2021 年度 前期 代数学 4

更新日時 2021-06-21 12:18:44　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) **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。 □

(1.2) **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、拡大次数 $[\mathbb{Q}(\alpha):\mathbb{Q}]$ が 2 のベキである。 □

(1.3) **問題** 作図可能ではない代数的数を 2 つあげよ。

(1.4) **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、$\theta = 360°/n$ 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。 □

(1.5) **問題** 上の命題の証明に関して、次の問いに答えよ。
(1) 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を証明せよ。
(2) $\mathbb{Q}(\zeta)\supset\mathbb{Q}(\cos\theta)$ は高々 2 次拡大であるのはなぜか答えよ。
(3) $\mathbb{Q}(\zeta)\supset\mathbb{Q}(\cos\theta)$ は一致しないが、それを用いるとどうして 2 次拡大であると言えるのか答えよ。

(1.6) **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。

(1.7) **例** i を虚数単位とする。1 の 4 乗根は、$1, -1, i, -i$ の 4 つである。このうち、4 乗して初めて 1 になるのは i と $-i$ のみであるから、1 の原始 4 乗根はこれら 2 つである。

(1.8) **問題** $n = 6, 8$ に対して、原始 n 乗根の個数をそれぞれ求めよ。

(1.9) **補題 (原始 n 乗根であるための条件)** n を正整数、$\theta = 360°/n$ 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。ただし、$\phi(n)$ は、オイラーの関数である。

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。 □

(1.10)　**問題**　上の補題の (1) を証明せよ。

(1.11)　**例**　オイラーの関数 $\phi(4) = 2$ なので、このことから直ちに 1 の原始 4 乗根は 2 個あるとわかる (ただし、それが i と $-i$ であることまではわからない)。

(1.12)　**問題**　$n = 12, 120$ に対して、原始 n 乗根の個数をそれぞれ求めよ。

§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)　**問題**　円周等分多項式 $\Phi_n(x)$ の次数が $\phi(n)$ であるのはなぜか答えよ。

(2.3)　**例 (円周等分多項式)**

$$\begin{aligned}
&\Phi_1(x) = x - 1, && \Phi_2(x) = x + 1, \\
&\Phi_3(x) = x^2 + x + 1, && \Phi_4(x) = x^2 + 1, \\
&\Phi_5(x) = x^4 + x^3 + x^2 + x + 1, && \Phi_6(x) = x^2 - x + 1, \\
&\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, && \Phi_8(x) = x^4 + 1.
\end{aligned}$$

Proof. 一部のみ示す。

[$\Phi_1(x)$] 1 の 1 乗根は 1 のみであり、これは原始 1 乗根でもある。よって、$\Phi_1(x) = x - 1$ である。

[$\Phi_2(x)$] 1 の 1 乗根は 1 と -1 である。これらのうち、2 乗して初めて 1 になるのは -1 のみであるから、原始 2 乗根は -1 の 1 個のみである。よって、$\Phi_2(x) = x + 1$ である。

[$\Phi_3(x)$] 1 の 3 乗根は $1, \frac{-1+\sqrt{3}i}{2}, \frac{-1-\sqrt{3}i}{2}$ である。$\phi(3) = 2$ なので原始 3 乗根は 2 個とわかっているが、これら 3 つのうち原始 3 乗根は、明らかに、$\frac{-1+\sqrt{3}i}{2}, \frac{-1-\sqrt{3}i}{2}$ である。よって、

$$\Phi_3(x) = \left(x - \frac{-1+\sqrt{3}i}{2}\right)\left(x - \frac{-1-\sqrt{3}i}{2}\right) = x^2 + x + 1$$

である。 □

(2.4) **問題** 上の例にある円周等分多項式 $\Phi_4(x)$ と $\Phi_6(x)$ を実際に求めよ。

(2.5) **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)。 $\square$

(2.6) **例** (1) 上の命題を用いて、$\Phi_5(x)$ を求める。$x^5 - 1 = \Phi_5(x)\Phi_1(x)$ だから、

$$\Phi_5(x) = \frac{x^5-1}{\Phi_1(x)} = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$$

(2) 上の命題を用いて、$\Phi_{10}(x)$ を求める。$x^{10}-1 = \Phi_{10}(x)\Phi_5(x)\Phi_2(x)\Phi_1(x)$ だから、

$$\begin{aligned}\Phi_{10}(x) &= \frac{x^{10}-1}{\Phi_5(x)\Phi_2(x)\Phi_1(x)} = \frac{x^{10}-1}{\Phi_5(x)\Phi_1(x)\cdot\Phi_2(x)} \\ &= \frac{x^{10}-1}{(x^5-1)\cdot(x+1)} = \frac{x^5+1}{x+1} = x^4 - x^3 + x^2 - x + 1\end{aligned}$$

(2.7) **問題** (2.5) を用いて、円周等分多項式 $\Phi_{12}(x)$, $\Phi_{18}(x)$ を求めよ。

(2.8) **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. モニック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、$x^n - 1$ をモニック多項式いくつかで割った Φ_n も整数係数である。 $\square$

(2.9) **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) 後述
(2) 略 □

(2.10) **問題** 上の補題の (1) を証明せよ。

円周等分多項式は $\mathbb{Q}$ 上既約であることが示せるが、まず、p が素数のときに $\Phi_p(x)$ が $\mathbb{Q}$ 上既約であることを次で示す。

(2.11) **命題 (円周等分多項式の既約性)** p が素数のとき $\Phi_p(x)$ は $\mathbb{Q}$ 上既約である。

Proof. p が素数だから、(2.5) より、$x^p - 1 = \Phi_p(x)\Phi_1(x) = \Phi_p(x)\cdot(x-1)$ である。ここで、$x = y+1$ と置き換えると、$(y+1)^p - 1 = \Phi_p(y+1)\cdot y$ となるので、

$$\Phi_p(x) = \Phi_p(y+1) = \frac{(y+1)^p - 1}{y}$$

である。この右辺の分子について、二項定理より、

$$\begin{aligned}(y+1)^p - 1 &= (y^p + \binom{p}{1}y^{p-1} + \binom{p}{2}y^{p-2} + \cdots + \binom{p}{p-1}y + 1) - 1 \\ &= y^p + \binom{p}{1}y^{p-1} + \binom{p}{2}y^{p-2} + \cdots + \binom{p}{p-1}y\end{aligned}$$

である。よって、

$$\Phi_p(x) = \Phi_p(y+1) = y^{p-1} + \binom{p}{1} y^{p-2} + \cdots + \binom{p}{p-1} y^0$$

となる。ここで、アイゼンシュタインの既約判定法と (2.9) (1) を用いると、$\Phi_p(x)$ は既約であるとわかる。 $\square$

(2.12) **問題** 上の証明の最後の部分、「アイゼンシュタインの既約判定法と (2.9) (1) を用いると、$\Phi_p(x)$ は既約であるとわかる」のはなぜか説明せよ。

(2.13) **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 $(0 \le k \le n-1)$ 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 $k \ge 2$ 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

この節では、正多角形が作図可能であるための必要十分条件をまとめる。十分条件については、証明なしに紹介するに留める。

(3.1) **定理 (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) **問題** 円周等分多項式や、(1.2)、(1.4) あたりを参考にして、上の定理を証明せよ。

(3.3) **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。

(3.4) **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 $\boldsymbol{F}$**-同型写像**であるといい、E_1 と E_2 は $\boldsymbol{F}$**-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 $\boldsymbol{F}$**-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. まず、写像 $\phi : F(\alpha) \to F(\beta)$ ($g \in F[x]$ に対して $g(\alpha) \mapsto g(\beta)$) が、well-defined であることを示す。

α が代数的なので $F(\alpha) = F[\alpha]$ であるから、$F(\alpha)$ の元は、ある多項式 $g \in F[x]$ に対して、$g(\alpha)$ と表せる。多項式 $g, h \in F[x]$ に対して、$g(\alpha) = h(\alpha)$ とすると、$g(x) - h(x)$ は α を根に持つので、最小多項式 $f(x)$ で割り切れる。従って、β の最小多項式も $f(x)$ だから $g(x) - h(x)$ は β も根に持つ。よって、$g(\beta) = h(\beta)$ なので、ϕ は well-defined である。

写像 ϕ が、(H1)–(H3) を満たすこと、全単射であること、F 上恒等写像であることは、どれも簡単であるから ϕ は F-同型である。 $\square$

(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。

【ヒント】単射であることと核が 0 であることが同値であることを用いる。

イデアルを学んでいれば、核が 0 であることは次のように証明できる。$\mathrm{Ker}\,\phi$ 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。

また、イデアルの知識がなくても次のように証明できる。$\mathrm{Ker}\,\phi$ が 0 でないと仮定して、0 でない $a \in \mathrm{Ker}\,\phi$ をとったとして、$\phi(aa^{-1})$ を 2 通りに計算して矛盾を導けばよい。

(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、

$$\#\,\mathrm{Aut}_F(E) = \#\{a \in E \mid f(a)=0\} \tag{2}$$

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、$\mathrm{Aut}(E)$, $\mathrm{Aut}_F(E)$ は写像の合成に関して群をなすことを示せ。

【ヒント】G が群であるとは、G 上に演算が定義されていて、

(G1) $(xy)z = x(yz)$ $(x,y,z \in G)$

(G2) 単位元 e が存在 $(ex = xe = e$ $(x \in G))$

(G3) $x \in G$ に対して逆元 x^{-1} が存在 $(xx^{-1} = x^{-1}x = e)$

を満たすことであった。

演算が定義されていることについては、$\phi, \psi \in \mathrm{Aut}(E)$ に対し、合成写像 $\phi \circ \psi$ が再び $\mathrm{Aut}(E)$ に属することを言えばよい。つまり、以下を示せばよい。

(H1) $\phi \circ \psi(1) = 1$
(H2) $\phi \circ \psi(x + y) = \phi \circ \psi(x) + \phi \circ \psi(y)$ $(x, y \in E)$
(H3) $\phi \circ \psi(xy) = \phi \circ \psi(x)\phi \circ \psi(y)$ $(x, y \in E)$

単位元については、恒等写像が単位元である。

逆元については、$\phi \in \mathrm{Aut}(E)$ に対して、これは全単射だから逆写像 ϕ^{-1} が存在するが、この ϕ^{-1} が上の (H1)–(H3) を満たすことを言えばよい。

(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 $F(\alpha)$ を部分体に持つような代数閉体とするとき、

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

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) も参照)。例えば、$1 + 2i \in \mathbb{C}$ を考えたとき、$\mathbb{R}$ 上の最小多項式は、$x^2 - 2x + 5$ である。この根は、$1 \pm 2i$ であり、両方とも $\mathbb{C}$ に属する。このようなことが、すべての $a + bi \in \mathbb{C}$ に言えることが、正規拡大の条件である。

(2) $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ は正規拡大ではない。なぜなら、$\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$ の $\mathbb{Q}$ 上の最小多項式 $x^3 - 2$ の他の 2 根は虚数解なので、$\mathbb{R}$ の部分体であり、虚数を含まない $\mathbb{Q}(\sqrt[3]{2})$ に属さないからである。

(3) 2 次拡大は正規拡大である。なぜなら F の 2 次拡大 E に属する元 $\alpha \in E$ は (高々) 2 次方程式の根であるから、$x^2 + sx + t$ $(s, t \in F)$ の根になるが、もう 1 つの根を β とすると、解と係数の関係より、

$$\begin{aligned} \alpha + \beta &= -s, \\ \alpha\beta &= t \end{aligned}$$

なので、特に、$\beta = -s - \alpha \in E$ である。

(4) 従って、$\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ は正規拡大である。(1) の $\mathbb{C} \supset \mathbb{R}$ が正規拡大であることも、(3) よりわかる。

(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 (これは F が標数 0 ならば常に成立。後述)。このとき、E の $\mathrm{Aut}_F(E)$-不変部分体

$$E^{\mathrm{Aut}_F(E)} = \{\alpha \in E \mid \phi(\alpha) = \alpha\ (\phi \in \mathrm{Aut}_F(E))\}$$

は F に等しい。

∗ $E^{\mathrm{Aut}_F(E)} \supset F$ は $\mathrm{Aut}_F(E)$ の定義よりわかる。

Proof. $E^{\mathrm{Aut}_F(E)} \subset F$ 示せばよいので、$\alpha \in E^{\mathrm{Aut}_F(E)}$ を仮定して $\alpha \in F$ を示せばよい。対偶をとり、$\alpha \notin F$ を仮定して $\alpha \notin E^{\mathrm{Aut}_F(E)}$ であることを示す。

$\alpha \notin F$ とすると、α の F 上の最小多項式の次数は 2 以上である。α の最小多項式には重根がないので、別の根 β が存在し、正規拡大なので $\beta \in E$ である。(4.2) のようにして、F-同型 ϕ を $\phi : F(\alpha) \to F(\beta)$ $(g(\alpha) \mapsto g(\beta)$, g は F 上の多項式) と定めると、$\phi(\alpha) = \beta$ なので、α を固定しない F-同型

ϕ が得られ、これは E の F-同型に拡張される (シュタイニッツの定理を用いる。詳細は省略する)。

この同型も ϕ で表すと、$\phi \in \mathrm{Aut}_F(E)$ である。α は $\phi \in \mathrm{Aut}_F(E)$ で固定されないので、$\alpha \notin E^{\mathrm{Aut}_F(E)}$ である。以上により、$E^{\mathrm{Aut}_F(E)} \subset F$ が示された。 $\square$

(5.4) **注意** 1 を何度加えると 0 になるかを、体の**標数**と呼ぶ。$\mathbb{C}$ やその部分体のように、1 を何度加えても 0 にならない場合は標数は 0 とする。例えば、$\mathbb{F}_2 = \mathbb{Z}/(2)$ は標数 2 である。

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、$f(x) \in F[x]$ を既約多項式であり、かつ、適当な拡大体で $f(x)$ が重根 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だから、$f(x)$ は重根を持たないとわかった。

体の標数が 0 ではない場合で、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。実際、根は $\pm i$ (i は虚数単位) だから、分解体は、$\mathbb{R}(i,-i)=\mathbb{R}(i)=\mathbb{C}$ である。

(2) $\mathbb{Q}$ 上 x^2-2 の分解体は $\mathbb{Q}(\sqrt{2})$ である。実際、根は $\pm\sqrt{2}$ だから、分解体は、$\mathbb{Q}(\sqrt{2},-\sqrt{2})=\mathbb{Q}(\sqrt{2})$ である。

(3) $\mathbb{Q}$ 上 x^3-1 の分解体は $\mathbb{Q}(\omega)$ である。ただし $\omega=(-1+\sqrt{-3})/2$。実際、$x^3-1=(x-1)(x^2+x+1)$ より、根は、$1,\omega,\omega^2$ (これらは 1 の 3 乗根) だから、分解体は、$\mathbb{Q}(1,\omega,\omega^2)=\mathbb{Q}(\omega)$ である。

(6.3) 問題 次の多項式の $\mathbb{Q}$ 上の分解体を求めよ。

(1) x^2-3

(2) x^4-4

(6.4) 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 E に属することに注意すれば、$f=f_1f_2\cdots f_r$ と定めると、f のすべての根は E に属するから、f の分解体は E に含まれる。

また、f の根には、$\alpha_1,\dots,\alpha_r$ がすべて含まれるから、f の分解体は $E=F(\alpha_1,\dots,\alpha_r)$ を含む。よって、f の分解体は E に等しい。

十分性。E が、ある多項式 $f(x)\in F[x]$ の分解体であるとする。$\alpha\in E$ とし、同じ最小多項式を持つ β をとる。F-同型 $F(\alpha)\to F(\beta)$ ($\alpha\mapsto\beta$) は $\phi\colon E\to E'$ に拡張される (E' は $F(\beta)$ を含むある体。シュタイニッツの定理を使えばよいが詳細は省略)。ϕ は F-同型だから f を変えず、従って f の根を f の根に写すから、$E'=\phi(E)\subset E$。特に、$\beta=\phi(\alpha)\in\phi(E)\subset E$ だ

から、α の最小多項式のすべての根は E に属することになり、$E \supset F$ は正規拡大である。 $\square$

(6.5) **問題** この節で触れたもの以外に正規拡大を 1 つあげ、正規拡大である理由を述べよ。

§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** (または、**可換群**) と呼ぶ。

(7.2) **例** (1) $G = \{e\}$
(2) 次の群はすべて**位数** (群の要素の数) が 2 であり、かつ、乗積表も一致するから同型な群である。
$G = \{e, \sigma\}$ $(\sigma^2 = e)$

$G = \mathbb{Z}/(2)$

$G = \{1, -1\}$

(3) $\mathbb{Z}/(3)$ と $\mathbb{Z}/(4)$ の乗積表 (演算は和なので、実際には乗積でなく和の表) は、それぞれ次のようになる。

$$\begin{array}{c|ccc} + & \overline{0} & \overline{1} & \overline{2} \\ \hline \overline{0} & \overline{0} & \overline{1} & \overline{2} \\ \overline{1} & \overline{1} & \overline{2} & \overline{0} \\ \overline{2} & \overline{2} & \overline{0} & \overline{1} \end{array} \qquad \begin{array}{c|cccc} + & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \hline \overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{0} \\ \overline{2} & \overline{2} & \overline{3} & \overline{0} & \overline{1} \\ \overline{3} & \overline{3} & \overline{0} & \overline{1} & \overline{2} \end{array}$$

(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。実際、$\overline{1}$ を含む群があれば、和で閉じていることから、$\overline{1} + \overline{1} = \overline{2}$ を含み、$\mathbb{Z}/(3)$ 全体に一致してしまう。また、$\overline{2}$ を含む群も、同様にして、$\mathbb{Z}/(3)$ 全体に一致してしまう。
(3) $\mathbb{Z}/(4)$ の非自明な部分群は $\{\overline{0}, \overline{2}\}$ のみである。これも、(2) と同様にして、$\overline{1}$ や $\overline{3}$ を含む場合は全体に一致してしまうからである。

(7.5)　**問題**　4 次対称群 S_4 の置換を

$$\alpha = (12)(34), \qquad \beta = (13)(24), \qquad \gamma = (14)(23)$$

と置く。
(1) $G = \{e, \alpha, \beta, \gamma\}$ は S_4 の部分群であることを示せ。
(2) G の非自明な部分群は、$H_1 = \{e, \alpha\}$, $H_2 = \{e, \beta\}$, $H_3 = \{e, \gamma\}$ の 3 つであることを示せ。

(7.6)　**問題**　$G = \mathbb{Z}/(6)$ の部分群をすべて決定せよ。

(7.7)　**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、位数は無限大と定める。

　$\{e, g, g^2, \ldots, g^{n-1}\}$ 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。

(7.8)　**例**　(1) 位数が 1 である元は単位元のみである。
(2) $\mathbb{Z}/(m) = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ を考える。$\overline{1} \in \mathbb{Z}/(4)$ の位数は 4 であり、$\overline{2} \in \mathbb{Z}/(4)$ の位数は 2 である。
　$\mathbb{Z}/(m)$ は巡回群であり、$\mathbb{Z}/(m) = \langle \overline{1} \rangle$ である。
(3) 5 次対称群 S_5 の元 $\sigma = (12)(345)$ の位数は 6 であり、$\langle \sigma \rangle = \{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^5\} = \{\mathrm{id}, (12)(345), (354), (12), (345), (12)(354)\}$ である。

(7.9)　**問題**　3 次対称群のすべての元について、その位数を求めよ。

(7.10)　**例 (部分群の決定)**　$G = S_3$ の非自明な部分群は、$\langle (12) \rangle$, $\langle (23) \rangle$, $\langle (13) \rangle$, $\langle (123) \rangle$ であることが以下のようにしてわかる。

後述の (7.13) により、部分群の位数は 1、2、3、6 のいずれかであることがわかるから、非自明な部分群の位数は 2、3 のいずれかであるので、このことを用いて部分群を決定する。

まず、位数 2 の部分群は、単位元ともう 1 つの元からなる。単位元以外の元は位数 2 でなくてはならないので、$\langle(12)\rangle, \langle(23)\rangle, \langle(13)\rangle$ に限られることがわかる。

次に位数 3 の部分群を考える。$\langle(123)\rangle = \{e, (123), (132)\}$ は位数 3 の部分群であるが、その他にないことを示す。もしも、部分群が (123) を含めば、その部分群は $\langle(123)\rangle$ を含み、部分群が (132) を含む場合もその部分群は $\langle(123)\rangle$ を含むから、(123) または (132) を含む位数 3 の部分群は $\langle(123)\rangle$ に限られる。

従って、残る可能性としては、$e, (12), (23), (13)$ から、単位元を含む 3 つの元を選んで位数 3 の部分群を作れるかということが問題になる。ところが、

$$(12)(23) = (123), \qquad (12)(13) = (132), \qquad (23)(13) = (123)$$

なので、どのように 3 つの元を選んでも、積で閉じることはできないから、位数 3 の部分群は作れない。

以上により、$G = S_3$ の非自明な部分群は、$\langle(12)\rangle, \langle(23)\rangle, \langle(13)\rangle, \langle(123)\rangle$ の 4 通りである。

(7.11) **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。

(7.12) **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、

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

(7.13) **定理** [ラグランジュの定理] 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。つまり、H の要素数に等しい。
(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。

Proof. (1) $g_1H \cap g_2H$ が空集合ではないと仮定し、$g_1H = g_2H$ を示せばよい。$g_1H \cap g_2H$ が空集合ではないので、$x \in g_1H \cap g_2H$ を取れる。すると、$h_1, h_2 \in H$ を用いて、$x = g_1h_1 = g_2h_2$ と表せるから、$g_1 = g_2h_2h_1^{-1}$ である。

$g_1h \in g_1H$ を取ったとき、$g_1h = g_2h_2h_1^{-1}h \in g_2H$ だから、$g_1H \subset g_2H$ である。逆の包含関係も同様であるから、$g_1H = g_2H$ である。

(2) $f : g_1H \to g_2H$ $(g_1h \mapsto g_2h)$ と定めると全単射になるので、要素の数は等しい。剰余類のうち 1 つは $eH = H$ であるから、どの剰余類も要素の数が H と等しい。

(3) G は、H を法とする剰余類で共通部分のない和集合に分類される。

$$G = g_1H \cup g_2H \cup \cdots \cup g_kH$$

(2) によりどの剰余類も要素の数は H と等しいから、G の位数は H の位数の倍数である。

(4) $g \in G$ で生成される巡回群 $\langle g \rangle$ は、位数が g の位数に等しい G の部分群であるから、(3) より g の位数は G の位数の約数である。 □

(7.14) **系** 位数が素数 p である群は巡回群であり、非自明な部分群はない。

(7.15) **問題** 上の系を証明せよ。【ヒント】単位元以外の元の位数が p であることを示し、これを用いる。

§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) 例 (1) $\mathbb{Q}$ 上 x^2-2 のガロア群は、位数 2 の群 $\{e,\sigma\}$ $(\sigma^2=e)$ である。

実際、$f=x^2-2$ の $\mathbb{Q}$ 上の分解体は、$\mathbb{Q}(\sqrt{2})$ だから、$Gal(f)=\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))$ である。(4.5) より、$Gal(f)$ は 2 つの元からなることがわかる。そのうち 1 つは恒等写像 $e=\mathrm{id}$ であるが、(4.3) (2) により、もう 1 つは、$\sigma : a+b\sqrt{2}\mapsto a-b\sqrt{2}$ であることがわかる。$\sigma^2=e$ だから、$Gal(f)=\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))=\{e,\sigma\}$ $(\sigma^2=e)$ である。

(2) $\mathbb{Q}$ 上 x^4-10x^2+1 のガロア群は、$\{e,\sigma,\tau,\sigma\tau\}$ $(\sigma^2=\tau^2=e,\sigma\tau=\tau\sigma)$ である。これを以下で示す。

$f=x^4-10x^2+1$ の根を求めると、まず、$(x^2)^2-10(x^2)+1=0$ を解いて、$x^2=5\pm2\sqrt{6}$ となり、二重根号を外して平方根をとれば、$x=\pm(5\pm2\sqrt{6})=\pm\sqrt{2}\pm\sqrt{3}$ (複号任意) である。よって、f の分解体は、

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

である。代数学 3 でも見たが、$\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$ なので、$\mathbb{Q}(\sqrt{2}+\sqrt{3})\supset\mathbb{Q}$ は 4 次拡大であり、f は $\sqrt{2}+\sqrt{3}$ の最小多項式であることもわかる。

従って、求めるガロア群は、$Gal(f)=\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}+\sqrt{3}))$ である。$E\supset F$ が単項拡大の場合の $\mathrm{Aut}_F(E)$ は、(4.5) によりわかり、その元は、$\sqrt{2}+\sqrt{3}$ を、その最小多項式 f の 4 つの根に写す 4 通りである。つまり、

$$\phi_1:\sqrt{2}+\sqrt{3}\mapsto\sqrt{2}+\sqrt{3}\qquad\phi_2:\sqrt{2}+\sqrt{3}\mapsto\sqrt{2}-\sqrt{3}$$
$$\phi_3:\sqrt{2}+\sqrt{3}\mapsto-\sqrt{2}+\sqrt{3}\qquad\phi_4:\sqrt{2}+\sqrt{3}\mapsto-\sqrt{2}-\sqrt{3}$$

で定まる 4 通りである。これらを、よりわかり易く整理すれば、

$$\begin{aligned}
\phi_1 &: \sqrt{2} \mapsto \sqrt{2}, & \sqrt{3} &\mapsto \sqrt{3} \\
\phi_2 &: \sqrt{2} \mapsto \sqrt{2}, & \sqrt{3} &\mapsto -\sqrt{3} \\
\phi_3 &: \sqrt{2} \mapsto -\sqrt{2}, & \sqrt{3} &\mapsto \sqrt{3} \\
\phi_4 &: \sqrt{2} \mapsto -\sqrt{2}, & \sqrt{3} &\mapsto -\sqrt{3}
\end{aligned}$$

となる。これは、$\alpha = \sqrt{2} + \sqrt{3}$ と置けば、$\sqrt{2} = (\alpha - \alpha^{-1})/2$ なので、$\phi_2(\sqrt{2}) = \phi_2((\alpha - \alpha^{-1})/2) = (\phi_2(\alpha) - \phi_2(\alpha)^{-1})/2$ などと計算することで求められる。

従って、$e = \phi_1$, $\sigma = \phi_2$, $\tau = \phi_3$ と置けば、$Gal(f) = \{e, \sigma, \tau, \sigma\tau\}$ ($\sigma^2 = \tau^2 = e$, $\sigma\tau = \tau\sigma$) であることがわかる。

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

(2) $\mathbb{R}$ 上 $x^2 + x + 1$ 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。

【ヒント】(1) は前の例の (1) と同様である。(2) は、$\mathbb{R}$ 上 $f = x^2 + x + 1$ が既約なので、その根 ω, ω^2 の最小多項式は f であることがわかる。よって、(4.5) を用いることができる。(3) は前の例の (2) と同様にすればよい。

(8.4) **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。 □

§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。

＊ このとき (5.3) が使える。

(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)。

特に、標数 0 の場合は、ガロア拡大と正規拡大は同じ概念である。また、正規拡大は、ある多項式による分解体と同じであった。

(10.2)　**例**　$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbb{Q}$ はガロア拡大である。実際、$f = x^4 - 10x^2 + 1$ の分解体だからと思ってもよいし、$g = (x^2 - 2)(x^2 - 3)$ の分解体だからと思ってもよい。

(10.3)　**問題**　ガロア拡大の例を 1 つあげよ。

(10.4) 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 上の F-自己同型群 $\mathrm{Aut}_F(E)$ 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 (10.4) 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。

(11.2) 例 (1) 体の拡大 $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ は、2 次拡大だから正規拡大であり、標数 0 なので、ガロア拡大である。(8.2) (1) にもあるように、$Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = \{e, \sigma\}$ ($\sigma^2 = e$) である。

(2) $x^4 - 4$ の $\mathbb{Q}$ 上の分解体を E とすると、以下で示すように、$Gal(E/\mathbb{Q}) = \{e, \sigma, \tau, \sigma\tau\}$ ($\sigma^2 = \tau^2 = e$, $\sigma\tau = \tau\sigma$) である。

虚数単位を i とすると、$x^4 - 4 = (x^2 - 2)(x^2 + 2) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{2}i)(x + \sqrt{2}i)$ だから、

$$E = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{2}i, -\sqrt{2}i) = \mathbb{Q}(\sqrt{2}, \sqrt{2}i)$$

である。$E \supset \mathbb{Q}$ は、分解体だから正規拡大であり、標数 0 だからガロア拡大である。

ガロア群 $Gal(E/\mathbb{Q})$ の元は、$x^4 - 4$ の 4 根の置換と見なせるから、4 根 $\pm\sqrt{2}, \pm\sqrt{2}i$ それぞれの写り先を決めれば定まる。

ガロア群 $Gal(E/\mathbb{Q})$ の元のひとつを ϕ とする。まず、ϕ による $\sqrt{2}$ の写り先を β とすると、写像は $\mathbb{Q}$-同型であるから、$\sqrt{2}$ の像を β とすると $(\sqrt{2})^2$ の像は β^2 であり、$2 \in \mathbb{Q}$ の像は 2 なので、$\beta^2 = 2$ である。よって、$\sqrt{2}$ の像は、4 根のうち $\pm\sqrt{2}$ の 2 通りに限られる。

次に $-\sqrt{2}$ の像は、

$$\phi(-\sqrt{2}) = \phi(-1)\phi(\sqrt{2}) = -\phi(\sqrt{2}) = -\beta$$

だから、$\sqrt{2}$ の像が決まれば選択の余地はない。

同様にして、$\sqrt{2}i$ の像を $\gamma = \phi(\sqrt{2}i)$ とすると、γ は $\pm\sqrt{2}i$ に限られ、$-\sqrt{2}i$ の像は自動的に $-\gamma$ になることもわかる。

以上より、単なる 4 根の置換ならば 24 通りあるが、ガロア群 $Gal(E/\mathbb{Q})$ の元は 4 通りしかないことがわかった。よって、

$$\begin{aligned} &e = \mathrm{id}_E \quad (E \text{ 上の恒等写像}) \\ &\sigma : E \to E \quad (\sqrt{2} \mapsto -\sqrt{2},\ \sqrt{2}i \mapsto \sqrt{2}i) \\ &\tau : E \to E \quad (\sqrt{2} \mapsto \sqrt{2},\ \sqrt{2}i \mapsto -\sqrt{2}i) \end{aligned}$$

と定めると、

$$Gal(E/\mathbb{Q}) = \{e, \sigma, \tau, \sigma\tau\}$$

である。

(11.3)　**問題**　(1) 体の拡大 $\mathbb{C} \supset \mathbb{R}$ がガロア拡大である理由を述べ、ガロア群を求めよ。

(2) 体の拡大 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbb{Q}$ がガロア拡大である理由を述べ、ガロア群を求めよ。

§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。

Proof. (1) $E \supset L$ が正規拡大であることを示す。$\alpha \in E$ の L 上の最小多項式を $f(x) \in L[x]$ とし、F 上の最小多項式を $g(x) \in F[x]$ とする。f と g を L 上の多項式と見たとき、ともに α を根に持ち f は既約だから、f は g を割り切る。従って、f の根は g の根でもあり、$E \supset F$ が正規拡大だから、g の根は E の元である。よって、$E \supset L$ は正規拡大である。

また、$E \supset F$ が分離拡大なので、g は重根を持たず、その因数である f も重根を持たないから、$E \supset L$ も分離拡大である。

以上より、$E \supset L$ はガロア拡大である。

(2) 前半は (10.4) (2) からわかる。

後半は、(5.3) より、$L = E^{\mathrm{Aut}_L(E)}$ だから、前半の式を用いると、$[E : L] = [E : E^{\mathrm{Aut}_L(E)}] = \#\,\mathrm{Aut}_L(E)$ となり、(1) より、これは $\#Z_G(L)$ に等しい。

(3) $Z_G(E^H) \supset H$ は定義により明らかで、(2) より、$\#Z_G(E^H) = [E : E^H] = \#H$ なので、$Z_G(E^H) = H$ である。

また、(1) より $Z_G(L) = Gal(E/L) = \mathrm{Aut}_L(E)$ なので、(5.3) より、$E^{Z_G(L)} = E^{\mathrm{Aut}_L(E)} = L$ である。

(4) 略 □

(12.2) **例** ガロア群の部分群と、中間体の 1 対 1 対応の例を見てみる。

(1) $\mathbb{C} \supset \mathbb{R}$ を考えると、$Gal(\mathbb{C}/\mathbb{R}) = \{e, \sigma\}$ $(\sigma^2 = e)$ であり、$Gal(\mathbb{C}/\mathbb{R})$ には非自明な部分群がない。よって、$\mathbb{C} \supset \mathbb{R}$ には、真の中間体がない。

ただし、これは拡大次数の連鎖律からもわかることである。

(2) $\mathbb{Q}(\sqrt{2},\sqrt{3}) \supset \mathbb{Q}$ を考える。(8.2) (2) より、ガロア群は $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \{e,\sigma,\tau,\sigma\tau\}$ ($\sigma^2 = \tau^2 = e$, $\sigma\tau = \tau\sigma$) であった。ただし、σ は $\sqrt{3}$ を -1 倍する写像、τ は $\sqrt{2}$ を -1 倍する写像である。

$Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ の非自明な部分群は、$H_1 = \{e,\sigma\}$, $H_2 = \{e,\tau\}$, $H_3 = \{e,\sigma\tau\}$ の 3 つである (後述の問題) から、$\mathbb{Q}(\sqrt{2},\sqrt{3}) \supset \mathbb{Q}$ の真の中間体も 3 つであり、それらは、それぞれ、H_1, H_2, H_3 の不変部分体である。$\mathbb{Q}(\sqrt{2},\sqrt{3})$ の元は、$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ ($a,b,c,d \in \mathbb{Q}$) と表せることから、真の中間体は、

$$\mathbb{Q}(\sqrt{2},\sqrt{3})^{H_1} = \mathbb{Q}(\sqrt{2}),$$
$$\mathbb{Q}(\sqrt{2},\sqrt{3})^{H_2} = \mathbb{Q}(\sqrt{3}),$$
$$\mathbb{Q}(\sqrt{2},\sqrt{3})^{H_3} = \mathbb{Q}(\sqrt{6})$$

だとわかる。

(3) x^3-2 の $\mathbb{Q}$ 上の分解体を E とし、ガロア拡大 $E \supset \mathbb{Q}$ を考え、真の中間体を求めてみる $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$ ($\omega = (-1+\sqrt{3}i)/2$) だから、(8.4) より $Gal(E/\mathbb{Q})$ は、これら 3 根の置換からなる 3 次対称群 S_3 の部分群である。

また、$E = \mathbb{Q}(\sqrt[3]{2},\omega)$ なので、$\mathbb{Q}(\sqrt[3]{2},\omega) \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ に連鎖律を用いると、$[E:\mathbb{Q}] = 6$ とわかる。従って、(12.1) (2) の後半と (1) より、$\#Gal(E/\mathbb{Q}) = 6$ とわかるので、$Gal(E/\mathbb{Q}) = S_3$ である。

各置換が $\sqrt[3]{2}$ と ω を何に写すか、具体的に見てみる (中間体を求めるだけならば、ここまで具体的に像を計算する必要はないが)。まず、(12) は、$\alpha_1 = \sqrt[3]{2}$ と $\alpha_2 = \sqrt[3]{2}\omega$ を交換するので、$\sqrt[3]{2}$ の像は $\sqrt[3]{2}\omega$ であり、$\omega = \alpha_2/\alpha_1$ の (12) による像は、$\alpha_1/\alpha_2 = \omega^{-1} = \omega^2$ である。次に、(23) は、$\alpha_2 = \sqrt[3]{2}\omega$ と $\alpha_3 = \sqrt[3]{2}\omega^2$ を交換するので、$\omega = \alpha_3/\alpha_2$ を $\alpha_2/\alpha_3 = \omega^{-1} = \omega^2$ に写す。$\sqrt[3]{2} = \alpha_2/\omega$ は、$\alpha_3/\omega^2 = \sqrt[3]{2}$ に写す。また、(123) は、$\sqrt[3]{2} = \alpha_1$ を $\alpha_2 = \sqrt[3]{2}\omega$ に写し、$\omega = \alpha_2/\alpha_1$ を $\alpha_3/\alpha_2 = \omega$ に写す。このようにして他の

置換についても計算すると、次のようになる。

置換	e	(12)	(23)	(13)	(123)	(132)
$\sqrt[3]{2}$ の像	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
ωの像	ω	ω^2	ω^2	ω^2	ω	ω

(7.10) により、S_3 の非自明な部分群は、$H_1 = \langle(23)\rangle$, $H_2 = \langle(13)\rangle$, $H_3 = \langle(12)\rangle$, $H_4 = \langle(123)\rangle$ の 4 つであった。従って、$E \supset \mathbb{Q}$ の真の中間体も 4 つある。まず、E^{H_1} について、$\#H_1 = 2$ だから、$[E : E^{H_1}] = 2$ であり、従って、$[E^{H_1} : \mathbb{Q}] = 3$ である。$\alpha_1 = \sqrt[3]{2} \in E$ は H_1 で固定されるので、$\sqrt[3]{2} \in E^{H_1}$ であり、これより、$\mathbb{Q}(\sqrt[3]{2}) \subset E^{H_1}$ である。しかし、$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ だから、$E^{H_1} = \mathbb{Q}(\sqrt[3]{2})$ である。

次に、E^{H_4} について、上と同様にして、$[E^{H_4} : \mathbb{Q}] = 2$ がわかる。また、上の表から、(123) は ω を固定するので、$\mathbb{Q}(\omega) \subset E^{H_4}$ であるが、$[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ なので、$E^{H_4} = \mathbb{Q}(\omega)$ である。

(12.3)　**問題**　(1) 群 $G = \{e, \sigma, \tau, \sigma\tau\}$ $(\sigma^2 = \tau^2 = e,\ \sigma\tau = \tau\sigma)$ の非自明な部分群は、$H_1 = \{e, \sigma\}$, $H_2 = \{e, \tau\}$, $H_3 = \{e, \sigma\tau\}$ の 3 つであることを示せ。

(2) 上の例の (3) の表において、(13) と (132) による像は計算なしに記しているので、これらを計算せよ。

(3) 上の例の (3) について、中間体 E^{H_2} と E^{H_3} を計算せよ。

(4) $x^4 - 4$ の $\mathbb{Q}$ 上の分解体を E とするとき、ガロア拡大 $E \supset \mathbb{Q}$ の真の中間体をすべて求めよ。

(12.4)　**問題**　(1) $x^n - 1$ の $\mathbb{Q}$ 上の分解体を E とするとき、$\#Gal(E/\mathbb{Q}) = \phi(n)$ であることを示せ。

(2) x^5-1 の $\mathbb{Q}$ 上の分解体を E とするとき、$Gal(E/\mathbb{Q})$ が位数 4 の巡回群であることを示せ。【ヒント】偏角が $2\pi/5$ である 1 の原始 5 乗根を ζ とすると、(4.5) やその証明により、4 つの $\mathbb{Q}$-同型 ϕ_i $(i=1,2,3,4)$ は、ζ を ζ^i に写すもので与えられる。そして、例えば ϕ_2 のベキで、すべての ϕ_i $(i=1,2,3,4)$ が得られることを言えばよい。

(3) (2) の $E\supset\mathbb{Q}$ の真の中間体を求めよ。

(12.5)　**定義**　$\alpha_1,\alpha_2,\ldots,\alpha_n$ の**基本対称式** $e_1,e_2,\ldots,e_n$ を次で定める。

$$
\begin{aligned}
e_1 &= \alpha_1+\alpha_2+\cdots+\alpha_n,\\
e_2 &= \alpha_1\alpha_2+\cdots+\alpha_1\alpha_n\\
&\quad +\alpha_2\alpha_3+\cdots+\alpha_2\alpha_n\\
&\quad +\alpha_3\alpha_4+\cdots+\alpha_3\alpha_n+\cdots+\alpha_{n-1}\alpha_n,\\
&\ \vdots\\
e_n &= \alpha_1\alpha_2\cdots\alpha_n
\end{aligned}
$$

(12.6)　**定理**　体 F 上の一般の n 次多項式 (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。

特に、$\alpha_1,\alpha_2,\ldots,\alpha_n$ を変数とし、これらの基本対称式を $e_1,e_2,\ldots,e_n$ とするとき、

$$F(\alpha_1,\ldots,\alpha_n)^{S_n}=F(e_1,\ldots,e_n)$$

である。

Proof. $\alpha_1,\alpha_2,\ldots,\alpha_n$ を F 上の変数とし、$E=F(\alpha_1,\ldots,\alpha_n)$ と置き、$\alpha_1,\ldots,\alpha_n$ の基本対称式 $e_1,\ldots,e_n$ を用いて、$L=F(e_1,\ldots,e_n)$ と置く。

一般の n 次多項式を $f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ とすると、

$$\begin{aligned}f(x)&=x^n-(\alpha_1+\cdots+\alpha_n)x^{n-1}+\cdots\\&\qquad\cdots+(-1)^{n-1}(\alpha_1\cdots\alpha_{n-1}+\cdots+\alpha_2\cdots\alpha_n)x+(-1)^n\alpha_1\alpha_2\cdots\alpha_n\\&=x^n-e_1x^{n-1}+\cdots+(-1)^{n-1}e_{n-1}x+(-1)^ne_n\end{aligned}$$

なので、$f\in L[x]$ である。よって、f の L 上の分解体が E となるので、$E\supset L$ はガロア拡大であり、示すべきことは、$Gal(E/L)=S_n$ である。

　S_n は $\alpha_1,\ldots,\alpha_n$ の置換で E 上の同型として作用するが、基本対称式 $e_1,\ldots,e_n$ を変えないから、L 上恒等写像であり、$Gal(E/L)$ の元を与える。さらに、異なる置換は異なる L-同型を与えることも容易だから、$\#Gal(E/L)\geq\#S_n$ である。また、(8.4) より、$Gal(E/L)\subset S_n$ なので、$Gal(E/L)=S_n$ である。 $\square$

(12.7)　**定理**　F を体、$\alpha_1,\alpha_2,\ldots,\alpha_n$ を変数とし、$e_1,e_2,\ldots,e_n$ を基本対称式とする。多項式環 $F[\alpha_1,\alpha_2,\ldots,\alpha_n]$ に n 次対称群 S_n が変数の置換で作用するとき、S_n-不変な多項式全体 (つまり対称式全体) は、基本対称式の多項式で表せる。つまり、

$$F[\alpha_1,\alpha_2,\ldots,\alpha_n]^{S_n}=F[e_1,e_2,\ldots,e_n]$$

である。

　＊高校までの例で言えば、$\alpha^2+\beta^2$ のような対称式が、$(\alpha+\beta)^2-2\alpha\beta$ のように、$e_1=\alpha+\beta$ と $e_2=\alpha\beta$ で表せることである。

Proof. e_i は対称式なので S_n-不変であるから、$e_i\in F[\alpha_1,\alpha_2,\ldots,\alpha_n]^{S_n}$ $(i=1,2,\ldots,n)$ なので、$F[\alpha_1,\ldots,\alpha_n]^{S_n}\supset F[e_1,\ldots,e_n]$ は言える。

　逆を示す。対称式 $f\in F[\alpha_1,\ldots,\alpha_n]^{S_n}$ をとる。S_n の元で f を写したとき、各単項式の次数は変わらないので、f の斉次成分は対称式である。よって、f を d 次斉次式としてよい。

n と d に関する帰納法で示す。$n=1$ の場合と $d=0$ の場合は定理は明らかである。

$n \geq 1$ と $d \geq 1$ が与えられたとき、n 未満の場合や、d 未満の場合は定理が成立していると仮定する。f に $\alpha_n = 0$ を代入すると、$\alpha_1, \ldots, \alpha_{n-1}$ に関する対称式になるから、帰納法の仮定より、F 上の $n-1$ 変数多項式 A を用いて、

$$f(\alpha_1, \ldots, \alpha_{n-1}, 0) = A(e'_1, \ldots, e'_{n-1})$$

と表せる。ただし、e'_i $(i = 1, \ldots, n-1)$ は $\alpha_1, \ldots, \alpha_{n-1}$ に関する基本対称式である。

$f(\alpha_1, \ldots, \alpha_n) - A(e_1, \ldots, e_{n-1})$ は対称式であり、$\alpha_n = 0$ を代入すると 0 であるから、$\alpha_1, \ldots, \alpha_n$ のどれに 0 を代入しても 0 になる。従ってこの式は、$e_n = \alpha_1 \cdots \alpha_n$ で割り切れる。

$$f(\alpha_1, \ldots, \alpha_n) - A(e_1, \ldots, e_{n-1}) = e_n B(\alpha_1, \ldots, \alpha_n)$$

と表せる。さらに、左辺が対称式なので、B は $d-n$ 次の対称式である。帰納法の仮定より、$B(\alpha_1, \ldots, \alpha_n) = C(e_1, \ldots, e_n)$ と書けるので、

$$f(\alpha_1, \ldots, \alpha_n) = A(e_1, \ldots, e_{n-1}) + e_n C(e_1, \ldots, e_n) \in F[e_1, e_2, \ldots, e_n]$$

である。 □

§13　3 次方程式の解の公式

(13.1)　**3 次方程式の簡略化**　一般の実数係数 3 次方程式 $ax^3 + bx^2 + cx + d = 0$ $(a \neq 0)$ の解の公式を与えることは、やや複雑なので、この方程式を簡単な形に変換する。

まず、$a=1$ としても一般性を失わない。次に、$y=x+\frac{b}{3}$ と置くと、この方程式は実数 A, B を用いて、$y^3+Ay+B=0$ と書ける。従って、改めて y を x に直すと、

$$x^3+Ax+B=0$$

を考えればよい。

(13.2) **定理 (判別式)** 実数係数 3 次方程式 $x^3+Ax+B=0$ の 3 解を x_1, x_2, x_3 とする。

$$\Delta=\big((x_1-x_2)(x_2-x_3)(x_1-x_3)\big)^2$$

と定め、この方程式の**判別式**と呼ぶ。このとき、

(1) $\Delta=0$ ならば、方程式は重解を持つ。
(2) $\Delta>0$ ならば、方程式は異なる 3 実解を持つ。
(3) $\Delta<0$ ならば、方程式は 1 実解と共役な 2 虚数解を持つ。
(4) $\Delta=-27B^2-4A^3$ である。

Proof. 方程式は重解を持つか、異なる 3 実解を持つか、1 実解と共役な 2 虚数解を持つかのいずれかである。

重解を持つ場合は、$\Delta=0$ になるのは明らか。異なる 3 実解を持つ場合、$\Delta>0$ であるのも明らか。

1 実解と共役な 2 虚数解を持つ場合は、$x_1\in\mathbb{R}$ とすると、x_1-x_2 と x_1-x_3 は共役であり、その積は実数である。また、x_2-x_3 は純虚数である。よって、Δ^2 は純虚数の平方だから負である。以上により、(1)、(2)、(3) は示せた。

(4) を示す。x_1, x_2, x_3 の基本対称式を e_1, e_2, e_3 とすると、Δ は 6 次の対称式であるから、$e_3^2,\ e_3e_2e_1,\ e_3e_1^3,\ e_2^3,\ e_2^2e_1^2,\ e_2e_1^4,\ e_1^6$ の $\mathbb{R}$ 上の 1 次結合

で表せるが、$e_1 = 0$ に注意すると、

$$\Delta = ke_3^2 + le_2^3$$

と表せる。$(x_1, x_2, x_3) = (1, -1, 0)$ と置くと、$\Delta = 4$, $e_2 = -1$, $e_3 = 0$ なので、$l = -4$ がわかる。また、$(x_1, x_2, x_3) = (1, \omega, \omega^2)$ と置くと、$\Delta = -27$, $e_2 = 0$, $e_3 = 1$ なので、$k = -27$ がわかる。よって、

$$\Delta = -27e_3^2 - 4e_2^3 = -27(-B)^2 - 4A^3 = -27B^2 - 4A^3$$

である。 □

(13.3) 3 次方程式の解法

■u, v **の定義** 3 次方程式 $x^3 + Ax + B = 0$ を考える。3 解を x_1, x_2, x_3 と置き、x_1, x_2, x_3 の基本対称式を e_1, e_2, e_3 と置く。このとき、$x_1 \in \mathbb{R}$ としてよく、解と係数の関係より、

$$e_1 = 0, \quad e_2 = A, \quad e_3 = -B$$

である。

1 の 3 乗根 $\omega = (1 + \sqrt{3})/2$ を用いて、

$$u = x_1 + \omega x_2 + \omega^2 x_3$$
$$v = x_1 + \omega^2 x_2 + \omega x_3$$

と置く。ここで、x_1 と x_2 を交換する作用を考えると、u は ωv に移り、v は $\omega^2 v$ に移る。他の変数の交換でも、ω の冪が変わるが同様の結果になるので、$u^3 + v^3$, u^3v^3 は x_1, x_2, x_3 の対称式である。従って、$u^3 + v^3$, u^3v^3 は、x_1, x_2, x_3 の基本対称式 e_1, e_2, e_3 で表せる。

■u^3, v^3 **の満たす方程式**　まず、u^3+v^3 は 3 次であるから、e_1^3, e_1e_2, e_3 の $\mathbb{R}$ 上の 1 次結合で表せる。しかし、$e_1=0$ なので、e_3 の定数倍である。$(x_1,x_2,x_3)=(1,\omega,\omega^2)$ と置くと、$(u,v)=(0.3)$ であることに注意すると、$u^3+v^3=ke_3=kx_1x_2x_3$ と置き、$(x_1,x_2,x_3)=(1,\omega,\omega^2)$ を代入すると、$k=27$ を得る。よって、$u^3+v^3=27e_3$ である。

次に、u^3v^3 は 6 次であるから、$e_1=0$ に注意すると、e_2^3, e_3^2 の 1 次結合で書ける。$u^3v^3=le_2^3+me_3^2$ と置き、$(x_1,x_2,x_3)=(1,\omega,\omega^2)$ を代入すると、$m=0$ を得る。

$(x_1,x_2,x_3)=(1,-1,0)$ のとき、$uv=3$ となることに注意すると、$u^3v^3=le_2^3$ に、$(x_1,x_2,x_3)=(1,-1,0)$ を代入すると $l=-27$ を得る。

以上より、

$$u^3+v^3=27e_3=-27B,\quad u^3v^3=-27e_2^3=-27A^3$$

であるから、u^3, v^3 は、2 次方程式

$$t^2+27Bt-27A^3=0$$

の 2 解である。

■u, v **を求める**　この 2 次方程式の判別式は $D=-27\Delta$ であることがわかる。u^3, v^3 は 2 次方程式の解だが、u, v は、それぞれ 3 通り、合計 9 通りの場合がある。

(i) $\Delta\geq 0$ の時: x_1, x_2, x_3 は実数である。従って、$u=\overline{v}$ であるから、u, v のの場合の数は 3 通りに減る。u は 3 通りあるが、3 乗根をとるので ω 倍、ω^2 倍異なるものが得られているが、それは、x_1, x_2, x_3 の置換で得られるものだから、3 通りのどれをとっても良い。

(ii)$\Delta<0$ の時: 2 次方程式は異なる 2 実解を持つので、u^3, v^3 は実数である。また、$x_1\in\mathbb{R}$ とすると $x_2=\overline{x_3}$ なので、u, v も実数である。よって、単に実数の範囲で 3 乗根をとればよいから、u, v の交換を除けば 1 通りしかない。

■x_1, x_2, x_3 **を求める**　u, v が求まれば、

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1 + \omega x_2 + \omega^2 x_3 = u \\ x_1 + \omega^2 x_2 + \omega x_3 = v \end{cases}$$

を Cramer の公式で解けばよい。係数行列の行列式は、Vandermonde の行列式であり、$-3\sqrt{3}i$ であるので、

$$\begin{cases} x_1 &= \frac{(\omega-\omega^2)(u+v)}{-3\sqrt{3}i} = \frac{u+v}{3}, \\ x_2 &= \frac{(\omega-1)(u-(\omega+1)v)}{-3\sqrt{3}i} = \frac{\omega u+\omega^2 v}{3}, \\ x_3 &= \frac{(\omega-1)(v-(\omega+1)u)}{-3\sqrt{3}i} = \frac{\omega^2 u+\omega v}{3}, \end{cases}$$

となる。

(13.4)　**例**　$x^3 - 3x = 0$ を解く。$A = -3$, $B = 0$ なので、判別式は $\Delta = 4 \cdot 3^3 > 0$ である。u^3, v^3 は $t^2 + 3^6 = 0$ の解だから、$\pm 3^3 i$ である。$u = -3i$ ととれるが、$\Delta > 0$ だから $v = \overline{u} = 3i$ となる。これより、$(x_1, x_2, x_3) = (0, \sqrt{3}, -\sqrt{3})$.

(13.5)　**問題**　次の 3 次方程式を、解の公式を用いて解け。

(1) $x^3 + 2x = 0$
(2) $x^3 + 2 = 0$
(3) $27x^3 - 18x + 4 = 0$

(13.5) の解答　(1) $x^3+Ax+B = 0$ と照らすと、$A = 2$, $B = 0$ である。この方程式の判別式は $\Delta = -27B^2 - 4A^3 = -32$ である。$t^2+27Bt-27A^3 = 0$

より、

$$t^2 - 3^3 \cdot 2^3 = 0$$

を解くと、$t = \pm\sqrt{2^3 \cdot 3^3}$ であるが、これが u^3, v^3 である。$\Delta < 0$ だから、u, v は実数の範囲での 3 乗根となるので、$u = \sqrt{6}$, $v = -\sqrt{6}$ となる。よって、解は、$\omega = (-1 + \sqrt{-3})/2$ とすると、

$$x_1 = \frac{u+v}{3} = \frac{\sqrt{6} - \sqrt{6}}{3} = 0,$$
$$x_2 = \frac{\omega u + \omega^2 v}{3} = \frac{\omega\sqrt{6} - \omega^2\sqrt{6}}{3} = \frac{\sqrt{6}(\omega - \omega^2)}{3} = \frac{\sqrt{6}\sqrt{3}i}{3} = \sqrt{2}i,$$
$$x_3 = \frac{\omega^2 u + \omega v}{3} = -\sqrt{2}i$$

(2) $x^3 + Ax + B = 0$ と照らすと、$A = 0$, $B = 2$ である。この方程式の判別式は $\Delta = -27B^2 - 4A^3 = -108$ である。$t^2 + 27Bt - 27A^3 = 0$ より、

$$t^2 + 54t = 0$$

を解くと、$t = 0, -54$ であるが、これが u^3, v^3 である。$\Delta < 0$ だから、u, v は実数の範囲での 3 乗根となるので、$u = 0$, $v = -3\sqrt[3]{2}$ となる。よって、解は、$\omega = (-1 + \sqrt{-3})/2$ とすると、

$$x_1 = \frac{u+v}{3} = \frac{-3\sqrt[3]{2}}{3} = -\sqrt[3]{2},$$
$$x_2 = \frac{\omega u + \omega^2 v}{3} = \frac{v}{3}\omega^2 = -\sqrt[3]{2}\omega^2,$$
$$x_3 = \frac{\omega^2 u + \omega v}{3} = \frac{v}{3}\omega = -\sqrt[3]{2}\omega$$

(3) $x^3 + Ax + B = 0$ と照らすと、$A = -2/3$, $B = 4/27$ である。この方程式の判別式は $\Delta = -27B^2 - 4A^3 = 48/27$ である。$t^2 + 27Bt - 27A^3 = 0$ より、

$$t^2 + 4t + 8 = 0$$

を解くと、$t=-2\pm 2i$ であるが、これが u^3, v^3 である。$\Delta>0$ だから、u, v は互いに共役である。$-2\pm 2i$ は偏角が 135° で、絶対値が $2\sqrt{2}$ であるから、その 3 乗根 (の 1 つ) は、偏角が 45° で、絶対値が $\sqrt{2}$ なので、$u=1+i$、従って、$v=1-i$ である。よって、解は、$\omega=(-1+\sqrt{-3})/2$ とすると、

$$\begin{aligned}
x_1 &= \frac{u+v}{3} = \frac{(1+i)+(1-i)}{3} = \frac{2}{3},\\
x_2 &= \frac{\omega u+\omega^2 v}{3} = \frac{\omega u+\overline{\omega u}}{3} = \frac{-1-\sqrt{3}}{3},\\
x_3 &= \frac{\omega^2 u+\omega v}{3} = \frac{\overline{\omega v}+\omega v}{3} = \frac{-1+\sqrt{3}}{3}.
\end{aligned}$$

§14　剰余群

(14.1)　**定義 (群)**　集合 G が**群**であるとは、G に演算 ab $(a, b\in G)$ 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。

演算が「定義されている」というのは、G の元 a と b があったとき、演算の結果 ab が再び G に属することを言う。G は演算で**閉じている**とも言う。

(14.2)　**定義 (正規部分群)**　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**と言う。つまり、H が次を満たすことを

言う。

(S1) $a, b \in H$ ならば $ab \in H$
(S2) $a \in H$ ならば $a^{-1} \in H$

群 G の部分群 N が, 任意の $a \in G$ に対して $aNa^{-1} = N$ を満たすとき、N を G の**正規部分群**と言い、$N \triangleleft G$ と書く。

アーベル群の部分群は常に正規部分群である。

(14.3) **例** $S_3 = \{e, (12), (13), (23), (123), (132)\}$ を考える。

$H = \langle(23)\rangle = \{e, (23)\}$ は、部分群であるが、正規部分群ではない。実際、

$$(12)H(12)^{-1} = (12)\{e, (23)\}(12) = \{e, (12)(23)(12)\} = \{e, (13)\} \neq H$$

である。

$N = \langle(123)\rangle = \{e, (123), (132)\}$ は正規部分群である。直接証明するならば、すべての $a \in S_3$ について、$aNa^{-1} = N$ を示せばよいが、$a \in N$ のときは明らかに成立なので、$a = (12), (13), (23)$ について示せばよい。$a = (12)$ のときに示せば他は同様なので、$a = (12)$ のときのみ示す。

$$\begin{aligned}(12)N(12)^{-1} &= (12)\{e, (123), (132)\}(12) \\ &= \{e, (12)(123)(12), (12)(132)(12)\} = \{e, (132), (123)\} = N\end{aligned}$$

なので、N は S_3 の正規部分群である。

また、N が正規部分群であることは、S_3 の N による左剰余類分解と右剰余類分解を比較してもわかる。つまり、$a \in S_3 - N$ を用いて、

$$\begin{aligned}S_3 &= N \cup aN \quad \text{左剰余類分解} \\ S_3 &= N \cup Na \quad \text{右剰余類分解}\end{aligned}$$

と表せるので、$aN = Na$、つまり、$aNa^{-1} = N$ である。また、$a \in N$ の

ときは $aNa^{-1} = N$ は明らかなので、任意の a に対して $aNa^{-1} = N$ が言えたから N は正規部分群である。

(14.4) **命題** 群 G の部分群 H が、指数 2、つまり、剰余集合 G/H が 2 つの剰余類からなるならば、H は G の正規部分群である。

Proof. 上の $N \lhd S_3$ と同じ議論で証明できる。 □

(14.5) **問題** 4 次対称群 S_4 には自然に 3 次対称群 S_3 が部分群として含まれている。S_3 は S_4 の正規部分群かどうか調べよ。

(14.6) **剰余群** N を G の正規部分群とする。左剰余集合 $G/N = \{aN \mid a \in G\}$ に演算を $aN\,bN = (ab)N$ で定義することができ、これを G の N による**剰余群**と呼ぶ。

(14.7) **例** (1) S_3 の正規部分群 $N = \langle(123)\rangle = \{e, (123), (132)\}$ による剰余群は、$S_3/N = \{N, (12)N\}$ である。

(2) 加法群 $\mathbb{Z}$ の部分群 $n\mathbb{Z}$ による剰余群は、

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} = \{0+\mathbb{Z}, 1+\mathbb{Z}, \ldots, (n-1)+\mathbb{Z}\}$$

である。これは、$1+\mathbb{Z}$ で生成される n 次の**巡回群**である。

(14.8) **問題** $G = \langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$ を、x で生成される位数 n の巡回群とする。H が G の部分群であるとき、H も巡回群であることを示せ。

【ヒント】(この問題は剰余群とは直接関係はない) H に属する元 $x^j \in H$ $(0 \le j \le n-1)$ のうち、j が最小のものを考え、$H = \langle x^j \rangle$ を示せばよい。

$H \supset \langle x^j \rangle$ は明らかだが、仮に、$H \supsetneq \langle x^j \rangle$ だとすると、$x^k \in H$ であって、$x^k \notin \langle x^j \rangle$ となるものが存在する。k を j で割った商を p、余りを r $(0 \le r < j)$ とすると、$k = jp + r$ なので $x^k = (x^j)^p x^r$ である。これより $x^r \in H$ となるが j の最小性より $r = 0$ となる。ここで矛盾が生じている。

(14.9) **問題** G を有限群、H をその正規部分群とするとき、$|G/H| = |G|/|H|$ を示せ。

§15 可解群

(15.1) **定義 (可解群)** (1) 群 G の部分群の列

$$G = G_n \supset G_{n-1} \supset \cdots \supset G_0 = \{e\}$$

が**アーベル正規列**であるとは、$i = 1, 2, \dots, n$ に対して、G_{i-1} は G_i の正規部分群であり、剰余群 G_i/G_{i-1} がアーベル群であることを言う。

(2) 群 G がアーベル正規列を持つとき、**可解群**であると言う。

さらに、群 G が可解群のとき、各剰余群 G_i/G_{i-1} が素数位数の巡回群になるように、アーベル正規列をとれることが知られている。

(15.2)　例　(1) アーベル群は可解群である。実際、アーベル群 G に対して、$G \supset \{e\}$ はアーベル正規列である。

従って、2 次対称群 S_2 は可解である。

(2) 3 次対称群 S_3 は可解である。実際 $S_3 \supset A_3 \supset \{e\}$ はアーベル正規列である。ただし、A_n は n 次交代群である。

(15.3)　例題　4 次対称群 S_4 は可解である。例えば、$S_4 \supset A_4 \supset V_4 \supset \{e\}$ がアーベル正規列である。ただし、$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ である。

Proof. まず、V_4 が A_4 の部分群であることを示す。V_4 の元はすべて偶置換であるから、A_4 の部分集合であることはよい。V_4 のどの元も自分自身が逆元であるから、逆元では閉じている。

積で閉じていることについては、まず $(12)(34) \cdot (13)(24) = (14)(23)$ であることが言え、他の積については、文字を入れ替えただけなので、同様に言える。以上より、V_4 は A_4 の部分群である。

続いて、列がアーベル正規列であることを示す。$S_4 \rhd A_4$ であることは指数 2 だからよく、剰余群は位数 2 だからアーベル群である。$V_4 \rhd \{e\}$ もよく、V_4 はアーベル群だから剰余群もアーベル群である。最後に、$A_4 \rhd V_4$ については、正規部分群であることが言えれば、剰余群は位数が 3 だからアーベル群だとわかるので、あとは正規部分群であることを言えばよい。

A_4 の元であって、巡回置換分解したときに、2 つの互換の積になるのは、V_4 の単位元以外の 3 つしかない。よって、次の補題から、V_4 は S_4 の正規部分群であることが言える。 □

(15.4) **補題** n 次対称群 S_n の、巡回置換分解された元

$$\sigma = (i_1 i_2 \cdots i_r)(j_1 j_2 \cdots j_s) \cdots$$

と $\tau \in S_n$ があるとき、次の等式が成り立つ。

$$\tau\sigma\tau^{-1} = (\tau(i_1)\tau(i_2)\cdots\tau(i_r))(\tau(j_1)\tau(j_2)\cdots\tau(j_s))\cdots$$

Proof. $(\tau\sigma\tau^{-1})(\tau(i_1)) = \tau\sigma(i_1) = \tau(i_2)$ のように計算できることからわかる。 □

(15.5) **問題** 二面体群は可解であることを示せ。ただし、n 次の二面体群 $I(n)$ とは、正 n 角形の合同変換群であり、以下の元からなる位数 $2n$ の群である。

$$I(n) = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \quad \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\}$$

ただし、σ は正 n 角形の $2\pi/n$ 回転を表す位数 n の元、τ はある 1 つの対称軸に関する対称変換を表す位数 2 の元であり、従って、$\sigma^n = \tau^2 = e$, $\tau\sigma = \sigma^{-1}\tau$ を満たす。なお、$\sigma^k\tau$ は τ の対称軸を $2k\pi/n$ 回転した対称軸に関する対称変換を表す位数 2 の元である。

(15.6) **定理** 5 次交代群 A_5 は可解ではない。

Proof. A_5 の $\{e\}$ ではない正規部分群 H をとる。これが A_5 に等しいことを示せば、正規部分群は自明な 2 つしかないことがわかる。すると、アーベル正規列の最初の正規部分群が $\{e\}$ しかなく、A_5 がアーベル群ではないか

ら、アーベル正規列が存在しないこととなり、A_5 が可解ではないことが示せる。

よって、以下で H が A_5 に等しいことを示す。偶置換は偶数個の互換の積で書けるので、文字に重複のない互換 2 つの積はすべて H に含まれることを示せばよい (重複のある $(12)(23)$ も $(12)(45)\cdot(45)(23)$ と思えばよいから)。

■Step 1. H が長さ 3 の巡回置換を 1 つ含むこと　S_5 の単位元ではない元 σ の巡回置換分解の形は、

$$(abcde),\quad (abcd),\quad (abc)(de),\quad (abc),\quad (ab)(cd),\quad (ab)$$

のいずれかであるが、このうち偶置換は $(abcde)$, (abc), $(ab)(cd)$ の 3 通りである。

さて、H の単位元ではない元 σ をとり、巡回置換分解が (abc) の形ならば、Step 1 で証明すべきことは残っていない。

次に、σ が $(abcde)$ の形だとする。文字を入れかえて (12345) としてよい。$\tau=(123)\in A_5$ をとると、H が A_5 の正規部分群だから、$\tau\sigma\tau^{-1}\in H$ であり、従って $\tau\sigma\tau^{-1}\cdot\sigma^{-1}\in H$ である。

$$\tau\sigma\tau^{-1}\cdot\sigma^{-1}=(123)(12345)(321)(54321)=(241)$$

だから、この場合も H は長さ 3 の巡回置換を含む。

最後に、σ が $(ab)(cd)$ の形だとする。文字を入れかえて $(12)(34)$ としてよい。$\tau=(345)\in A_5$ をとると、H が A_5 の正規部分群だから、$\tau\sigma\tau^{-1}\in H$ であり、従って $\sigma\cdot\tau\sigma\tau^{-1}\in H$ である。

$$\sigma\cdot\tau\sigma\tau^{-1}=(12)(34)(345)(12)(34)(543)=(345)$$

だから、この場合も H は長さ 3 の巡回置換を含む。以上よりすべての場合で H は長さ 3 の巡回置換を含む。

■Step 2. **H が長さ 3 の巡回置換をすべて含むこと**　文字を取り替えて、$(123) \in H$ とする。任意の異なる i, j, k $(i, j, k \in \{1, 2, 3, 4, 5\})$ をとる。このとき $\tau \in A_5$ を

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i & j & k & x & y \end{pmatrix}$$

と定める。ただし、x, y は i, j, k 以外の 2 文字で、偶置換になるように順序を決める (一方は偶置換で他方は奇置換)。すると、(15.4) より、$H \ni \tau(123)\tau^{-1} = (ijk)$ なので、H が長さ 3 の巡回置換をすべて含むことが示せた。

■Step 3. **文字に重複のない互換 2 つの積はすべて H に含まれること**　任意の異なる $i, j, k, l \in \{1, 2, 3, 4, 5\}$ をとる。$(ijk)(jkl) = (ij)(kl)$ だから、文字に重複のない互換 2 つの積はすべて H に含まれる。 □

(15.7)　**命題**　G が可解群ならば、その部分群 H も可解群である。

Proof. G を可解群とすると、アーベル正規列 $G = G_n \supset G_{n-1} \supset \cdots \supset G_0 = \{e\}$ があるが、一斉に部分群 H と共通部分をとり、

$$H = G_n \cap H \supset G_{n-1} \cap H \supset \cdots \supset G_0 \cap H = \{e\}$$

という部分群の列が得られる。H が可解群であることを示すためには、これがアーベル正規列であることを示せばよい。

　まず、$G_{i-1} \cap H$ が $G_i \cap H$ の正規部分群であることを示す。$x \in G_i \cap H$ を取ると、$x \in G_i$ だから、$x(G_{i-1} \cap H)x^{-1} \subset xG_{i-1}x^{-1} = G_{i-1}$ であり、$x \in H$ だから、$x(G_{i-1} \cap H)x^{-1} \subset xHx^{-1} = H$ である。従って、$x(G_{i-1} \cap H)x^{-1} \subset G_{i-1} \cap H$ であり、正規部分群であることが示せた。

次に $(G_i \cap H)/(G_{i-1} \cap H)$ がアーベル群であることを示す。$x, y \in G_i \cap H$ をとると、G_i/G_{i-1} がアーベル群であることから、$xyG_{i-1} = yxG_{i-1}$、従って、$x^{-1}y^{-1}xy \in G_{i-1}$ であり、従って、$x^{-1}y^{-1}xy \in G_{i-1} \cap H$ である。これより。$xy(G_{i-1} \cap H) = yx(G_{i-1} \cap H)$ だから、$(G_i \cap H)/(G_{i-1} \cap H)$ はアーベル群である。 □

(15.8) **問題** $n \geq 5$ のとき、n 次対称群 S_n は可解ではないことを示せ。

§16 冪根拡大

(16.1) **方程式の可解性** 体 F 上の多項式 $f(x) \in F[x]$ のとき、方程式 $f(x) = 0$ が、四則と冪根で解けるということを、体の言葉で表してみる。

f の F 上の分解体を E とすると、f の各根は E に属しており、それが F の元から四則と冪根で表せるのは、

$$E = L_m \supset L_{m-1} \supset \cdots \supset L_0 = F,$$

ただし、$L_i = L_{i-1}(\sqrt[n_{i-1}]{a_{i-1}})$ ($a_{i-1} \in L_{i-1}$ は $x^{n_{i-1}} - a_{i-1} \in L_{i-1}[x]$ の 1 つの根)、という体の拡大の列があることである。

一般には、$F(\sqrt[n]{a})$ の形の拡大は正規拡大とは限らないので、注意が必要である。1 の原始 n 乗根も付加されていれば正規拡大になる。

(16.2) **定理** 体 F は 1 の原始 n 乗根を含み、$E \supset F$ が n 次のガロア拡大であるとする。このとき、$Gal(E/F)$ が巡回群であることと、$E = F(\sqrt[n]{a})$ (つまり、ある多項式 $x^n - a \in F[x]$ の 1 つの根による単項拡大) であることは同値である。

Proof. [$\Rightarrow$] $Gal(E/F)$ を n 次の巡回群とし、$\sigma \in Gal(E/F) = \mathrm{Aut}_F(E)$ をその生成元とする。σ は体の F-同型であることから、E を F 上の n 次元ベクトル空間と見たとき、σ は E 上の線型写像になる。線型写像は、適当に E の基底を選んだとき n 次の正方行列で表現される。

σ の固有値を λ, その固有ベクトルを α とすると、$\sigma(\alpha) = \lambda\alpha$ であるが、σ を n 回作用させると、$\sigma^n(\alpha) = \lambda^n\alpha$ となり、$\sigma^n = \mathrm{id}$ より、λ は 1 の n 乗根で、F に属するとわかる。

さらに、σ の位数が n であるから σ の固有値には 1 の原始 n 乗根があるはずである (要証明)。

$\zeta \in F$ を 1 の原始 n 乗根で、σ の固有値とし、その固有ベクトルを β とする。$Gal(E/F) = \{\mathrm{id}, \sigma, \ldots, \sigma^{n-1}\}$ であり、$\sigma^k(\beta) = \zeta^k\beta$ だから、β を固定する $Gal(E/F)$ の元は恒等写像 id のみであり、ガロア理論の基本定理から $F(\beta) = E$ がわかる。

$\sigma(\beta^n) = (\sigma(\beta))^n = (\zeta\beta)^n = \beta^n$ だから、β^n は $Gal(E/F)$ で固定されるので F の元である。つまり、β はある F の元の n 乗根なので、$E = F(\beta) \supset F$ は n 乗根による単項拡大である。

[$\Leftarrow$] $E = F(\sqrt[n]{a})$ $(a \in F)$ とする。$[E : F] = n$ なので、$\sqrt[n]{a}$ の F 上の最小多項式は $x^n - a \in F[x]$ である。1 の原始 n 乗根を $\zeta \in F$ とし、$\zeta\sqrt[n]{a}$ を考えると、これも n 乗して a になるので、既約多項式 $x^n - a$ の根である。よって、$\sqrt[n]{a}$ を $\zeta\sqrt[n]{a}$ に写す E 上の F-同型 $\sigma \in Gal(E/F) = \mathrm{Aut}_F(E)$ が存在し、これは明らかに位数 n である。$|Gal(E/F)| = n$ だから、$Gal(E/F)$ は位数 n の元 σ で生成される n 次の巡回群である。 $\square$

(16.3) **問題** A を n 次正方行列とするとき、複素数を成分に持つ n 次正則行列 P を用いて、$P^{-1}AP$ が上三角行列になるようにできることを示せ(**行列の三角化**)。

【ヒント】n に関する帰納法で示す。$n=1$ のときは既に A は三角化されている。

n 次正方行列まで三角化ができるとし、A を $n+1$ 次正方行列とする。A の固有値 λ をとり、その固有ベクトルを v_0 とする。v_0 を含む $\mathbb{C}^{n+1}$ の基底 $v_0, w_1, w_2, \ldots, w_n$ をとり、これらを並べた行列 $Q = (v_0 w_1 w_2 \cdots w_n)$ を作ると、

$$Q^{-1}AQ = \begin{pmatrix} \lambda & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix}$$

と書ける。この行列の 2 行以降、2 列以降の n 次正方行列部分を B と置くと、n 次正則行列 R を用いて、

$$R^{-1}BR = \begin{pmatrix} * & * & \cdots & * \\ 0 & * & & * \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & * \end{pmatrix}$$

と三角化できる。この Q, R を用いて、A を三角化する $n+1$ 次正則行列 P を作ればよい。

(16.4) **問題** $0 \leq k \leq n$ のとき、n 次正方行列が k-上三角行列 (ここだけの用語) であることを、$j-i<k$ のとき、(i,j) 成分が 0 であるということで定める。つまり、上三角行列であり、さらに対角成分の k 個上の成分までがすべて 0 であることである。特に、通常の上三角行列は 0-上三角行列である。

このとき、A が n 次の k-上三角行列、B が n 次の l-上三角行列であるとき、積 AB は $(k+l)$-上三角行列であることを示せ。

【ヒント】AB の (i,j) 成分は $\sum_{t=1}^{n} a_{it}b_{tj}$ であるが、$a_{it} \neq 0$ であるのは $t-i \geq k$ の場合に限られ、$b_{tj} \neq 0$ であるのは $j-t \geq l$ の場合に限られるから、$a_{it}b_{tj} \neq 0$ であるのは $j-i$ がどういう場合に限られるかがわかる。これより、AB の (i,j) 成分が 0 でないのがどういう場合に限られるかがわかる。

(16.5) **問題** n 次正方行列 A が、

$$A = \begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

の形であるとする (「$*$」の部分は任意で、成分ごとに異なってもよい)。A を何乗かすると単位行列になるならば、A 自身が単位行列であることを示せ。

【ヒント】E を単位行列、$B = A - E$ とする。B は「$*$」の部分であり、1-上三角行列である。A を k 乗すると単位行列になるとすると、$E = A^k = (E+B)^k = E + \binom{k}{1}B + \cdots + \binom{k}{k-1}B^{k-1} + B^k$ である。ここで、右辺で対角成分の 1 つ上に 0 でない成分がある項は $\binom{k}{1}B$ だけであるから、左辺が単位行列であることより B は 2-上三角行列でなくてはならない。すると、右辺で対角成分の 2 つ上に 0 でない成分がある項は $\binom{k}{1}B$ だけであるから、以下、反復すると $B = 0$ がわかる。

(16.6) **問題** (16.2) の $\sigma \in Gal(E/F)$ を考える。σ の固有値全体の集合は群をなすことを示せ。

【ヒント】固有値 λ の固有ベクトル α と固有値 λ' の固有ベクトル α' をとる。$\alpha\alpha'$ が固有値 $\lambda\lambda'$ の固有ベクトルであることが示せ、また、α^{-1} が固有

値 λ^{-1} の固有ベクトルであることが示せる。積で閉じているので単位元を含むことも示せる。

(16.7) **問題** (16.2) の $\sigma \in Gal(E/F)$ を考える。σ の固有値には、1 の原始 n 乗根があることを示せ。

【ヒント】固有値の集合は群をなすが、n 次巡回群の部分群になるので、やはり巡回群である。その生成元 λ を 1 の原始 m 乗根とする $(m|n)$。σ を行列とみて、三角化すると、三角化の手順を見ると対角成分には固有値が並ぶことがわかる。従って、三角化された行列を A とすると、A^m は、対角成分がすべて 1 である上三角行列である。A^m は n/m 乗すると $A^n = E$ になるので、すると、(16.5) より、$A^m = E$ がわかる。ところが σ の位数は n であるから、$m = n$ とわかる。

(16.8) **定理 (ガロア理論の基本定理の復習)** $E \supset F$ 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、$Z_G(L) = \{g \in G \mid g(\alpha) = \alpha \quad (\alpha \in L)\}$ 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。

(16.9) **定理** F が 1 の原始 $n!$ 乗根を含むとする。n 次多項式 $f(x) \in F[x]$ をとり、その F 上の分解体を E とする。このとき、$f(x)$ の根が F の元から四則と冪根で書けることは、$Gal(f) = Gal(E/F)$ が可解群であることと同値である。

∗ 1 の原始 $n!$ 乗根を含むならば、k を $n!$ の約数としたとき、1 の原始 k 乗根も含むことに注意する。

Proof. $[\Leftarrow]$ $G = Gal(E/F)$ が可解であるとすると、アーベル正規列

$$G = G_m \supset G_{m-1} \supset \cdots \supset G_0 = \{e\}$$

が取れ、ガロア理論の基本定理により、これに対応する部分体の列

$$F = L_m \subset L_{m-1} \subset \cdots \subset L_0 = E$$

が取れる。ただし、$L_k = E^{G_k}$ である。

(15.1) の最後の注意により、各 G_i/G_{i-1} は巡回群としてよく、さらに、その位数は $|G|$ の約数になるが、(8.4) より G は S_n の部分群とみなせるので、$[L_{i-1} : L_i]$ は $n!$ の約数である。従って、(16.2) より、各拡大 $L_{k-1} \supset L_k$ は冪根を付加した単項拡大である。よって、E の元は F の元から四則と冪根で表せるので、特に F の根は F の元から四則と冪根で表せる。

$[\Rightarrow]$ F の根が F の元から四則と冪根で表せるとすると、体の拡大の列

$$F = L_m \subset L_{m-1} \subset \cdots \subset L_0 = E,$$

ただし、$L_{k-1} = L_k(\sqrt[n_k]{a_k})$ $(a_k \in L_k)$、が取れ、ガロア理論の基本定理により、これに対応する部分群の列

$$G = G_m \supset G_{m-1} \supset \cdots \supset G_0 = \{e\}$$

が取れる。ただし、$G_k = Z_G(L_k)$ である。F が 1 の冪根を含むから、$L_{k-1} \subset L_k$ はガロア拡大であり、(16.2) より $Gal(L_{k-1}/L_k)$ は n_k 次巡回群である。また、これは、(16.8) より、$Gal(L_{k-1}/L_k) \cong Gal(E/L_k)/Z_{Gal(E/L_k)}(L_{k-1}) = G_k/(G_k \cap G_{k-1}) = G_k/G_{k-1}$ と同型である。よって、上の部分群の列はアーベル正規列であるので、$Gal(f) = G$ は可解群である。 □

(16.10) **定理** $f \in \mathbb{Q}[x]$、L を $\mathbb{Q}$ 上の f の分解体とする。また、ζ を 1 の原始 m 乗根とし、$F = \mathbb{Q}(\zeta)$、E を F 上の f の分解体とする。このとき、$Gal(E/F)$ が可解群ならば $Gal(L/\mathbb{Q})$ も可解群である。

Proof. まず、F は、円周等分多項式 $\Phi_m(x)$ の $\mathbb{Q}$ 上の分解体だから、$F \supset \mathbb{Q}$ はガロア拡大である。また、E は $\Phi_m(x)f(x)$ の $\mathbb{Q}$ 上の分解体であるから、$E \supset \mathbb{Q}$ はガロア拡大である。そこで、$G = Gal(E/\mathbb{Q})$, $H = Gal(E/F)$ と置く。

$F \supset \mathbb{Q}$ はガロア拡大だから、$Gal(F/\mathbb{Q}) \cong G/H$ であるが、これは $\mathbb{Z}/(m)$ の単元群であり、特にアーベル群である。よって、$H = Gal(E/F)$ は仮定により可解群であり、G/H も可解群だから、G は可解群である。

$S = Gal(E/L)$ と置くと、$L \supset \mathbb{Q}$ がガロア拡大だから、S は $G = Gal(E/\mathbb{Q})$ の正規部分群である。すると、$Gal(L/\mathbb{Q}) \cong G/S$ だから、これは可解群である。 □

(16.11) **命題** 群 G とその正規部分群 H があるとする。このとき、G が可解群であることと、H と G/H の両方が可解群であることは同値である。

Proof. まだ □