathrm{P}_i\mathrm{P}_j\right| = \gamma$ をみたすような 2 点 $\mathrm{P}_i, \mathrm{P}_j$ を得ることができることである.

---

明らかに，$\sqrt[3]{2}$ が作図可能数であることと立方体の倍積は同値であり，$\sqrt{\pi}$ が作図可能数であることと円積 (円の正方形化) は同値である.

以下，SC-作図可能な数の集合を $\Gamma_{\mathrm{SC}}$，または単に $\Gamma$ で表す:

$$\Gamma_{\mathrm{SC}} = \Gamma \stackrel{\mathrm{def}}{=} \left\{\gamma \in \mathbb{R} \,\middle|\, \gamma \text{ is SC-constructible}\right\}.$$

**THEOREM 1.5.4 (平方根で表される数)**

$\Gamma_{\mathrm{SC}} = \Gamma$ は $\mathbb{R}$ の部分体であり，更に次が成り立つ：

(i) $\Gamma$ は有理数体 $\mathbb{Q}$ を含む：$\mathbb{Q} \subset \Gamma$.

(ii) $\alpha \in \Gamma,\ \alpha > 0 \Rightarrow \sqrt{\alpha} \in \Gamma$.

---

*Proof.*

$\alpha, \beta \in \Gamma$ とすると，定義より $|\alpha|$，$|\beta|$ を長さにもつ線分 (の端点) は作図可能である．長さ (線分) を移すことができるから，$|\alpha+\beta|$，$|\alpha-\beta|$ を長さとする線分 (の端点) も作図可能である.

同様に $|\alpha\beta|$，$\left|\frac{\alpha}{\beta}\right|$ を長さにもつ線分 (の端点) も作図可能である.

よって，作図可能な数の集合 $\Gamma_{\mathrm{SC}}$ は有理演算について閉じているから，体である.

初期集合 $\{\mathrm{P}_0,\, \mathrm{P}_1\}$ について，$\left|\mathrm{P}_0\mathrm{P}_1\right| = 1 \in \Gamma$ であるから,

$$1,\ 1+1,\ 1+1+1,\ \cdots;\quad 1-1,\ 1-1-1,\ 1-1-1-1,\ \cdots$$

は作図可能であり，よって $\Gamma$ は整数環 $\mathbb{Z}$ を部分集合として含む：$\mathbb{Z} \subset \Gamma$.

$n \in \mathbb{Z},\ m \in \mathbb{Z}^+$ について $\frac{n}{m} \in \Gamma$ であるから，$\Gamma$ は有理数体を含む：$\mathbb{Q} \subset \Gamma$.

さらに $\alpha \in \Gamma$ であれば，Figure 1.3 (p. 22) の作図を実行すれば，$\sqrt{|\alpha|}$ が作図できるから，$\sqrt{|\alpha|} \in \Gamma$.

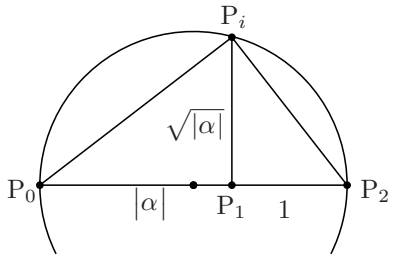
■

Theorem 1.5.4 (p.21) から，次が解る：

有理数体 $\mathbb{Q}$ から出発して,

- 有理演算を実行することと
- 平方根を作ること

Figure 1.3: $\sqrt{|\alpha|}$ の作図 (NY)




の 2 つの操作により得られる実数はすべて作図可能である.

これを体の理論のことばで言い換えたのが，次の Theorem 1.5.5 である：

**THEOREM 1.5.5 (有限列の存在)**

$\gamma \in \mathbb{R}$ が SC-作図可能であるのは，次をみたすような正の実数の有限列 $\gamma_1, \gamma_2, \ldots, \gamma_n$ が存在する場合である：

$$\begin{aligned}
\gamma_1 \in \mathbb{F}_1 \qquad & \mathbb{F}_1 = \mathbb{Q}, \\
\gamma_2 \in \mathbb{F}_2 \qquad & \mathbb{F}_2 = \mathbb{F}_1(\sqrt{\gamma_1}), \\
\gamma_3 \in \mathbb{F}_3 \qquad & \mathbb{F}_3 = \mathbb{F}_2(\sqrt{\gamma_2}), \\
& \cdots \\
\gamma_n \in \mathbb{F}_n \qquad & \mathbb{F}_n = \mathbb{F}_{n-1}(\sqrt{\gamma_{n-1}}), \\
\gamma \in \mathbb{F}_{n+1} \qquad & \mathbb{F}_{n+1} = \mathbb{F}_n(\sqrt{\gamma_n}).
\end{aligned}$$

---

*Proof.*

Theorem 1.5.4 (p.21) より明らか. ■

この Theorem 1.5.5 (p.22) は，体の昇鎖

$$\mathbb{Q} = \mathbb{F}_1 \subset \mathbb{F}_2 \subset \mathbb{F}_3 \subset \cdots \subset \mathbb{F}_n \subset \mathbb{F}_{n+1}$$

の存在を主張していることに注意しよう．この昇鎖は，次の課題である「作図不能な数」に関する考察で，決定的な役割を果たす.

# § 1–6. 作図不能性証明

## 1.6.1 作図不能数

§1.5 (p.19) では，有理数から出発して，平方根を求めることを有限回，有理演算を有限回，施して得られる数，例えば

$$2 + \sqrt{3 - \sqrt{\frac{2}{7} + \sqrt{2}}}$$

は，RC-作図可能であることを見た．これが，Theorem 1.5.4 (p.21)，Theorem 1.5.5 (p.22) の意味であった.

この §1.6 では，この逆を考えよう．つまり

すべての作図可能数は，有理数体 $\mathbb{Q}$ から出発して，有理演算と平方根をとる演算を有限回施すことによって得られるか?

を考察する.

次の Theorem 1.6.1 は，この問に YES!と答える：

**THEOREM 1.6.1 (作図可能数は平方根で表される)**

$\gamma \in \mathbb{R}$ が作図可能である，つまり $\gamma \in \Gamma_{\mathrm{SC}}$ であるならば，次をみたすような $\gamma_1, \gamma_2, \ldots, \gamma_n \in \mathbb{R}^+$ が存在する：

$$\begin{aligned}
&\gamma_1 \in \mathbb{F}_1 \qquad \mathbb{F}_1 = \mathbb{Q},\\
&\gamma_2 \in \mathbb{F}_2 \qquad \mathbb{F}_2 = \mathbb{F}_1(\sqrt{\gamma_1}),\\
&\gamma_3 \in \mathbb{F}_3 \qquad \mathbb{F}_3 = \mathbb{F}_2(\sqrt{\gamma_2}),\\
&\qquad\cdots\\
&\gamma_n \in \mathbb{F}_n \qquad \mathbb{F}_n = \mathbb{F}_{n-1}(\sqrt{\gamma_{n-1}}),\\
&\gamma \in \mathbb{F}_{n+1} \qquad \mathbb{F}_{n+1} = \mathbb{F}_n(\sqrt{\gamma_n}).
\end{aligned}$$

---

*Proof.*

§1.6.3 (p.25) で証明する. ■

この定理を，我々の主定理 (**Principal Theorem, Hauptsatz**) とし，

**実 2 次体の作図可能性定理　CTQ**

**Constructibility Theorem of Real Quadratic Field**

と呼ぶ.

この **CTQ** は，Theorem 1.5.5 (p.22) の逆であることに注意しよう.

**THEOREM 1.6.2 (作図可能数の次数)**

$grg \in \mathbb{R}$ が作図可能である，つまり $\alpha \in \Gamma_{\mathrm{SC}}$ ならば，$\gamma$ は $\mathbb{Q}$ 上代数的であり，かつその $\mathbb{Q}$ 上の次数は 2 の非負整数べきである：

$$\gamma \in \Gamma_{\mathrm{SC}} \Rightarrow \exists s \in \mathbb{N}\,;\, \deg(\gamma, \mathbb{Q}) = 2^s.$$

---

*Proof.*

$\gamma \in \Gamma$ とし，Theorem 1.6.1 (p.23) で $\gamma$ を作図する過程でででてくる数を

$$\gamma_1, \gamma_2, \ldots, \gamma_n$$

とする．以下，$i \in \mathbb{Z}^+$, $1 \leq i \leq n$ として，実数 $\sqrt{\gamma_i}$ は多項式 $X^2 - \gamma_i$ の zero 点であるが，$\gamma_i \in \mathbb{F}_i$ であるから，この多項式は $\mathbb{F}_i[X]$ に属する．よって Definition 1.2.7 (p.6) によって

$$\deg(\sqrt{\gamma_i}, \mathbb{F}_i) = 1 \text{ or } 2.$$

また $\mathbb{F}_{i+1} = \mathbb{F}_{\sqrt{\gamma_i}}$ であるから，

$$[\mathbb{F}_{i+1} : \mathbb{F}_i] = 1 \text{ or } 2.$$

このような体の拡大を順次行えば，体の昇鎖

$$\mathbb{Q} = \mathbb{F}_i \subseteq \mathbb{F}_2 \subseteq \cdots \subseteq \mathbb{F}_n \subseteq \mathbb{F}_{n+1}$$

が得られるから，$\gamma$ は $\mathbb{Q}$ 上代数的である.

更に，体の昇鎖

$$\mathbb{Q} \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{F}_{n+1}$$

を考えれば，$\deg(\gamma, \mathbb{Q})$ は $[\mathbb{F}_{n+1} : \mathbb{Q}]$ の約数であり，よって，ある $s \in \mathbb{N}$ が存在して

$$\deg(\gamma, \mathbb{Q}) = 2^s.$$

■

### 1.6.2　3 大作図問題の不可能性

Theorem 1.6.1 (p.23)，つまり我々の主定理 CTQ の証明は後回しにしてあるが，この定理さえ認めれば，立方体倍積問題と任意角の 3 等分問題についてその不可能性を証明するのは容易である．証明は帰謬法による．つまり

> もし作図が可能であるとすれば，$\mathbb{Q}$ 上の次数が 2 のべきではないような作図可能数が存在することになり，Theorem 1.6.2 (p.23) に矛盾する

という線で，証明が行われる．意外なほど**アッケナイ !!**

**THEOREM 1.6.3 (立方体倍積の不可能性)**

与えられた立方体の倍積立方体の 1 辺は，SC-作図不能である．

---

*Proof.*

体積が 2 である立方体の 1 辺は $\sqrt[3]{2}$ である．よって立方体の倍積は，長さ 1 の単位線分から始めて，SC-Rule に従って，長さ $\sqrt[3]{2}$ の線分の端点を作図することと同値である．

もし立方体の倍積が可能であると仮定すれば，$\sqrt[3]{2}$ は作図可能数である：$\sqrt[3]{2} \in \Gamma_{\mathrm{SC}}$.

ところが，Example 1.4.9 (p.17) により

$$\mathrm{irr}\left(\sqrt[3]{2}, \mathbb{Q}\right) = X^3 - 2$$

であるから，

$$\deg\left(\sqrt[3]{2}, \mathbb{Q}\right) = 3$$

である．$3 = 2^s$ をみたす $s \in \mathbb{N}$ は存在しないから，立方体倍積は作図不能である:

$$\sqrt[3]{2} \notin \Gamma_{\mathrm{SC}}.$$

■

**THEOREM 1.6.4 (任意角 3 等分の不可能性)**

任意に与えられた角を 3 等分する直線は RC-作図不能である．

---

*Proof.*

もし任意角の 3 等分が可能であるならば，特に大きさ $\frac{\pi}{3}$ を 3 等分して $\frac{\pi}{9}$ を作図することができる．このとき，簡単な作図によって $\frac{\pi}{9}$ を 1 つの鋭角にもつ直角 3 角形を作図できるから，$\cos\frac{\pi}{9}$ の値を長さとする線分の端点が作図可能である．

ところが，$\mathbb{Q}$ 上の $\cos\frac{\pi}{9}$ の最小多項式 (**人呼んで「3 倍角公式」!**)

$$\mathrm{irr}\left(\cos\frac{\pi}{9}, \mathbb{Q}\right)$$

の次数は 3 次であるから，

$$\deg\left(\cos\frac{\pi}{9}, \mathbb{Q}\right) = 3.$$

従って $\cos\frac{\pi}{9} \notin \Gamma_{\mathrm{SC}}$ であるから，立方体倍積の場合と同様にして，$\frac{\pi}{3}$ を 3 等分することは不可能である．■

**THEOREM 1.6.5 (円積の不可能性)**

与えられた円に等しい面積をもつ正方形は，SC-作図不能である．

---

*Proof.*

半径 1 の円の面積は $\pi$ であるから，もし円の正方形化が可能であるとすれば，$\sqrt{\pi}$ を長さとする線分の端点が作図可能である．

このとき，$\sqrt{\pi}$ は $\mathbb{Q}$ 上代数的であることになるが，$(\sqrt{\pi})^2 = \pi$ であるから，$\pi$ も $\mathbb{Q}$ 上代数的であるはずである．

ところが，$\pi$ は $\mathbb{Q}$ 上代数的でない (残念ながら今は証明できない) から，円積は SC-作図不能である．

■

### 1.6.3 主定理 CTQ 証明

ではいよいよ，我々の主定理 **CTQ** Theorem 1.6.1 (p.23)，つまり

**実 2 次体の作図可能性定理**
**Constructibility Theorem of Real Quadratic Field**

の証明に入る．まず，次の定義を用意する：

**Definition 1.6.6 ($\mathbb{F}$ 点，$\mathbb{F}$ 直線，$\mathbb{F}$ 円)**
$\mathbb{F}$ を $\mathbb{R}$ の部分体とする．

- ある点が $\mathbb{F}$ 点であるとは，その点の $x$-, $y$- 座標がどちらも $\mathbb{F}$ の要素であることである．
- ある直線が $\mathbb{F}$ 直線であるとは，その直線が 2 つの $\mathbb{F}$ 点を通ることである．
- ある円が $\mathbb{F}$ 円であるとは，その中心が $\mathbb{F}$ 点であり，かつ半径が 2 つの $\mathbb{F}$ 点間の距離に等しいことである．

---

**Example 1.6.7**

(a) 点 $(2, 1)$ は $\mathbb{Q}$ 点である．
(b) 点 $\left(1, \sqrt{2}\right)$ は $\mathbb{Q}\left(\sqrt{2}\right)$ 点である．
(c) 直線 $y = 2x$ は $\mathbb{Q}$ 直線である．2 つの $\mathbb{Q}$ 点 $(0, 0)$，$(1, 2)$ を通るからである．
(d) 直線 $y = \sqrt{2}\,x$ は $\mathbb{Q}\left(\sqrt{2}\right)$ 直線であるが，$\mathbb{Q}$ 直線ではない．
(e) 円 $x^2 + y^2 = 4$ は $\mathbb{Q}$ 円である．
(f) 円 $x^2 + y^2 = 2$ は $\mathbb{Q}\left(\sqrt{2}\right)$ 円である．

---

**Example 1.6.8**

$\mathbb{Q}$ 直線 $y = x$ と $\mathbb{Q}$ 円 $x^2 + y^2 = 4$ の交点は $\left(\sqrt{2}, \sqrt{2}\right)$ と $\left(-\sqrt{2}, -\sqrt{2}\right)$ であるから，$\mathbb{Q}$ 点ではなく $\mathbb{Q}\left(\sqrt{2}\right)$ 点である．

---

ある作図の過程で，すでに $\mathrm{P}_0, \mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_k$ が得られたとする．適当に座標系を定めたとき，すべての点 $\mathrm{P}_0, \mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_k$ が $\mathbb{F}$ 点であるような，$\mathbb{R}$ の部分体 $\mathbb{F}$ を考える．

S. C. Rule (i), (ii) に従って作図を進めるとき，新たな点 $\mathrm{P}_{k+1}, \mathrm{P}_{k+2}, \cdots, \mathrm{P}_{k+n}$ を得るが，それらの点は次のうちのどれかである：

(a) 2 本の $\mathbb{F}$ 直線の交点 ;
(b) $\mathbb{F}$ 直線と $\mathbb{F}$ 円の交点 ;
(c) 2 つの $\mathbb{F}$ 円の交点.

次の補題は，新たに得られる点の座標は，高々「平方根が増える」だけであることを主張する:

**Lemma 1.6.9**

$\mathbb{F}$ を $\mathbb{R}$ の部分体とする．

(a) 2 本の $\mathbb{F}$ 直線が 1 点で交わるとき，その交点は $\mathbb{F}$ 点である．
(b) $\mathbb{F}$ 直線と $\mathbb{F}$ 円が交わるとき，その交点が $\mathbb{F}\left(\sqrt{\alpha}\right)$ 点であるような正の実数 $\alpha$ が存在する．
(c) 2 つの $\mathbb{F}$ 円が交わるとき，その交点が $\mathbb{F}\left(\sqrt{\alpha}\right)$ 点であるような正の実数 $\alpha$ が存在する．

---

*Proof.*

$\mathbb{F}$ 直線の方程式は

$$ax + by + c = 0 \tag{1.10}$$

と表され，ここで $a,\, b,\, c \in \mathbb{F},\ a^2 + b^2 \neq 0$ である．また，$\mathbb{F}$ 円は

$$x^2 + y^2 + px + qy + r = 0 \tag{1.11}$$

で表され，$p,\, q,\, r \in \mathbb{F}$ である．

(a) 2 本の $\mathbb{F}$ 直線が交わるとき，その交点の座標は (1.10) の形をした 2 式からなる 1 次の連立方程式を解くことによって得られる．このときに用いられるのは，$\mathbb{F}$ 上の有理演算 (**rational operations on** $\mathbb{F}$) — 加減乗除 — のみであるから，交点は $\mathbb{F}$ 点である．

(b) $\mathbb{F}$ 直線と $\mathbb{F}$ 円が交わるとき，その交点は (1.10) と (1.11) を連立してできる 2 次方程式の解として求められる．2 次方程式の解を与える algorithm

$$x_1,\, x_2 = (x_1 + x_2) \pm \sqrt{(x_1 - x_2)^2}$$

からただちに解るように，この解 $x_1$ と $x_2$ は，

$$\alpha = (x_1 - x_2)^2 \in \mathbb{F}$$

とすれば $\mathbb{F}\big(\sqrt{\alpha}\big)$ に含まれるから，交点は $\mathbb{F}\big(\sqrt{\alpha}\big)$ 点である．

(c) 2 つの $\mathbb{F}$ 円

$$x^2 + y^2 + p_1 x + q_1 y + r_1 = 0,$$
$$x^2 + y^2 + p_2 x + q_2 y + r_2 = 0$$

の交点は，この内の一方の $\mathbb{F}$ 円と，直線

$$(p_1 - p_2)\, x + (q_1 - q_2)\, y + r_1 - r_2 = 0$$

の交点である．この直線は 2 つの $\mathbb{F}$ 点

$$\left(0,\, -\frac{r_1 - r_2}{q_1 - q_2}\right), \quad \left(-\frac{r_1 - r_2}{p_1 - p_2},\, 0\right)$$

を通るから $\mathbb{F}$ 直線である．よって (b) の場合に帰着されるから，ある $\alpha \in \mathbb{F}$ について，2 つの $\mathbb{F}$ 円の交点は $\mathbb{F}\big(\sqrt{\alpha}\big)$ 点となる．

■

以上の準備によって，主定理 **CTQ** — Theorem 1.6.1 (p.23) — の証明が可能となる：

### Proof of CRT

*Proof.*

$\gamma$ を SC-作図可能数とする： $\gamma \in \Gamma_{\mathrm{SC}}$.
作図可能数の定義 Definition 1.5.3 (p.21) によって，点列

$$\mathrm{P}_0,\ \mathrm{P}_1,\ \mathrm{P}_2,\ \cdots,\ \mathrm{P}_n$$

が存在して，これらの 2 点間の距離が $\big|\gamma\big|$ である．
初期集合 $\{\mathrm{P}_0,\, \mathrm{P}_1\}$ について $\big|\mathrm{P}_0\mathrm{P}_1\big| = 1$ であるから，$\mathrm{P}_0\,(0,\, 0)\,, \mathrm{P}_1\,(1,\, 0)$ として，座標系を設定することができる．$\mathrm{P}_0$ と $\mathrm{P}_1$ は $\mathbb{Q}$ 点であることに着目する．証明は帰納法による．
$\mathbb{F}_1 = \mathbb{Q}$ とする．$1 \leq k \leq n-1$ なる $k$ について，$\mathrm{P}_0,\ \mathrm{P}_1,\ \mathrm{P}_2,\ \cdots,\ \mathrm{P}_k$ がすべて $\mathbb{F}_k$ 点であると仮定する．ただしここで，$\mathbb{F}_k$ は $\mathbb{R}$ の部分体である．
SC Rule によって，次の点 $\mathrm{P}_{k+1}$ は次のいずれかである：

(i) 2 本の $\mathbb{F}_k$ 直線の交点；

(ii) $\mathbb{F}_k$ 直線と $\mathbb{F}_k$ 円の交点；
(iii) 2 個の $\mathbb{F}_k$ 円の交点.

従って，Lemma 1.6.9 (p.25) により，点 $\mathrm{P}_{k+1}$ はある正の実数 $\gamma_k$ について

$$\mathbb{F}_{k+1} = \mathbb{F}_k\left(\sqrt{\gamma_k}\right), \quad \gamma_k \in \mathbb{F}_k$$

と定められる体 $\mathbb{F}_{k+1}$ の点，つまり $\mathbb{F}_{k+1}$ 点である.
$\mathbb{F}_k \subset \mathbb{F}_{k+1}$ であるから，次が言える：

$$\mathrm{P}_0,\ \mathrm{P}_1,\ \mathrm{P}_2,\ \cdots,\ \mathrm{P}_{k+1} \text{ は } \mathbb{F}_{k+1} \text{ 点である.}$$

従って，$k$ に関する帰納法によって正の実数の列

$$\gamma_1,\ \gamma_2,\ \ldots,\ \gamma_n$$

が存在して，次をみたす：

$$\begin{aligned}
&\gamma_1 \in \mathbb{F}_1, \quad \mathbb{F}_1 = \mathbb{Q},\\
&\gamma_2 \in \mathbb{F}_2, \quad \mathbb{F}_2 = \mathbb{F}_1\left(\sqrt{\gamma_1}\right),\\
&\gamma_3 \in \mathbb{F}_3, \quad \mathbb{F}_3 = \mathbb{F}_2\left(\sqrt{\gamma_2}\right),\\
&\quad \cdots\\
&\gamma_n \in \mathbb{F}_n, \quad \mathbb{F}_n = \mathbb{F}_{n-1}\left(\sqrt{\gamma_{n-1}}\right).
\end{aligned}$$

従って，$\mathbb{F}_n$ の点からなる点列 $\mathrm{P}_0,\ \mathrm{P}_1,\ \mathrm{P}_2,\ \cdots,\ \mathrm{P}_n$ のうち，どの 2 点間の距離 $|\gamma|$ も，$\mathbb{F}_n$ のある要素の平方根である．つまり

$$\exists \gamma_n \in \mathbb{F}_n,\ \gamma_n > 0\ ;\ \gamma \in \mathbb{F}_n\left(\sqrt{\gamma_n}\right)$$

が言えた. ■