

## 2015 年度 前期 代数学演習 2

更新日時 2015-07-27 18:59:03 担当 和地 輝仁

### 目次

1 シラバス抜粋	1
2 授業のノート	2
§1 多項式の高ア群	2
§2 ガロア理論の基本定理	3
§3 代数方程式の解の公式	5
§4 演習問題	7
§5 演習問題の解答	7

## 1 シラバス抜粋

授業の目標 代数学 1、代数学 2、代数学 3 などで学んだ、線型代数、群、環、体の理論の演習を通して、これらに対する理解や習熟を深める。また、専門的な数学が初歩的な算数・数学に対しても統一的な視点を与え、その深い理解には不可欠であることを実感できる。

### 到達目標

1. 複素数の性質や演算に習熟する。
2. 対称群の性質や演算に習熟する。
3. 行列式・逆行列の計算や性質に習熟する。
4. 線型代数の理論を抽象的なベクトル空間に適用できる。
5. 環とイデアルの性質に習熟する。

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. 行列の基本変形の演習 1 | 9. 逆行列の演習 2     |
| 2. 行列の基本変形の演習 2 | 10. 逆行列の演習 3    |
| 3. 行列の簡約化の演習 1  | 11. 行列式の演習 1    |
| 4. 行列の簡約化の演習 2  | 12. 行列式の演習 2    |
| 5. 連立方程式の演習 1   | 13. 行列式の応用の演習 1 |
| 6. 連立方程式の演習 2   | 14. 行列式の応用の演習 2 |
| 7. 連立方程式の演習 3   | 15. 行列式の応用の演習 3 |
| 8. 逆行列の演習 1     | 16. 期末試験        |

成績評価 期末試験 (50%) と、毎回の演習問題の状況 (50%) で成績を評価する。原則として全ての時間の出席を求めるが、やむを得ない理由で欠席をする (した) 場合はできるだけ速やかに申し出て、指示を受けること。

## 2 授業のノート

### §1 多項式のガロア群

(1.1) 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  $\phi: F_1 \rightarrow F_2$  が準同型写像 であるとは, 次の条件を満たすことを言う.

- (i)  $\phi(1) = 1$ ,
- (ii)  $\phi(a + b) = \phi(a) + \phi(b)$  ( $a, b \in F_1$ ),
- (iii)  $\phi(ab) = \phi(a)\phi(b)$  ( $a, b \in F_1$ )

(2) 2つの体  $F_1, F_2$  があるとき, 写像  $\phi: F_1 \rightarrow F_2$  が同型写像 であるとは,  $\phi$  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ひ,  $F$  上の自己同型写像全体のなす集合を  $\text{Aut}(F)$  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  $\phi: E_1 \rightarrow E_2$  があるとす.  $\phi$  が  $F$  上恒等写像であるとき,  $\phi$  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  $F$ -自己同型写像と言ひ,  $E$  上の  $F$ -自己同型写像全体のなす集合を  $\text{Aut}_F(E)$  で表す.

(1.2) 問題  $\phi: E \rightarrow F$  を体の準同型とするととき, 次を示せ.

- (1)  $\phi(0) = 0$
- (2)  $\phi(-1) = -1$
- (3)  $\phi(a - b) = \phi(a) - \phi(b)$  ( $a, b \in E$ )
- (4)  $\phi(ab^{-1}) = \phi(a)(\phi(b))^{-1}$  ( $a, b \in E, b \neq 0$ )
- (5)  $\phi$  は単射である.

(1.3) 問題 次の問に答えよ.

- (1)  $F$  を体とするととき,  $\text{Aut}(F)$  は写像の合成を演算とする群をなすことを示せ.
- (2) 体の拡大  $E \supset F$  があるとき,  $\text{Aut}_F(E)$  は群をなすことを示せ.
- (3) 有限次拡大  $E \supset F$  があるとき (実は代数拡大でも示せる),  $F$  上恒等写像である  $E$  の自己準同型写像は同型であることを示せ.

(1.4) 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.*  $\phi: F(\alpha) \rightarrow F(\beta)$  ( $p(\alpha) \mapsto p(\beta)$  ( $p \in F[x]$ )) と定める.

[ $\phi$  が well-defined であること]  $F[\alpha] = F(\alpha)$ ,  $F[\beta] = F(\beta)$  だから  $\phi: F[\alpha] \rightarrow F[\beta]$  と考える. すると,  $f$  が最小多項式であることを用いれば示される.

[ $\phi$  が体の準同型であること] 明らか.

[ $\phi$  が全単射であること]  $\phi$  の定義より容易.

[ $\phi$  が  $F$  上恒等写像であること] 明らか. □

(1.5) 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  $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ .

(1.6) 命題  $F$  上代数的な元  $\alpha$  の最小多項式が  $f(x) \in F[x]$  であり,  $E = F(\alpha)$  であるとき,

$$\#\text{Aut}_F(E) = \#\{a \in E \mid f(a) = 0\} \quad (1)$$

*Proof.*  $E = F[\alpha]$  だから,  $E$  上の  $F$ -自己同型は  $\alpha$  の像で決まる (なぜ?).  $\alpha$  の像も  $f$  の根 (なぜ?) だから命題が言える. □

(1.7) 問題 次の問に答えよ。

- (1)  $\mathbb{C}$  上の  $\mathbb{R}$ -自己同型をすべて言え。
- (2)  $\mathbb{Q}(\sqrt{2})$  上の  $\mathbb{Q}$ -自己同型をすべて言え。
- (3)  $\omega$  を 1 の原始 3 乗根 (の 1 つ) とするとき、 $\mathbb{Q}(\omega)$  上の  $\mathbb{Q}$ -自己同型をすべて言え。

(1.8) 問題  $F$  上代数的な元  $\alpha$  の最小多項式が  $f(x)$  であり、 $\Omega$  を  $F$  を部分体に持つような代数閉体とする。

$$\#\{\phi: F \hookrightarrow \Omega \mid F \text{ から } \phi \text{ の像への } F\text{-同型}\} = (f \text{ の } \Omega \text{ における根の個数})$$

(1.9) 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。

(1.10) 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  $\sqrt[3]{2}X^3 - 2$  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)  $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2})$  も  $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$  も 2 次拡大だから正規拡大であるが、 $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$  は違う。

(1.11) 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  $\text{Aut}_F(E)$ -不変部分体  $E^{\text{Aut}_F(E)}$  は  $F$  に等しい。

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

(1.12) 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。

(1.13) 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  $\omega = (-1 + \sqrt{-3})/2$ 。

(1.14) 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。

(1.15) 定義 (多項式のカロア群) 体  $F$  に対し、 $f \in F[X]$  の分解体を  $E$  とするとき、 $\text{Aut}_F(E)$  を  $f$  のガロア群と呼び、 $\text{Gal}(f)$  と書く。

(1.16) 群の復習 演算 (積) を持ち、結合法則を満たし、単位元が存在し、逆元が存在すること。

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

(1.18) 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。

## §2 ガロア理論の基本定理

(2.1) 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。

(2.2) 事実 標数 0 の体の拡大は分離拡大である。

■ 定理 (有限次分離拡大は単項拡大)  $E \supset F$  が有限次分離拡大ならば、 $E = F(\alpha)$  となる  $\alpha \in E$  が存在する。

■ 定理  $E \supset F$  が有限次拡大のとき、これが単項拡大であることと、中間体が有限個であることは同値である。

■ 問題 (1)  $E \supset F$  を体の拡大とし、 $f \in F[x]$  とする。 $f$  が  $E[x]$  の中で既約ならば  $F[x]$  の中でも既約である。

(2)  $E \supset L \supset F$  を体の拡大とする。 $\alpha \in E$  の  $F$  上の最小多項式を  $f \in F[x]$  とし、 $L$  上の最小多項式を  $g \in L[x]$  とする。このとき  $L[x]$  の中で、 $g$  は  $f$  を割り切る。

(2.3) 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)。

(2.4) 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  $F = E^G$  と置くと、

(1)  $E \supset F$  はガロア拡大

(2)  $[E : F] = \#G$

である。

(2.5) 問題 群  $G$  が体  $E$  に作用しており、 $H$  を  $G$  の部分群とする。このとき、 $E^G \subset E^H$  である。

(2.6) 定義 (ガロア群)  $E \supset F$  をガロア拡大とすると、 $\text{Aut}_F(E)$  をガロア拡大  $E \supset F$  のガロア群と呼び、 $\text{Gal}(E/F)$  と書く。

分離性と (1.11) 定理、及び (2.4) 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、 $F = E^{\text{Aut}_F(E)}$  なることである。

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

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

$$\text{Gal}(E/L) = Z_G(L)$$

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、

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

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、

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

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、 $\text{Gal}(L/F) \simeq G/Z_G(L)$ 、つまり、 $\text{Gal}(L/F) \simeq \text{Gal}(E/F)/\text{Gal}(E/L)$  である。

(2.8) 例 (1)  $E$  を  $x^2 - 2$  の  $\mathbb{Q}$  上の分解体とすると、 $E = \mathbb{Q}(\sqrt{2})$  であり、 $E \supset \mathbb{Q}$  はガロア拡大である。このとき、 $[E : \mathbb{Q}] = 2$  だから、 $\#\text{Gal}(E/\mathbb{Q}) = 2$  である。 $\text{Gal}(E/\mathbb{Q})$  は 2 次対称群  $S_2$  の部分群であるから、 $S_2$  に等しい。

$Gal(E/\mathbb{Q})$  に自明でない部分群がないから、 $E \supset \mathbb{Q}$  には真の中間体はない。

(2)  $E$  を  $(x^2 - 2)(x^2 - 3)$  の  $\mathbb{Q}$  上の分解体、つまり、 $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  とする。 $E = \mathbb{Q}(\sqrt{2} + \sqrt{3})$  と単項拡大で表せるから、 $Gal(E/\mathbb{Q}) = Aut_{\mathbb{Q}}(E)$  の元の個数は、 $\sqrt{2} + \sqrt{3}$  の最小多項式の  $E$  に属する根の個数だから 4 である。

その 4 つの  $E$  上の  $\mathbb{Q}$  同型は、 $\sqrt{2} + \sqrt{3}$  を、 $\pm\sqrt{2} \pm \sqrt{3}$  に写すものだから、 $\sqrt{2}$  を  $-\sqrt{2}$  に写す元  $\sigma$  と、 $\sqrt{3}$  を  $-\sqrt{3}$  に写す元  $\tau$  で生成される。つまり、 $Gal(E/\mathbb{Q})$  は 2 次の巡回群  $\mathbb{Z}/(2)$  の 2 つの直積  $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$  である。

非自明な部分群は 3 つあり、 $\sigma$  で生成される 2 次の巡回群と、 $\tau$  で生成される 2 次の巡回群と、 $\sigma\tau$  で生成される 2 次の巡回群であり、それぞれ、部分体  $\mathbb{Q}(\sqrt{3})$ ,  $\mathbb{Q}(\sqrt{2})$ ,  $\mathbb{Q}(\sqrt{6})$  に対応する。

(3)  $E$  を  $x^3 - 2$  の  $\mathbb{Q}$  上の分解体とすると、 $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$  であり ( $\omega = (-1 + \sqrt{-3})/2$ )、 $[E : \mathbb{Q}] = 6$  であるから、(1) と同様にして、 $Gal(E/\mathbb{Q}) = S_3$  である。 $S_3$  の作用は、 $\alpha_i = \sqrt[3]{2}\omega^{i-1}$  ( $i = 1, 2, 3$ ) の置換である。

$S_3$  には非自明な部分群が 4 つある。位数 3 の部分群は (1 2 3) で生成される巡回群  $N$  である。位数 2 の部分群は 3 つあって、それぞれ、(2 3), (1 3), (1 2) で生成される群であり、順に  $H_1, H_2, H_3$  と書くことにする。

$\omega$  は  $N$  の作用で不変だとわかるので、 $N$  と対応する部分体は  $\mathbb{Q}(\omega)$  である。 $H_i$  は  $\alpha_i$  を固定するので、対応する部分体は  $\mathbb{Q}(\alpha_i)$  である。

(2.9) 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。

### §3 代数方程式の解の公式

(3.1) 3 次方程式の判別式

$$x^3 + a_1x^2 + a_2x + a_3 = 0$$

を考える。 $y = x - a_1/3$  という変換により、 $y^3 + py + q = 0$  の形にできるから、はじめから

$$x^3 + px + q = 0, \quad (p, q \in \mathbb{R})$$

を考える。

$$D = \left( (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \right)^2$$

とおき、方程式  $x^3 + px + q = 0$  の判別式と呼ぶ。

(3.2) 命題 方程式  $x^3 + px + q = 0$  の判別式  $D$  は、 $D = -27q^2 - 4p^3$  である。

(3.3) 命題 方程式  $x^3 + px + q = 0$  の判別式  $D$  について次が成り立つ。

- (1)  $D = 0$  ならば、方程式は重解を持つ。
- (2)  $D > 0$  ならば、方程式は異なる 3 実数解を持つ。
- (3)  $D < 0$  ならば、方程式は、1 実数解と、互いに共役な虚数解を持つ。

*Proof.* 前の命題より、 $D \in \mathbb{R}$  である。すべての逆を示す (転換法)。(1) と (2) は明らか。(3) について、 $x_1 \in \mathbb{R}$ ,  $x_3 = \overline{x_2}$  のとき、 $x_2 = a + bi$  とすると、

$$\begin{aligned} \left( (x_1 - x_2)(x_1 - \overline{x_2})(x_2 - \overline{x_2}) \right)^2 &= \left( (x_1 - x_2)(\overline{x_1 - x_2}) \cdot 2bi \right)^2 \\ &= |x_1 - x_2|^4 \cdot (-4b^2) < 0 \end{aligned}$$

□

(3.4) 3 次方程式の解の公式

$$x^3 + a_1x^2 + a_2x + a_3 = 0$$

を考える。 $y = x - a_1/3$  という変換により、 $y^3 + py + q = 0$  の形にできるから、はじめから

$$x^3 + px + q = 0, \quad (p, q \in \mathbb{R})$$

を考える。3 解を  $x_1, x_2, x_3$  とし、

$$\begin{aligned} u &= x_1 + x_2\omega + x_3\omega^2, \\ v &= x_1 + x_2\omega^2 + x_3\omega \end{aligned}$$

とおくと、 $u^3 + v^3, u^3v^3$  は  $x_1, x_2, x_3$  に関する対称式である (要確認)。したがって、 $e_1 = 0$  だから、 $u^3 + v^3$  は  $e_3$  の定数倍になり、 $u^3v^3$  は  $e_2^3$  と  $e_3^3$  の 1 次結合になる。 $x_1, x_2, x_3$  に具体的に値を代入すれば、

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

とわかるから、 $u^3, v^3$  は、 $t^2 + 27qt - 27p^3 = 0$  の解である。この 2 次方程式の判別式が、方程式  $x^3 + px + q = 0$  の判別式  $D$  の負数倍になっている (要確認)。

判別式が 0 以上のとき、解  $x_i$  はすべて実数だから、 $u$  と  $v$  は共役である。 $u$  を 1 つ決めると (どれでも結果は同じ)  $v = \bar{u}$  も決まる。判別式が負のときは、 $x_1 \in \mathbb{R}$  とすると、 $u^3, v^3$  は実数であり、また、 $u$  も  $v$  も実数だから実数の範囲で 3 乗根をとる。

こうして  $u$  と  $v$  が決まれば、連立方程式

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

を解けばよい。係数行列の行列式は  $-3\sqrt{3}i$  であり、Cramer の公式を用いれば、

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

と  $x_i$  が求まる。

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

(3.6) 4 次方程式の解の公式

(3.7) 定理 体  $F$  が 1 の原始  $n$  乗根を含むとし、 $E \supset F$  が  $n$  次ガロア拡大とする。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。

*Proof.* これは証明できるのです。 □

(3.8) 定義 (可解群) 群  $G$  が可解群であるとは、 $G$  の部分群の列

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

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。

(3.9) 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。

(3.10) 事実 上の定理の、 $F$  が原始  $n!$  根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。

(3.11) 5 次以上の代数方程式の解の公式 可解ではない群を含む群は可解ではなく、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、(2.9) 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。

(3.12) 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、 $f(x) = 0$  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  $\alpha_4, \alpha_5$  とする。 $f$  が既約だから、(1.4) 命題より、任意の  $i, j$  に対して、 $\alpha_i$  を  $\alpha_j$  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、 $\alpha_i$  と  $\alpha_j$  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、 $\alpha_i$  と  $\alpha_j$  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。  $\square$

## §4 演習問題

(4.1) 問題 次の拡大は正規拡大かどうか答えよ。

- (1)  $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$
- (2)  $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2})$
- (3)  $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$
- (4)  $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$
- (5)  $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \supset \mathbb{Q}$

(4.2) 問題 次の群のすべての部分群を決定せよ。そのうち、正規部分群はどれか。ただし、 $\omega = (-1 + \sqrt{3})/2$ ,  $i = \sqrt{-1}$  とする。また、 $D_4$  は 4 文字の置換 (の一部) からなる集合である。

- (1)  $S_2$  (2 次対称群)
- (2)  $S_3$
- (3)  $C_3 = \{1, \omega, \omega^2\}$
- (4)  $C_4 = \{1, i, -1, -i\}$
- (5)  $D_4 = \{\text{id}, (1234), (1432), (13)(24), (12)(34), (14)(23), (13), (24)\}$

(4.3) 問題 次のガロア拡大について、拡大次数、ガロア群、ガロア群のすべての非自明な部分群、すべての中間体を答えよ。

- (1)  $x^2 - 2$  の  $\mathbb{Q}$  上の分解体を  $E$  としたときの、 $E \supset \mathbb{Q}$ .
- (2)  $x^3 - 2$  の  $\mathbb{Q}$  上の分解体を  $E$  としたときの、 $E \supset \mathbb{Q}$ .
- (3)  $x^4 - 2$  の  $\mathbb{Q}$  上の分解体を  $E$  としたときの、 $E \supset \mathbb{Q}$ .

(4.4) 問題  $x^3 - 2$  の  $\mathbb{Q}$  上の分解体を  $E$  とし、ガロア拡大  $E \supset \mathbb{Q}$  を考える。 $F \supset \mathbb{Q}$  がガロア拡大になっているような中間体  $F$  を求めよ。

(4.5) 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)  $27x^3 - 18x + 4 = 0$

## §5 演習問題の解答

(4.1) の解答 (1) 正規拡大 (2 次拡大だから)

(2) 正規拡大 (2 次拡大だから)

(3) 正規拡大ではない ( $x^4 - 2$  の虚数の根は  $\mathbb{Q}(\sqrt[4]{2})$  に属さない)。

(4) 正規拡大ではない ( $x^3 - 2$  の虚数の根は  $\mathbb{Q}(\sqrt[3]{2})$  に属さない)。

(5) 正規拡大 ( $\sqrt{2} + \sqrt{3}$  の最小多項式のすべての根  $\pm\sqrt{2} \pm \sqrt{3}$  (複号任意) は  $\mathbb{Q}(\sqrt{2} + \sqrt{3})$  に属する)

(4.2) の解答 (1)  $S_2$  は位数が 2 だから、すべての部分群は、 $H_1 = S_2 = \{\text{id}, (12)\}$ ,  $H_2 = \{\text{id}\}$  である。 $S_2$  は可換群だから、すべての部分群は正規部分群である。

(2)  $S_3$  は位数が 6 だから、その部分群の位数は、1, 2, 3, 6 である。まず、 $H_1 = S_3, H_2 = \{\text{id}\}$  は自明な部分群である。位数 2 の部分群は、位数 2 の置換で生成されるが、位数 2 の置換は互換だから、 $H_3 = \{\text{id}, (12)\}$ ,  $H_4 = \{\text{id}, (23)\}$ ,  $H_5 = \{\text{id}, (13)\}$  の 3 通りである。位数 3 の部分群は、そこに含まれる置換の位数が 3 の約数、つまり 1 か 3 である。位数 3 の置換は、長さ 3 の巡回置換 (123) と (132) であるが、互いに逆元である。よって位数 3 の部分群は、 $H_6 = \{\text{id}, (123), (132)\}$  である。以上が  $S_3$  の部分群すべてである。

自明な部分群  $H_1, H_2$  は正規部分群であることは明らかである。(13)(12)(13)<sup>-1</sup> = (13)(12)(13) = (23) だから、 $H_3$  は正規部分群ではない。同様に、 $H_4, H_5$  も正規部分群ではない。 $A_3$  は偶置換全体であるから、 $\sigma \in A_3, \tau \in S_3$  のとき、 $\tau\sigma\tau^{-1}$  は偶置換となり  $A_3$  に属することより、 $A_3$  は正規部分群である。

(3)  $C_3$  は位数が 3 だから、その部分群の位数は 1 か 3 である。よって、 $H_1 = C_3, H_2 = \{\text{id}\}$  がすべての部分群である。

$C_3$  は可換群だから、すべての部分群は正規部分群である。

(4)  $C_4$  の位数は 4 だから、その部分群の位数は 1 か 2 か 4 である。まず、 $H_1 = C_4, H_2 = \{1\}$  が自明な部分群である。位数 2 の部分群は位数 2 の元で生成されるから、 $H_3 = \{1, -1\}$  である。

$C_4$  は可換群だから、すべての部分群は正規部分群である。

(5)  $D_4$  の位数は 8 だから、その部分群の位数は 1, 2, 4, 8 である。まず、 $H_1 = D_4, H_2 = \{\text{id}\}$  が自明な部分群である。位数 2 の部分群は位数 2 の元で生成されるから、 $H_3 = \{\text{id}, (13)(24)\}$ ,  $H_4 = \{\text{id}, (12)(34)\}$ ,  $H_5 = \{\text{id}, (14)(23)\}$ ,  $H_6 = \{\text{id}, (13)\}$ ,  $H_7 = \{\text{id}, (24)\}$  である。位数 4 の部分群は、まず、位数 4 の元で生成される  $H_8 = \{\text{id}, (1234), (1432), (13)(24)\}$  がある。位数 4 の部分群は、他に、位数 2 の元を 3 つ含むものが、

$H_9 = \{\text{id}, (13), (24), (13)(24)\}$ ,  $H_{10} = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$  の 2 つある。以上が  $D_4$  の部分群すべてである。

自明な部分群  $H_1, H_2$  は正規部分群であることは明らかである。 $\tau = (1234)$  とすると、 $\tau(12)(34)\tau^{-1} = (14)(23)$ ,  $\tau(14)(23)\tau^{-1} = (12)(34)$ ,  $\tau(13)\tau^{-1} = (24)$ ,  $\tau(24)\tau^{-1} = (13)$  であることから、 $H_4, H_5, H_6, H_7$  は正規部分群ではない。 $H_3, H_8, H_9, H_{10}$  は正規部分群である (詳細略)。

(4.3) の解答 (1)  $E = \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$  は  $\mathbb{Q}$  上 2 次拡大である。 $\text{Gal}(E/\mathbb{Q}) = \{\text{id}, \sigma\}$  ( $\sigma$  は複素共役)。ガロア群に非自明な部分群はない。従って中間体もない。

(2)  $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$  である (ただし、 $\omega = (-1 + \sqrt{-3})/2$ )。  $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$  は、 $E \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$  だから、6 次拡大である。ガロア群は  $S_3$  の部分群であるが、6 次拡大だから  $S_3$  に等しい。ガロア群の非自明な部分群は 4 つある。

$$H_1 = \{\text{id}, (23)\},$$

$$H_2 = \{\text{id}, (13)\},$$

$$H_3 = \{\text{id}, (12)\},$$

$$A_3 = \{\text{id}, (123), (132)\}.$$

ただし、 $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$  の順に解の番号を 1, 2, 3 とした。対応する中間体は、

$$E^{H_1} = \mathbb{Q}(\sqrt[3]{2}),$$

$$E^{H_2} = \mathbb{Q}(\sqrt[3]{2}\omega),$$

$$E^{H_3} = \mathbb{Q}(\sqrt[3]{2}\omega^2),$$

$$E^{A_3} = \mathbb{Q}(\omega)$$

である。

(3)  $E = \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}, -\sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i)$  である ( $i = \sqrt{-1}$ )。よって、 $E \supset \mathbb{Q}$  は 8 次拡大である。ガロア群の元による根  $\sqrt[4]{2}$  の像 (4 通りの可能性)



を決めると、 $-\sqrt[4]{2}$  の像もその  $-1$  倍に決まる。 $\sqrt[4]{2}i$  の像と  $-\sqrt[4]{2}i$  の像も同じく  $-1$  倍の関係にある。これと、元が 8 つであることから、

$$\text{Gal}(E/\mathbb{Q}) = \{\text{id}, (13), (24), (13)(24), (12)(34), (14)(23), (1234), (1432)\}.$$

ガロア群の非自明な部分群は位数が 2 か 4 であるが、位数 2 のものが 5 つ、位数 4 のものが 3 つある。

$$H_1 = \{\text{id}, (13)\},$$

$$H_2 = \{\text{id}, (24)\},$$

$$H_3 = \{\text{id}, (13)(24)\},$$

$$H_4 = \{\text{id}, (12)(34)\},$$

$$H_5 = \{\text{id}, (14)(23)\},$$

$$B_1 = \{\text{id}, (1234), (13)(24), (1432)\},$$

$$B_2 = \{\text{id}, (13), (24), (13)(24)\},$$

$$B_3 = \{\text{id}, (12)(34), (13)(24), (14)(23)\}.$$

対応する中間体は、

$$E^{H_2} = \mathbb{Q}(\sqrt[4]{2}),$$

$$E^{B_1} = \mathbb{Q}(i)$$

などである。

(4.4) の解答  $\text{Gal}(E/\mathbb{Q}) = S_3$  であり、 $S_3$  の非自明な部分群 4 つのうち、正規部分群は  $A_3 = \{\text{id}, (123), (132)\}$  だけである。 $\omega = (-1 + \sqrt{-3})/2$  と置くと、 $A_3$  に対応する中間体は、 $F = \mathbb{Q}(\omega)$  であり、このとき、 $F \supset \mathbb{Q}$  はガロア拡大になる。

(4.5) の解答 (1)  $x^3 + px + q = 0$  と照らすと、 $p = 2, q = 0$  である。この方程式の判別式は  $D = -27q^2 - 4p^3 = -32$  である。 $t^2 + 27qt - 27p^3 = 0$  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。 $D < 0$  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)  $x^3 + px + q = 0$  と照らすと、 $p = 0, q = 2$  である。この方程式の判別式は  $D = -27q^2 - 4p^3 = -108$  である。 $t^2 + 27qt - 27p^3 = 0$  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。 $D < 0$  だから、 $u, v$  は実数の範囲での 3 乗根となるので、 $u = 0, v = -\sqrt[3]{2}$  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)  $x^3 + px + q = 0$  と照らすと、 $p = -2/3, q = 4/27$  である。この方程式の判別式は  $D = -27q^2 - 4p^3 = 48/27$  である。 $t^2 + 27qt - 27p^3 = 0$  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。 $D > 0$  だから、 $u, v$  は互いに共役である。 $-2 \pm 2i$  は偏角が  $135^\circ$  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  $45^\circ$  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、

$$x_1 = \frac{u+v}{3} = \frac{(1+i) + (1-i)}{3} = \frac{2}{3},$$

$$x_2 = \frac{\omega u + \omega^2 v}{3} = \frac{\omega u + \bar{\omega} u}{3} = \frac{-1 - \sqrt{3}}{3},$$

$$x_3 = \frac{\omega^2 u + \omega v}{3} = \frac{\bar{\omega} v + \omega v}{3} = \frac{-1 + \sqrt{3}}{3}.$$