2019 年度 前期 代数学 4

更新日時 2019-05-28 22:04:59　担当 和地 輝仁

目次

1 シラバス抜粋

授業概要 代数学 3 までに学んだ体と体の拡大の理論を利用して、作図問題や代数方程式解の公式の存在の問題を学ぶ授業です。

到達目標

1. 正多角形の作図可能性と体の理論との関係を理解する。
2. ガロア理論の初歩を知る。
3. 代数方程式の解の公式と体の理論との関係を理解する。

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. 原始 n 乗根
2. 円周等分多項式
3. 正多角形の作図可能性
4. 準同型、同型、F-同型
5. 正規拡大
6. 分解体
7. 群の復習
8. 多項式のガロア群
9. 分離拡大
10. ガロア拡大
11. ガロア群
12. ガロア理論の基本定理
13. 可解群
14. 代数方程式の解の公式
15. 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．

備考 受講するためには、代数学 1、代数学 2、代数学 3 を履修していることが望ましいです。

2 授業のノート

§1 原始 n 乗根

代数学 3 で学んだ実数が作図可能であるための条件を復習してから、正多角形が作図可能であるための条件を原始 n 乗根を用いて述べる。

(1.1) 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。 □

(1.2) **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。

■問題 $n = 4, 6$ で原始 n 乗根の個数を求めよ。

(1.3) **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。 □

§2 円周等分多項式

(2.1) **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。

(2.2) **例 (円周等分多項式)**

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

(2.3) **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)。 □

(2.4) **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。 □

(2.5) **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. (1) 簡単。(2) (1) とフェルマーの小定理より。 □

(2.6) **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。 □

§3 正多角形の作図不可能性

(3.1) **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。

(3.2) **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。

(3.3) **正多角形の作図可能性一覧** $p=2^m+1$ の形の 3 以上の素数があれば、$\phi(p)=2^m$ だから、正 p 角形は作図可能であるが、この形の整数は、$p=3,5,17,257,65537$ の 5 種類しか知られておらず、これ以外にないと予想されてもいる。

一般に、3 以上の整数 n の素因数分解を

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad (p_1, p_2, \ldots, p_k \text{ は相異なる素数})$$

とすると、オイラーの関数は

$$\phi(n) = p_1^{a_1-1}(p_1-1) \cdot p_2^{a_2-1}(p_2-1) \cdots p_k^{a_k-1}(p_k-1) \quad (a_i \geq 1)$$

であるが、これが 2 の冪になるには、、各 $i = 1, 2, \ldots, k$ に対して、$p_i - 1$ が 2 の冪であり、$a_i > 1$ ならば $p_i = 2$ でなくてはならない。

$p = 2^m + 1$ の形の 3 以上の素数が $p = 3, 5, 17, 257, 65537$ の 5 種類だと仮定すれば、3 以上の整数 n が

$$n = 2^b \cdot 3^{a_1} \cdot 5^{a_2} \cdot 17^{a_3} \cdot 257^{a_4} \cdot 65537^{a_5} \quad (b \geq 0,\ a_i = 0, 1)$$

の形のときに限り、正 n 角形は作図可能である。

§4 準同型、同型、F-同型

(4.1) **定義 (準同型、同型、F-同型)** (1) 2 つの体 F_1, F_2 があるとき、写像 $\phi : F_1 \to F_2$ が**準同型写像** であるとは、次の条件を満たすことを言う。

(H1) $\phi(1) = 1$,
(H2) $\phi(a+b) = \phi(a) + \phi(b)$ $(a, b \in F_1)$,
(H3) $\phi(ab) = \phi(a)\phi(b)$ $(a, b \in F_1)$

(2) 2 つの体 F_1, F_2 があるとき、写像 $\phi : F_1 \to F_2$ が**同型写像** であるとは、ϕ が全単射な準同型であることをいい、このとき、F_1 と F_2 は**同型**であるという。

また、F_1 と F_2 が同じ体 F であるとき、F から F への同型写像を F 上の**自己同型写像**と言い、F 上の自己同型写像全体のなす集合を $\mathbf{Aut}(\boldsymbol{F})$ で表す。

(3) 体の拡大 $E_1 \supset F$ と $E_2 \supset F$ があり、体の同型写像 $\phi : E_1 \to E_2$ があるとする. ϕ が F 上恒等写像であるとき、ϕ を **F-同型写像**であるといい、E_1 と E_2 は **F-同型**であるという。

また、E_1 と E_2 が同じ体 E であるとき、E から E への F-同型写像を E 上の **F-自己同型写像**と言い、E 上の F-自己同型写像全体のなす集合を $\mathbf{Aut}_{\boldsymbol{F}}(\boldsymbol{E})$ で表す。

(4.2) **命題** 体の拡大 $E \supset F$ を考える。既約多項式 $f(x) \in F[x]$ があるとき、$\alpha, \beta \in E$ が共に f の根ならば、$F(\alpha) \simeq_F F(\beta)$ (F-同型) である.

Proof. (Well-defined な) 環同型写像 $\phi : F[\alpha] \to F[\beta]$ $(f(\alpha) \mapsto f(\beta))$ があるが、これが、$1/f(\alpha)$ を $1/f(\beta)$ に写せば、体の同型写像でもある。α も β も最小多項式が同じ f だから、**??** 定理の証明により、$1/f(\alpha)$ も $1/f(\beta)$ も、同じ多項式 p を用いて $p(\alpha)$, $p(\beta)$ と書ける. p が多項式なので ϕ は $p(\alpha)$ を $p(\beta)$ に写すから、ϕ は体の同型写像である。

また、ϕ が F 上恒等写像なのは明らかだから、ϕ は F-同型写像である。 □

(4.3) **例** (1) $\mathbb{R}$ 上代数的な元 $i = \sqrt{-1}$ と $-i$ は、同じ最小多項式 $x^2 + 1$ を持つ。よって、$\mathbb{R}(i)$ と $\mathbb{R}(-i)$ は $\mathbb{R}$-同型であり (この場合はより強く両者は等しい)、複素共役 $a + bi \mapsto a - bi$ が $\mathbb{R}$-同型写像である.

(2) $\mathbb{Q}(\sqrt{2})$ では $a + b\sqrt{2} \mapsto a - b\sqrt{2}$.

(4.4) **問題** 体の準同型 $\phi : E \to F$ は単射である。

Proof. $\operatorname{Ker}\phi$ は E の体のイデアルだから、0 か E 自身のいずれかであるが、$\phi(1) = 1$ なので 0 である。よって単射。 □

(4.5) **命題** F 上代数的な元 α の最小多項式が $f(x)$ であり、$E = F(\alpha)$ であるとき、

$$\#\operatorname{Aut}_F(E) = \#\{a \in E\ ;\ f(a) = 0\} \tag{2}$$

Proof. E の元は α の多項式だから、F-同型は α の像で決まる。α の像も f の根だから命題が言える。 □

(4.6) **問題** $E \supset F$ を体の拡大とするとき、$\operatorname{Aut}(E)$, $\operatorname{Aut}_F(E)$ は写像の合成に関して群をなすことを示せ。

(4.7) **命題** F 上代数的な元 α の最小多項式が $f(x)$ であり、Ω を F を部分体に持つような代数閉体とするとき、

$$\#\{\phi : F \hookrightarrow \Omega\ ;\ \text{体の準同型}\ \} = (f\ \text{の}\ \Omega\ \text{における根の個数})$$

Proof. 上の命題と同様。 □

§5 正規拡大

(5.1) **定義 (正規拡大)** 体の有限次拡大 $E \supset F$ が**正規拡大**であるとは、任意の $\alpha \in E$ の最小多項式のすべての根が E の元であることをいう。

(5.2) **例** (1) $\mathbb{C} \supset \mathbb{R}$ は正規拡大である ((3) 参照)。

(2) $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ の正規拡大ではない。なぜなら最小多項式 $x^3 - 2$ の他の 2 根は $\mathbb{Q}(\sqrt[3]{2})$ に属さない。

(3) 2 次拡大は正規拡大である。なぜなら 2 次拡大に属する元は (高々) 2 次方程式の根であるから、解と係数の関係を用いるとわかる。

(4) したがって、$\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ は正規拡大である。

(5.3) **定理** 有限次正規拡大 $E \supset F$ であり、任意の $\alpha \in E$ の最小多項式が重根を持たないとする。このとき、E の $\mathrm{Aut}_F(E)$-不変部分体 $E^{\mathrm{Aut}_F(E)}$ は F に等しい。

$*$ F を含むことは $\mathrm{Aut}_F(E)$ の定義よりわかる.

Proof. まず、α が F に属さないということは、最小多項式の次数が 2 以上ということである。α の最小多項式の別の根 (は重解がないので存在するが) を β とし、$F(\alpha) \to F(\beta)$ $(g(\alpha) \mapsto g(\beta))$ と定めると、α を固定しない F 同型が得られ、これは E の F-同型に拡張される。 □

(5.4) **注意** 標数 0 の体 F では、(最小多項式のような) 既約多項式が重根を持たない。なぜなら、$f(x) \in F[x]$ を既約、かつ、適当な拡大体で重根 α を持つとすると、$f(\alpha) = f'(\alpha) = 0$ なので、既約性より f は f' を割り切る。次数を見ればこれは不可能。

既約多項式が重根を持つ例としては、$F = \mathbb{F}_2(t)$ を有理関数体とし、$f(x) = x^2 - t \in F[x]$ がある。実際、1 つの根を α とすると、$f' = 0$ より、α は重根であり、$f(x) = (x - \alpha)^2$ でなくてはならないが、$f(x) = x^2 + \alpha^2 =$

$x^2-\alpha^2$ となり、$t=\alpha^2$ である。f が可約なのは $\alpha\in F$ と同値だが、$\alpha\notin F$ なので、f は F 上既約である。

§6 分解体

(6.1) **定義 (分解体)** 体 F に対して、多項式 $f(x)\in F[x]$ のすべての根を付け加えた体を、f の F 上の**分解体**という。

(6.2) **例** (1) $\mathbb{R}$ 上 x^2+1 の分解体は $\mathbb{C}$ である。
(2) $\mathbb{Q}$ 上 x^2-2 の分解体は $\mathbb{Q}(\sqrt{2})$ である。
(3) $\mathbb{Q}$ 上 x^3-2 の分解体は $\mathbb{Q}(\sqrt[3]{2},\omega)$ である。ただし $\omega=(-1+\sqrt{-3})/2$。

(6.3) **定理** 体の拡大 $E\supset F$ が正規拡大であるための必要十分条件は、E がある多項式 $f(x)\in F[x]$ の分解体であることである。

Proof. 必要性。正規拡大を仮定する。$E=F(\alpha_1,\dots,\alpha_r)$ とし、α_j の最小多項式を f_j とする。f_j の根はすべて F に属することに注意すれば、$f=f_1f_2\cdots f_r$ と定めた f のすべての根で F を拡大すれば E になる。

十分性。$\alpha\in E$ とし、同じ最小多項式を持つ $\beta\in E$ をとる。F-同型 $F(\alpha)\to F(\beta)$ $(\alpha\mapsto\beta)$ は $\phi:E\to E'$ に拡張される (E' は $F(\beta)$ を含むある体)。ϕ は F-同型だから f を変えず、従って f の根を変えないから、$E'=\phi(E)\subset E$。特に、$\beta=\phi(\alpha)\in\phi(E)\subset E$ だから、f のすべての根は E に属することになり、$E\subset F$ は正規拡大である。 □

§7 群の復習

(7.1) **群の定義** 集合 G が**群**であるとは、G に演算 $a \cdot b$ $(a, b \in G)$ が定義されており、次の条件を満たすことをいう。

(G1) $(ab)c = a(bc)$ $(a, b, c \in G)$ (結合法則)
(G2) ある元 $e \in G$ が存在して、任意の $a \in G$ に対して $ea = ae = a$ を満たす。このような元 e を **単位元**という。
(G3) 任意の $a \in G$ に対して、$b \in G$ が存在して $ab = ba = e$ を満たす。このような b を a の**逆元**といい、$\boldsymbol{a^{-1}}$ と書く。

群 G が、

(G4) $ab = ba$ $(a, b \in G)$ (交換法則)

を満たすとき、 G を**アーベル群**と呼ぶ。

(7.2) **例** (1) $G = \{e\}$
(2) 次の群はすべて同型である (乗積表が一致)
$G = \{e, \sigma\}$ $(\sigma^2 = e)$
$G = \mathbb{Z}/(2)$
$G = \{1, -1\}$
(3) $G = \mathbb{Z}/(3)$
(4) $G = \mathbb{Z}/(4)$
$G = \{e, (12)(34), (13)(24), (14)(23)\}$

(7.3) **定義 (部分群)** 群 G の部分集合 H が、G と同じ演算に関して群であるとき、H を G の**部分群**という。つまり、積と逆元で閉じている空ではない (単位元を含む、と言い換えてもよい) G の部分集合を部分群と呼ぶ。

(7.4) **例 (部分群)**

(1) $\{e\}$, G はともに G の部分群である。これらは**自明な部分群**と呼ばれる。
(2) $\mathbb{Z}/(3)$ の部分群は自明なもののみである。
(3) $\mathbb{Z}/(4)$ の非自明な部分群は $\{\overline{0}, \overline{2}\}$ のみである。
(4) $G = \{e, (12)(34), (13)(24), (14)(23)\}$ の非自明な部分群は、$H_1 = \{e, (12)(34)\}$, $H_2 = \{e, (13)(24)\}$, $H_3 = \{e, (14)(23)\}$ の 3 つである。

(7.5) **定義 (位数、巡回群)** 群 G の元 g の位数とは、$g^n = e$ となる最小の正整数である。そのような n が存在しない時、位数は無限大とする。

$\{e, g, g^2, \ldots, g^{n-1}\}$ は G の部分群である。このように、1 つの元のベキで表される元全体のなす群を**巡回群**と呼び、$\langle g \rangle$ と表す。

(7.6) **例** (1) 位数が 1 である元は単位元のみである。
(2) $\mathbb{Z}/(m)$ は巡回群である。
(3) $\overline{1} \in \mathbb{Z}/(4)$ の位数は 4 であり、$\overline{2} \in \mathbb{Z}/(4)$ の位数は 2 である。

(7.7) **例 (部分群の決定)** (1) $G = \mathbb{Z}/(6)$ の部分群は G, $\{0\}$, $\langle 2 \rangle$, $\langle 3 \rangle$.
(2) $G = S_3$ の部分群は、G, $\{e\}$, $\langle (12) \rangle$, $\langle (23) \rangle$, $\langle (13) \rangle$, $\langle (123) \rangle$

(7.8) **剰余類** 群 G とその部分群 H があるとき、$g \in G$ に対して、

$$gH = \{gh \mid h \in H\}$$

と定め、H を法とする g で代表される**左剰余類**と呼ぶ。また、

$$Hg = \{hg \mid h \in H\}$$

と定め、H を法とする g で代表される**右剰余類**と呼ぶ。

(7.9) **例** (1) $G = \mathbb{Z}/(4)$ とその部分群 $H = \{\overline{0}, \overline{2}\}$ に対して、

$$\overline{0} + H = H, \qquad \overline{1} + H = \{\overline{1}, \overline{3}\}, \qquad \overline{2} + H = H \qquad \overline{3} + H = \{\overline{1}, \overline{3}\}$$

である。

(2) $G = \{e, (12)(34), (13)(24), (14)(23)\}$ とその部分群 $H = \{e, (12)(34)\}$ に対して、

$$\begin{aligned} eH &= H, \\ (12)(34)H &= H, \\ (13)(24)H &= \{(13)(24), (14)(23)\}, \\ (14)(23)H &= \{(13)(24), (14)(23)\} \end{aligned}$$

(7.10) **定理** H を有限群 G の部分群とする。

(1) $g_1, g_2 \in G$ に対し、H の剰余類 g_1H と g_2H は、等しいか、共通部分が空集合であるかのいずれかである。つまり、G は共通部分のない剰余類の和集合に分類される。

(2) H を法とする剰余類 gH たちは、すべて要素の数が等しい。

(3) H の位数は G の位数の約数である。

(4) $g \in G$ の位数は G の位数の約数である。

(7.11) **系** 位数が素数である群は巡回群である。また非自明な部分群はない。

(7.12) **例** 3 次対称群 S_3 の非自明な部分群は、

$$\langle(12)\rangle,\ \langle(23)\rangle,\ \langle(13)\rangle,\ \langle(123)\rangle$$

の 4 つである。

§8 多項式のガロア群

(8.1) **定義 (多項式のガロア群)** 体 F に対し、$f \in F[x]$ の分解体を E とするとき、$\mathrm{Aut}_F(E)$ を f の**ガロア群**と呼び、$\boldsymbol{Gal(f)}$ と書く。

(8.2) **定理** F を体とし、多項式 $f \in F[x]$ の根 $\alpha_1, \alpha_2, \ldots, \alpha_n$ がすべて異なるとする. このとき、ガロア群 $Gal(f)$ は、n 次対称群 S_n の部分群である.

Proof. $E = F(\alpha_1, \ldots, \alpha_n)$ と置く。$Gal(f) = \mathrm{Aut}_F(E)$ の元 σ は、体の F-同型だから、各 α_i $(i = 1, \ldots, n)$ の像が決まれば決定する $\sigma(f) = f$ より、f の根の σ による像は再び f の根であるから、α_i の像は、ある j を用いて α_j になる。よって、σ は n 個の根の置換を引き起こすから、$Gal(f)$ は S_n の部分群である。 □

(8.3) **問題** (1) $\mathbb{R}$ 上 x^2+1 のガロア群を求めよ。
(2) $\mathbb{Q}$ 上 x^2-2 のガロア群を求めよ。
(3) $\mathbb{Q}$ 上 x^4-22x^2+1 のガロア群を求めよ。
(4) $\mathbb{R}$ 上 x^2+x+1 のガロア群を求めよ。

§9 分離拡大

(9.1) **定義 (分離拡大)** 体の拡大 $E \supset F$ が**分離拡大**であるとは、任意の $\alpha \in E$ の最小多項式が重根を持たないことを言う。

(9.2) **事実** 標数 0 の体の拡大は分離拡大である.

§10 ガロア拡大

(10.1) **定義 (ガロア拡大)** 体の有限次拡大 $E \supset F$ が**ガロア拡大**であるとは、正規拡大かつ分離拡大であることを言う (つまり、E の元の最小多項式のすべて根は E に属し、重根はないこと)。

(10.2) **補題** 有限群 G が、体 E に忠実に作用しているとする (つまり、作用が恒等写像になるのは G の単位元のみ)。E の G-不変部分体を $F = E^G$ とおくと、

(1) $E \supset F$ はガロア拡大
(2) $[E:F] = \#G$

である。

§11 ガロア群

(11.1) **定義 (ガロア群)** $E \supset F$ をガロア拡大とするとき、E の $\mathrm{Aut}_F(E)$-不変部分体 $E^{\mathrm{Aut}_F(E)}$ をガロア拡大 $E \supset F$ の**ガロア群**と呼び、$\boldsymbol{Gal(E/F)}$ と書く。

分離性と (5.3) 定理、及び (10.2) 補題より、$E \supset F$ がガロア拡大であるための必要十分条件は、$F = E^{\mathrm{Aut}_F(E)}$ なることである。

§12 ガロア理論の基本定理

(12.1) **定理 (ガロア理論の基本定理)** $E \supset F$ をガロア拡大、$G = Gal(E/F)$ をそのガロア群とする。

(1) 任意の**中間体** L (つまり、$E \supset L \supset F$ なる体) に対して、$E \supset L$ はガロア拡大であり、そのガロア群は、

$$Gal(E/L) = Z_G(L)$$

である。ここで。$Z_G(L) = \{g \in G\,;\, g(\alpha) = \alpha \quad (\alpha \in L)\}$ である。

(2) H を G の部分群とするとき、

$$[E : E^H] = \#H$$

であり、また、中間体 L に対して、

$$[E : L] = \#Z_G(L)$$

である.

(3) H を G の部分群とするとき、

$$Z_G(E^H) = H$$

であり、また、中間体 L に対して、

$$E^{Z_G(L)} = L$$

である。

この対応で $E \supset F$ の中間体と、G の部分群が 1 対 1 に対応する。

(4) (3) の 1 対 1 対応では、共役部分体が共役部分群に対応する。したがって、特に、中間体 L が F 上のガロア拡大であることと、$Z_G(L)$ が G の正規部分群であることが同値になる。さらに、このとき、$Gal(L/F) \simeq G/Z_G(L)$ である。

(12.2) **定理** 一般の n 次多項式 $f(x) \in F[x]$ (つまり、根は F 上の (超越的な) 変数である) のガロア群は、n 次対称群 S_n である。

§13 可解群

§14 3 次方程式の解の公式

§15 4 次方程式の解の公式

(15.1) **定理** 体 F が 1 の原始 n 乗根を含むとし、$E \supset F$ が n 次のガロア拡大とする. このとき、ガロア群 $Gal(E/F)$ が巡回群であるための必要十分条件は、E が F 上の**ベキ根拡大**であることである.

ここに、$E \supset F$ がベキ根拡大であるとは、$a \in F$ の n 乗根に相当する元 $\alpha \in E$ $(\alpha^n = a)$ を用いて、$E = F(\alpha)$ と表せることである。

(15.2) **定義 (可解群)** 群 G が**可解群**であるとは、G の部分群の列

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_n = G$$

であって、H_i は H_{i+1} の正規部分群になっており、剰余群 H_{i+1}/H_i は巡回群であるようなものが存在することを言う。

(15.3) **定理** 体 F は、1 の原始 $n!$ 乗根を含むとする。F 上の n 次代数方程式 $f(x) = 0$ の解が F の元から四則とベキ根で書けるための必要十分条件は、ガロア群 $Gal(f)$ が可解群であることである。

(15.4) **事実** 上の定理の、F が原始 $n!$ を含むという仮定は外すことができる。したがって、方程式の係数を複素数体で考えても有理数体で考えても、解の公式の存在については同等である.

(15.5) **5 次以上の代数方程式の解の公式** 可解ではない群の部分群は可解ではなく、5 次交代群 A_5 は可解ではないことが知られている。したがって、5 次対称群 S_5 も可解ではなく、また、$n \geq 5$ のとき、S_n も可解ではない。よって、(12.2) 定理より、5 次以上の代数方程式に四則とベキ根のみからなる解の公式は存在しない。

(15.6) **例** $f(x) = x^5 - 10x + 2$ のガロア群は S_5 である。よって、方程式 $f(x) = 0$ の解は四則とベキ根では表せない。

Proof. 事実: 5 次対称群 S_5 は可解群ではない。
よって、$Gal(f) = S_5$ を示せばよい。

その 1: $p = 2$ として Eisenstein の既約判定法を用いると、f は既約である。

その 2: 増減表を書けば、$f(x) =)$ はちょうど 3 個の実数解を持つことがわかる。よって、残りの 2 解は共役な複素数 2 つである。

その 3: $Gal(f)$ は複素共役を含む。したがって、$Gal(f)$ は実数解を動かさず、虚数解 2 つを入れ替える元を持つ。

その 4: f の 3 実数根を $\alpha_1, \alpha_2, \alpha_3$、2 虚数根を α_4, α_5 とする。f が既約だから、(4.2) 命題より、任意の i, j に対して、α_i を α_j に写すような $Gal(f)$ の元がある。

その 3 と合わせると、(ちょっと頑張る必要があるが) $Gal(f)$ は任意の i, j に対して、α_i と α_j を交換し、他の根を動かさないような元を持つことがわかる。

その 5: 任意の i, j に対して、α_i と α_j を交換し、他の根を動かさないような元 $(i\ j)$ を含む S_5 の部分群は、S_5 自身である。なぜなら、任意の置換は $(i\ j)$ の積に書くことができるからである。 □

3 演習問題

(50.1) **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。

(50.2) **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。

(50.3) **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。

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

(50.5) **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。

(50.6) **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。

(50.7) **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。

(50.8) **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。

(50.9) **問題** 30 度が 3 等分できないことを証明せよ。

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

(50.11) **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。

(50.12) **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。

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

(50.14) **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。

4 演習問題の解答

(50.1) **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) **??** を見よ。
(3) **??** を見よ。
(4) **??** 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)

(50.2) **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。

(50.3) 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。

(50.4) 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。

(50.5) の解答 **??** (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。

(50.6) **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、**??**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。

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

(50.8) **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)。

(50.9) **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、**??** 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。

(50.10) **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。

(50.11) 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。

(50.12) 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)

(50.13) 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。

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

(50.14) 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。