2019 年度 後期 代数学 3

担当 和地 輝仁

目次

1 シラバス抜粋

到達目標

1. いろいろな体とその性質を知る。
2. 作図と体の関係を理解する。
3. 代数方程式の根の公式と体の関係を知る。

授業計画 順序を交換する場合もあるので注意すること。

1. 環
2. 有理整数環
3. 剰余環
4. 多項式環
5. 既約多項式
6. イデアル
7. 体
8. ベクトル空間の復習
9. 体の拡大
10. 作図問題
11. 正多角形の作図可能性
12. 正規拡大
13. 分解体
14. 多項式のガロア群
15. 根の公式
16. 期末試験

成績評価 期末試験 (80%) と、毎回の演習問題の状況 (20%) で成績を評価する。原則として全ての時間の出席を求めるが、やむを得ない理由で欠席をする (した) 場合はできるだけ速やかに申し出て、指示を受けること。

2 授業のノート

§1 環

(1.1) **定義 (環、可換環)** 2 種類の演算、和と積が定義された集合 R が**環**であるとは、次の条件 (R1) から (R7) を満たすときを言う。

(R1) 和が結合法則を満たす
(R2) 和が交換法則を満たす
(R3) 和の単位元 0 が存在する $(a+0=0+a=a)$
(R4) 和の逆元が存在する $(a+(-a)=0$ なる $-a$ の存在)
(R5) 積が結合法則を満たす
(R6) 0 とは異なる積の単位元 1 が存在する $(a\cdot 1=1\cdot a=a)$
(R7) 分配法則が成立する $(a(b+c)=ab+ac,\ (a+b)c=ac+bc)$

さらに、

(R8) 積が交換法則を満たす

も成立しているとき、R を **可換環**と呼ぶ。

可換環ではない環にも、$n\times n$ 行列全体のなす環 n **次全行列環**など重要なものがあるが、この講義では可換環のみを学ぶ。

(1.2) **例 (数のなす環)** 環の定義は条件が多く思えるかも知れないが、数の集合であれば、単に **1 と 0 を含み、和、差、積で閉じている集合**は環である、ということである。

(1) まず、複素数全体の集合 $\mathbb{C}$、実数全体の集合 $\mathbb{R}$、有理数全体の集合 $\mathbb{Q}$、整数全体の集合 $\mathbb{Z}$ はすべて環である。
(2) 偶数全体の集合 $2\mathbb{Z}$ は、1 を含まないので環ではない。ただし、それ以

外の条件は満たしている。
(3) $\{a+b\sqrt{2} \mid a,b$ は整数 $\}$ は環である。
(4) m を法とした $\mathbb{Z}$ の剰余環 $\mathbb{Z}/(m)$ は (その名どおり) 環である。

§2 有理整数環の剰余環

(2.1) 定義 (有理整数環の剰余環) (0 ではない整数) m に対して、m を法とした合同の関係について、$\mathbb{Z}$ の**剰余集合**を考える。つまり、次で定まる**剰余類**

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

のなす集合

$$\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

を考え、これを $\mathbb{Z}/(\boldsymbol{m})$ と書く。$\mathbb{Z}/(m)$ に次の演算が矛盾なく定まる。

$$\overline{a}+\overline{b} = \overline{a+b}, \qquad \overline{a}-\overline{b} = \overline{a-b}, \qquad \overline{a}\overline{b} = \overline{ab}$$

(2.2) 定義 (単元、零因子、整域) 環 R において、

(1) $a \in R$ が乗法の逆元を持つとき、a を**単元**という。ここに、a の逆元とは、$ab=1$ を満たす $b \in R$ である。
(2) 0 ではない $b \in R$ に対して $ab=0$ となるような $a \in R$ を R の**零因子**という。特に 0 は常に零因子である。
(3) 0 以外の零因子を持たない環を**整域**という。

(2.3) 例 (単元、零因子、整域)

(1) 環 $\mathbb{Z}$ の単元は 1 と -1 のみである。
(2) 環 $\mathbb{Z}/(4)$ の単元は $\overline{1}, \overline{3}$ である。
(3) 環 $\mathbb{Z}/(5)$ の単元は $\overline{1}, \ldots, \overline{4}$ である。
(4) 環 $\mathbb{Z}/(4)$ の零因子は $\overline{2}$ である。
(5) 環 $\mathbb{Z}/(5)$ は整域である。
(6) $\mathbb{Z}$ は整域である。

(2.4) **補題 (単元は零因子ではない)** 環 R において、単元は零因子ではない。

(2.5) **問題 ($\mathbb{Z}/(m)$ の零因子、逆元)**

(1) $\mathbb{Z}/(18)$ の零因子をすべて書け。
(2) それ以外の元は単元であるが、それらの逆元をそれぞれ求めよ。

(2.6) **補題 ($\mathbb{Z}$ の剰余環の元が逆元を持つための必要十分条件)** a, m を整数とすると、$\mathbb{Z}/(m)$ において次が成り立つ。
(1) a と m が互いに素ならば $\overline{a}$ は単元である。
(2) a と m が互いに素ではないならば $\overline{a}$ は零因子である。従って特に、$\mathbb{Z}/(m)$ の元は単元か零因子かのいずれか一方である。

Proof. (1) ベズーの方程式 $ax + my = 1$ を満たす x が、$\overline{a}$ の逆元 $\overline{x}$ を与える。

(2) $d = (a, m) > 1$ とおき、$a = a'd$, $m = m'd$ と表す。$m' < m$ であるから、$\overline{m'} \neq \overline{0}$ である。ここで、$\overline{a}\overline{m'} = \overline{a'}\overline{m} = \overline{0}$ なので、$\overline{a}$ は零因子である。 □

(2.7) **問題 (剰余環における逆元)** $\mathbb{Z}/(13)$ において、$\overline{5}$, $\overline{7}$, $\overline{9}$ の逆元を求めよ。

(2.8) **定義 (体)** 0 以外のすべての元が単元であるような環を**体**と呼ぶ。例えば実数全体の集合 $\mathbb{R}$ は体である。また、(2.4) より、体は整域である。

(2.9) **命題 ($\mathbb{Z}/(m)$ が体であるための必要十分条件)** 2 以上の整数 m に対して、$\mathbb{Z}/(m)$ が体であるための必要十分条件は、m が素数であることである。

Proof. (2.6) □

(2.10) **問題 (標数)** 例えば体 $\mathbb{Z}/(p)$ では、1 を繰り返し加えていくと p 回目で始めて 0 になる。このように $m \cdot 1 = 0$ となる最小の m を体の**標数**と言う。また、実数体 $\mathbb{R}$ のように 1 を何回加えても 0 にならない場合は、標数は 0 と定める。体の標数が 0 でないならば、素数であることを示せ。

§3 多項式環

(3.1) **定義 (多項式環)** 環 R の元を係数に持つような x の多項式全体の集合を

$$R[x] = \left\{ a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \;\middle|\; \begin{array}{l} n \geq 0, \\ a_0, \ldots, a_n \in R \end{array} \right\}$$

で表し、R 上の **1 変数多項式環**と呼ぶ。また、$f \in R[x]$ の**次数**を $\deg f$ で表す。

(3.2) **割り算の恒等式** R を環、$f, g \in R[x]$ とする。g の最高次係数が単元 (例えば 1) のとき、

$$f = gp + r \qquad (p, r \in R[x],\ \deg r < \deg g)$$

と一意的に書ける。

(3.3) **定理 (剰余の定理、因数定理)** 環 R 上の多項式 $f \in R[x]$ と、$a \in R$ に対して、

(1) f を $x - a$ で割った余りは、$f(a)$ に等しい。
(2) f が $x - a$ $(a \in R)$ で割り切れるための必要十分条件は $f(a) = 0$ となることである。

$*$ $f(a) = 0$ となることを a は f の**根**であると言う。

(3.4) **問題** $\mathbb{Z}$ 上の多項式環 $\mathbb{Z}[x]$ の単元をすべて言え。また、$\mathbb{R}[x]$ の単元をすべて言え。

§4 多項式の既約性

(4.1) **定義 (既約、可約)** 環 R 上の多項式環 $R[x]$ の多項式 $f \in R[x]$ が**可約**であるとは、f よりも次数の低い 2 つの多項式 $g, h \in R[x]$ によって $f = gh$ と書けることを言う。$f \in R[x]$ が**既約**であるとは、可約ではないことを言う。

(4.2) **例 (既約多項式)** 例えば、$\mathbb{Z}$ 係数の 1 次多項式は無数にあるが、$\mathbb{Z}/(2)$ 係数に持つ 1 次多項式は、x と $x + \bar{1}$ の 2 つしかない。このような有限性を用いて、$\mathbb{Z}/(2)$ 係数の既約多項式を決定できる。

まず、$\mathbb{Z}/(2)$ 係数の 2 次多項式は、

$$x^2, \quad x^2 + \bar{1}, \quad x^2 + x, \quad x^2 + x + \bar{1}$$

の 4 つしかなく、このうち 1 次式 2 つの積になっているのは 3 つであり、残る $x^2 + x + \bar{1}$ が唯一の既約多項式である。

因数定理を利用することもできる。可約な 3 次式は必ず 1 次式の因数を持つ、1 次式は x と $x + \bar{1}$ だけなので、$x = \bar{0}$ か $x = \bar{1}$ を代入すると $\bar{0}$ になる。$\mathbb{Z}/(2)$ 係数の 3 次多項式は、

$$x^3, \quad x^3 + \bar{1}, \quad x^3 + x, \quad x^3 + x + \bar{1}$$
$$x^3 + x^2, \quad x^3 + x^2 + \bar{1}, \quad x^3 + x^2 + x, \quad x^3 + x^2 + x + \bar{1}$$

の 8 つであるが、このうち、$x = \bar{0}$ を代入しても $x = \bar{1}$ を代入しても $\bar{0}$ にならない、$x^3 + x^2 + x + \bar{1}$ と $x^3 + x + x + \bar{1}$ の 2 つが既約な 3 次多項式である。

(4.3) **命題** 整数係数の多項式 $f \in \mathbb{Z}[x]$ が既約ならば、係数を有理数まで広げて $\mathbb{Q}[x]$ の中で考えても既約である。

(4.4) **命題** $f \in \mathbb{Z}[x]$ と、素数 p に対して、係数をすべて $K = \mathbb{Z}/(p)$ で考えた多項式を $\overline{f} \in K[x]$ と書くことにする。$\mathbb{Z}[x]$ の中で $f = gh$ ならば、$K[x]$ の中で、$\overline{f} = \overline{g}\overline{h}$ である。

特に、f の最高次係数が p の倍数でなく、$\overline{f}$ が $K[x]$ で既約ならば、f も既約である。

Proof. 前半は明らか。後半もほぼ明らかだが、係数の条件は $\deg f = \deg \overline{f}$ を保証するためにある。 □

(4.5) **例** 次の整数係数多項式は有理数係数の範囲で考えて既約である。

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

(4.6) **命題 (アイゼンシュタインの既約判定法)** 整数係数の多項式 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ が、ある素数 p に対して次の 2 条件を満たすとき、f は既約である。

(i) $a_0, a_1, \ldots, a_{n-1}$ は p の倍数。

(ii) a_0 は p^2 の倍数ではない。

Proof. (4.4) を用いずに係数の吟味だけで証明することもできるが、(4.4) を用いた証明を与える。

(i) と (ii) を満たすが、可約な多項式 f が存在したと仮定する。$f = gh$ ($\deg g = m$, $\deg h = n - m$, $1 \leq m < n$) とする。係数を p で法をとり $\overline{f} = \overline{g}\overline{h}$ と書くと、(i) より左辺は $\overline{f} = x^n$ であるが、これは $x^m x^{n-m}$ としか分解しないから、$\overline{g} = x^m$, $\overline{h} = x^{n-m}$ である。すると g, h の定数項はともに p の倍数であるから、f の定数項は p^2 の倍数である。これは (ii) に反するから矛盾である。よって f は既約である。 □

(4.7) **例** 次の整数係数多項式は有理数係数の範囲で考えて既約である。

(1) $x^2 - 2$
(2) $x^2 - 3x + 3$
(3) $x^3 + 6x^2 - 4x + 18$
(4) $x^3 + 3x^2 + 5x + 5$
(5) 素数 p に対して、$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ と定めると、既約多項式である。

§5 イデアル

(5.1) **定義 (イデアル)** 環 R の空ではない部分集合 I が R の**イデアル**であるとは、次の 2 条件を満たすことを言う。

(I1) $a, b \in I$ ならば $a + b \in I$
(I2) $x \in R$, $a \in I$ ならば $xa \in I$

(5.2) **例** (1) 環 R の 0 のみからなる部分集合 $\{0\}$ はイデアルである。これを (0) と書く。

(2) 環 R の部分集合 R (自分自身) はイデアルである。(0) と R を R の**自明なイデアル**と呼ぶ。

(3) 環 R の元 a に対して、a の倍元からなる部分集合を

$$(a) = \{ka \mid k \in R\}$$

と書くと、これは R のイデアルである。1 つの元で**生成**されているので**単項イデアル**と呼ぶ。

(4) 環 R の元 $a_1, a_2, \ldots, a_n$ に対して、

$$(a_1, a_2, \ldots, a_n) = \{k_1a_1 + \cdots + k_na_n \mid k_1, \ldots, k_n \in R\}$$

と定めると、R のイデアルになる。これを $a_1, a_2, \ldots, a_n$ で**生成されるイデアル**と呼ぶ。

(5) $a \in R$ に対して、$(a) = R$ であるための必要十分条件は、a が単元であることである。特に、R が体であるための必要十分条件は、R のイデアルは (0) か R しかないことである。

(5.3) **命題** 整域 $\mathbb{Z}$ のイデアルはすべて単項イデアルである。

Proof. 自明なイデアル (0) は単項イデアルだからこれ以外のイデアルを考える。イデアル $I \subset \mathbb{Z}$ に属する最小の正整数を a とする。0 ではない整数 $x \in I$ が a で割り切れないと仮定すると、$x = qa + r$ $(0 < r < a)$ であるが、$r = x - qa \in I$ かつ $r < a$ となり a の取り方に矛盾する。よって、x は a の倍数となり $I = (a)$ である。 □

(5.4) **定義 (PID)** すべてのイデアルが単項イデアルであるような整域を**単項イデアル整域 (PID)** と呼ぶ。

(5.5) **命題 (最大公約数、最小公倍数)** $a, b \in \mathbb{Z}$ の最大公約数が d、最小公倍数が l のとき、

$$(a, b) = (d), \qquad (a) \cap (b) = (l)$$

である。

Proof. $\mathbb{Z}$ は単項イデアル整域だから、$(a, b) = (d')$ なる d' は存在する。$a, b \in (d')$ より、a, b は d' の倍数、つまり、d' は a, b の公約数である。逆に、d'' が a, b の公約数ならば、$sa + tb$ は d'' の倍数になるから、$(d'') \supset (a, b) = (d')$ となり、d'' は d' の約数となる。つまり d' は a, b の最大公約数である。

次に最小公倍数を考える。$(a) \cap (b) = (l')$ なる l' が存在する。$l' \in (a)$ かつ $l' \in (b)$ だから l' は a, b の公倍数である。また、l'' が a, b の公倍数であるとき、$l'' \in (a)$ かつ $l'' \in (b)$ より、$(l'') \subset (a) \cap (b) = (l')$ だから、l'' は l' の倍数である。つまり l'' は a, b の最小公倍数である。 □

(5.6) **定義 (イデアルの和・積)** 環 R のイデアル I, J に対して、

$$I + J = \{a + b \mid a \in I,\ b \in J\},$$
$$IJ = (\{ab \mid a \in I,\ b \in J\} \text{ で生成されるイデアル})$$

と定める。

(5.7) **補題** I, J を環 R のイデアルとすると、

$$I + J \supset I \supset I \cap J \supset IJ$$

である。

Proof. 略 □

(5.8) **例** 環 R の元 a, b について、
(1) $(a) + (b) = (a, b)$
(2) $(a)(b) = (ab)$
(3) $(4) + (6)$ を単項イデアルで書け。
(4) $(4) \cap (6)$ を単項イデアルで書け。
(5) $(4)(6)$ を単項イデアルで書け。

(5.9) **定義 (剰余環)** I を環 R のイデアルとする。$f \in R$ に対して、

$$\overline{f} = \{g \in R \mid f - g \in I\}$$

と定める。そして、

$$R/I = \{\overline{f} \mid f \in R\}$$

と置き、R の I に関する剰余環と呼ぶ。

$\mathbb{Z}/(m)$ の場合と同様に、和・差・積が矛盾なく定義できるので、R/I は環をなす。また、$\overline{f}$ は $f + I$ とも書く。

(5.10) **問題** $R = \mathbb{R}[x]$ を多項式環、$f \in R$ とし、$I = (f)$ とおく。剰余環 $R/I = \mathbb{R}[x]/(f)$ を考える。
(1) $g, h \in R$ に対して、g を f で割った余りと、h を f で割った余りが等しいことと、$\overline{g} = \overline{h}$ であることは、必要十分であることを示せ。

以下では、$f = x^2 + 1$ とする。

(2) R/I のすべての元は、1 次式 $g \in R$ を用いて $\overline{g}$ の形で表せることを示せ。
(3) $\overline{x^2} = \overline{-1}$ を示せ。
(4) $a, b, c, d \in \mathbb{R}$ とする。R/I における $\overline{a + bx}$ と $\overline{c + dx}$ の演算は、複素数 $a + bi$ と $c + di$ の演算と同等であることを示せ (演算が同等になる全単射があるとき、2 つの環を同型であると言う)。

§6 体

(6.1) **定義 (体)** 集合 F が**体**であるとは、次の条件を満たすことをいう。

(F1) F は環である
(F2) 積が交換法則を満たす $(ab = ba)$
(F3) 0 でない元 x に対して、$xy = 1$ なる $y \in F$ (x の逆元) が存在する

(6.2) **定義 (例)**

(1) 有理数全体の集合 $\mathbb{Q}$, 実数全体の集合 $\mathbb{R}$, 複素数全体の集合 $\mathbb{C}$ は体である。

(2) 整数全体の集合 $\mathbb{Z}$, 多項式全体のなす集合 $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ (**多項式環**) は環である。
(3) 分数式全体のなす集合 $\mathbb{Q}(x)$, $\mathbb{R}(x)$, $\mathbb{C}(x)$ (**有理関数体**) は体である。
(4) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ は体である。

(6.3) **問題** 次の問に答えよ。

(1) $a, b \in \mathbb{Q}$ に対し、$a^2 - 2b^2 = 0$ ならば、$a = 0$ かつ $b = 0$ であることを示せ。
(2) $a, b, c, d \in \mathbb{Q}$ に対し、$a + b\sqrt{2} = c + d\sqrt{2}$ ならば $a = c$ かつ $b = d$ であることを示せ。

§7 ベクトル空間の復習

(7.1) **ベクトル空間** 集合 V が体 F 上の**ベクトル空間**であるとは、V 上に和と、F の元によるスカラー倍が定義され、次を満たすことを言うのであった。

(V1) = (R1) 和が結合法則を満たす
(V2) = (R2) 和が交換法則を満たす
(V3) = (R3) 和の単位元 0 が存在する
(V4) = (R4) 和の逆元が存在する
(V5) $1v = v$ (1 倍)
(V6) スカラー倍の結合法則 $k(lv) = (kl)v$ を満たす
(V7) 分配法則を満たす ($(k + l)v = kv + lv$, $k(v + w) = kv + kw$)

(7.2) **例**

(1) $\mathbb{R}^n$ は $\mathbb{R}$ 上のベクトル空間である。
(2) $m \times n$ 行列の全体 $\mathrm{Mat}(m, n; \mathbb{R})$ は $\mathbb{R}$ 上のベクトル空間である。
(3) $\mathbb{Q}[x]$ は $\mathbb{Q}$ 上のベクトル空間である。同様に、体 F 上の多項式環 $F[x]$ は F 上のベクトル空間である。
(4) $\mathbb{Q}$ は $\mathbb{Q}$ 上のベクトル空間である。同様に、体 F は F 上のベクトル空間である。
(5) $\mathbb{R}$ は $\mathbb{Q}$ 上のベクトル空間であるが、$\mathbb{Q}$ は $\mathbb{R}$ 上のベクトル空間ではない。
(6) 体 E の**部分体** F があるとき、E は F 上のベクトル空間である。

(7.3) **生成する部分空間** F 上のベクトル空間 V の元 $v_1, v_2, \ldots, v_k$ が**生成する部分空間**とは、これらの F 上の **1 次結合**全体のなす集合、つまり、

$$\{a_1 v_1 + \cdots + a_k v_k \mid a_j \in F\}$$

で定まる集合のことである。

(7.4) **1 次独立、1 次従属、基底、次元** F 上のベクトル空間 V の元 $v_1, v_2, \ldots, v_k$ が **1 次独立**であるとは、$a_j \in F$ により、$a_1 v_1 + \cdots + a_k v_k = 0$ と書けているならば、$a_j = 0$ $(j = 1, 2, \ldots, k)$ となることである。言い換えると、$a_j, b_j \in F$ により、

$$a_1 v_1 + \cdots + a_k v_k = b_1 v_1 + \cdots + b_k v_k$$

ならば、$a_j = b_j$ $(j = 1, 2, \ldots, k)$ と**係数比較**ができることを言う。

1 次独立ではないことを **1 次従属**と言い、V を生成する 1 次独立な集合を V の**基底**と呼ぶ。基底の濃度は基底の取り方によらないことが知られている。この濃度を V の F 上の**次元**と呼び、$\dim_F V$ あるいは単に $\dim V$ と書く。

(7.5) **例**

(1) $\mathbb{R}^n$ の $\mathbb{R}$ 上の基底として、標準基底からなる $\{e_1, e_2, \ldots, e_n\}$ が取れる。$\mathbb{R}^n$ は $\mathbb{R}$ 上 n 次元である。
(2) $\mathbb{C}$ の $\mathbb{R}$ 上の基底として $\{1, i\}$ が取れる。$\mathbb{C}$ は $\mathbb{R}$ 上 2 次元である。
(3) $\mathbb{Q}$ は $\mathbb{Q}$ 上の基底として $\{1\}$ が取れるので、$\mathbb{Q}$ 上 1 次元である。
(4) $\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 上の基底として $\{1, \sqrt{2}\}$ が取れるので、$\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$ である。
(5) $\mathbb{R}[x]$ の高々 2 次式のなす集合 $\mathbb{R}[x]_{\leq 2}$ はベクトル空間であり、$\{1, x, x^2\}$ が $\mathbb{R}$ 上の基底としてとれるから、$\dim_{\mathbb{R}} \mathbb{R}[x]_{\leq 2} = 3$ である。
(6) $\mathbb{Q}[x]$ の $\mathbb{Q}$ 上の基底として、無限集合 $\{1, x, x^2, \ldots\}$ が取れるから、$\mathbb{Q}[x]$ は $\mathbb{Q}$ 上無限次元である。

§8 体の拡大

(8.1) **定義 (拡大体)** (同じ演算に関する) 2 つの体 $E \supset F$ があるとき、F は E の**部分体**、E は F の**拡大体**という。このとき、体の拡大 E/F があるとも書く。

(8.2) **定義 (拡大次数)** 体の拡大 $E \supset F$ があるとき, E の F 上のベクトル空間としての次元を, E の F 上の**拡大次数**といい, $[\boldsymbol{E : F}]$ と書く. このとき, E は F の $\boldsymbol{n}$ **次拡大**などと言う.

言い換えると、ある n 個の元 $e_1, e_2, \ldots, e_n \in E$ があって、任意の $x \in E$ が、$x = a_1 e_1 + a_2 e_2 + \cdots + a_n e_n$ $(a_j \in F)$ と一意的に書けるとき、E は F の n 次拡大である。

(8.3) **例 (拡大体)**

(1) $\mathbb{C} \supset \mathbb{R}$ は 2 次拡大である。
(2) $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ は 2 次拡大である。
(3) $\mathbb{Q} \supset \mathbb{Q}$ は 1 次拡大である。
(4) $\mathbb{R} \supset \mathbb{Q}$ は無限次拡大である。

(8.4) **定義 (単項拡大)** 体の拡大 $E \supset F$ があるとき、$\alpha \in E$ と F を含むような E の最小の部分体を $\boldsymbol{F(\alpha)}$ と書き、F の α による**単項拡大**と言う。分母が 0 にならないような α の分数式全体のなす集合が、$F(\alpha)$ に他ならない。

(8.5) **例 (単項拡大)**

(1) 既に見た $\mathbb{Q}(\sqrt{2})$ は、$\mathbb{Q}$ 上の $\sqrt{2}$ による単項拡大である。
(2) $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ である。
(3) $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ である。

(8.6) **定義 (最小多項式、代数拡大)** 体の拡大 $E \supset F$ があるとする。

(1) $\alpha \in E$ に対して、$f(\alpha) = 0$ を満たすような 0 ではない多項式 $f(x) \in F[x]$ が存在するとき、α は F 上**代数的**であるという。また、そのような多項式が存在しないとき α は F 上**超越的**であるという。
(2) $\alpha \in E$ のとき、$f(x) \in F[x]$ が α の F 上の**最小多項式**であるとは、f が次の条件を満たすことを言う。

(M1) $f(x) \neq 0$
(M2) $f(\alpha) = 0$
(M3) $f(x)$ はモニック (最高次の係数が 1 ということ)
(M4) 上の 3 条件を満たす多項式のうち次数が最小

(3) すべての E の元が F 上代数的であるとき、$E \supset F$ を**代数拡大**という。

(8.7) **例 (最小多項式、代数拡大、超越数)**

(1) $\mathbb{R} \supset \mathbb{Q}$ は代数拡大ではないことが知られている。例えば、円周率 $\pi = 3.1415\cdots$ や自然対数の底 $e = 2.71828\cdots$ は、有理数係数多項式によるどんな n 次方程式の解にもならないことが知られている。その証明はここではしない。そのような実数を**超越数**という。
(2) 体の拡大 $\mathbb{R} \supset \mathbb{Q}$ に対して、$\sqrt{2} \in \mathbb{R}$ の最小多項式は $f(x) = x^2 - 2$ である。なぜなら、(i) $\sqrt{2}$ は $x^2 - 2 = 0$ の解であり、(ii) $f(x)$ はモニックであり、(iii) 仮に 1 次の最小多項式があれば、$x - \sqrt{2}$ にならざるを得ないがこれは有理数係数ではないから、$f(x)$ は最小次数であるからである。
(3) 体の拡大 $\mathbb{C} \supset \mathbb{R}$ に対して、虚数単位 $i \in \mathbb{C}$ の最小多項式は $f(x) = x^2+1$ である。

(8.8) **命題 (有限次拡大は代数拡大)** 有限次拡大は代数拡大である。したがって、特に、$\mathbb{R} \supset \mathbb{Q}$ が無限次の拡大であることがわかる。

Proof. 超越的な α があると、α^i たちが 1 次独立になり、有限次拡大ではなくなる。 □

(8.9) **命題 (最小多項式と既約性)** $E \supset F$ を体の拡大とする。$\alpha \in E$, $f \in F[x]$ のとき次は同値である。

(i) f は α の F 上の最小多項式である。
(ii) f は α を根に持ち、f はモニックであり、f は F 上既約多項式である。

Proof. ($\Downarrow$) $f = gh$ ならば g か h が α を根に持ち、$\deg f$ の最小性に矛盾。($\Uparrow$) f を最小多項式 g で割った余り R は α を根に持ち、$\deg g$ の最小性から $R = 0$. よって g は f を割るが f が既約なので $f = g$。 □

(8.10) **例 (最小多項式)**

(1) $\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式は $x^3 - 2$ である。
(2) $\sqrt{2} + \sqrt{3}$ の $\mathbb{Q}$ 上の最小多項式は $x^4 - 10x^2 + 1$ である。ただし、4 次が最小の次数であることは、今はまだわからない。

(8.11) **定理 (元が代数的であるための条件)** 体の拡大 $E \supset F$ と、$\alpha \in E$ があるとき次の条件は同値である。

(i) α は F 上代数的である。
(ii) $F[\alpha]$ は体である。
(iii) $F[\alpha] = F(\alpha)$.

ただし、$F(\alpha)$ は F の α による単項拡大 (α の分数式全体のなす体) であり、$F[\alpha]$ は F の元を係数に持つ α の多項式全体のなす環である。

Proof. [(ii)$\Leftrightarrow$(iii)] $F(\alpha)$ の最小性より従う。

[(ii)$\Rightarrow$(i)] 背理法で示す。α が超越的だと仮定する。$f(x) = x$ と置くと $f(\alpha) = \alpha$ となる。$F[\alpha]$ が体なので $g(\alpha) = \alpha^{-1}$ となる $g(x)$ が存在する。

$f(\alpha)g(\alpha) = \alpha\alpha^{-1} = 1$ だから、$fg - 1$ は α を根に持ち、超越性より 0。$fg = 1$ の次数を比較して矛盾。

[(i)⇒(ii)] $\alpha \in E$ が F 上代数的とし、$f(x) \in F[x]$ を α の最小多項式とする。$f(x)$ は既約であったことに注意する。

任意の多項式 $g(x) \in F[x]$ であって、$g(\alpha) \neq 0$ なるものをとる。仮に g が f で割り切れるとすると、$g(\alpha) = 0$ となってしまうので、g は f で割り切れず、f の既約性より g と f は互いに素である。よって、多項式 $p(x), q(x) \in f[x]$ が存在してベズーの等式

$$g(x)p(x) + f(x)q(x) = 1$$

が成立する。これに $x = \alpha$ を代入すると、$f(\alpha) = 0$ に注意すれば $g(\alpha)p(\alpha) = 1$ となり、$g(\alpha)$ に逆元 $p(\alpha) \in F[\alpha]$ が存在することがわかる。したがって、$F[\alpha]$ の 0 でない任意の元には逆元が存在するので体である。 □

(8.12) **例 (α による単項拡大の元を α の多項式で表す)**

(1) 虚数単位 $i = \sqrt{-1}$ は $\mathbb{R}$ 上代数的であり、実数係数の i の分数式は、実数係数の i の多項式に書き換えられる。
(2) $\dfrac{1}{1 + \sqrt[3]{2} + \sqrt[3]{4}}$ を $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ $(a, b, c \in \mathbb{Q})$ の形に表せ。
(3) $\alpha = \sqrt{2} + \sqrt{3}$ とする。$\sqrt{2} - \sqrt{3}$ を α の $\mathbb{Q}$ 係数多項式で書け。

(8.13) **命題 (単項拡大の拡大次数)** 体の拡大 $E \supset F$ と、F 上代数的な元 $\alpha \in E$ があり、α の最小多項式の次数を n とする。このとき次が成り立つ。

(1) $F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\}$
(2) $[F(\alpha) : F] = n$

Proof. (1) $F(\alpha) = F[\alpha]$ だから、$F[x]$ の元を最小多項式で割った余りを考えればよい。(2) $1, \alpha, \ldots, \alpha^{n-1}$ の 1 次独立性を言えばよい。 □

(8.14) **問題 (単項拡大の拡大次数と最小多項式の次数)** $E \supset F$ を体の拡大、$f \in F[x]$ を既約多項式とし、$\alpha \in E$ を f の根とする。$[F(\alpha) : F] = \deg f$ であることを示せ。

(8.15) **例 (拡大次数と最小多項式の次数)**

(1) 単項拡大 $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ は、(8.3) 例 (1) により 2 次拡大であった。また、$\sqrt{-1}$ の最小多項式は、(8.7) 例 (3) により、2 次式 $x^2 + 1$ であり、拡大次数と最小多項式の次数が一致している。
(2) (8.10) (1) より、単項拡大 $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ の拡大次数は 3 である。

(8.16) **定理 (拡大次数の連鎖律)** 3 つの体による 2 つの有限次拡大 $L \supset E \supset F$ があるとき、

$$[L : F] = [L : E][E : F].$$

Proof. E の F 上の基底を e_i とし、L の E 上の基底を l_j とすると、L の元が $e_i l_j$ の 1 次結合で書けることと、これらが F 上 1 次独立であることが言える。 □

(8.17) **例 (最小多項式を求める)** $\sqrt{2}+\sqrt{5}$ の $\mathbb{Q}$ 上の最小多項式を求めよ.

(解) $\alpha = \sqrt{2}+\sqrt{5}$ とおく。まず、$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2},\sqrt{5})$ を証明する。ただし、$F(a,b,\dots)$ は、体 F と、元 $a,b,\dots$ を含む最小の体であり、それは、F を係数とする $a,b,\dots$ の分数式全体の集合である。明らかに、$\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2},\sqrt{5})$ である。また、$3/\alpha = \sqrt{5}-\sqrt{2}$ だから、

$$\frac{1}{2}\left(\alpha + \frac{3}{\alpha}\right) = \frac{1}{2}(\sqrt{2}+\sqrt{5}+\sqrt{5}-\sqrt{2}) = \sqrt{5}$$

となるので、$\sqrt{5} \in \mathbb{Q}(\alpha)$ である。したがって、$\alpha - \sqrt{5} = \sqrt{2}$ も $\mathbb{Q}(\alpha)$ に属する。よって、$\mathbb{Q}(\alpha) \supset \mathbb{Q}(\sqrt{2},\sqrt{5})$ であり、以上より、$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2},\sqrt{5})$ である。

次に、$[\mathbb{Q}(\sqrt{2}),\sqrt{5}) : \mathbb{Q}(\sqrt{2})] = 2$, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q})] = 2$ であるから、(8.16) より、$[\mathbb{Q}(\alpha : \mathbb{Q}] = 4$ である。したがって、$\alpha = \sqrt{2}+\sqrt{5}$ の最小多項式の次数は 4 である。

$\alpha = \sqrt{2}+\sqrt{5}$ の両辺を 2 乗して、$\alpha^2 = 7+2\sqrt{10}$. 7 を移項してから両辺を 2 乗すると、$\alpha^4 - 14\alpha + 49 = 40$. よって、$\alpha^4 - 14\alpha + 9 = 0$. したがって、最小多項式は $x^4 - 14x + 9$ である。

§9 作図問題

(9.1) **定義 (作図可能性)** 平面上の**作図可能な点**を次のように定める。

(1) $\mathrm{O}(0,0)$ と $\mathrm{A}(0,1)$ は作図可能な点とする。
(2) 既にわかっている作図可能な点のみを用いて、異なる 2 点間に直線を引く、あるいは、ある点を中心としある 2 点間の距離を半径とする円を書き、得られた 2 円、2 直線あるいは円と直線の交点は作図可能であるとする。

つまり、長さ 1 の線分が与えられたときに、定規とコンパスのみを用いた有限回の手順による作図で得られる点である。

また、作図可能な点の x 座標または y 座標となっている実数を**作図可能な実数**と呼ぶ。ある複素数が**作図可能**であるとは、平面を複素数平面と思ったときに、その複素数に対応する点が作図可能であることを言う。

(9.2) **例** 自由に直線を引いたり、円を描いたりできるわけではないので、普段考える作図よりも制約が強いことには注意が必要だが、次のような作図は可能である。

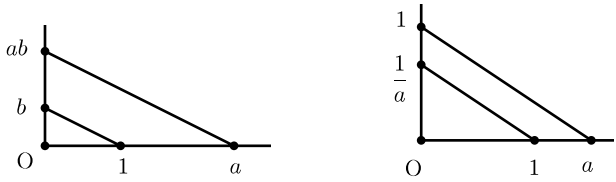
(1) $(n, 0)$ $(n \in \mathbb{Z})$ は作図可能である。従って、コンパスを用いるとき、いくらでも大きい半径がとれる。
(2) 直線 l と、その直線上にない点 A が与えられたとき、l に平行で A を通る直線や、l に垂直で A を通る直線を書くことができる。
(3) 直線 l と、l 上の点 A が与えられたとき、l に垂直で A を通る直線を書くことができる。
(4) 与えられた線分を n 等分できる。
(5) (m, n) $(m, n \in \mathbb{Z})$ は作図可能である。従って、(a, b) $(a, b \in \mathbb{Q})$ は作図可能である。
(6) 有理数は作図可能である。

(9.3) **補題** 次の 3 条件は同値である。

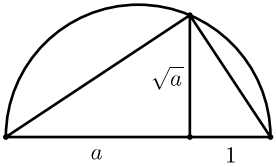
(i) a は作図可能な実数である。
(ii) $(a, 0)$ は作図可能な点である。
(iii) $(0, a)$ は作図可能な点である。

(9.4) **命題 (作図可能な数のなす体)** 作図可能な数は体をなす。

Proof. 和と差で閉じていることは容易。積と商は図を見よ。 □



(9.5) **命題 (平方根の作図)** 正の実数 a が作図可能ならば、$\sqrt{a}$ も作図可能である。



(9.6) **命題** 次は同値である。
(1) α は作図可能な実数である。
(2) $\mathbb{Q}$ から 2 次拡大の反復で得られるある拡大体 F があり、$\alpha \in F$ である。

Proof. [(2)⇒(1)] $\mathbb{S}$ は平方根で閉じているから、作図可能な数を係数に持つ 2 次方程式 $ax^2 + bx + c = 0$ の実数解は作図可能である。従って、$\mathbb{Q}$ から出発して 2 次拡大を反復して得られる拡大体 F があるとき ($F \subset \mathbb{R}$)、F の元は作図可能である。

[(1)⇒(2)] 作図により n 個の点 $\mathrm{P}_1(x_1, y_1)$, $\mathrm{P}_2(x_2, y_2)$, …, $\mathrm{P}_n(x_n, y_n)$ が与えられたとき、$\mathbb{Q}$ の拡大体 F_n を

$$F_n = \mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$$

で定める。

さて、上の n 個の点のうちの 2 点を結ぶ直線の方程式 $ax+by=c$ を考えると、a, b, c が F_n の元になるように書ける。また、1 点を中心とし、ある 2 点間の距離を半径とする円の方程式 $(x-a)^2+(y-b)^2=r^2$ を考えると、a, b, r^2 が F_n の元になるように書ける。

こうして得られた円や直線の交点 P_{n+1} を作成すると、その x 座標と y 座標は連立方程式の解として得られるが、

2 **直線の交点のとき**: その解は F_n に属する (F_n 上の 1 次方程式の解だから)。

円と直線の交点のとき: その解は F_n の高々 2 次拡大体に属する (F_n 上の 2 次方程式の解だから)。

2 **円の交点のとき**: その解は F_n の高々 2 次拡大体に属する。

□

(9.7) **定理 (作図可能性)** 実数 α が作図可能であることは、$\mathbb{Q}$ から出発して 2 次拡大を反復して $\mathbb{Q}(\alpha)$ が得られることと必要十分である。

Proof. 十分性は直前で証明済み。必要性を証明する。$\alpha \in \mathbb{R}$ を作図可能とすると (2) により、2 次拡大の列

$$F_n \supset \cdots \supset F_0 = \mathbb{Q} \qquad (\alpha \in F_n)$$

が存在する。$F_n \supset \mathbb{Q}(\alpha)$ だから、この列の $\mathbb{Q}(\alpha)$ との共通部分をとると、

$$\mathbb{Q}(\alpha) = F'_n \supset \cdots \supset F'_0 = \mathbb{Q}$$

という列が得られるが、$F'_{i+1}/F'_i \to F_{i+1}/F_i$ という自然な単射があるから、隣接する体の拡大次数は 1 か 2 である。このうち拡大次数が 2 になるところだけ取り出して列を作ればよい。 □

(9.8) **定理 (数が作図可能であるための必要条件)** 実数 α が作図可能であるならば、$[\mathbb{Q}(\alpha):\mathbb{Q}]$ が 2 のベキである。

(9.9) **注意** 上の定理 (9.8) の逆は成立しない。以下に反例をあげる。

$\alpha \in \mathbb{R}$ を $\mathbb{Q}$ 上の既約多項式 x^4+x+1 の 1 つの根とすると、$[\mathbb{Q}(\alpha):\mathbb{Q}]=4$ である。$\mathbb{Q}(\alpha) \supset F \supset \mathbb{Q}$ が 2 次拡大の列となるような中間の体 F が存在しないことを背理法で示す。そこで、そのような体 F が存在したと仮定する。α は F 上 2 次拡大だから、F 上の多項式 x^2+sx+t $(s,t \in F)$ の根である。すると x^4+x+1 はこの多項式の倍元になるから、$x^4+x+1=(x^2+sx+t)(x^2+s'x+t')$ $(s',t' \in F)$ と表せるが、3 次と 0 次の係数を比較すると、$s'=-s$, $t'=t^{-1}$ である。$x^4+x+1=(x^2+sx+t)(x^2-sx+t^{-1})$ の両辺の係数を比較して、

$$\begin{cases} t+t^{-1}-s^2=0 \\ st^{-1}+st=1 \end{cases}$$

を得る。これより t を消去すると、$s^6-4s^4-1=0$ を得る。

さて、ここで、$s^2 \in F$ を考えると、s^2 は $\mathbb{Q}$ 上の多項式 x^3-4x^2-1 の根であり、この多項式は $\mathbb{Q}$ 上既約である。(なぜならば、$\mathbb{Q}$ 上因数分解できたとすると $\mathbb{Z}$ 係数になるので、必ず現れる 1 次の因子は $x \pm 1$ でなくてはならないが、∓ 1 は根ではない。) 従って、F の元 s^2 の $\mathbb{Q}$ 上の最小多項式が 3 次であり、$[\mathbb{Q}(s^2):\mathbb{Q}]=3$ は $F \supset \mathbb{Q}(s^2) \supset \mathbb{Q}$ に矛盾する。

(9.10) **例**

(1) 正 5 角形 (をなす 5 点) が作図できることと、実数 $\cos 72^\circ = (\sqrt{5}-1)/4$

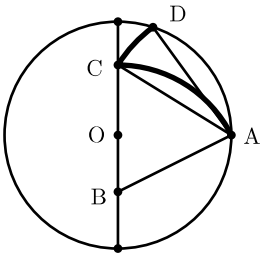
が作図可能であることは同値である。この値は $\mathbb{Q}$ の 2 次拡大 (例えば $\mathbb{Q}(\sqrt{5})$) に属するから、正 5 角形は作図可能である。

(2) 2 の 3 乗根は作図可能ではない。なぜなら $\sqrt[3]{2}$ の最小多項式は 3 次だからである。したがって、体積 2 の立方体の 1 辺の長さは作図可能ではない。

(3) 40° は作図可能ではない。つまり、120° の 3 等分や、正 9 角形の作図も可能ではない。なぜなら、$\alpha = \cos 40^\circ$ とすると、$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ より、$8\alpha^3 - 6\alpha + 1 = 0$ である。$8x^3 - 6x + 1$ は既約である (なぜなら、x を $y/2$ に取り換えた $y^3 - 3y + 1$ は、$\mathrm{mod}\,2$ すると $y^3 + y + 1$ と既約であるから。$\leftarrow f \in \mathbb{Z}[x]$ を $\mathrm{mod}\,p$ して次数が落ちず既約なら元も既約) から、α の最小多項式である。$\mathbb{Q}(\alpha) \subset \mathbb{Q}$ が 3 次拡大だから α は作図可能ではない。

(9.11) **事実 (正多角形の作図可能性)** 正 n 角形が作図可能であるための必要十分条件は、オイラーの関数 $\phi(n)$ が 2 のベキであることである (§10 で詳しく見る)。

(9.12) **問題 (正 5 角形の作図)** 正 5 角形を定規とコンパスで作図せよ.



§10 正多角形の作図可能性

(10.1) 命題 (正多角形の作図可能性と体の拡大) n を 3 以上の整数、$\theta = 360^\circ/n$ とし、$\zeta = \cos\theta + i\sin\theta$ と置く。単位円周に内接する正 n 角形の n 頂点が作図可能であるための必要十分条件は、

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_m = \mathbb{Q}(\zeta) \tag{1}$$

となる 2 次拡大の列が存在することである。

Proof. まず、正 n 角形が作図可能であることと、$\cos\theta$ が作図可能であることは同等であることに注意する。

$\zeta + \zeta^{-1} = 2\cos\theta$ だから、$\cos\theta \in \mathbb{Q}(\zeta)$ であり、体の包含関係 $\mathbb{Q}(\zeta) \supset \mathbb{Q}(\cos\theta)$ が得られる。ζ は虚数だから、両者は一致しない。$\mathbb{Q}(\cos\theta)$ 上の z の 2 次式

$$(z-\zeta)(z-\zeta^{-1}) = z^2 - (\zeta+\zeta^{-1})z + 1 = z^2 - 2\cos\theta\cdot z + 1$$

は ζ を根に持つから、$\mathbb{Q}(\zeta) \supset \mathbb{Q}(\cos\theta)$ は高々 2 次拡大であり、一致しないので 2 次拡大である。

[必要性] $\cos\theta$ が作図可能であるとすると、

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_l = \mathbb{Q}(\cos\theta)$$

なる 2 次拡大の列があるが、これに 2 次拡大 $\mathbb{Q}(\zeta) \supset \mathbb{Q}(\cos\theta)$ を継ぎ足せば所望の列 (1) が得られる。

[十分性] 列 (1) が存在するとすると、この列の体を一斉に $\mathbb{Q}(\cos\theta)$ と共通部分を取ると、

$$\mathbb{Q} = E_0 \subset E_1 \subset \cdots \subset E_m = \mathbb{Q}(\cos\theta) \qquad (E_i = F_i \cap \mathbb{Q}(\cos\theta))$$

という列が得られるが、隣接する拡大は 1 次または 2 次拡大である。1 次拡大の部分は省くことにすると、$\mathbb{Q}$ から $\mathbb{Q}(\cos\theta)$ への 2 次拡大の列が得られるから、$\cos\theta$ は作図可能である。 □

(10.2) **定義 (原始 n 乗根)** n を正整数とする。複素数 ξ が 1 の**原始 n 乗根**であるとは、$\xi^n = 1$ かつ $\xi^k \neq 1$ $(1 \leq k \leq n-1)$ なるときを言う。

(10.3) **補題 (原始 n 乗根であるための条件)** n を正整数、$\theta = 360^\circ/n$ とし、$\zeta = \cos\theta + i\sin\theta$ と置く。

(1) ζ は原始 n 乗根である。
(2) 正整数 k に対して、ζ^k が原始 n 乗根であるための必要十分条件は、$(k, n) = 1$ となることである。特に、相異なる 1 の原始 n 乗根は $\phi(n)$ 個ある。

Proof. (1) は明らか。(2) を示す。ζ^k が l 乗して初めて 1 になるとすると、$kl = n\alpha$ と表せ、l の最小性から $(l, \alpha) = 1$ となる。$\beta = (n, k)$ とおき、$n = n'\beta$, $k = k'\beta$ とすると、$(n', k') = 1$ である。$kl = n\alpha$ より、$k'l = n'\alpha$ となり、$(l, \alpha) = (n', k') = 1$ より $n = l\beta$ である。したがって、$\beta = (n, k) = 1$ であることと、$l = n$ であることは同値である。 □

(10.4) **定義 (円周等分多項式)** 正整数 n に対して、多項式 $\Phi_n(x)$ を

$$\Phi_n(x) = \prod_{\xi \text{ は } 1 \text{ の原始 } n \text{ 乗根}} (x - \xi)$$

と定め、**円周等分多項式**と呼ぶ。特に次数は $\phi(n)$ である。

(10.5) **例 (円周等分多項式)**

$$\Phi_1(x) = x - 1, \qquad \Phi_2(x) = x + 1,$$
$$\Phi_3(x) = x^2 + x + 1, \qquad \Phi_4(x) = x^2 + 1,$$
$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1, \qquad \Phi_6(x) = x^2 - x + 1,$$
$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \qquad \Phi_8(x) = x^4 + 1.$$

(10.6) **命題 ($x^n - 1$ の因数分解)** n を正整数とするとき、

$$x^n - 1 = \prod_{d \text{ は } n \text{ の約数}} \Phi_d(x)$$

である。したがって特に、

$$n = \sum_{d \text{ は } n \text{ の約数}} \phi(d)$$

である。

Proof. $d|n$ のとき、すべての d 乗根は n 乗根である。反対に n 乗根はある原始 d 乗根であり、そのとき $d|n$ である ($\xi^n = 1$ が $\xi^d = 1$ ならば n を d で割って余り 0)。 □

(10.7) **定理 (円周等分多項式の係数の整数性)** $\Phi_n(x)$ の係数は整数であり、モニックである。

Proof. Monic 多項式で割っても係数は整数のままだから、帰納法により、$x^n - 1$ を monic いくつかで割った Φ_n も整数係数。 □

(10.8) **補題** p を素数とする。

(1) $1 \leq k \leq p-1$ のとき、$\binom{p}{k}$ は p の倍数である。
(2) $g(x) \in (\mathbb{Z}/(p))[x]$ に対して、$g(x)^p = g(x^p)$ である。

Proof. (2) は、(1) とフェルマーの小定理より。 □

(10.9) **定理 (円周等分多項式の既約性)** $\Phi_n(x)$ は $\mathbb{Q}$ 上既約である。

Proof. まず、$\theta = 360^\circ/n$ とし、$\zeta = \cos\theta + i\sin\theta$ と置くと、$\Phi_n(x)$ の根は ζ^k $(0 \leq k \leq n-1)$ かつ $(k,n) = 1$ なるものたちであった。また、$\mathbb{Q}$ 上の既約性と $\mathbb{Z}$ 上の既約性は同等だから、$\Phi_n(x)$ の $\mathbb{Q}$ 上の因数は、整数係数多項式としてよい。

さて、$\Phi_n(x)$ が既約ではないと仮定し、$\Phi_n(x)$ の既約な因数のうち ζ を根に持つものを $f(x) \in \mathbb{Z}[x]$ とする。原始 n 乗根 ζ^k を、f の根ではないもののうち、k が最小の正整数であるものとする。ζ^k の最小多項式を $g(x) \in \mathbb{Z}[x]$ とする。f と g はともに既約であり、共通ではない根を持つから互いに素であり、さらに、ともに $x^n - 1$ の因数であるから、$f(x)g(x)$ も $x^n - 1$ の因数である。

ζ は f の根だから $k \geq 2$ であり、k の素因数 p が存在する ($(k,n) = 1$ より $(p,n) = 1$ であることを後で用いる)。$G(x) = g(x^p)$ と置くと、$\zeta^{k/p}$ は G の根であり、k の最小性より f の根でもあるから、f の既約性より $G(x) = f(x)h(x)$ と書ける $(h(x) \in \mathbb{Z}[x])$。多項式の係数を $\mathbb{Z}/(p)$ に写したものを $\overline{f}$ のように書くことにすると、

$$\overline{g}(x)^p = \overline{g}(x^p) = \overline{G}(x) = \overline{f}(x)\overline{h}(x)$$

となり、$(\mathbb{Z}/(p))[x]$ において、$\overline{g}$ と $\overline{f}$ は共通根を持つことがわかる。

したがって、$(\mathbb{Z}/(p))[x]$ において、x^n-1 は重根を持つが、$(p,n)=1$ より、x^n-1 とその微分は共通根を持たないから矛盾である。よって、$\Phi_n(x)$ は既約である。 □

(10.10) **系 (正 n 角形の作図不可能性)** 3 以上の整数 n に対し、$\phi(n)$ が 2 のベキでないならば、正 n 角形は作図可能ではない。

(10.11) **事実 (正 n 角形の作図可能性)** 3 以上の整数 n に対し、$\phi(n)$ が 2 のベキならば、正 n 角形は作図可能である。

§11 演習問題

(11.1) **問題** 環の定義を書け。また、体の定義を書け。

(11.2) **問題** 次の集合は、環か否か。環でない場合は、どうして環ではないか答えよ。

(1) 正の整数全体
(2) 0 以上の整数全体
(3) 偶数全体
(4) 奇数全体
(5) 整数全体 $\mathbb{Z}$
(6) 有理数全体 $\mathbb{Q}$
(7) 実数全体 $\mathbb{R}$
(8) 複素数全体 $\mathbb{C}$
(9) 整数係数の多項式全体 $\mathbb{Z}[x]$
(10) 有理数係数の多項式全体 $\mathbb{Q}[x]$
(11) 実数係数の多項式全体 $\mathbb{R}[x]$
(12) 複素数係数の多項式全体 $\mathbb{C}[x]$

(11.3) **問題** 整数 m に対して、m を法とする剰余環 $\mathbb{Z}/(m)$ は、剰余類 $\overline{0},\overline{1},\ldots,\overline{m-1}$ からなる集合であった。剰余類 $\overline{k}$ も、集合として定めてい

たが、その定義を言え。

(11.4) **問題** 単元の定義を言え。また、次の環における単元をすべて書け
(a) $\mathbb{Z}$ (b) $\mathbb{Z}/(2)$ (c) $\mathbb{Z}/(3)$ (d) $\mathbb{Z}/(6)$ (e) $\mathbb{Z}[x]$ (f) $\mathbb{Q}$

(11.5) **問題** 零因子の定義を言え。また、次の環における零因子をすべて書け
(a) $\mathbb{Z}$ (b) $\mathbb{Z}/(2)$ (c) $\mathbb{Z}/(3)$ (d) $\mathbb{Z}/(6)$ (e) $\mathbb{Z}[x]$ (f) $\mathbb{Q}$

(11.6) **問題** 次の問に答えよ。

(1) 整域の定義を言え。
(2) 正整数 m に対して、剰余環 $\mathbb{Z}/(m)$ が整域であるための必要十分条件を言え。
(3) 次のうち整域をすべて言え。
(a) $\mathbb{Z}$ (b) $\mathbb{Z}/(2)$ (c) $\mathbb{Z}/(3)$ (d) $\mathbb{Z}/(6)$ (e) $\mathbb{Z}[x]$ (f) $\mathbb{Q}$

(11.7) **問題** 剰余環 $\mathbb{Z}/(11)$ において、$\overline{3}$ の逆元を求めよ。

(11.8) **問題** 次の多項式は整数係数の範囲で既約か否か。また、有理数係数ではどうか。

(1) $x^2 + 3x + 1$
(2) $x^2 + 3x + 3$
(3) $x^2 + 3x + 9$

(4) x^3+3x^2+6x+1
(5) x^3+3x^2-1
(6) x^4+3x^3+3

(11.9) **問題** 次の集合は、体であるか、または、体ではないが環であるか答えよ。

(1) 正の整数全体
(2) 0 以上の整数全体
(3) 偶数全体
(4) 奇数全体
(5) 整数全体 $\mathbb{Z}$
(6) 有理数全体 $\mathbb{Q}$
(7) 実数全体 $\mathbb{R}$
(8) 複素数全体 $\mathbb{C}$
(9) 整数係数の多項式全体 $\mathbb{Z}[x]$
(10) 有理数係数の多項式全体 $\mathbb{Q}[x]$
(11) 実数係数の多項式全体 $\mathbb{R}[x]$
(12) 複素数係数の多項式全体 $\mathbb{C}[x]$
(13) 整数係数の分数式全体 $\mathbb{Z}(x)$
(14) 実数係数の分数式全体 $\mathbb{R}(x)$

(11.10) **問題** 次の集合は、ベクトル空間かどうか答えよ。ベクトル空間になる場合は、スカラーとなりうる体の例もあげよ。

(1) 整数全体 $\mathbb{Z}$
(2) 有理数全体 $\mathbb{Q}$
(3) 複素数全体 $\mathbb{C}$
(4) 整数係数の多項式全体 $\mathbb{Z}[x]$
(5) 実数係数の多項式全体 $\mathbb{R}[x]$
(6) 整数係数の n 次正方行列全体 $\mathrm{Mat}(n,n;\mathbb{Z})$
(7) 有理数係数の $m\times n$ 行列全体 $\mathrm{Mat}(m,n;\mathbb{Q})$

(11.11) **問題** 次の問に答えよ。

(1) 体の拡大次数の定義を言え。
(2) 体の単項拡大の定義を言え。

(3) 体の拡大 $E \supset F$ があるとき、$\alpha \in E$ の F 上の最小多項式の定義を言え。
(4) 体の代数拡大の定義を言え。
(5) 2 次の代数拡大の例を 1 つあげよ。

(11.12) **問題** 体の拡大 $\mathbb{C} \supset \mathbb{R}$ について答えよ。

(1) 拡大次数を答えよ。
(2) $\mathbb{C}$ の $\mathbb{R}$ 上の基底を 1 組答えよ。
(3) $\{1+i, 1-i\}$ が $\mathbb{C}$ の $\mathbb{R}$ 上の基底であることを証明せよ。

(11.13) **問題** $\mathbb{Q}$ 上 1 次独立であるような 2 つの無理数をあげよ。$\mathbb{Q}$ 上 1 次従属であるような 2 つの無理数をあげよ。

(11.14) **問題** 次の数は $\mathbb{Q}$ 上代数的か否か。代数的ならば最小多項式も答えよ。
(1) $\sqrt{3}$ (2) $\sqrt{3}+1$ (3) $\dfrac{1}{\sqrt{3}}$

(11.15) **問題** 2 次の単項拡大 $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ に対して、$\mathbb{Q}(\sqrt{2})$ の任意の元は、$a+b\sqrt{2}$ $(a, b \in \mathbb{Q})$ と $\sqrt{2}$ の有理数係数 1 次多項式で書けた。では、4 次の単項拡大 $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$ に対して、$\mathbb{Q}(\sqrt[4]{2})$ の元はどのような形で書けるか。

(11.16) **問題** 次の問に答えよ。

(1) 体の拡大 $\mathbb{Q}(\sqrt{3}+\sqrt{2}) \supset \mathbb{Q}$ の拡大次数を求めよ。
(2) $\sqrt{3}+\sqrt{2}$ の $\mathbb{Q}$ 上の最小多項式を求めよ。

(11.17) **問題** 次の問に答えよ。

(1) 平面上のある点が作図可能であることの定義を言え。
(2) ある実数が作図可能であることの定義を言え。

(11.18) **問題** 実数 α に対し、$F = \mathbb{Q}(\alpha)$ とおき、次の 3 条件を考える。

(a) α は作図可能である。
(b) 体の 2 次拡大の列 $\mathbb{Q} \subset F_1 \subset F_2 \subset \cdots \subset F_n = F$ がある。
(c) 拡大次数 $[F : \mathbb{Q}]$ は 2 のベキである。

このとき、3 条件の間の関係を、「(a) ならば (b) だが逆は不成立」とか「(b) と (c) は同値」とか「(a) は (c) の必要条件でも十分条件でもない」のように答えよ。

(11.19) **問題** 30 度が 3 等分できないことを証明せよ。

(11.20) **問題** 正 16 角形、正 17 角形、正 18 角形は作図可能か否か。

(11.21) **問題** 次の問に答えよ。

(1) 1 の 6 乗根は 6 つあるが、そのうち原始 6 乗根はいくつあるか。
(2) 円周等分多項式 $\Phi_6(x)$ を求めよ。

(3) 円周等分多項式 $\Phi_7(x)$ を求めよ。

(11.22) **問題** n を正整数とするとき次の問に答えよ。

(1) 1 の原始 n 乗根の定義を言え。
(2) 1 の原始 12 乗根の個数を言え。
(3) 1 の原始 n 乗根の個数を言え。

(11.23) **問題** 円周等分多項式 $\Phi_8(x)$ を求めよ。

(11.24) **問題** $\Phi_n(x)$ を円周等分多項式とするとき次の問に答えよ。

(1) $\Phi_{100}(x)$ の次数を言え。
(2) 円周等分多項式 $\Phi_{24}(x)$ を、x^{24} と、$\Phi_d(x)$ $(1 \leq d \leq 23)$ を用いて表せ。
(3) $\Phi_{71}(x)$ を求めよ。
(4) $\Phi_{18}(x)$ を求めよ。

§12 問題の解答

(11.1) **の解答** (6.1) を見よ。

(11.2) **の解答** (1) 環ではない (0 を含まない)。(2) 環ではない (差で閉じていない)。(3) 環ではない (1 を含まない)。(4) 環ではない (0 を含まない)。(5) から (12) はすべて環である。

(11.3) **の解答** (2.1) を見よ。

(11.4) の解答　単元の定義は (2.2) を見よ。
(a) $1, -1$　(b) $\overline{1}$　(c) $\overline{1}, \overline{2}$　(d) $\overline{1}, \overline{5}$　(e) $1, -1$　(f) 0 以外すべて

(11.5) の解答　零因子の定義は (2.2) を見よ。
(a) 0　(b) $\overline{0}$　(c) $\overline{0}$　(d) $\overline{0}, \overline{2}, \overline{3}, \overline{4}$　(e) 0　(f) 0

(11.6) の解答　(1) (2.2) を見よ。
(2) (2.9) と同じ条件 ($\mathbb{Z}/(m)$ が体であるのは、$\mathbb{Z}/(m)$ が整域であることと実は同値)。
(3) (a), (b), (c), (e), (f)

(11.7) の解答　$11x + 3y = 1$ の整数解を (互除法を用いるなどして) 求めると、$(x, y) = (2, -7)$ である。よって $11 \cdot 2 - 3 \cdot 7 = 1$ だが、これを mod11 すると、$3 \cdot (-7) \equiv 1 \pmod{11}$ である。よって $\overline{3}$ の逆元は、$(\overline{3})^{-1} = \overline{-7}$ ($\overline{-7}$ を $\overline{4}$ に変形してもよい)。

(11.8) の解答　(4.3) により、整数係数の範囲での既約性と、有理数係数の範囲での既約性は同じであることに注意しておく。

また、$\mathbb{Z}/(2)$ 係数の多項式として、$x^2 + x + 1$ や $x^3 + x^2 + 1$ は既約である。なぜなら、可約ならば 1 次の因数があるはずだが、$x = \overline{0}$ を代入しても、$x = \overline{1}$ を代入しても 0 にならないから、x でも $x + \overline{1}$ でも割り切れないことがわかるからである。この事実は (4.4) を使うときに必要である。

(1) から (6) まですべて既約である。(1) から (5) までは、(4.4) において $p = 2$ とすればわかる。(2) と (6) は、(4.6) において $p = 3$ とすればわかる。

(11.9) の解答

(1) 環ではない (0 を含まない)。

(2) 環ではない (差で閉じていない)。
(3) 環ではない (1 を含まない)。
(4) 環ではない (0 を含まない)。
(5) 環である。体ではない (2 の逆元がない)。
(6) 体である。
(7) 体である。
(8) 体である。
(9) 環である。体ではない (x の逆元がない)。
(10) 環である。体ではない (x の逆元がない)。
(11) 環である。体ではない (x の逆元がない)。
(12) 環である。体ではない (x の逆元がない)。
(13) 体である。
(14) 体である。

(11.10) の解答

(1) ベクトル空間ではない (スカラー倍がない)。
(2) ベクトル空間である。スカラーの例は $\mathbb{Q}$.
(3) ベクトル空間である。スカラーの例は $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ など。
(4) ベクトル空間ではない (スカラー倍がない)。
(5) ベクトル空間である。スカラーの例は $\mathbb{Q}, \mathbb{R}$ など。
(6) ベクトル空間ではない (スカラー倍がない)。
(7) ベクトル空間である。スカラーの例は $\mathbb{Q}$.

(11.11) の解答 (1) 体の拡大 $E \supset F$ の拡大次数とは、E を F 上のベクトル空間と見たときの次元のことである。
(2) (8.4) を見よ。
(3) (8.6) を見よ。
(4) (8.6) を見よ。
(5) $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$. ($\sqrt{2}$ の $\mathbb{Q}$ 上の最小多項式 $x^2 - 2$ が 2 次式だから)

(11.12) の解答 (1) $\sqrt{-1}$ の $\mathbb{R}$ 上の最小多項式 x^2+1 の次数が 2 だから、$\mathbb{C}=\mathbb{R}(\sqrt{-1})\supset\mathbb{R}$ は 2 次拡大。
(2) $\{1,i\}$. なぜなら、任意の複素数は $a,b\in\mathbb{R}$ を用いて、$a+bi$ とただ 1 通りに表せるから。
(3) [生成すること] 任意の複素数 $a+bi$ $(a,b\in\mathbb{R})$ に対して、$a+bi=p(1+i)+q(1-i)$ を満たす $p,q\in\mathbb{R}$ が取れる。実際、両辺の係数比較をすると、$p=(a+b)/2$, $q=(a-b)/2$ である。
[1 次独立性] $p(1+i)+q(1-i)=0$ $(p,q\in\mathbb{R})$ とすると、$(p+q)+(p-q)i=0$ より、

$$\begin{cases} p+q=0 \\ p-q=0 \end{cases}$$

であり、これを解くと $p=q=0$ だから、$1+i$ と $1-i$ は $\mathbb{R}$ 上 1 次独立である。

(11.13) の解答 [$\mathbb{Q}$ 上 1 次独立] $\sqrt{2}$, $\sqrt{3}$.
(証明) $a,b\in\mathbb{Q}$ により、$a\sqrt{2}+b\sqrt{3}=0$ と書けたとする。$a\neq 0$ ならば、変形して、$\sqrt{6}=-3b/a$ と書けるが、これは $\sqrt{6}$ が無理数であることに反する。よって $a=0$ であり、したがって $b=0$. つまり、$\sqrt{2}$ と $\sqrt{3}$ は $\mathbb{Q}$ 上 1 次独立である。
[$\mathbb{Q}$ 上 1 次従属] $\sqrt{2}$, $-\sqrt{2}$.
(証明) $a=b=1$ により、$a\sqrt{2}+b(-\sqrt{2})=0$ と書けるから。

(11.14) の解答 まず、$\alpha\in\mathbb{R}$ の $\mathbb{Q}$ 上の最小多項式が 1 次式ならば、それは $x-\alpha$ になるしかなく、これが $\mathbb{Q}$ 上の多項式だから $\alpha\in\mathbb{Q}$ である。対偶をとれば、無理数の最小多項式は 2 次以上であるとわかる。
(1) $x=\sqrt{3}$ を変形して、$x^2-3=0$ であり、これより低い次数の最小多項式はありえないので、最小多項式は x^2-3 である。

(2) $x=\sqrt{3}+1$ より、$x-1=\sqrt{3}$. これを変形して、$x^2-2x-2=0$ だから、最小多項式は x^2-2x-2 である。

(3) $x=1/\sqrt{3}$ より、$x^2-1/3=0$. よって最小多項式は $x^2-1/3$ である。

(11.15) の解答 (8.13) (1) より、$a+b\sqrt[4]{2}+c\sqrt[4]{4}+d\sqrt[4]{8}$ $(a,b,c,d\in\mathbb{Q})$ の形で書ける。

(11.16) の解答 (1) まず、$\mathbb{Q}(\sqrt{3}+\sqrt{2})=\mathbb{Q}(\sqrt{3},\sqrt{2})$ を示す。$\alpha=\sqrt{3}+\sqrt{2}$ と置くと、$\alpha+\alpha^{-1}=2\sqrt{3}$ であるが、$\mathbb{Q}(\alpha)$ は体であるから、$\alpha+\alpha^{-1}$ を含む。よって、$\sqrt{3}\in\mathbb{Q}(\alpha)$ である。したがって、$\sqrt{2}=\alpha-\sqrt{3}\in\mathbb{Q}(\alpha)$ である。これらより、$\mathbb{Q}(\sqrt{2},\sqrt{3})\subset\mathbb{Q}(\alpha)$ がわかる。反対の包含関係は、$\alpha\in\mathbb{Q}(\sqrt{2},\sqrt{3})$ より明らかだから、$\mathbb{Q}(\sqrt{3}+\sqrt{2})=\mathbb{Q}(\sqrt{3},\sqrt{2})$ が示された。

$\sqrt{3}$ の $\mathbb{Q}$ 上の最小多項式は x^2-3 であり、$\sqrt{2}$ の $\mathbb{Q}(\sqrt{3})$ 上の最小多項式は x^2-2 であるから、$\mathbb{Q}(\sqrt{3},\sqrt{2})\supset\mathbb{Q}(\sqrt{3})\supset\mathbb{Q}$ は 2 次拡大の連続である。よって、(8.16) より、全体が 4 次拡大となるので、$\mathbb{Q}(\alpha)\supset\mathbb{Q}$ も 4 次拡大である。

(2) α の最小多項式は (1) より 4 次式である。$x=\sqrt{3}+\sqrt{2}$ を変形すると $x^4-10x^2+1=0$ となるから、α の最小多項式は x^4-10x^2+1 である。

(11.17) の解答 (1) (9.1) の「$\cdots$ 作図可能な点と呼ぶ。」までを見よ。
(2) (9.1) の最後の段落。

(11.18) の解答 (a) と (b) は同値、(b) ならば (c) である ((c) ならば (b) には反例があり不成立)。

(11.19) の解答　$\alpha = \cos 10^\circ$ が作図可能ではないことを証明すればよい。sin の 3 倍角の公式 $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$ を用いると、

$$\sin 30^\circ = 3\alpha - 4\alpha^3$$
$$8\alpha^3 - 6\alpha + 1 = 0$$

を得る。多項式 $8x^3 - 6x + 1$ は、(9.10) で証明したように既約多項式であるから、α の最小多項式である。よって、$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ となり、これが 2 のベキではないから、α は作図可能ではない。

(11.20) の解答　オイラーの関数は、$\phi(16) = 8$, $\phi(17) = 16$, $\phi(18) = 6$ だから、2 のベキである正 16 角形、正 17 角形は作図可能、正 18 角形は作図可能ではない。

(11.21) の解答　(1) 1 の 6 乗根は複素数平面の単位円周の 6 等分点であり、偏角 60° のものを ζ とすると、$1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5$ の 6 つである。原始 6 乗根とは、これらのうち、6 乗して初めて 1 になるものである。実際に計算してみてもよいが、0 乗から 5 乗のうち 6 と互いに素な、1 乗と 5 乗したものが原始 6 乗根である。よって 2 個。
(2) 上の記号を用いると、原始 6 乗根は ζ と ζ^5 であるから、

$$\Phi_6(x) = (x - \zeta)(x - \zeta^5) = x^2 - (\zeta + \zeta^5)x + \zeta^6.$$

ここで、$\zeta^6 = 1$ であり、また、ζ と ζ^5 は、実部が等しく $\cos 60^\circ = 1/2$ であり、虚部はちょうど符号が逆で、$\pm\sin 60^\circ$ である。よって、$\Phi_6(x) = x^2 - x + 1$ である。
(3) ζ を、上とは違い、$\zeta = \cos(360^\circ/7) + i\sin(360^\circ/7)$ とおく。すると、ζ^k $(k = 1, 2, 3, 4, 5, 6)$ が原始 7 乗根なので、

$$\Phi_7(x) = (x - \zeta)(x - \zeta^2)(x - \zeta^3)(x - \zeta^4)(x - \zeta^5)(x - \zeta^6)$$

である。他方、x^7-1 の 7 つの根が 1 の 7 乗根だから、

$$x^7-1=(x-1)(x-\zeta)(x-\zeta^2)(x-\zeta^3)(x-\zeta^4)(x-\zeta^5)(x-\zeta^6)$$

である。よって、これらより、

$$\Phi_7(x)=\frac{x^7-1}{x-1}=x^6+x^5+x^4+x^3+x^2+x+1$$

である。

(11.22) の解答 (1) 複素数 ζ が 1 の原始 n 乗根であるとは、$\zeta^n=1$ かつ、n 未満の正整数 k に対して $\zeta^k\neq 1$ を満たすことを言う。
(2) 4 個。(複素数平面の単位円周の 12 等分点のうち、偏角が、$\pm 30^\circ, \pm 150^\circ$ の点)
(3) $\phi(n)$ (オイラーの関数)

(11.23) の解答 1 の 8 乗根 ζ を $\zeta=\cos 45^\circ+i\sin 45^\circ$ ととる。1 の原始 8 乗根は、$\zeta,\zeta^3,\zeta^5,\zeta^7$ である。

$$\begin{aligned}\Phi_8(x)&=(x-\zeta)(x-\zeta^3)(x-\zeta^5)(x-\zeta^7)\\&=\frac{x^8-1}{(x-1)(x-\zeta^2)(x-\zeta^4)(x-\zeta^6)}\\&=\frac{x^8-1}{(x-1)(x-i)(x+1)(x-i)}\\&=\frac{x^8-1}{(x^2-1)(x^2+1)}\\&=\frac{(x^4-1)(x^4+1)}{(x^4-1)}=x^4+1.\end{aligned}$$

(11.24) の解答 (1) $\deg \Phi_{100}(x) = \phi(100) = \phi(25)\phi(4) = 20 \cdot 2 = 40$.
(2)24 の約数が $1, 2, 3, 4, 6, 8, 12$ なので、

$$\Phi_{24}(x) = \frac{x^{24} - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_8(x)\Phi_{12}(x)}$$

(3) 71 が素数なので、$\Phi_{71}(x) = 1 + x + x^2 + \cdots + x^{70}$.
(4) $x^{18} - 1 = (x^9 - 1)(x^9 + 1) = (x^9 - 1)(x^3 + 1)(x^6 - x^3 + 1)$ であるが、$x^9 - 1$ の根は 9 乗根であり、$x^3 + 1$ の根は 3 乗すると -1 だから 6 乗根である。Φ_{18} の根は原始 18 乗根だから、Φ_{18} は $x^6 - x^3 + 1$ の因数になっている。ところで、$\deg \Phi_{18} = \phi(18) = 6$ だから、次数を考えれば、$\Phi_{18}(x) = x^6 - x^3 + 1$ である。