2011 年度 後期 代数学 3

更新日時 2012-02-02 18:59:08　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. 体の定義
2. 部分体
3. 拡大体
4. 単項拡大
5. 代数拡大
6. 代数閉体
7. 作図可能性
8. 点の作図と体の拡大
1. 正多角形の作図可能性
2. 準同型
3. 正規拡大
4. 分解体
5. 多項式のガロア群
6. 根の公式
7. 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

講義のノートの概略を記す．また、問題については、板書できなかったものも追加して記す。

§1 体

(1.1) **定義 (体)** 集合 R が**環**であるとは、R に和と積が定義されて、次の条件 (R1) から (R7) を満たすことをいう。

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

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

(1.2) **定義 (例)**

(1) 有理数全体の集合 $\mathbb{Q}$ は体である。
(2) 実数全体の集合 $\mathbb{R}$ は体である。
(3) 複素数全体の集合 $\mathbb{C}$ は体である。
(4) 整数全体の集合 $\mathbb{Z}$ は体ではない。
(5) 有理数を係数にもつ x の多項式全体のなす集合 $\mathbb{Q}[x]$ は環である (**多項式環**) が、体ではない。
(6) 実数や複素数を係数にもつ x の多項式環 $\mathbb{R}[x]$ や $\mathbb{C}[x]$ も環であるが、体ではない。
(7) 有理数係数の分数式全体の集合 $\mathbb{Q}(x)$ は体である。整数、実数や複素数が係数である場合でも、$\mathbb{Z}(x), \mathbb{R}(x)$ や $\mathbb{C}(x)$ は体である。
(8) $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ は体である。

(1.3) **問題** $a,b\in\mathbb{Q}$ に対し、$a+b\sqrt{2}\neq 0$ ならば $a^2-2b^2\neq 0$ であることを示せ。

(1.4) **問題** $a,b,c,d\in\mathbb{Q}$ 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。

§2 ベクトル空間の復習

(2.1) **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 $((k+l)v=kv+lv,\ k(v+w)=kv+kw)$

(2.2) **例**

(1) $\mathbb{Q}$ 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。
(2) $\mathbb{Q}[x]$ 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。
(3) $\mathbb{Q}(x)$ は $\mathbb{Q}$ 上のベクトル空間である。

(4) $\mathbb{Q}(\sqrt{2})$ は $\mathbb{Q}$ 上のベクトル空間である。
(5) $\mathbb{C}$ は $\mathbb{R}$ 上のベクトル空間である。
(6) 体 F の**部分体** E があるとき、F は E 上の上のベクトル空間である。

(2.3) **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、

$$\{a_1v_1 + \cdots + a_kv_k \mid a_j \in F\}$$

で定まる集合のことである。

(2.4) **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、$a_1v_1 + \cdots + a_kv_k = 0$ 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、

$$a_1v_1 + \cdots + a_kv_k = b_1v_1 + \cdots + b_kv_k$$

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。

(2.5) **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) $\mathbb{Q}[x]$ 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。
(5) $\mathbb{Q}(\sqrt{2})$ 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。
(6) $\mathbb{R}[x]$ 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。

§3 体の拡大

(3.1) **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。

(3.2) **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、$x = a_1e_1 + a_2e_2 + \cdots + a_ne_n$ $(a_j \in F)$ と一意的に書けるとき、E は F の n 次拡大である。

(3.3) **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) $\mathbb{R} \supset \mathbb{Q}$ は無限次拡大である。
(4) $\mathbb{Q} \supset \mathbb{Q}$ は 1 次拡大である。

(3.4) **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。

(3.5) **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。

(3.6) **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) $\alpha \in E$ が F 上代数的であるとき、$f(\alpha) = 0$ となる 0 ではない多項式のうち、次数が最小で、最高次の係数が 1 であるものを α の**最小多項式**と言う。
(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。

(3.7) **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) $f(x)$ の最高次である 2 次の係数は 1 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。

(3.8) **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。

(3.9) **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 の最高次係数は 1 であり、f は F 上既約多項式である。

(3.10) **例 (最小多項式)** $\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式は $X^3 - 2$ である。

(3.11) **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)⇔(iii)] $F(\alpha)$ の最小性より従う。

[(ii)⇒(i)] α が超越的ならば、X を不定元としたとき、$F[X] \to F[\alpha]$ $(f(X) \mapsto f(\alpha))$ は同型になる。したがって $F[\alpha]$ は体ではない。よって対偶が示せた。

[(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。 □

(3.12) **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。

(3.13) 例 (最小多項式) $\alpha=\sqrt{2}+\sqrt{3}$ とする。

(1) α の $\mathbb{Q}$ 上の最小多項式を求めよ。ただし、最小多項式が 4 次であることを用いてよい。
(2) $\sqrt{2}-\sqrt{3}$ が、体 $\mathbb{Q}$ の単項拡大 $\mathbb{Q}(\alpha)$ に含まれることを示せ。
(3) $\sqrt{2}-\sqrt{3}$ を α の多項式で書け。

(解 (1)) $\alpha=\sqrt{2}+\sqrt{3}$ の両辺を 2 乗すると、$\alpha^2=5+2\sqrt{6}$ であり、ここで 5 を移項してから両辺を 2 乗すると、$\alpha^4-10\alpha^2+25=24$ だから、$\alpha^4-10\alpha^2+1=0$ である。従って、x^4-10x^2+1 は α を根に持ち、最小多項式の次数が 4 次であることからこれが最小多項式である。

(解 (2)) $1/\alpha$ の分母を有理化すると $\sqrt{3}-\sqrt{2}$ なので、$\sqrt{2}-\sqrt{3}=-1/\alpha$ は $\mathbb{Q}(\alpha)$ に含まれる。

(解 (3)) $\sqrt{2}-\sqrt{3}$ を α の分数式で書けば $-1/\alpha$ である。これを多項式に直すために $\mathbb{Q}(\alpha)$ における $-\alpha$ の逆元を、α の多項式で表したい。最小多項式 $f(x)=x^4-10x^2+1$ を $-x$ で割ると、商が $-x^3+10x$、余りが 1 だから、

$$f(x)=-x(-x^3+10x)+1$$

である。これに $x=\alpha$ を代入すると、$0=-\alpha(-\alpha^3+10\alpha)+1$ だから、$-\alpha(\alpha^3-10\alpha)=$ となり。$-\alpha$ の逆元は $\alpha^3-10\alpha$ である。

(3.14) 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) $[F(\alpha):F]=n$

(3.15) 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、(3.3) 例 (1) により 2 次拡大であった。また、$\sqrt{-1}$ の最小多項式は、(3.7) 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) (3.10) より、単項拡大 $\mathbb{Q}(\sqrt[3]{2})\supset\mathbb{Q}$ の拡大次数は 3 である。

(3.16) 系 (単項拡大の拡大次数と最小多項式の次数) $E\subset F$ を体の拡大、$f\in F[x]$ を既約多項式とする。$\alpha\in E$ を f の根とすると、$[F(\alpha):F]=\deg f$ である。

(3.17) 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、

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

(3.18) 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、$F(a,b,\ldots)$ は、体 F と、元 $a,b,\ldots$ を含む最小の体であり、それは、F を係数とする $a,b,\ldots$ 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、(3.17) 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。※ (3.13) では、最小多項式の次数の最小性、あるいは、既約性を調べることができなかったので、その次数を 4 だと与えていたが、今回はその次数をきちんと求めた。

§4 代数学の基本定理

(4.1) **事実 (代数学の基本定理)** 複素数係数の n 次方程式は、複素数の範囲で必ず解を持つ。従って、重解も数えると、複素数係数の n 次方程式は、ちょうど n 個の解を持つ。

代数学の基本定理はここでは証明しないが、複素数体に限らず、解の個数に関しては次が成立する。

(4.2) **命題 (根の個数の上限)** R を整域、つまり 0 以外に零因子を持たない可換環とする。R 係数の n 次多項式 $f(x) \in R[x]$ の根の個数は、高々n 個である。

(4.3) **定義 (代数閉体)** 代数方程式 (多項式による方程式) が必ず解を持つような体を**代数閉体**という。例えば、複素数体 $\mathbb{C}$ は、代数学の基本定理より代数閉体であるが、有理数体 $\mathbb{Q}$ や実数体 $\mathbb{R}$ は代数閉体ではない。

(4.4) **命題 (代数閉体であるための条件)** 体 Ω に対して次の条件は同値である.

(1) Ω は代数閉体である。
(2) $\Omega[X]$ に属する多項式は必ず Ω に根を持つ。
(3) $\Omega[X]$ に属する多項式は 1 次式の積に因数分解する。
(4) Ω の代数拡大は存在しない。

(4.5) **事実 (代数閉包の存在)** 体 F の代数閉体であるような拡大体のうち最小のものを、F の**代数閉包**という。任意の体 F に対して、その代数閉包は存在する。例えば、実数体 $\mathbb{R}$ の代数閉包は、複素数体 $\mathbb{C}$ である。

§5 作図問題

(5.1) **定義 (作図可能性)** 平面上に原点 O と、点 $(1,0)$ が与えられたとき、平面上の点集合の部分集合 $\mathbb{P}$ を次のように定める。

(1) $\mathbb{P}_1 = \{\mathrm{O}, (1,0)\}$ と置く。
(2) $\mathbb{P}_1, \mathbb{P}_2, \ldots, \mathbb{P}_n$ まで定まっているとする。$\mathbb{P}_n$ に属する異なる 2 点間に直線を引く、あるいは、$\mathbb{P}_n$ に属する 1 点を中心とし $\mathbb{P}_n$ に属する異なる 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を Q として、$\mathbb{P}_{n+1} = \mathbb{P}_n \cup \{\mathrm{Q}\}$ と定める。
(3) $\mathbb{P} = \bigcup_{n \geq 0} \mathbb{P}_n$ と定める。

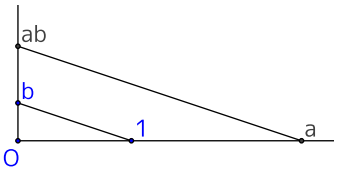
つまり、長さ 1 の線分が与えられたときに、定規とコンパスのみを用いた有限回の手順による作図で得られる点集合である。$\mathbb{P}$ の点を**作図可能**な点と呼ぶ。

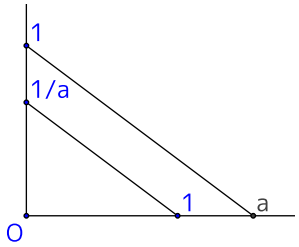
また、ある実数が**作図可能**であるとは、それが $\mathbb{P}$ のある点の x 座標または y 座標として得られることを言う。ある複素数が**作図可能**であるとは、平面を複素数平面と思ったときに、その複素数に対応する点が作図可能であることを言う。

(5.2) **例 (作図入門)**

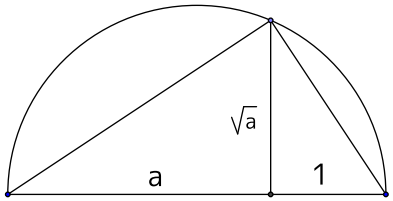
(1) 直線 ℓ と、その直線上にない点 A が与えられたとき、ℓ に平行で A を通る直線を書くことができる。
(2) 直線 ℓ と、その直線上にない点 A が与えられたとき、ℓ に垂直で A を通る直線を書くことができる。
(3) 直線 ℓ と、ℓ 上の点 A が与えられたとき、ℓ に垂直で A を通る直線を書くことができる。
(4) 直線 ℓ と、ℓ 上の点 A が与えられたとき、A を通り ℓ となす角が 60° である直線を書くことができる。

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





(5.4) **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。



よって、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。したがって、$\mathbb{Q}$ 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。

(5.5) **点の作図と体の拡大** 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

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

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。

(5.6) **命題 (作図可能な数による拡大次数)** 平面上の点 (x,y) が作図可能ならば、$\mathbb{Q}$ から出発して 2 次拡大を反復して得られる拡大体 F $(F\subset\mathbb{R})$ であって、$x,y\in F$ となるものが存在する。したがって、α を作図可能な数とすると、$\mathbb{Q}$ から出発して 2 次拡大を反復して得られる拡大体 F $(F\subset\mathbb{R})$ であって、$\alpha\in F$ となるものが存在する。

(5.7) **定理 (数が作図可能であるための必要十分条件)** 実数 α が作図可能であるための必要十分条件は、$F=\mathbb{Q}(\alpha)$ の部分体の列であって、隣接する体どうしは 2 次拡大になっている列、

$$\mathbb{Q}=F_0\subset F_1\subset\cdots\subset F_n=F$$

が存在することである。特に、$[F:\mathbb{Q}]$ が 2 のべキ 2^m の形でなければ、α は作図可能ではない。

Proof. [十分性] 上のような列があれば、(5.4) より F の元はすべて、特に α は作図可能である。

[必要性] $\alpha\in\mathbb{R}$ を作図可能とすると、(5.6) により、2 次拡大の列

$$\mathbb{Q}\subset F_1'\subset\cdots\subset F_n'=F'\qquad(\alpha\in F')$$

が存在する。$F'\supset\mathbb{Q}(\alpha)$ に注意しておく。列の体それぞれの $F=\mathbb{Q}(\alpha)$ との共通部分を、$F_i=F_i'\cap F$ とおけば、

$$\mathbb{Q}\subset F_1\subset\cdots\subset F_n=F$$

という列が得られるが、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。 □

(5.8) **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、$\bmod 2$ すると $y^3 + y + 1$ と既約であるから。$\leftarrow f \in \mathbb{Z}[x]$ を $\bmod p$ 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。

(5.9) **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 (§6 で詳しく見る)。

(5.10) **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.

§6 正多角形の作図可能性

(6.1) **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。 □

(6.2) **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 $\xi^k \neq 1$ $(1 \le k \le n-1)$ なるときを言う。

(6.3) **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。

(6.4) **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。

(6.5) **例 (円周等分多項式)**

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

(6.6) **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。

(6.7) **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、最高次の係数は 1 である。

(6.8) **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。

(6.9) **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、$\theta = 360°/n$ 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。 □

(6.10) **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。

(6.11) **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。

§7 演習問題

(7.1) **問題** 環の定義を書け。また、体の定義を書け。

(7.2) **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 $\mathbb{R}(x)$

(7.3) **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 $\mathrm{Mat}(m,n;\mathbb{Q})$

(7.4) **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。

(7.5) **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。

(7.6) **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。

(7.7) **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) $\dfrac{1}{\sqrt{3}}$

(7.8) **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。

(7.9) **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。

(7.10) **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。

(7.11) **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。

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

(7.13) **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。

(7.14) **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。

§8 問題の解答

(7.1) **の解答** (1.1) を見よ。

(7.2) **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) 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。

(7.3) **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 $\mathbb{Q}$.

(7.4) **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) (3.4) を見よ。
(3) (3.6) を見よ。
(4) (3.6) 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)

(7.5) **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。

(7.6) **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。$a\neq0$ 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。

(7.7) **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。

(7.8) **の解答**　(3.17) (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。

(7.9) **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、(3.17) 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。

(7.10) **の解答**　(1) (5.1) の「$\cdots$ 作図可能な点と呼ぶ。」までを見よ。
(2) (5.1) の最後の段落。

(7.11) **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)。

(7.12) **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。

(7.13) **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 $\zeta^k\neq1$ 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、$\pm30^\circ$, $\pm150^\circ$ の点)
(3) $\phi(n)$ (オイラーの関数)

(7.14) 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。