平成 16 年度代数学 B

講義ノート

広島大学大学院理学研究科　　都築 暢夫

この講義の目標

この講義の目的は、体の理論・ガロア理論を解説し、その応用として

(1) ギリシアの 3 大作図不能問題
(2) 作図可能な正多角形の決定
(3) 一般の 5 次以上の方程式の非可解性

を考察することにある。

体とは、加減乗除をもつ代数系である。与えられた体係数の方程式がいかに解けるか — これは昔からの大問題であった。もちろん現在も方程式を解くというのは代数幾何や数論幾何の中心的課題である。方程式を解くと、その解を含む新しい体 (拡大体) ができる。その相対的な状況を、いかに考察するのかという基本的枠組みを与えるのが体論・ガロア理論である。

作図可能とは何かというと、定規とコンパスをある決められたルールに従い有限回の操作で作図することができる図形のことである。ギリシアの 3 大作図不能問題とは、

- 立方倍積問題 : 与えられた立方体の 2 倍の体積を持つ立方体一辺の作図
- 角の 3 等分問題 : 任意の角の 3 等分線の作図
- 円積問題 : 与えられた円と同じ面積の正方形の作図

のことである。作図可能性と方程式には関係があり、作図問題は方程式の問題と置き換えられる。体の理論 (正しく言うと、体の拡大次数の概念) により、3 大作図不能問題は 19 世紀になって最終的に解決された。

代数的に解ける (可解性) とは、方程式の解が方程式の係数の加減乗除とそのべき根を有限回とった形で表されるということである。例えば 2 次方程式

$$ax^2 + bx + c = 0 \ (a \neq 0)$$

の解は、よく知られているように

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

となり、係数の加減乗除とそのべき根をとった形で表され、代数的に解ける。3, 4 次の方程式も一般に代数的に解ける。しかし、5 次以上になると状況は変わる。アーベルは 1824 年に 5 次以上の方程式が一般には代数的に解けないことを証明した。ガロアは各方程式がいつ代数的に解けるかという条件を、体の自己同型から定まるガロア群といものを用いて説明した。ガロアが創始した「ガロア理論」と呼ばれる理論を解説し、方程式の可解性を考察することがこの講義の最終目標の一つである。

Contents

1. 体

この章では、体の定義、体拡大とその拡大次数について解説する。

1.1. **定義.** 環とは加減乗に関して閉じた代数系で、体とは加減乗除に関して閉じた代数系のことである。

定義 1.

(1) R が可換環とは、加法 $+$ と乗法 $\times$ の 2 つの二項演算を持つ集合で、以下の条件を満たすものをいう。
  (a) $(R,+)$ はアーベル群である。すなわち、
    (i) $(a+b)+c=a+(b+c)\,(\forall a,b,c\in R)$
    (ii) $\exists 0\in R$ s.t. $a+0=0+a=a\,(\forall a\in R)$
    0 を零元という。
    (iii) $\forall a\in R,\exists b\in R$ s.t. $a+b=b+a=0$
    b を a の加法に関する逆元といい、$-a$ で表す。
    (iv) $a+b=b+a\,(\forall a,b\in R)$
  (b) $(R,\times)$ はモノイドで、モノイドとしての単位元 1 (通常単に単位元という) は $(R,+)$ の零元 0 と異なる。すなわち、
    (v) $(a\times b)\times c=a\times(b\times c)\,(\forall a,b,c\in R)$
    (vi) $\exists 1\in R\,(1\neq 0)$ s.t. $a\times 1=1\times a=a\,(\forall a\in R)$
    (vii) $a\times b=b\times a\,(\forall a,b\in R)$
  (c) 分配則 $(a+b)\times c=a\times c+b\times c\,(\forall a,b,c\in R)$ が成り立つ。
(2) R が整域とは、R が可換環であり、任意の $a,b\in R$ に対して次の条件を満たすものをいう。
  (viii) $ab=0\Rightarrow a=0$ または $b=0$
(3) R が体とは、R が可換環であり、次の条件を満たすものをいう。
  (ix) $a\neq 0\,(\forall a\in R)\Rightarrow\exists b\in R\,\text{s.t.}\,ab=ba=1$
  可換環 R において、上の条件を満たす a を単元という。さらに、b を a の乗法に関する逆元といい、a^{-1} で表す。

この講義では、単に環といえば可換環を意味する。乗法に関して非可換な体 (条件 (vi) を満たさない体) を斜体という。

命題 2.

環において、「体 $\Rightarrow$ 整域」 が成り立つ。

$\because$ $ab=0, a\neq 0$ とする。a^{-1} が存在し、$b=a^{-1}ab=a^{-1}\times 0=0$ となる。よって、整域である。□

例 3.
(1) 自然数全体の集合 $\mathbb{N}=\{0,1,2,\cdots\}$ は環でない。
(2) 有理整数全体の集合 $\mathbb{Z}=\{0,\pm 1,\pm 2,\cdots\}$ は整域であるが、体ではない。$\mathbb{Z}$ を有理整数環という。
(3) 有理数全体の集合 $\mathbb{Q}$、実数体全体の集合 $\mathbb{R}$、複素数体全体の集合 $\mathbb{C}$ は体である。それぞれ、有理数体、実数体、複素数体という。

例 4.
$K=\{a+b\sqrt{2}\in\mathbb{R}\,|\,a,b\in\mathbb{Q}\}$ は体である。

$\because$ $(\sqrt{2})^2=2$ なので、K が加法と乗法に関して閉じていることがわかる。K が環となることも容易に確かめられる。$\sqrt{2}$ は無理数なので、a,b のどちらかが 0 でなければ $a\pm\sqrt{2}b\neq 0$ となる。よって、$a^2-2b^2\neq 0$ であり、

$$(a+b\sqrt{2})^{-1}=\frac{a-b\sqrt{2}}{a^2-2b^2}\in K$$

である。0 でない元は可逆なので、体である。□

命題 5.

R を環とすると、零元、各元の加法に関する逆元、単位元、0 でない元の乗法に関する逆元は一意的である。

$\because$ a を 0 でない元とする。b, b' が a の逆元とすると

$$b = 1 \times b = (b'a)b = b'(ab) = b' \times 1 = b'$$

となり、逆元は一意である。他も同様。 □

1.2. **体拡大.** 2 つの体の間の関係を述べる。

定義 6.

(1) L を体とする。L の部分集合 K が L の部分体であるとは、L の加法と乗法に関して K が体になっていて、乗法の単位元を共有するものをいう。
(2) K が体 L の部分体のとき、L を K の拡大体という。通常、L/K の記号で体の拡大を表す。
(3) L/K を体拡大とする。K を含む L の部分体を拡大 L/K の中間体という。

例 7.
(1) $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ は体拡大の列である。$\mathbb{R}$ は体拡大 $\mathbb{C}/\mathbb{Q}$ の中間体になっている。
(2) K を例 4 で定めた体とする。

$$\mathbb{Q} \subset K \subset \mathbb{R}$$

は体拡大の列である。K は体拡大 $\mathbb{R}/\mathbb{Q}$ の中間体になっている。

命題 8.

L を体、K を L の部分集合で、L の 0 でない元を少なくとも一つ要素に持つとする。このとき、「$a, b \in K \Rightarrow a - b, ab^{-1} \in K\,(b \neq 0)$」が成り立つならば、$K$ は L の部分体である。

命題 9.

L を体とする。
(1) M を体拡大 L/K の中間体とすると、M は K の拡大体である。
(2) M/K と L/M を体拡大とすると、L/K は体拡大である。

記号を一つ導入する。共通部分が体になることは、定義の次の補題から保証される。補題の証明は命題 8 を適用すればよい。

定義 10.

L/K を体拡大とし、X を L の部分集合とする。中間体

$$K(X) = \bigcap_{M:\ \text{中間体} \supset X} M$$

を L に含まれる X で生成される K の拡大体という。$X = \{x_1, x_2, \cdots, x_n\}$ のとき、$K(X) = K(x_1, x_2, \cdots, x_n)$ と表す。

補題 11.

L/K を体拡大とし、$\{M_\lambda\}_{\lambda\in\Lambda}$ を中間体の族とする。このとき、

$$M = \bigcap_{\lambda\in\Lambda} M_\lambda$$

は、L/K の中間体である。

例 12.

K を例 4 の体とすると、実数体 $\mathbb{R}$ の中で $K = \mathbb{Q}(\sqrt{2})$ である。

$\because$ K は $\mathbb{R}/\mathbb{Q}$ の中間体で、$\sqrt{2} \in K$ なので、

$$K \supset \mathbb{Q}(\sqrt{2})$$

となる。一方、$\mathbb{Q}(\sqrt{2})$ は $\mathbb{Q}$ と $\sqrt{2}$ を含む体だから、$a + b\sqrt{2}\,(a, b \in \mathbb{Q})$ なる $\mathbb{R}$ の元を含む。よって、$K \subset \mathbb{Q}(\sqrt{2})$ である。したがって、等号が示せた。 □

1.3. **拡大次数.** 拡大体は、元の体上のベクトル空間である。体拡大の最も基本的な不変量である拡大次数は、ベクトル空間の次元で定義される。

定理 13.

L/K を体拡大とすると、L は K ベクトル空間である。

$\because$ L の加法がベクトル空間としての加法を、乗法が K の L へのスカラー倍を与える。ベクトル空間になることは、体の公理から明らか。 □

定義 14.

L/K を体拡大とする。

(1) L が K 上有限次元ベクトル空間のとき、L/K を有限次体拡大という。L の K 上の次元を体拡大 L/K の次数といい、$[L : K]$ で表す。

(2) L が K 上無限次元ベクトル空間のとき、L/K を無限次体拡大という。体拡大 L/K の次数は無限大と定め、$[L : K] = \infty$ と表す。

例 15.

(1) $[\mathbb{R} : \mathbb{Q}] = \infty, [\mathbb{C} : \mathbb{Q}] = \infty.$

$\because$ 例えば、濃度の議論を使え。 □

(2) $[\mathbb{C} : \mathbb{R}] = 2.$

(3) $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$

定理 16.

L/K を体拡大、M をその中間体とする。このとき、次は同値である。

(i) L/K は有限次体拡大である。

(ii) M/K と L/M はともに有限次体拡大である。

上の同値な条件が成り立つとき

$$[L : K] = [M : K][L : M]$$

となる。(この式は、$\infty = \infty$ を含めると、一般に成り立つ。)

$\because$ (i) $\Rightarrow$ (ii) は明らか。
(ii) $\Rightarrow$ (i) M の K 上の一組の基底を $m_1, m_2, \cdots, m_e$ とし、L の M 上の一組の基底を $l_1, l_2, \cdots, l_d$ とする。すると、$l_i m_j \, (1 \leq i \leq d, 1 \leq j \leq e)$ は L の K 上の一組の基底になる。実際、

$$\sum_{i,j} a_{ij} l_i m_j = 0 \ (a_{ij} \in K)$$

とすると、$l_1, l_2, \cdots, l_d$ は M 上の L の基底なので、各 i に対して

$$\sum_{j} a_{ij} m_j = 0$$

となる。$m_1, m_2, \cdots, m_e$ は K 上の M の基底なので、$a_{ij} = 0 \, (\forall i, j)$ となる。L が K 上 $l_i m_j$ たちで生成されることは明らか。
上の証明は、同値な条件 (i) と (ii) がなりたつとき

$$[L : K] = de = [M : K][L : M]$$

となることも示している。 □

系 17.

素数次数の拡大 L/K の中間体は K または L のみである。

命題 18.

体拡大 L/K において、「$L = K \iff [L : K] = 1$」である。

$\because$ L は K を含み、K 上 1 次元だから。 □

命題 19.

L/K を有限次拡大とする。ある $\alpha_1, \cdots, \alpha_n \in L$ が存在して $L = K(\alpha_1, \cdots, \alpha_n)$ となる。

$\because$ 拡大次数 $[L : K]$ に関する帰納法で証明する。$[L : K] = 1$ のときは何も証明することはない。$[L : K] > 1$ とする。$\alpha \in L \setminus K$ に対して $L = K(\alpha)$ ならばよい。$L \neq K(\alpha)$ とすると、$[L : K(\alpha)] = [L : K]/[K(\alpha) : K] < [L : K]$ なので、ある $\beta_1, \cdots, \beta_m \in L$ が存在して

$$L = K(\alpha)(\beta_1, \cdots, \beta_m) = K(\alpha, \beta_1, \cdots, \beta_m)$$

となるので、命題は成り立つ。 □

例 20.
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ は $\mathbb{Q}$ を含む $\mathbb{R}$ の部分体であり、

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \,|\, a, b, c, d \in \mathbb{Q}\}$$

となる。よって、

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$$

となる。明らかに $\mathbb{Q}(\sqrt{2})$ は $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ の中間体となる。定理 16 から、$\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$ は有限次拡大で

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]/[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4/2 = 2$$

となる。

$\because$ $L = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \,|\, a, b, c, d \in \mathbb{Q}\}$ とおく。

$$\begin{aligned}(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) + (s + t\sqrt{2} + u\sqrt{3} + v\sqrt{6}) \\ = (a + s) + (b + t)\sqrt{2} + (c + u)\sqrt{3} + (d + v)\sqrt{6} \\ (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})(s + t\sqrt{2} + u\sqrt{3} + v\sqrt{6}) \\ = (as + bt + cu + dv) + (at + bs + 3cv + 3du)\sqrt{2} \\ +(au + 2bv + cs + 2dt)\sqrt{3} + (av + bu + ct + ds)\sqrt{6}\end{aligned}$$

となるので、L は加法と乗法に関して閉じている。$\mathbb{R}$ が体なので、加法と乗法に閉じた L が環となることは明らか。

$1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ が L の $\mathbb{Q}$ 上の基底になることを示す。

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$$

とする。$a = b = c = d = 0$ でないとして矛盾を導く。a, b, c, d のいずれか一つは 3 の倍数でないとしてよい。

$$\begin{aligned}a + b\sqrt{2} &= -c\sqrt{3} - d\sqrt{6} \\ a^2 + 2ab\sqrt{2} + 2b^2 &= 3c^2 + 6cd\sqrt{2} + 6d^2\end{aligned}$$

$\sqrt{2}$ は無理数なので、

$$\begin{cases} a^2 + 2b^2 = 3c^2 + 6d^2 \\ 2ab = 6cd \end{cases}$$

となる。

(i) $c = d = 0$ のときは、$a = b = 0$ となり、仮定に反する。

(ii) $c \neq 0, d = 0$ とすると、a, b の一方が 0 になる。$a = 0$ とすると $2b^2 = 3c^2$ となり、両辺の 3 の因子に着目すると、右辺は 3 の偶数乗、左辺は奇数乗になり矛盾である。$b = 0$ のときも同様。また、$c = 0, d \neq 0$ のときも同様である。

(iii) $cd \neq 0$ とする。2 番目の式から、a, b のいずれかは 3 の倍数である。一番目の式から、他方も 3 の倍数である。再び 2 番目の式から、c, d の一方は 3 の倍数となる。再び一番目の式を用いて、c, d はともに 3 の倍数である。
a, b, c, d のすべてが 3 の倍数となり、矛盾が生じた。

これで、L が $\mathbb{Q}$ 上の 4 次元ベクトル空間になることが証明できた。各行が 0 でない 4 つの L の元の積

$$(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})(a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6})(a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6})(a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6})$$

は 0 でない有理数になるので、L の 0 でない元は乗法に関して可逆である。したがって、L は体であり、

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

となる。

以上で、$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ が $\mathbb{Q}$ 上の 4 次拡大体であることが示せた。 □

例 21.

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ である。

$\because$ $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbb{Q}(\sqrt{2} + \sqrt{3})$ は明らか。$\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ を示せば、$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2} + \sqrt{3})$ となる。

$\alpha = \sqrt{2} + \sqrt{3}$ とする。$\alpha^2 - 2\sqrt{2}\alpha + 2 = (\alpha - \sqrt{2})^2 = (\sqrt{3})^2 = 3$ より、

$$\sqrt{2} = \frac{\alpha^2 - 1}{2\alpha}, \quad \sqrt{3} = \frac{\alpha^2 + 1}{2\alpha}$$

となるので、ともに $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ に属する。 □

問 1.

$d = -1$ または $d = \pm p_1 p_2 \cdots p_r$ (p_i たちは互いに異なる素数) とする。

(1) $\sqrt{d}$ は無理数 (= 有理数でない複素数) であることを証明せよ。

(2) $F = \mathbb{Q}(\sqrt{d})$ は $\mathbb{Q}$ 上の 2 次拡大体であることを示せ。

問 2.
Cauchy 列である有理数列全体の集合に同値関係を入れて、実数体を構成せよ。また、実数体の公理を満たすことを確認せよ。

問 3.
(1) 可算濃度・連続濃度について勉強せよ。
(2) 例 15 を証明せよ。

2. 体の作り方

体の作り方は、整域の商体をとるのと環の極大イデアルに関する剰余体をとるという 2 通りの方法がある。この章では、それらの構成について述べる。

2.1. **体の同型.** 環の準同型と同型の定義を復習する。

定義 22.

R と S を環とする。

(1) 写像 $\varphi : R \to S$ が環準同型とは、次の条件を満たすものである。
  (i) $\varphi(a+b) = \varphi(a) + \varphi(b)\ (\forall\, a, b \in R)$
  (ii) $\varphi(ab) = \varphi(a)\varphi(b)\ (\forall\, a, b \in R)$
  (iii) $\varphi(1) = 1$

(2) 環準同型 $\varphi : R \to S$ が同型とは、ある環準同型 $\psi : S \to R$ が存在して、

$$\psi \circ \varphi = \mathrm{id}_R \text{ かつ } \varphi \circ \psi = \mathrm{id}_S$$

となるものをいう。

(3) R と S が同型とは、ある同型である準同型 $\varphi : R \to S$ が存在することをいう。

環 A 上の A 多元環に対して、A 環準同型や A 同型が同様に定義される。これらの定義は省略する。

補題 23.

$\varphi : R \to S$ を環の準同型とする。

(1) $\varphi(-a) = -\varphi(a)$
(2) $\varphi(a^{-1}) = \varphi(a)^{-1}$

系 24.

体からの環準同型は単射である。

$\because$ 体では 0 でない元は可逆元だから、その像も可逆になり 0 でない。 □

命題 25.

$\varphi : R \to S$ を環の準同型とする。このとき、次は同値である。

(i) φ は同型である。
(ii) φ は全単射である。

$\because$ (ii) $\Rightarrow$ (i) を証明する。φ は全単射なので、集合としての逆写像

$$\varphi^{-1} : S \to R$$

が環準同型になればよい。$a, b \in S$ に対して

$$\varphi(\varphi^{-1}(a+b)) = a + b = \varphi(\varphi^{-1}(a)) + \varphi(\varphi^{-1}(b)) = \varphi(\varphi^{-1}(a) + \varphi^{-1}(b))$$

となる。φ は単射より

$$\varphi^{-1}(a+b) = \varphi^{-1}(a) + \varphi^{-1}(b)$$

である。他の条件も同様に示せるので、φ^{-1} は環準同型である。 □

定義 26.

2 つの体 K と L が同型とは、環として同型なことを言う。

2.2. **商体.** 有理整数環から有理数体の構成法を一般化する。

定理-定義 27.

R を整域とする。このとき、体 K と単射環準同型 $\iota : R \to K$ の組 (K, ι) で、以下の普遍性 $(*)$ を満たすものがただ一つ存在する。この組 (K, ι) を R の商体という。通常は、R を K の部分環とみなし、単に商体 K とする。

$(*)$ 任意の体 F と任意の単射環準同型 $\theta : R \to F$ に対して、環準同型 $\alpha : K \to F$ で図式

$$\begin{array}{ccc} R & \xrightarrow{\iota} & K \\ & \theta \searrow \quad \swarrow \alpha & \\ & F & \end{array}$$

が可換になるものがただ一つ存在する。

$\because$ 組 (K, ι) を具体的に構成して、普遍性 $(*)$ を満たすことを証明する。

集合 $R \times (R \setminus \{0\})$ 上に関係 $\sim$ を

$$(a, b) \sim (c, d) \iff ad - bc = 0$$

と定める。すると、$\sim$ は同値関係である (簡単なので証明は略)。K を $R \times (R \setminus \{0\})$ の $\sim$ による同値類全体の集合

$$K = R \times (R \setminus \{0\}) / \sim$$

とする。(a, b) で代表される同値類を $\dfrac{a}{b}$ と表す。K の加法と乗法を

$$\begin{array}{rcl} \dfrac{a}{b} + \dfrac{c}{d} & = & \dfrac{ad + bc}{bd} \\ \dfrac{a}{b} \dfrac{c}{d} & = & \dfrac{ac}{bd} \end{array}$$

と定めると、これは代表元の取り方によらず定まる。K は $\dfrac{0}{1}$ を零元 0、$\dfrac{1}{1}$ を単位元 1 とする体になることは、定義 1 の公理を確かめることからわかる。

写像 $\iota : R \to K$ を

$$\iota(a) = \frac{a}{1}$$

と定めると、ι は単射環準同型になることが確かめられる。

$\because$ ι が単射になることのみチェックする。$\iota(a) = 0 = \frac{0}{1}$ とすると

$$a = a \times 1 = 0 \times 1 = 0$$

となり、ι の核　$\ker(\iota)$ は 0 のみである。したがって、ι は単射である。 □

普遍性 $(*)$ が成り立つこと：$\alpha : K \to F$ を

$$\alpha(\frac{a}{b}) = \frac{\theta(a)}{\theta(b)}$$

と定める。α は代表元の取り方によらず定まり、環準同型になる。

$$\alpha(\frac{a}{b}) = \frac{\alpha(\iota(a))}{\alpha(\iota(b))} = \frac{\theta(a)}{\theta(b)}$$

より、α は θ のみで決まる。よって、α の唯一性がいえ、普遍性 $(*)$ が成り立つ。

組 (K,ι) の唯一性：(K',ι') をもう一つの組とする。(K,ι) と (K',ι') に関する普遍性から、2つの図式

$$\begin{array}{ccc} R & \xrightarrow{\iota} & K \\ & {\scriptstyle\iota'}\searrow \quad \swarrow{\scriptstyle\alpha} & \\ & K' & \end{array} \qquad \begin{array}{ccc} R & \xrightarrow{\iota'} & K' \\ & {\scriptstyle\iota}\searrow \quad \swarrow{\scriptstyle\beta} & \\ & K & \end{array}$$

が可換になる。(K,ι) と (K',ι') の普遍性から

$$\beta\circ\alpha=\mathrm{id}_K \qquad \alpha\circ\beta=\mathrm{id}_{K'}$$

となる。したがって、 商体は一意的である。 □

例 28.
体 K の商体は K 自身である。

例 29.
(1) 有理整数環 $\mathbb{Z}$ の商体は有理数体 $\mathbb{Q}$ である。
(2) K を体とする。多項式環 $K[x]$ の商体を有理多項式体 $K(x)$ という。

例 30.
L/K を体拡大、$\alpha\in L$ とする。$K[\alpha]$ の商体は $K(\alpha)$ である。

2.3. **極大イデアルと剰余体.** この節では、極大イデアルによる剰余体について復習する。

定義 31.

R を環とする。
(1) R の空でない部分集合 I がイデアルとは、
(i) $x,y\in I\ \Rightarrow\ x+y\in I.$
(ii) $a\in R, x\in I\ \Rightarrow\ ax\in I.$
R のことを単位イデアルという。単位イデアルでないイデアルを真のイデアルという。
(2) R の真のイデアル $\mathfrak{p}$ が素イデアルであるとは、

$$ab\in\mathfrak{p}\ \Rightarrow\ a\in\mathfrak{p}\ \text{または}\ b\in\mathfrak{p}$$

となることをいう。
(3) R のイデアル $\mathfrak{m}$ が極大イデアルであるとは、R の真のイデアル I に対して

$$\mathfrak{m}\subset I\ \Rightarrow\ I=\mathfrak{m}$$

が成り立つものをいう。

命題-定義 32.

I を環 R の真のイデアルとする。環と環準同型の組 $(\overline{R},\pi:R\to\overline{R})$ で、以下の普遍性 $(**)$ を満たすものがただ一つ存在する。

$(**)$ 任意の環 S と任意の環準同型 $\varphi:R\to S$ で $\varphi(I)=\{0\}$ となるものに対して、環準同型 $\psi:\overline{R}\to S$ で図式

$$\begin{array}{ccc} R & \xrightarrow{\pi} & \overline{R} \\ & {\scriptstyle\varphi}\searrow \quad \swarrow{\scriptstyle\psi} & \\ & S & \end{array}$$

が可換になるものがただ一つ存在する。

特に、$\pi:R\to\overline{R}$ は全射である。組 $(\overline{R},\pi:R\to\overline{R})$ のことを R の I による剰余環といい、通常は π を省略して環 $\overline{R}$ のみを R/I と表す。

∵ 剰余環 R/I の構成を復習する。R 上に以下のように関係 $\sim$ を入れる。

$$a \sim b \Longleftrightarrow a - b \in I$$

すると、$\sim$ は同値関係になる。$\sim$ による同値類全体の集合を R/I と表し、自然な全射 $R \to R/I$ による $a \in R$ の像を $\overline{a}$ で表す。R/I に加法と乗法を

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \\ \overline{a}\overline{b} &= \overline{ab} \end{aligned}$$

と定める。上の定義は代表元の取り方によらず定まり、well-defined である。普遍性と唯一性が成り立つことは、定理 27 の証明とほぼ同じ。 □

命題 33.

I を環 R のイデアルとする。
(1) I が素イデアル $\Leftrightarrow R/I$ が整域.
(2) I が極大イデアル $\Leftrightarrow R/I$ が体.

∵ (2) のみ証明する。$\Rightarrow$ の証明 : I を極大イデアルと仮定する。$x \in R$ に対して、$\overline{x} \neq \overline{0}$ が R/I で可逆になることを証明する。

$$J = \{ax + y \,|\, a \in R, y \in I\}$$

とおくと、J は R の I を含むイデアルになる。$x \notin I$ かつ $x = x + 0 \in J$ で、I は極大イデアルだから $J = R$ となる。よって、ある $a \in R$ と $y \in I$ が存在して

$$ax + y = 1$$

となる。これは、$\overline{ax} = \overline{1}$ を意味し、$\overline{x}$ は R/I で可逆である。
$\Leftarrow$ の証明 : R/I が体と仮定する。I を含む R の真のイデアル J に対し、$J = I$ を証明する。すると、I は極大イデアルである。$x \in J \setminus I$ とする。R/I は体なので、$\overline{ax} = \overline{1}$ となる $a \in R$ が存在する。よって、

$$1 \in ax + I \subset J$$

となり、J が真のイデアルであることに矛盾する。したがって、$J = I$ である。 □

系 34.

極大イデアルは素イデアルである。

∵ 体は整域だから。 □

Zorn の補題を用いると次の極大イデアルの存在定理が証明できる。

定理 35.

I を環 R の真のイデアルとする。I を含む極大イデアルが存在する。

2.4. p **元体.** 有理整数環 $\mathbb{Z}$ のイデアルを復習する。

定義 36.

環 R が単項イデアル整域 (principal ideal domain, P.I.D. と略記する) とは、任意のイデアルが高々一つの元で生成されている整域のことをいう。

$a \in R$ で生成される R のイデアルを (a) と表すことにする。

定理 37.

a を 0 でない整数とする。任意の整数 b に対して

$$b = qa + r \quad (0 \leq r < |a|)$$

となる整数 q, r が存在する。

定理 38.

(1) 有理整数環 $\mathbb{Z}$ は P.I.D. である。
(2) 次の集合の射は全単射である。

$$\begin{array}{ccc} \{\mathbb{Z} \text{ の極大イデアル}\} & \to & \{\text{ 素数全体の集合 }\} \\ (a) & \mapsto & a\ (a > 0). \end{array}$$

さらに、$\mathbb{Z}$ の極大イデアルでない素イデアルは零イデアル (0) のみ。

命題-定義 39.

p を素数とする。 剰余環 $\mathbb{Z}/(p)$ は p 個の元からなる体である。この体を $\mathbb{F}_p$ と表し、p 元体という。

2.5. **体の標数.** 環の準同型定理を復習し、部分体の中で一番小さな体 (素体) を調べる。

定理 40.

$\varphi : R \to S$ を環準同型とする。
(1) φ の核 $\ker(\varphi) = \{a \in R \,|\, \varphi(a) = 0\}$ は R の真のイデアルである。
(2) φ の像 $\mathrm{im}(\varphi)(= \varphi(R))$ は S の部分環になる。
(3) φ が誘導する写像

$$\begin{array}{ccc} R/\ker(\varphi) & \to & \mathrm{im}(\varphi) \\ \overline{a} & \mapsto & \varphi(a) \end{array}$$

は環の同型となる。

体に標数という概念を導入する。

命題 41.

任意の環 R に対して、環準同型 $\mathbb{Z} \to R$ がただ一つ存在する。

$\because$ 写像 $\varphi : \mathbb{Z} \to R$ を

$$n \mapsto \begin{cases} 1 + 1 + \cdots + 1\,(n\text{個}) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -\varphi(-n) & \text{if } n < 0 \end{cases}$$

と定める。正整数 m, n に対して

$$mn = 1 + 1 + \cdots + 1\,(mn\text{個})$$

を利用すると、φ が環準同型であることが証明できる。$\mathbb{Z}$ はアーベル群として 1 で生成されるから、$\mathbb{Z}$ から R への環準同型は φ のみである。 □

命題-定義 42.

K を体とする。ただ一つ存在する環準同型 $\varphi : \mathbb{Z} \to K$ の核 $\ker(\varphi)$ は素イデアルである。$\ker(\varphi) = (0)$ のとき、体 K は標数 0 といい、ある素数 p に対して $\ker(\varphi) = (p)$ のとき、体 K は標数 p という。K の標数を $\mathrm{char}(K)$ と表す。

$\because$ K は体だから K の部分環 $\mathrm{im}(\varphi)$ は整域である。定理 33 と準同型定理 40 より $\ker(\varphi)$ は素イデアルになるので、定理 38 から主張が成り立つ。 □

定理 27 と命題 32 の普遍性から次が成り立つ。

系-定義 43.

K を体とする。

(1) $\mathrm{char}(K) = 0 \iff \mathbb{Q} \subset K$.
(2) $\mathrm{char}(K) = p > 0 \iff \mathbb{F}_p \subset K$.

K に含まれる $\mathbb{Q}$ または $\mathbb{F}_p$ を K の素体という。

問 4.
Zorn の補題を勉強せよ。さらに、定理 35 を証明せよ。

問 5.
定理 37, 38 を証明せよ。

問 6.
集合の直積 (または位相空間の直積) を普遍性を用いて定義し、直積の存在を証明せよ。

3. 多項式環と既約多項式

体の拡大は、多項式環をその極大イデアルで割った剰余体として作るのが最も一般的な方法である。この章では多項式環について復習をする。

3.1. 多項式環は P.I.D.

K を体とする。この節では、K 上の一変数多項式環 $K[x]$ (単に多項式環という) が P.I.D. であることを復習する。

集合 $\overline{\mathbb{N}}$ を

$$\overline{\mathbb{N}} = \mathbb{N} \cup \{-\infty\}$$

と定め、$\mathbb{N}$ 上の加法を

$$a + (-\infty) = -\infty + a = -\infty \ (\forall\, a \in \overline{\mathbb{N}})$$

と延長する。また、順序を

$$-\infty < a$$

と延長する。

補題 44.

a, b, c を $\overline{\mathbb{N}}$ の元とする。
(1) $\overline{\mathbb{N}}$ 上の加法は結合則、すなわち

$$(a+b)+c = a+(b+c)$$

を満たす。
(2) $\overline{\mathbb{N}}$ 上の関係 $\leq$ は順序の公理
(i) $a \leq a$.
(ii) $a \leq b$ かつ $b \leq a \Rightarrow a = b$.
(iii) $a \leq b$ かつ $b \leq c \Rightarrow a \leq c$.
を満たす。さらに、$\overline{\mathbb{N}}$ は全順序集合で、任意の空でない部分集合に極小元が存在する。

定義 45.

K 上の多項式 $f(x) \in K[x]$ に対して $\overline{\mathbb{N}}$ に値を持つ次数 $\deg(f(x))$ を

$$\deg(f(x)) = \begin{cases} n & \text{if } f(x) = a_0 x^n + \cdots + a_n \ (a_i \in K, a_0 \neq 0) \\ -\infty & \text{if } f(x) = 0 \end{cases}$$

と定める。

命題 46.

$f(x), g(x) \in K[x]$ とする。
(1) $\deg(f(x)) = -\infty \iff f(x) = 0$.
(2) $\deg(f(x)+g(x)) \leq \inf\{\deg(f(x)), \deg(g(x))\}$.
(3) $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.

定理 47.

$f(x) \in K[x], f(x) \neq 0$ とする。任意の $g(x) \in K[x]$ に対して、ある $q(x), r(x) \in K[x]$ で

$$g(x) = q(x)f(x) + r(x) \quad (\deg(r(x)) < \deg(f(x)))$$

を満たすものが存在する。

∵ $\deg(g(x))$ に関する帰納法で証明する。$\deg(g(x)) < \deg(f(x))$ ならば $q(x) = 0, r(x) = g(x)$ とすればよい。$\deg(g(x)) \geq \deg(f(x))$ とし、$f(x)$ と $g(x)$ それぞれの次数を m と n $(m \leq n)$、最大次数の係数を a, b とする。$a, b \neq 0$ なので、

$$\deg\left[g(x) - \frac{b}{a}x^{n-m}f(x)\right] < \deg(g(x))$$

となる。帰納法の仮定より、

$$g(x) - \frac{b}{a}x^{n-m}f(x) = s(x)f(x) + t(x) \quad (\deg(t(x)) < \deg(f(x)))$$

となるので、$q(x) = \frac{b}{a}x^{n-m} + s(x), r(x) = t(x)$ と置けばよい。 □

定理 48.

$K[x]$ は P.I.D. である。

∵ I を $K[x]$ の零イデアルでないイデアルとする。(零イデアルは (0) なので、明らかに単項イデアルである。)

$$n = \inf\{\deg(f(x)) \mid f(x) \in I, f(x) \neq 0\}$$

とおくと、右辺の集合は空集合でない。命題 46 (1) から $-\infty$ を含まず、補題 44 から n は自然数になる。$f(x) \in I$ を

$$\deg(f(x)) = n$$

となる元とする。以下、$I = (f(x))$ を示す。

$I \supset (f(x))$ は明らか。$g(x) \in I$ とする。定理 47 から

$$g(x) = q(x)f(x) + r(x) \quad (\deg(r(x)) < \deg(f(x)))$$

を満たす $q(x), r(x) \in K[x]$ が存在する。I はイデアルなので

$$r(x) = g(x) - q(x)f(x) \in I$$

となる。$f(x)$ の次数の最小性から、$\deg(r(x)) = -\infty$ でなければならない。よって、$r(x) = 0$ となり、

$$g(x) = q(x)f(x)$$

である。したがって、$I \subset (f(x))$ である。 □

定義 49.

$f(x), g(x) \in K[x]\,(f(x) \neq 0)$ とする。$f(x)$ が $g(x)$ を割り切るとは、$g(x) \in (f(x))$ となることをいう。記号では、$f(x) \mid g(x)$ と表す。

3.2. **既約多項式.** 任意の多項式は既約多項式という基本的なものの積に書き表せる。これは、整数における素数と素因数分解に対応する。

命題 50.

$K[x]^\times$ を $K[x]$ の単元群とすると $K[x]^\times = K^\times$ となる。

∵ $K^\times \subset K[x]^\times$ は明らか。$f(x)g(x) = 1$ とすると、命題 46 (3) から

$$\deg(f(x)) + \deg(g(x)) = \deg(f(x)g(x)) = \deg(1) = 0$$

となるので、$f(x)$ と $g(x)$ はともに 0 次である。よって、$K[x]^\times = K^\times$ である。 □

定義 51.

(1) $f(x) \in K[x]$ を 0 でない多項式とする。$f(x)$ が単多項式 (monic) とは、$f(x)$ の最大次数の係数が 1 であるものをいう。
(2) $p(x) \in K[x]$ を 0 でも単元でもない多項式とする。$p(x)$ が既約 (irreducible) 多項式とは、

$$p(x) = f(x)g(x)$$

と表せるとき、$f(x)$ または $g(x)$ が $K[x]$ の単元になるものをいう。$p(x)$ が既約でないとき可約という。

例 52.

$K[x]$ の 1 次多項式は既約である。

例 53.

(1) $f(x) = ax^2 + bx + c \in \mathbb{R}[x]\,(a \neq 0)$ を実数係数の 2 次多項式とし、$D = b^2 - 4ac$ を判別式とする。このとき、

$$f(x) \text{ が既約} \iff D < 0$$

が成り立つ。
(2) $g(x) \in \mathbb{R}[x]$ を実数係数の奇数次多項式とする。このとき、$g(x)$ は可約である。

定理 54.

(1) 次の集合の射は全単射である。

$$\begin{array}{ccc} \{K[x] \text{ の単多項式}\} & \to & \{K[x] \text{ のイデアル}\} \setminus \{(0)\} \\ f(x) & \mapsto & (f(x)). \end{array}$$

(2) 次の集合の射は全単射である。

$$\begin{array}{ccc} \{K[x] \text{ の既約単多項式}\} & \to & \{K[x] \text{ の極大イデアル}\} \\ p(x) & \mapsto & (p(x)). \end{array}$$

さらに、$K[x]$ の極大イデアルでない素イデアルは零イデアル (0) のみ。

$\because$ (1) $K[x]$ が P.I.D. であることと命題 50 から明らか。
(2) $K[x]$ は整域なので、(1) から以下の 2 つのことを示せばよい。
1° $K[x]$ の零イデアルでない素イデアル $(p(x))$ に対し、$p(x)$ が既約多項式であること。
2° $p(x)$ を既約多項式とすると、$(p(x))$ が極大イデアルになること。
1° の証明：$p(x) = f(x)g(x)$ とする。$(p(x))$ は素イデアルなので、$f(x) \in (p(x))$ または $g(x) \in (p(x))$ となる。$f(x) \in (p(x))$ とすると、ある　$h(x) \in K[x]$ が存在して

$$f(x) = h(x)p(x)$$

となる。よって、

$$f(x) = h(x)p(x) = f(x)g(x)h(x)$$

となる。$K[x]$ は整域なので、$g(x)h(x) = 1$　となり、$g(x)$ は単元である。したがって、$p(x)$ は既約多項式である。$g(x) \in (p(x))$ の場合も同じ。
2° の証明：　$(p(x))$ を含むイデアルが存在するとする。$K[x]$ は P.I.D. なので、$(p(x)) \subset (f(x)) \neq K[x]$ となる多項式 $f(x)$ が存在するとする。$p(x) \in (f(x))$ なので、ある $g(x) \in K[x]$ が存在して

$$p(x) = f(x)g(x)$$

となる。$p(x)$ は既約多項式なので、$g(x)$ は単元になる。よって、$(f(x)) = (p(x))$ である。したがって、$(p(x))$ は極大イデアルである。　□

定理-定義 55.

$f(x) \in K[x]$ を 0 でも単元でもない多項式とする。このとき、$a \in K^\times$ といくつかの既約単多項式 $p_1(x), p_2(x), \cdots, p_d(x)$ が存在して

$$f(x) = ap_1(x)p_2(x)\cdots p_d(x)$$

と表せる。この表示は、順番を除いて一意的である。この表示を $f(x)$ の既約分解といい、各 $p_i(x)$ のことを $f(x)$ の既約因子という。

$\because$ 既約多項式の積で表されることを、次数 $\deg(f(x))$ に関する帰納法で証明する。$f(x)$ が既約多項式のときは、何もすることがない。既約でないとすると、ある次数が 1 以上の 2 つの多項式 $g(x)$ と $h(x)$ が存在して

$$f(x) = g(x)h(x)$$

となる。命題 46 (3) から、$g(x)$ と $h(x)$ の次数は $f(x)$ の次数より小さい。帰納法の仮定から、$f(x)$ は既約多項式の積で表せる。

表示の一意性を証明する。

$$f(x) = bq_1(x)q_2(x)\cdots q_e(x) \quad (b \in K^\times, q_i(x) \text{ 既約単多項式})$$

と既約多項式の積で表示できたとする。最大次数の係数を比較して、$a = b$ となる。定理 54 (2) から $(p_1(x))$ は素イデアルである。

$$q_1(x)q_2(x)\cdots q_e(x) \in (f(x)) \subset (p_1(x))$$

より、ある j が存在して $(q_j(x)) \subset (p_i(x))$ となる。$(q_j(x))$ は極大イデアルなので、

$$(q_j(x)) = (p_i(x))$$

となる。定理 54 (2) の全単射性から、

$$q_j(x) = p_i(x)$$

となる。次数に関する帰納法を適用すると、順番を除いた既約多項式の積表示一意性を得る。 □

3.3. **多項式の根.** 多項式の根という概念を復習しておく。

定義 56.

$f(x) \in K[x]$ を 0 でない多項式とする。$\alpha \in K$ が $f(x)$ の根とは、$f(\alpha) = 0$ となる元のことをいう。

命題 57.

$f(x) \in K[x]$ を 0 でない多項式、$\alpha \in K$ とする。このとき、次は同値になる。
(i) α は $f(x)$ の根である。
(ii) $x - \alpha$ は $f(x)$ の 1 次の既約因子である。

$\because$ 定理 47 から $f(x) = (x - \alpha)q(x) + r\,(r \in K)$ となる $q(x) \in K[x]$ がとれる。このとき、「$f(\alpha) = 0 \Leftrightarrow r = 0$」である。 □

定理 58.

$f(x) \in K[x]$ を 0 でない多項式で、その次数を d とする。このとき、$f(x)$ の根は高々 d 個存在する。

$\because$ 定理 55 から、$f(x)$ は単元か既約多項式の積で表される。命題 46 を用いると、既約因子は高々 d 個がわかる。命題 57 から、根になるのは 1 次の既約因子のみ。 □

問 7.
例 53 を証明せよ。

問 8.
$\mu \subset K^\times$ を体の乗法群の有限部分群とする。このとき、μ は巡回群であることを証明せよ。

4. 単拡大

体拡大の構成において、一つの元で生成される拡大 – 単拡大 – は最も基本的なものである。この章では、単拡大について解説する。

この章を通して、L/K を体拡大とする。

4.1. 代数的・超越的.

代数拡大という概念を導入する。

定義 59.

$\alpha \in L$ とする。
(1) α が K 上代数的とは、ある 0 でない K 係数多項式 $f(x)$ が存在して α が K の根になることをいう。
(2) α が K 上超越的とは、K 上代数的でないことをいう。

例 60.

(1) $\sqrt{2} \in \mathbb{R}$ は $\mathbb{Q}$ 上代数的である。
(2) $\pi \in \mathbb{R}$ は $\mathbb{Q}$ 上超越的である。

定義 61.

(1) 体拡大 L/K が代数的とは、L のすべての元が代数的であることをいう。
(2) 体拡大 L/K が超越的とは、代数的でないことをいう。

例 62.

(1) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ は代数拡大である。
$\because$ $\alpha = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})\,(a, b \in \mathbb{Q})$ とする。$f(x) = x^2 - 2ax + a^2 - 2b^2 \in \mathbb{Q}[x]$ とおくと、α は $f(x)$ の根である。 □

(2) $\mathbb{Q}(\pi)/\mathbb{Q}$ は超越拡大である。
(3) 体拡大 $\mathbb{R}/\mathbb{Q}$ と $\mathbb{C}/\mathbb{Q}$ は超越的である。
(4) 体拡大 $\mathbb{C}/\mathbb{R}$ は代数的である。

命題 63.

体の有限次拡大は代数的である。

$\because$ L/K を体の有限次拡大で拡大次数が n とする。任意の $\alpha \in L\,(\alpha \neq 0)$ が代数的であることを示す。
$[L : K] = n$ なので、$1, \alpha, \alpha^2, \cdots, \alpha^n$ は K 上 1 次従属である。よって、

$$a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1} + a_n = 0$$
$$(a_0, \cdots, a_n) \neq (0, \cdots, 0)$$

となる。したがって、ある 0 でない K 係数多項式が存在して、α はその根になる。 □

例 64.

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ (例 20) なので、$\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ は代数拡大である。

4.2. **最小多項式.** 代数的元の最小多項式を定義する。

命題-定義 65.

$\alpha \in L$ を K 上の代数的な元とする。α を根にもつ K 上の単多項式 $p(x)$ で、α を根にもつ任意の多項式 $f(x)$ に対して $p(x) \,|\, f(x)$ となるものがただ一つ存在する。$p(x)$ を α の K 上の最小多項式といい、この講義では $p_{\alpha,K}(x)$ と表す。

$\because$ α を根に持つ多項式の全体 I は、$K[x]$ の真のイデアルになる。α は K 上代数的なので、零イデアルない。I の単多項式である生成元 (定理 54 (1)) が、求める性質を満たす。 □

命題 66.

$\alpha \in L$ を K 上の代数的な元とする。α の K 上の最小多項式 $p_{\alpha,K}(x)$ は既約である。

$\because$ $p_{\alpha,K}(x)$ の K 上の既約分解を

$$p_{\alpha,K}(x) = q_1(x)q_2(x)\cdots q_d(x)$$

とする。$p_{\alpha,K}(\alpha) = 0$ だから、ある i が存在して $q_i(\alpha) = 0$ となる。最小多項式の定義から、$p_{\alpha,K}(x) \,|\, q_i(x)$ となる。次数の関係から、$p_{\alpha,K}(x) = q_i(x)$ となり、$p_{\alpha,K}(x)$ は既約である。 □

代数的元の定義と最小多項式の定義から次が成り立つ。

命題 67.

$\alpha \in L$ を K 上の代数的な元とする。M を L/K の中間体とするとき、α は M 上代数的で、$M[x]$ の中で $p_{\alpha,M}(x) \,|\, p_{\alpha,K}(x)$ となる。

4.3. **単拡大.** 単拡大は、生成元の最小多項式による多項式環の剰余体として与えられる体である。

定義 68.

代数拡大 L/K が単拡大とは、ある $\alpha \in L$ が存在して $L = K(\alpha)$ となるものをいう。

定理 69.

$K(\alpha)$ を K の単拡大体とする。K 環準同型

$$\varphi : K[x] \to K(\alpha) \quad \sum a_n x^n \mapsto \sum a_n \alpha^n$$

は、体の同型

$$K[x]/(p_{\alpha,K}(x)) \cong K(\alpha)$$

を導く。さらに、

$$[K(\alpha) : K] = \deg(p_{\alpha,K}(x))$$

となる。

$\because$ $\ker(\varphi)$ は α を根にもつ多項式のなすイデアルなので、既約多項式である $p_{\alpha,K}(x)$ が生成元になる (命題 65, 66)。準同型定理と定理 54 から $\mathrm{im}(\varphi) = K[x]/(p_{\alpha,K}(x))$ は体になる。$\mathrm{im}(\varphi)$ は α を含む K の拡大体なので、$\mathrm{im}(\varphi) = K(\alpha)$ となる。

$n = \deg(p_{\alpha,K}(x))$ とする。$K[x]/(p_{\alpha,K}(x))$ において、$1, \overline{x}, \cdots, \overline{x}^{n-1}$ が K 上の基底となるので、$[K(\alpha) : K] = n$ である。 □

系 70.

$\alpha \in L$ とするとき、以下は同値である。
(i) α は K 上代数的である。
(ii) $[K(\alpha) : K] < \infty$.

$\because$ (i) $\Rightarrow$ (ii) は定理 69。(ii) $\Rightarrow$ (i) は命題 63。 □

命題 67 から次の補題が成り立つ。

補題 71.

$\alpha \in L$ を K 上の代数的な元とする。M を L/K の中間体とするとき

$$[M(\alpha) : M] \leq [K(\alpha) : K]$$

となる。

命題 72.

L/K を体拡大、M を中間体とする。このとき以下は同値である。
(i) L/K は代数的である。
(ii) L/M と M/K は代数的である。

$\because$ (i) $\Rightarrow$ (ii) は命題 67。
(ii) $\Rightarrow$ (i) の証明 : $\alpha \in L$ とする。α は M 上代数的で、その最小多項式を $p_{\alpha,M}(x) = x^n + a_1x^{n-1} + \cdots + a_n \in M[x]$ とする。すると、

$$K(\alpha) \subset K(a_1, \cdots, a_n, \alpha)$$

なので、命題 63 から $K(a_1, \cdots, a_n, \alpha)$ が K 上有限次拡大であればよい。$a_1, a_2, \cdots, a_n$ は K 上代数的で、補題 72 用いて拡大次数を評価すると

$$\begin{aligned} [K(a_1, \cdots, a_n, \alpha) : K] &= [K(a_1) : K][K(a_1, a_2) : K(a_1)] \cdots [K(a_1, \cdots, a_n, \alpha) : K(a_1, \cdots, a_n)] \\ &\leq [K(a_1) : K][K(a_2) : K] \cdots [K(a_n) : K]\deg(p_{\alpha,M}(x)) \\ &< \infty \end{aligned}$$

となる。 □

例 73.

$\mathbb{Q}$ の 2 次拡大のことを 2 次体という。F が 2 次体ならば、ある $d = -1$ または $d = \pm p_1p_2 \cdots p_r$ (p_i たちは互いに異なる素数) が存在して、$F = \mathbb{Q}(\sqrt{d})$ となる。(逆は、問 1。)

例 74.

$\alpha = \sqrt{2} + \sqrt{3}$ の $\mathbb{Q}$ 上の最小多項式は $p_{\alpha,\mathbb{Q}}(x) = x^4 - 6x^2 + 1$ である。

$\because$ $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ (例 21) なので、$[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$ (例 21) となる。よって、定理 69 から最小多項式の次数は 4 である。

$$\begin{aligned} &\alpha - \sqrt{2} = \sqrt{3} \\ &\alpha^2 - 2\sqrt{2}\alpha + 2 = 3 \\ &\alpha^2 - 1 = 2\sqrt{2}\alpha \\ &\alpha^4 - 2\alpha^2 + 1 = 8\alpha^2 \\ &\alpha^4 - 6\alpha^2 + 1 = 0 \end{aligned}$$

なので、$p_{\alpha,\mathbb{Q}}(x) = x^4 - 6x^2 + 1$ となる。 □

例 75.
$L = K(\alpha, \beta)$ を体 K の有限次拡大とし、拡大次数 $[K(\alpha) : K]$ と $[K(\beta) : K]$ は互いに素とする。このとき、

$$[L : K] = [K(\alpha) : K][K(\beta) : K]$$

となる。

$\because$ 定理 16 より $[L : K]$ は $[K(\alpha) : K]$ と $[K(\beta) : K]$ の倍数であり、補題 71 より $[K(\alpha) : K][K(\beta) : K]$ 以下である。 □

問 9.
π や e が $\mathbb{Q}$ 上超越的なことを証明せよ。

問 10.
L/K を体拡大とする。M を L の元で K 上代数的な元全体の集合とすると、M は L/K の中間体になることを証明せよ。

問 11.
L/K を有限次体拡大、L を K 上のベクトル空間とみなし、$e_1, e_2, \cdots, e_d\,(d = [L : K])$ を L の K 上の基底とする。$\alpha \in L$ に対して、K 線形写像 $l_\alpha : L \to L$ を $l_\alpha(v) = \alpha v$ で定め、その行列表示を

$$l_\alpha(e_1, e_2, \cdots, e_d) = (e_1, e_2, \cdots, e_d)A_\alpha$$

とする。写像

$$L \to \mathrm{Mat}(d, K) \quad \alpha \mapsto A_\alpha$$

を L の K 上の表現という。$\mathrm{Mat}(d, K)$ で K 上の d 次正方行列全体のなす環を表す。

(1) $\alpha, \beta \in L$ に対して、次を証明せよ。

$$\begin{aligned} A_{\alpha+\beta} &= A_\alpha + A_\beta \\ A_{\alpha\beta} &= A_\alpha A_\beta \end{aligned}$$

(2) $a \in K$ に対して、$A_a = aE_d$ を証明せよ。ただし、E_d で d 次の単位行列を表す。

問 12.
L/K を有限次体拡大とし、L の K 上の表現 $(\alpha \mapsto A_\alpha)$ を固定する。写像

$$\begin{aligned} T_{L/K} &: L \to K \quad \alpha \mapsto \mathrm{trace}(A_\alpha) \\ N_{L/K} &: L \to K \quad \alpha \mapsto \det(A_\alpha) \end{aligned}$$

と定めて、L の K 上のトレースとノルムという。

(1) $\alpha, \beta \in L$ に対して、次を証明せよ。

$$\begin{aligned} T_{L/K}(\alpha + \beta) &= T_{L/K}(\alpha) + T_{L/K}(\beta) \\ N_{L/K}(\alpha\beta) &= N_{L/K}(\alpha)N_{L/K}(\beta) \end{aligned}$$

(2) $a \in K, \alpha \in L$ に対して、次を証明せよ。

$$\begin{aligned} &T_{L/K}(a) = [L : K]a, \quad T_{L/K}(a\alpha) = aT_{L/K}(\alpha) \\ &N_{L/K}(a) = a^{[L:K]} \end{aligned}$$

(3) M を L/K の中間体とするとき、次を証明せよ。

$$\begin{aligned} T_{L/K} &= T_{M/K} \circ T_{L/M} \\ N_{L/K} &= N_{M/K} \circ N_{L/M} \end{aligned}$$

問 13.
L/K を有限次体拡大とし、L の K 上の表現 $(\alpha \mapsto A_\alpha)$ を固定する。

(1) A_α の最小多項式は $p_{\alpha,K}(x)$ になることを証明せよ。

(2) A_α の特性多項式は $p_{\alpha,K}(x)^{[L:K(\alpha)]}$ になることを証明せよ。

5. 既約性判定法

一般に、多項式が既約かどうか判定することは非常に難しい。既約多項式は、有理整数環における素数に対応する概念であることは既に見た。既約性の判定は、大きな自然数が素数かどうか判定するのが難しいのと同じである。

この章では、有理係数多項式が既約になる判定法を与える。

5.1. ガウスの補題.

「有理整数環上での既約性から有理数体上での既約性が従う」という役に立つ補題である。

定義 76.

0 でない整係数多項式 $f(x) = a_n x^n + a_{n-1}x^{n-1} + c\cdots + a_0 \in \mathbb{Z}[x]$ が原始的とは、$\mathbb{Z}$ のイデアルとして

$$(a_0, a_1, \cdots, a_n) = \mathbb{Z}$$

となるものをいう。

定理 77.

2 つの原始的多項式の積は原始的である。

$\because$ $f(x), g(x) \in \mathbb{Z}[x]$ を原始的多項式、すなわち、

$$\begin{aligned} f(x) &= a_0x^m + a_1x^{m-1} + \cdots + a_m \quad (a_0, a_1, \cdots, a_m) = (1) \\ g(x) &= b_0x^n + b_1x^{n-1} + \cdots + b_n \quad (b_0, b_1, \cdots, b_n) = (1) \end{aligned}$$

とする。$f(x)g(x)$ が原始的であることを証明するためには、任意の素数 p に対して $f(x)g(x)$ のある係数が p で割れないことを証明すればよい。

p を素数とする。$f(x)$ と $g(x)$ は原始的だから、ある自然数 $k\,(0 \le k \le m)$ と $l\,(0 \le l \le m)$ が存在して、

$$\begin{aligned} p \,|\, a_i \,(0 \le i \le k-1), \quad p \not| a_k \\ p \,|\, b_j \,(0 \le j \le l-1), \quad p \not| b_l \end{aligned}$$

となる。$f(x)g(x)$ の $x^{m+n-k-l}$ の係数は、

$$a_0b_{k+l} + a_1b_{k+l-1} + \cdots + a_{k-1}b_{l+1} + a_kb_l + a_{k+1}b_{l-1} + \cdots + a_{k+l-1}b_1 + a_{k+l}b_0$$

となる。ただし、$i > m$ のとき $a_i = 0$ とし、b_j についても同様とする。すると、a_kb_l 以外の項は k, l の仮定から p で割れ、a_kb_l は p で割れない。

したがって、$f(x)g(x)$ は原始的である。 □

系 78.

1 次以上の整係数単多項式が整係数多項式として既約ならば、有理係数多項式として既約である。

$\because$ $f(x)$ を 1 次以上の整係数単多項式で、有理係数多項式として

$$f(x) = g(x)h(x), \quad \deg(h(x)), \deg(g(x)) \ge 1$$

となるとする。正の有理数 a を、$ag(x)$ は原始的な整係数多項式になるようにとる。同様に、正の有理数 b を $bh(x)$ が原始的な整係数多項式となるようにとる。

$$abf(x) = ag(x) \times bh(x)$$

において、定理 77 を適用すると、右辺は原始的な整係数多項式の積だから $abf(x)$ も原始的である。$f(x)$ は整係数多項式なので、$ab = 1$ となる。したがって、$f(x)$ は、整係数多項式として 2 つの 1 次以上の多項式の積になる。 □

5.2. **アイゼンシュタインの既約性判定法.** ある特定の素数に着目して、既約性を判定する方法である。

定理 79.

p を素数とする。整係数単多項式

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \quad (n \geq 1)$$

が条件

$$p \,|\, a_i \,(1 \leq i \leq n), \quad p^2 \nmid a_n$$

を満たせば、$f(x)$ は整多項式として既約である。特に、有理多項式としても既約である。

$\because$ $f(x)$ が可約ならば、2 つの 1 次以上の単多項式の積になる。

$$f(x) = (x^l + b_1 x^{l-1} + \cdots + b_l)(x^m + c_1 x^{m-1} + \cdots + c_m), \quad m + l = n,\, l, m \geq 1$$

とする。$p \,|\, a_n$ かつ $p^2 \nmid a_n$ より $p \nmid b_l$ または $p \nmid c_m$ である。$p \nmid c_m$ とする。$k\,(0 \leq k \leq l-1)$ を $p \nmid b_k$ となる最大の自然数とする。このような k は存在する。定理 77 の証明と同様に見ると、x^{l-k} の係数 a_{k+m} は p で割れないことになる。$k + m > 0$ なので、$p \,|\, a_i \,(1 \leq i \leq n)$ に反する。$p \nmid b_l$ の場合も同様である。したがって、$f(x)$ は既約である。

特に以下は、系 78 に従う。 □

例 80.

(1) n を 1 以上の自然数とすると、$f(x) = x^n - 2$ は既約である。さらに、$[\mathbb{Q}(2^{\frac{1}{n}}) : \mathbb{Q}] = n$ である。

$\because$ $p = 2$ として、アイゼンシュタインの既約性判定法を満たすので既約である。 □

(2) $f(x) = x^4 + x^3 + x^2 + x + 1$ は既約である。ζ_5 で 1 の原始 5 乗根とすると $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ である。

$\because$ 実際、$x = y + 1$ とおくと、

$$f(x) = \frac{x^5 - 1}{x - 1} = \frac{(y+1)^5 - 1}{y} = y^4 + 5y^3 + 10y^2 + 10y + 5$$

となるので、アイゼンシュタインの既約性判定法により y の多項式として既約である。x から y は 1 次式としての変換なので、$f(x)$ は既約である。 □

例 81.

複素数 ω を 1 の原始 3 乗根、すなわち、$\omega^2 + \omega + 1 = 0$ の解とする。このとき、

$$[\mathbb{Q}(2^{\frac{1}{3}}, \omega) : \mathbb{Q}] = 6$$

となる。また、

$$\mathbb{Q}(2^{\frac{1}{3}}, \omega) = \mathbb{Q}(2^{\frac{1}{3}} + \omega)$$

である。

$\because$ 例 80 (1) から $[\mathbb{Q}(2^{\frac{1}{3}}) : \mathbb{Q}] = 3$ である。また、例 80 (2) と同様にして $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ である。したがって、例 75 より、拡大次数は 6 になる。単拡大になることは、例 21 と同様にできる。 □

5.3. **還元.** 整係数多項式の既約性判定は簡単ではない。しかし、有限体上の多項式としてみると既約性が判定できることがある。

p を素数とする。p を法とする自然な環準同型を

$$\mathbb{Z} \to \mathbb{Z}/(p) = \mathbb{F}_p \qquad a \mapsto \overline{a}$$

と表す。この環準同型は、整係数多項式上の環準同型

$$\mathbb{Z}[x] \to \mathbb{F}_p[x] \qquad f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \mapsto \overline{f}(x) = \overline{a}_0 x^n + \overline{a}_1 x^{n-1} + \cdots + \overline{a}_n$$

に延びる。この写像を、p を法とする還元射という。

命題 82.

整係数単多項式 $f(x)$ に対して、$\overline{f}(x)$ が既約ならば $f(x)$ も既約である。特に、有理係数多項式としても既約である。

$\because$ $f(x)$ が可約とする。すると、整係数単多項式 $g(x), h(x)\,(\deg(g(x)), \deg(g(x)) \geq 1)$ が存在して、$f(x) = g(x)h(x)$ となる。$\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ となる。$\overline{g}(x)$ と $\overline{h}(x)$ は 1 次以上の単多項式なので、$\overline{f}(x)$ は可約になる。

最後は、系 78 を適用させればよい。 □

例 83.

(1) $f(x) = x^2 + x + 1$ は有理係数多項式として既約である。

$\because$ 2 を法として、つまり $\mathbb{F}_2[x]$ の中で考える。$\overline{f}(x)$ は 2 次の単多項式だから、可約ならば 2 つの 1 次式の積になる。ところが、

$$\overline{f}(\overline{0}) = \overline{0}^2 + \overline{0} + \overline{1} = \overline{1} \neq \overline{0}$$
$$\overline{f}(\overline{1}) = \overline{1}^2 + \overline{1} + \overline{1} = \overline{1} \neq \overline{0}$$

なので、$\overline{f}(x)$ は 1 次の因子を持たない。したがって、命題 82 から $f(x)$ は既約である。 □

(2) $g(x) = x^4 + x + 1$ は有理係数多項式として既約である。

$\because$ 2 を法として、つまり $\mathbb{F}_2[x]$ の中で考える。$\overline{g}(x)$ は 4 次の単多項式だから、可約ならば 1 次因子を持つか 2 つの既約な 2 次式の積になるかどちらかである。

$$\overline{g}(\overline{0}) = \overline{0}^4 + \overline{0} + \overline{1} = \overline{1} \neq \overline{0}$$
$$\overline{g}(\overline{1}) = \overline{1}^4 + \overline{1} + \overline{1} = \overline{1} \neq \overline{0}$$

なので、$\overline{g}(x)$ は 1 次の因子を持たない。$\mathbb{F}_2[x]$ の 2 次単多項式は

$$x^2, x^2 + x = (x+1)x, x^2 + 1 = (x+1)^2, x^2 + x + 1$$

なので、既約式は $x^2 + x + 1$ のみである。

$$(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq \overline{g}(x)$$

であるから、$\overline{g}(x)$ は 2 次の既約因子を持たない。したがって、命題 82 から $g(x)$ は既約である。 □

問 14.

(1) p を素数とする。$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ が既約であることを証明せよ。

(2) $g(x) = x^6 + x^3 + 1$ が既約であることを証明せよ。

問 15.

(1) $f(x) = x^3 - x + 2$ が既約であることを証明せよ。

(2) $g(x) = x^4 + x^2 + x + 1$ が既約であることを証明せよ。

6. 代数閉体

解けない方程式があるとすると都合が悪い。この章では、任意の方程式が解ける体が、代数拡大体として存在することを解説する。ある意味安心のための存在である。

6.1. 複素数体 $\mathbb{C}$ は代数閉体.

経験的に、複素数体上では任意の方程式が解けること知られていた。それを最初に厳密に証明したのはガウスである。

定義 84.

体 K が代数閉体とは、任意の 1 次以上の K 係数多項式が K の中に少なくとも一つ根をもつものをいう。

定義から明らかに次が成り立つ。

命題 85.

K を体とする。このとき、以下は同値である。

(i) K は代数閉体である。

(ii) 任意の 1 次以上の K 係数多項式 $f(x)$ に対して、ある $a, \alpha_1, \cdots, \alpha_n \in K$ が存在して

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$$

となる。

(iii) K の拡大体に含まれる α が K 上代数的ならば、 α は K に含まれる。

(iv) L/K を代数拡大とすると、$L = K$ である。

(v) L/K を有限次代数拡大とすると、$L = K$ である。

ガウスは複素数体 $\mathbb{C}$ が代数閉体であること、すなわち、代数学の基本定理を証明した (1799 年)。

定理 86.

複素数体 $\mathbb{C}$ は代数閉体である。

代数学の基本定理は多くの証明が知られている。この講義では、ガロア理論を学んだ後に、その応用として証明する。

6.2. 代数閉包の存在.

代数閉包の存在定理を述べておく。2 つあれば同型が存在することにより、種々の概念が代数閉包の取り方によらなくなる。

定義 87.

K を体とする。体 $\overline{K}$ が K の代数閉包とは、$\overline{K}$ が K 上代数的かつ代数閉体となるものをいう。

Zorn の補題から次の定理が成り立つ。

定理 88.

K を体とする。

(1) K の代数閉包が存在する。

(2) $\overline{K}_1, \overline{K}_2$ を K の代数閉包とすると、ある K 同型 $\overline{K}_1 \cong \overline{K}_2$ が存在する。

例 89.

代数学の基本定理のもとで、$\overline{\mathbb{Q}}$ を複素数体 $\mathbb{C}$ の中での有理数体 $\mathbb{Q}$ 上代数的元全体とすると、$\overline{\mathbb{Q}}$ は $\mathbb{Q}$ の代数閉包である。

$\because$ $\overline{\mathbb{Q}}$ が体であること：α, β を $\mathbb{Q}$ 上代数的とすると

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}] < \infty$$

なので、 系 70 から $\mathbb{Q}(\alpha, \beta)$ は $\mathbb{Q}$ 上代数的である。よって、$\alpha + \beta, \alpha\beta, \alpha^{-1}\,(\alpha \neq 0)$ は $\mathbb{Q}$ 上代数的である。
$\overline{\mathbb{Q}}$ が代数閉体であること：$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \overline{\mathbb{Q}}[x]\,(n \geq 1)$ とし、$\alpha \in \mathbb{C}$ をその一つの根とする。すると、

$$\begin{aligned} [\mathbb{Q}(\alpha) : \mathbb{Q}] &\leq [\mathbb{Q}(a_1, \cdots, a_n, \alpha) : \mathbb{Q}] \\ &\leq [\mathbb{Q}(a_1, \cdots, a_n) : \mathbb{Q}][\mathbb{Q}(a_1, \cdots, a_n, \alpha) : \mathbb{Q}(a_1, \cdots, a_n)] \\ &< \infty \end{aligned}$$

となる。よって、系 70 から α は $\mathbb{Q}$ 上代数的である。 □

問 16.
代数学の基本定理とその周辺を勉強せよ。

問 17.
定理 88 を証明せよ。

7. 共役元

既約多項式の互いに共役な元の入れ替えを考察するというのが、ガロアによる方程式の理論の原型である。一方、自己同型は線形空間として体拡大をとらえる現代的方法である。この章では、両者の関係を解説する。

K を体とし、K の代数閉包 $\overline{K}$ を一つ固定する。種々の概念は、K 同型が存在するので代数閉包の取り方によらない。

7.1. 共役元.

既約方程式の 2 つの根それぞれが生成する体は同型である。この事実が、体の埋め込みや同型を作る上で役立つ。

定義 90.

$\alpha \in \overline{K}$ とする。α の K 上の共役元とは、最小多項式 $p_{\alpha,K}(x)$ の $\overline{K}$ の中での根のことをいう。

例 91.

$d = -1$ または $\pm p_1 \cdots p_r$ $(p_1, \cdots, p_r$ は相異なる素数$)$ とする。$a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})\,(a, b \in \mathbb{Q})$ の $\mathbb{Q}$ 上の共役元は $a + b\sqrt{d}$ と $a - b\sqrt{d}$ である。実際、$a + b\sqrt{d}$ の最小多項式を素因数分解すると

$$p_{a+b\sqrt{d},\mathbb{Q}} = x^2 - 2ax + a^2 - b^2 d = (x - a - b\sqrt{d})(x - a + b\sqrt{d})$$

となる。

定理 92.

$\alpha \in \overline{K}$ とし、β を α の共役元とする。このとき、体の K 同型

$$\varphi : K(\alpha) \to K(\beta)$$

で、$\varphi(\alpha) = \beta$ となるものがただ一つ存在する。

$\because$ $p_{\alpha,K}(x) = p_{\beta,K}(x)$ なので、K 同型の合成

$$\begin{array}{ccccc} K(\alpha) & \xleftarrow{\cong} & K[x]/(p_{\alpha,K}(x)) & \xrightarrow{\cong} & K(\beta) \\ \alpha & \longleftarrow & x & \mapsto & \beta \end{array}$$

が、α を β に移すものを与える。唯一性は、単拡大であることからわかる。 □

例 93.

ω を $\omega^2 + \omega + 1 = 0$ となる複素数とする。$2^{\frac{1}{3}} \in \mathbb{Q}(2^{\frac{1}{3}})$ の $\mathbb{Q}$ 上の共役元は $2^{\frac{1}{3}}, 2^{\frac{1}{3}}\omega$ と $2^{\frac{1}{3}}\omega^2$ である。実際、$\omega^3 = 1$ なので、$2^{\frac{1}{3}}$ の最小多項式を素因数分解すると

$$p_{2^{\frac{1}{3}},\mathbb{Q}} = x^3 - 2 = (x - 2^{\frac{1}{3}})(x - 2^{\frac{1}{3}}\omega)(x - 2^{\frac{1}{3}}\omega^2)$$

となる。$2^{\frac{1}{3}}$ は実数で $\mathbb{Q}(2^{\frac{1}{3}}) \subset \mathbb{R}$、$2^{\frac{1}{3}}\omega$ は虚数で $\mathbb{Q}(2^{\frac{1}{3}}) \not\subset \mathbb{R}$ となるので、

$$\mathbb{Q}(2^{\frac{1}{3}}) \neq \mathbb{Q}(2^{\frac{1}{3}}\omega)$$

となる。両者ともに $\mathbb{Q}$ 上 3 次 (例 80) なので、部分体は自明なものしかなく、

$$\mathbb{Q}(2^{\frac{1}{3}}) \cap \mathbb{Q}(2^{\frac{1}{3}}\omega) = \mathbb{Q}$$

となる。しかし、$\mathbb{Q}$ 上の体としては、

$$\mathbb{Q}(2^{\frac{1}{3}}) \cong \mathbb{Q}(2^{\frac{1}{3}}\omega)$$

である。

7.2. **埋め込み.** 既約方程式の根と体の埋め込みの関係を考察する。

定義 94.

L/K を体拡大とする。K 環準同型 $\iota : L \to \overline{K}$ を $\overline{K}$ への L の K 埋め込みという。$\mathrm{Hom}_K(L, \overline{K})$ で K 埋め込み全体の集合を表す。

命題 95.

$\alpha \in \overline{K}$ とし、$K(\alpha)/K$ を単拡大とする。

(1) $\iota \in \mathrm{Hom}_K(K(\alpha), \overline{K})$ とすると、$\iota(\alpha)$ は α の K 上の共役元になる。また、ι は $K(\alpha)$ と $K(\iota(\alpha))$ の同型を与える。

(2) 写像

$$\begin{array}{ccc} \mathrm{Hom}_K(K(\alpha), \overline{K}) & \longrightarrow & \{\beta \in \overline{K} \,|\, \beta \text{ は } \alpha \text{ の共役元 }\} \\ \iota & \mapsto & \iota(\alpha) \end{array}$$

は全単射である。

$\because$ (1) $p_{\alpha,K}(x)$ を α の K 上の最小多項式とする。ι は K 環準同型なので、

$$p_{\alpha,K}(\iota(\alpha)) = \iota(p_{\alpha,K}(\alpha)) = \iota(0) = 0$$

となる。よって、$\iota(\alpha)$ は α の共役元である。

明らかに $\iota(K(\alpha)) \subset K(\iota(\alpha))$ である。K 上の次元を比較して、$\iota(K(\alpha)) = K(\iota(\alpha))$ になる。環の準同型定理より、K 同型になる。

(2) 定理 92 と (1) を組み合わせると証明できる。 □

系 96.

$\alpha \in \overline{K}$ とすると、

$$\sharp\mathrm{Hom}_K(K(\alpha), \overline{K}) \leq [K(\alpha) : K]$$

である。等号が成り立つのは、$p_{\alpha,K}(x)$ に重根がないときで、そのときに限る。

ただし、重根とは次の意味である。

定義 97.

$f(x) \in K[x]$ を 1 次以上の多項式とし、$\overline{K}$ 上で

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

と既約分解を持つとする。$f(x)$ が $\overline{K}$ で重根をもつとは、$\alpha_1, \cdots, \alpha_n$ のいずれか 2 つが一致することをいう。

例 98.

p を素数、$K = \mathbb{F}_p(t)$ する。K の拡大 L を $L = K(t^{\frac{1}{p}}) = \mathbb{F}_p(t^{\frac{1}{p}})$ とする。このとき、

$$\sharp\mathrm{Hom}_K(L, \overline{K}) = 1$$

である。実際、$t^{\frac{1}{p}}$ の K 上の最小多項式は L 上では

$$p_{t^{\frac{1}{p}},K}(x) = x^p - t = (x - t^{\frac{1}{p}})^p$$

と既約分解される。K 埋め込みにおいて、$t^{\frac{1}{p}}$ の行き先は自分自身しかなく、L は K 上 $t^{\frac{1}{p}}$ で生成されるから、L の K 埋め込みはただ一つである。

命題 99.

L/K を有限次拡大とすると

$$\sharp\mathrm{Hom}_K(L,\overline{K})<\infty$$

となる。また、M を L/K の中間体とする。このとき、

$$\sharp\mathrm{Hom}_K(L,\overline{K})=\sharp\mathrm{Hom}_K(M,\overline{K})\sharp\mathrm{Hom}_M(L,\overline{K})$$

である。

$\because$ 命題 19 より $L=K(\alpha_1,\cdots,\alpha_n)$ と表せるから、命題 95 の証明と同様にして、

$$\sharp\mathrm{Hom}_K(L,\overline{K})<\infty$$

がわかる。制限写像

$$p:\mathrm{Hom}_K(L,\overline{K})\to\mathrm{Hom}_K(M,\overline{K})\quad \iota\mapsto\iota|_M$$

について以下を証明する。命題は (1) - (3) に容易に従う。

(1) p は全射である。

(2) $\sigma\in\mathrm{Hom}_K(L,\overline{K})$ に対して、

$$p^{-1}(\{p(\sigma)\})=\mathrm{Hom}_{\sigma(M)}(\sigma(L),\overline{K})\circ(\sigma|_L)$$

となる。

(3) $\sigma\in\mathrm{Hom}_K(L,\overline{K})$ に対して、$\overline{\sigma}:\overline{K}\to\overline{K}$ で $\overline{\sigma}|_L=\sigma$ となる K 同型をとる (定理 88 (2) により存在) と、写像

$$\begin{array}{ccc}\mathrm{Hom}_M(L,\overline{K}) & \longrightarrow & \mathrm{Hom}_{\sigma(M)}(\sigma(L),\overline{K})\\ \iota & \mapsto & \overline{\sigma}^{-1}\circ\iota\circ\overline{\sigma}^{-1}|_{\sigma(L)}\end{array}$$

は全単射になる。

(1) の証明 : $L=M(\alpha)$ とする。$p_{\alpha,M}(x)=x^n+a_1x^{n-1}+\cdots+a_n$ とし、β を $p^{\iota}_{\alpha,M}(x)=x^n+\iota(a_1)x^{n-1}+\cdots+\iota(a_n)$ の根とする。$p^{\iota}_{\alpha,M}(x)$ は既約なので、K 環準同型の合成

$$\begin{array}{ccccc}L=M(\alpha) & \overset{\cong}{\longleftarrow} & M[x]/(p_{\alpha,M}(x)) & \longrightarrow & \overline{K}\\ \sum a_i\alpha^i & & \sum a_ix^i & \mapsto & \sum\iota(a_i)\beta^i\end{array}$$

は、L の K 埋め込みになる。

一般には、L/M は単拡大の有限増加列で表せるから、増加列にあわせて順に K 埋め込みが延長できる。

(2) と (3) は写像が well-defined であることがわかれば、逆写像が容易に作れるので明らか。 □

系 100.

L/K を有限次拡大とすると $\sharp\mathrm{Hom}_K(L,K)\le[L:K]$ である。

$\because$ 命題 19 より、L/K は単拡大の増加列で表せる。不等号は、定理 16、系 96 と命題 99 により成り立つ。 □

7.3. **自己同型.** ガロア理論を現代風に展開する上で最も重要な概念である自己同型を導入する。

定義-命題 101.

(1) L を体とする。L の自己同型とは、L から L への同型のことをいう。L の自己同型全体は写像の合成に関して群になる。この群を自己同型群といい、$\mathrm{Aut}(L)$ と表す。

(2) L/K を体拡大とする。L の K 自己同型とは、L から L への K 同型のことをいう。L の K 自己同型全体は自己同型群の部分群になる。この群を K 自己同型群といい、$\mathrm{Aut}(L/K)$ と表す。

命題 102.

L/K を有限次代数拡大とし、L は $\overline{K}$ に含まれるとする。集合として

$$\mathrm{Aut}(L/K) = \{\iota \in \mathrm{Hom}_K(L, \overline{K}) \,|\, \iota(L) \subset L\}$$

となる。

$\because$ ι を L の $\overline{K}$ への K 埋め込みで、$\iota(L) \subset L$ とする。K 上の拡大次数が一致するので、$\iota(L) = L$ となる。よって、ι は L の K 自己同型である。 □

系 103.

L/K を有限次代数拡大とするとすると

$$\sharp\mathrm{Aut}(L/K) \leq [L : K]$$

である。

$\because$ 命題 100 より。 □

系 104.

$\alpha \in \overline{K}$ とし、$K(\alpha)/K$ を単拡大とする。写像

$$\begin{array}{ccc} \mathrm{Aut}(K(\alpha)/K) & \longrightarrow & \{\beta \in K(\alpha) \,|\, \beta \text{ は } \alpha \text{ の共役元 }\} \\ \iota & \mapsto & \iota(\alpha) \end{array}$$

は全単射である。

例 105.

(1) $\sharp\mathrm{Aut}(\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}) = 1$.
$\because$ 例 93 より、$\mathbb{Q}(2^{\frac{1}{3}}) \not\subset \mathbb{Q}(2^{\frac{1}{3}}\omega)$ かつ $\mathbb{Q}(2^{\frac{1}{3}}) \not\subset \mathbb{Q}(2^{\frac{1}{3}}\omega^2)$ より。 □

(2) $\sharp\mathrm{Aut}(\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}) = 2$. よって、$\mathrm{Aut}(\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.
$\because$ 例 80 (1) より、$2^{\frac{1}{4}}$ の最小多項式は、$p_{2^{\frac{1}{4}},\mathbb{Q}}(x) = x^4 - 2$ となるので、その共役元は $\pm 2^{\frac{1}{4}}, \pm 2^{\frac{1}{4}}\sqrt{-1}$ である。そのうち、$\mathbb{Q}(2^{\frac{1}{4}})$ に属するのは $\pm 2^{\frac{1}{4}}$ のみ。よって、系 104 から自己同型は 2 つである。 □

(3) $\sharp\mathrm{Aut}(\mathbb{F}_p(t^{\frac{1}{p}})/\mathbb{F}_p(t)) = 1$.
$\because$ 例 98 より。 □

問 18.

L/K を有限次拡大とする。

$$\sum_{\iota \in \mathrm{Hom}_K(L,\overline{K})} a_\iota \iota = 0 \,(a_\iota \in \overline{K}) \implies a_\iota = 0 \,(\forall \iota)$$

が成り立つ。

問 19.

(1) n を正の整数とする。$\mathrm{Aut}(\mathbb{Q}(2^{\frac{1}{n}})/\mathbb{Q})$ を求めよ。
(2) $\mathrm{Aut}(\mathbb{Q}(\sqrt{2+\sqrt{5}}/\mathbb{Q})$ を求めよ。

問 20.

$\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ を求めよ。

8. 分離拡大と正規拡大

体論における種々の概念、例えば代数性など、は、体に属するすべての元に対してある性質が成立することを要求する。しかし、多くの場合は生成元について問えば十分であることがわかる。この章で定義する分離性や正規性もそのような概念であり、共役元と埋め込み・自己同型の関係からわかる。

K を体とし、K の代数閉包 $\overline{K}$ を一つ固定する。種々の概念は、K 同型が存在するので代数閉包の取り方によらない。

8.1. 分離多項式と微分.

多項式の分離性の微分を用いた判定法を与える。

定義 106.

$f(x) \in K[x]$ を 0 でない多項式とする。
(1) $f(x)$ が $\overline{K}$ で重根をもたないとき、$f(x)$ を分離多項式という。
(2) $f(x)$ が分離多項式でないとき、非分離多項式という。

例 107.

p を素数とする。$\mathbb{F}_p[x]$ の中で、

$$x^p - 1 = (x-1)^p$$

となる。よって、$x^p - 1$ は分離的でない。

$\because$ 実際、

$$p \left| \begin{pmatrix} p \\ i \end{pmatrix} \right. \quad (0 < i < p)$$

となるので、二項定理から上の因数分解を得る。 □

多項式環上に微分を導入する。ライプニッツ・ルールが成り立つことは容易。

命題-定義 108.

K 線形写像

$$\frac{d}{dx} : K[x] \to K[x] \quad f(x) = \sum a_n x^n \mapsto f'(x) = \sum n a_n x^{n-1}$$

に対して、次が成り立つ。

$$\frac{d}{dx}(f(x)g(x)) = (\frac{d}{dx}f(x))g(x) + f(x)(\frac{d}{dx}g(x))$$

この写像を K 微分という。

命題 109.

$f(x) \in K[x]$ を 0 でない多項式とする。このとき、以下は同値である。
(i) $f(x)$ は分離多項式である。
(ii) $K[x]$ のイデアルとして、$(f(x), f'(x)) = K[x]$ となる。

$\because$ $f(x)$ が 0 でない定数のときは明らか。$f(x) \in K[x]$ を 1 次以上の多項式とし、$\overline{K}$ 上で

$$f(x) = a(x-\alpha_1)^{e_1}(x-\alpha_2)^{e_2}\cdots(x-\alpha_m)^{e_m}$$

と既約分解を持つとする。ただし、$\alpha_1, \cdots, \alpha_m$ は互いに異なり、$e_1, \cdots, e_m \geq 1$ とする。
(i) $\Rightarrow$ (ii) の証明：$f(x)$ は分離的より、$e_1 = \cdots e_m = 1$ である。

$$f'(x) = \sum_i a(x-\alpha_1)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_m)$$

となる。よって、

$$f'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j) \neq 0$$

となり、$f(x)$ と　$f'(x)$ は $\overline{K}$ で共通根をもたない。よって、$(f(x), f'(x)) = K[x]$ となる。
(ii) $\Rightarrow$ (i) の証明：$e_i \geq 2$ とする。すると、　$\overline{K}[x]$ で

$$x - \alpha_i \,|\, f'(x)$$

となる。よって、$(f(x), f'(x)) \neq K[x]$ となり、矛盾する。 □

系 110.

K の標数を 0 とすると、$K[x]$ の既約多項式は分離的である。

$\because$ $\mathrm{char}(K) = 0$ なので、少なくとも最高次数が消えないので $f'(x) \neq 0$ である。$f(x)$ は既約で、$\deg(f(x)) > \deg(f'(x))$ なので、$(f(x), f'(x)) = K[x]$ となる。 □

例 111.
p を素数とする。$x^p - t$ は $\mathbb{F}_p(t)[x]$ の既約多項式である。$\mathbb{F}_p(t)$ 上で微分すると

$$\frac{d}{dx}(x^p - t) = px^{p-1} = 0$$

となるので分離的でない。(例 98 も見よ。) 系 110 では標数 0 の仮定が必要である。

8.2. **分離拡大.**　分離拡大を導入する。

定義 112.

L/K を代数拡大とする。
(1) $\alpha \in L$ が K 上分離的とは、α の最小多項式 $p_{\alpha,K}(x)$ が分離的であることをいう。
(2) L/K が分離拡大とは、L の任意の元が K 上分離的である。

例 113.
L/K を 2 次拡大とする。
(1) 標数が 2 でないとすると、L/K は分離拡大である。
(2) 標数が 2 とし、$L = K(\alpha)$ とする。

$$L/K \text{ が分離拡大} \iff \alpha^2 \notin K.$$

がなりたつ。

$\because$ (1) $\alpha \in L$ とする。$\alpha \in K$ ならば α は K 上分離的である。$\alpha \notin K$ とする。α の最小多項式 $p_{\alpha,K}(x) = x^2 + ax + b$ の微分は $p'_{\alpha,K}(x) = 2x + a \neq 0$ なので、α は K 上分離的である。
(2) $\alpha^2 \in K$ とする。α は L を生成するから、K 上の最小多項式は 2 次式である。よって、$p_{\alpha,K}(x) = x^2 + \alpha^2 = (x + \alpha)^2$ となり、α は分離的でない。($-1 = 1$ に注意せよ。)
　$\alpha^2 \notin K$ とする。α の K 上の最小多項式は、$p_{\alpha,K}(x) = x^2 + ax + b\,(a \neq 0)$ となる。$p'(x) = a \neq 0$ だから、α は分離的である。 □

分離拡大でない代数拡大を非分離拡大という。例えば、素数 p に対して $\mathbb{F}_p(t^{\frac{1}{p}})/\mathbb{F}_p(t)$ は非分離拡大になる (例 98 または 例 111)。この講義では、非分離拡大を扱わない (問いを見よ)。

命題 114.

K の標数を 0 とする。K 上の代数拡大は分離拡大である。

$\because$ 系 110 より。 □

定理 115.

L/K を有限次代数拡大とする。このとき以下の条件は同値である。
(i) L/K は分離拡大である。
(ii) ある K 上分離的な元 $\alpha_1, \cdots, \alpha_n \in L$ が存在して $L = K(\alpha_1, \cdots, \alpha_n)$ となる。
(iii) ある K 上分離的な元 $\alpha \in L$ が存在して $L = K(\alpha)$ となる。
(iv) $\sharp \mathrm{Hom}_K(L, \overline{K}) = [L : K]$.

$\because$ (i) $\Rightarrow$ (ii) の証明：命題 19 より明らか。
(ii) $\Rightarrow$ (iii) の証明は次の補題を生成元の個数に関して帰納的に適用すればよい。 □

残りは次の補題を述べてから証明する。

補題 116.

L/K を有限次拡大で、K 上分離的な元 $a \in L$ と代数的な元 $b \in L$ により $L = K(a, b)$ とする。このとき、$c \in L$ が存在して $L = K(c)$ となる。また、a, b がともに K 上分離的ならば、c も K 上分離的である。

$\because$ K は位数が無限とする。$\overline{K}$ を L を含む K の代数閉包とする。a と b の最小多項式がそれぞれ

$$p_{a,K}(x) = (x - a_1)(x - a_2) \cdots (x - a_m) \quad a_i \in \overline{K}\,(1 \leq i \leq m),\ a_1 = a$$
$$p_{b,K}(x) = (x - b_1)(x - b_2) \cdots (x - b_n) \quad b_j \in \overline{K}\,(1 \leq j \leq n),\ b_1 = b$$

と $\overline{K}$ 上で既約分解するものとする。d を $(b_j - b_l)/(a_i - a_k)\,(i \neq k)$ と一致しない K の元とする。K の位数が無限より、d は存在する。$c = b + da$ とおく。すると、$p_{b,K}(c - da) = 0$ である。よって、$K(c)$ 上の多項式 $p_{b,K}(c - dx)$ と $p_{a,K}(x)$ は共通因子 $x - a$ を持ち、d の取り方と $p_{a,K}(x)$ が分離的であることから共通因子は $x - a$ だけである。また、共通因子は、$K(c)$ の多項式である。したがって、$a \in K(c)$ である。$b = c - da \in K(c)$ なので、$K(a, b) \subset K(c)$ となる。$K(c) \subset K(a, b)$ は明らかなので、$K(a, b) = K(c)$ である。

K が有限体のときは、L も有限体である。問 8 から、$L^\times$ は巡回群なので、その生成元を c とすると $L = K(c)$ と表せる。

$K(c) = L = K(a)(b)$ と考える。a, b は K 上分離的なので、系 96 と命題 99 を適用すると

$$\begin{aligned} \sharp \mathrm{Hom}_K(K(c), \overline{K}) &= \sharp \mathrm{Hom}_K(K(a), \overline{K}) \sharp \mathrm{Hom}_{K(a)}(K(a)(b), \overline{K}) \\ &= [K(a) : K][K(a)(b) : K(a)] \\ &= [K(c) : K] \end{aligned}$$

となる。再び、系 96 を適用して c は K 上分離的である。 □

$\because$ 定理の証明を続ける。
(iii) $\Rightarrow$ (iv) は系 96 より。
(iv) $\Rightarrow$ (i) の証明：$\alpha \in L$ とする。命題 99 と系 100 を適用して

$$\begin{aligned} [L : K] &= \sharp \mathrm{Hom}_K(L, \overline{K}) \\ &= \sharp \mathrm{Hom}_K(K(\alpha), \overline{K}) \sharp \mathrm{Hom}_{K(\alpha)}(L, \overline{K}) \\ &\leq [K(\alpha) : K][L : K(\alpha)] \\ &= [L : K] \end{aligned}$$

なので、 系 100 から

$$\sharp \mathrm{Hom}_K(K(\alpha), \overline{K}) = [K(\alpha) : K]$$

となる。系 96 から α は K 上分離的である。 □

系 117.

L/K を代数拡大、M を中間体とする。このとき以下は同値である。
(i) L/K は分離的である。
(ii) L/M と M/K は分離的である。

$\because$ (i) $\Rightarrow$ (ii) は明らか。
(ii) $\Rightarrow$ (i) の証明：L/K が有限次拡大とする。命題 99 と定理 115 から

$$\sharp\mathrm{Hom}_K(L,\overline{K}) = \sharp\mathrm{Hom}_K(M,\overline{K})\sharp\mathrm{Hom}_M(L,\overline{K}) = [M:K][L:M] = [L:K]$$

となるので、L/K は分離拡大である。
L/K が一般とする。$\alpha \in L$ とする。α の M 上の最小多項式の係数を K に添加した体を N とすると、$N(\alpha)/N$ と N/K は前半部分から有限次分離拡大である。よって、$N(\alpha)/K$ は分離拡大となり、α は K 上分離的である。 □

8.3. **正規拡大.** 正規拡大を導入する。

定義 118.

L/K を代数拡大とする。L/K が正規拡大とは、L の任意の元の K 上の共役元が L に属することをいう。

例 119.
2 次方程式の解と係数の関係より、2 次拡大は正規拡大である。

例 120.
$\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}$ は正規拡大でない。実際、$2^{\frac{1}{3}}$ の $\mathbb{Q}$ 上の共役元は例 93 から

$$2^{\frac{1}{3}}\omega, 2^{\frac{1}{3}}\omega^2 \notin \mathbb{Q}(2^{\frac{1}{3}})$$

である。

定理 121.

L/K を有限次代数拡大とする。このとき以下の条件は同値である。
(i) L/K は正規拡大である。
(ii) 各元の K 上の共役がすべて L に属する $\alpha_1, \cdots, \alpha_n \in L$ が存在して、$L = K(\alpha_1, \cdots, \alpha_n)$ となる。
(iii) $\mathrm{Aut}(L/K) = \mathrm{Hom}_K(L,\overline{K})$.

$\because$ (i) $\Rightarrow$ (ii) の証明：命題 19 より明らか。
(ii) $\Rightarrow$ (iii) の証明：L の K 埋め込みの像は、K 上 $\alpha_1, \cdots, \alpha_n$ で生成される元となるから L に属する。等号は、命題 102 に従う。
(iii) $\Rightarrow$ (i) の証明：$\alpha \in L$ とし、$\beta \in \overline{K}$ を α の K 上の共役元とする。すると、命題 95 から L の K 埋め込み ι で $\iota(\alpha) = \beta$ となるものが存在する。仮定より、ι は L の自己同型なので、$\beta = \iota(\alpha) \in L$ となる。 □

命題 122.

L/K を正規拡大とし、M をその中間体とする。このとき、L/M は正規拡大である。

$\because$ 命題 67 より。 □

8.4. **最小分解体.** 与えられた多項式が 1 次式の積に既約分解されるような最小の拡大を、最小分解体という。

定義 123.

$f(x) \in K[x]$ を 0 でない K 上の多項式とする。
(1) $\overline{K}/K$ の中間体 L が $f(x)$ の分解体とは、$f(x)$ の根がすべて L に属することをいう。
(2) $f(x)$ の K 上の最小分解体とは、分解体の中で包含関係に関して最小のものをいう。

命題 124.

$f(x) \in K[x]$ を 0 でない K 上の多項式とする。$f(x)$ の K 上の最小分解体 L が存在し、L/K は正規拡大である。さらに、$f(x)$ が分離多項式ならば L/K は分離拡大である。

$\because$ $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ とする。$L = K(\alpha_1, \cdots, \alpha_n)$ とおくと、L は $f(x)$ の K 上の最小分解体である。各 α_i の共役元は $f(x)$ の根になるので、定理 121 から L/K は正規拡大である。$f(x)$ が分離的だとすると、各 α_i も分離的なので、定理 115 から分離拡大である。 □

例 125.

$\mathbb{Q}$ 上の多項式 $f(x) = x^3 - 2$ の最小分解体は、$\mathbb{Q}(2^{\frac{1}{3}}, \omega)$ である。ただし、ω は $\omega^2 + \omega + 1 = 0$ を満たす複素数である。実際、$f(x)$ の根 $2^{\frac{1}{3}}, 2^{\frac{1}{3}}\omega, 2^{\frac{1}{3}}\omega^2$ であり、$\omega = 2^{\frac{1}{3}}\omega/2^{\frac{1}{3}}$ であるから、最小分解体は $2^{\frac{1}{3}}$ と ω で生成される。

例 126.

$\mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right)/\mathbb{Q}$ は正規拡大でない。また、$\sqrt{2+\sqrt{5}}$ の最小多項式 $p_{\sqrt{2+\sqrt{5}},\mathbb{Q}}(x)$ の最小分解体は $\mathbb{Q}\left(\sqrt{2+\sqrt{5}}, \sqrt{-1}\right)$ である。

$\because$ $\sqrt{2+\sqrt{5}} = a+b\sqrt{5}$ $(a, b \in \mathbb{Q})$ とおくと、$a^2+5b^2 = 2, 2ab = 1$ となり、$4a^4-8a^2+5 = 4\left(a^2-1\right)^2+1 = 0$ には有理数解がないから $\mathbb{Q}\left(\sqrt{5}\right) \subsetneq \mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right)$ となる。これより、$[\mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right) : \mathbb{Q}] = 4$ である。したがって、$\sqrt{2+\sqrt{5}}$ の $\mathbb{Q}$ 上の最小多項式は 4 次式で、

$$p_{\sqrt{2+\sqrt{5}},\mathbb{Q}}(x) = x^4 - 4x^2 - 1$$

となる。$p_{\sqrt{2+\sqrt{5}},\mathbb{Q}}(x)$ を複素数体上既約分解すると、

$$p_{\sqrt{2+\sqrt{5}},\mathbb{Q}}(x) = \left(x-\sqrt{2+\sqrt{5}}\right)\left(x+\sqrt{2+\sqrt{5}}\right)\left(x-\sqrt{2-\sqrt{5}}\right)\left(x+\sqrt{2-\sqrt{5}}\right)$$

となる。$\mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right)$ が $\mathbb{Q}$ 上正規拡大とすると、純虚数 $\sqrt{2-\sqrt{5}}$ が $\mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right)$ に属することになる。しかし、$\mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right) \subset \mathbb{R}$ なので、そんなことはない。$\mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right)$ は $\mathbb{Q}$ 上正規拡大でない。

以下、$\mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right)$ の最小分解体を求める。$\sqrt{2+\sqrt{5}}\sqrt{2-\sqrt{5}} = \sqrt{-1}$ なので、$p_{\sqrt{2+\sqrt{5}},\mathbb{Q}}(x)$ の最小分解体は $\mathbb{Q}\left(\sqrt{2+\sqrt{5}}, \sqrt{-1}\right)$ となる。したがって、$\mathbb{Q}\left(\sqrt{2+\sqrt{5}}, \sqrt{-1}\right)$ が求める体であり、その拡大次数は

$$\begin{aligned}\left[\mathbb{Q}\left(\sqrt{2+\sqrt{5}}, \sqrt{-1}\right) : \mathbb{Q}\right] &= \left[\mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right) : \mathbb{Q}\right]\left[\mathbb{Q}\left(\sqrt{2+\sqrt{5}}, \sqrt{-1}\right) : \mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right)\right] \\ &= 2 \times 4 = 8\end{aligned}$$

である。 □

問 21.
(1) n を正の整数とする。$\mathbb{Q}$ 上の多項式 $x^n - 2$ の最小分解体を求めよ。
(2) $\mathbb{Q}$ 上の多項式 $x^4 - 6x^2 - 2$ の最小分解体を求めよ。

問 22.
(1) K を標数 $p > 0$ の体、$\overline{K}$ を K の代数閉包、$\alpha \in \overline{K}$ とする。α が K 上純非分離的とは、α の K 上の共役元は α のみであることをいう。以下は、同値であることを証明せよ。
  (i) α は K 上純非分離的である。
  (ii) $\sharp \mathrm{Hom}_K(K(\alpha), \overline{K}) = 1$.
  (iii) $\exists e \geq 0$, $\alpha^{p^e} \in K$.
(2) K を標数 $p > 0$ の体、L/K を代数拡大とする。L/K が純非分離的とは、L のすべての元が K 上純非分離であることをいう。以下は、同値であることを証明せよ。
  (i) L/K 上純非分離拡大である。
  (ii) $\sharp \mathrm{Hom}_K(L, \overline{K}) = 1$.
  (iii) K 上純非分離的な元 $\alpha_1, \alpha_2, \cdots$ が存在して、$L = K(\alpha_1, \alpha_2, \cdots)$ となる。
(3) K を標数 $p > 0$ の体、L/K を有限次純非分離拡大とする。このとき、$[L : K]$ は p のべきであることを証明せよ。
(4) K を標数 $p > 0$ の体、L/K を非自明な有限次純非分離拡大とする。このとき、L/K のトレース $T_{L/K}$ は零写像であることを証明せよ。

問 23.
K を標数 $p > 0$ の体、L/K を代数拡大とする。
(1) L/K の中間体 K_i で K_i/K が純非分離拡大、L/K_i が分離拡大となるものがただひとつ存在することを証明せよ。
(2) L/K の中間体 K_s で K_s/K が分離拡大、L/K_s が純非分離拡大となるものがただひとつ存在することを証明せよ。
(3) $K_s \cap K_i = K$ は $L = K_i K_s$ (合成体、両者を含む最小の体) を証明せよ。
(4) K_i/K を有限次拡大とすると L/K_i も有限次拡大で、$[L : K_i] = [K_i : K]$ を証明せよ。その逆も成り立つこと証明せよ。

問 24.
K を標数 $p > 0$ の体、L/K を有限次体拡大とする。以下は、同値であることを証明せよ。
(i) L/K は分離拡大である。
(ii) トレース $T_{L/K}$ は零写像でない。

9. ガロア拡大と基本定理

この講義のメインテーマであるガロア拡大とその基本定理を解説する。

9.1. ガロア拡大.

定義 127.

L/K を代数拡大とする。L/K がガロア拡大とは、L/K が分離拡大かつ正規拡大のことをいう。L の K 上の自己同型群 $\mathrm{Aut}(L/K)$ をガロア群と呼び、$\mathrm{Gal}(L/K)$ と表す。

この講義では、有限次ガロア拡大を主に論ずる。

命題 128.

L/K をガロア拡大、M を中間体とすると、L/M はガロア拡大である。

$\because$ 命題 117, 122 より。 □

命題 129.

L/K をガロア拡大、M を K の拡大体とすると、ML/M はガロア拡大である。さらに、制限による写像 $\mathrm{Gal}(ML/M) \to \mathrm{Gal}(L/K)$ は単射である。

$\because$ L の元は K 上分離的かつ K 上の共役元はすべて L に属するから、ML/M はガロア拡大である。
$\sigma \in \mathrm{Gal}(ML/M)$ が、$\sigma|_L = \mathrm{id}_L$ とする σ は M 同型だから、$\sigma = \mathrm{id}_{ML}$ である。 □

例えば、$[L:K]$ と $[M:K]$ が互いに素のとき、$\mathrm{Gal}(ML/M) \to \mathrm{Gal}(L/K)$ は同型になる。

例 130.

L/K を 2 次拡大とする。

(1) 標数が 2 でないとすると、L/K はガロア拡大である。
(2) 標数が 2 とし、$L = K(\alpha)$、$p_{\alpha,K}(x) = x^2 + ax + b$ とする。このとき、例 113 と 119 より

$$L/K \text{ がガロア拡大} \iff a \neq 0$$

がなりたつ。

どちらの場合も、抽象的な群としてガロア群は $\mathbb{Z}/2\mathbb{Z}$ と同型である。

例 131.

(1) 命題 114 から、標数が 0 の場合は、ガロア拡大と正規拡大は同じである。
(2) 命題 124 から、分離多項式の最小分解体はガロア拡大である。

例 132.

$\mathbb{Q}(\sqrt{2},\sqrt{3})$ は $\mathbb{Q}$ 上のガロア拡大で、そのガロア群は

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

である。

$\because$ 実際、$\mathbb{Q}(\sqrt{2},\sqrt{3})$ は $\mathbb{Q}$ 上の $(x^2-2)(x^2-3)$ の最小分解体より、$\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ はガロア拡大である。よって、4 次のガロア拡大である (例 20)。

$\mathbb{Q}(\sqrt{2},\sqrt{3})$ の $\mathbb{Q}(\sqrt{3})$ 上の自己同型 σ を

$$\sigma(\sqrt{2}) = -\sqrt{2}$$

と定め、$\mathbb{Q}(\sqrt{2},\sqrt{3})$ の $\mathbb{Q}(\sqrt{2})$ 上の自己同型 τ を

$$\tau(\sqrt{3}) = -\sqrt{3}$$

と定める。すると、σ と τ は共に $\mathbb{Q}(\sqrt{2},\sqrt{3})$ の $\mathbb{Q}$ 上の自己同型になる。さらに、

$$\sigma^2=\tau^2=\mathrm{id},\quad ,\sigma\tau=\tau\sigma\neq\mathrm{id}$$

を満たす。実際、$\mathbb{Q}(\sqrt{2},\sqrt{3})$ の $\mathbb{Q}$ 上の基底として $1,\sqrt{2},\sqrt{3},\sqrt{6}$ が採れるので、各基底に対してチェックすればよい。例えば、

$$\sigma\tau(\sqrt{6})=\sigma(\tau(\sqrt{2}\sqrt{3}))=\sigma(\sqrt{2}\tau(\sqrt{3}))=\sigma(-\sqrt{2}\sqrt{3})=\sqrt{2}\sqrt{3}=\cdots=\tau\sigma(\sqrt{6})$$

となる。ガロア群 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ は位数 4 なので、アーベル群で、$\mathbb{Z}/4\mathbb{Z}$ または $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ のどちらかである。位数が 2 の元が 2 つ以上あるので、

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$$

となる。$\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ の元は $\mathrm{id},\sigma,\tau,\sigma\tau$ である。 □

定理-定義 133.

K の代数閉包を一つ固定する。L/K を有限次分離拡大とする。このとき、L を含む有限次ガロア拡大 N/K で、L を含む任意の K のガロア拡大体に含まれるものが存在する。N を L/K のガロア閉包という。

$\because$ L/K は単拡大で (定理 115)、その生成元の最小多項式の最小分解体を N とすればよい (例 131 (2))。 □

例 134.

例 125 より、次が成り立つ。

(1) $\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}$ はガロア拡大でない。

(2) $\mathbb{Q}(2^{\frac{1}{3}},\omega)/\mathbb{Q}$ は、$\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}$ のガロア閉包である。ただし、ω は $\omega^2+\omega+1=0$ を満たす複素数とする。

以下、ガロア群 $\mathrm{Gal}(\mathbb{Q}(2^{\frac{1}{3}},\omega)/\mathbb{Q})$ を決定する。$2^{\frac{1}{3}}$ と ω の行き先を決めれば $\mathbb{Q}(2^{\frac{1}{3}},\omega)$ の $\mathbb{Q}$ 上の自己同型は決まる。

$[\mathbb{Q}(2^{\frac{1}{3}},\omega):\mathbb{Q}(\omega)]=3$ なので、$2^{\frac{1}{3}}$ の $\mathbb{Q}(\omega)$ 上の共役元は $2^{\frac{1}{3}},2^{\frac{1}{3}}\omega,2^{\frac{1}{3}}\omega^2$ である。$\mathbb{Q}(\omega)$ 自己同型

$$\sigma:\mathbb{Q}(2^{\frac{1}{3}},\omega)\to\mathbb{Q}(2^{\frac{1}{3}},\omega)$$

を $\sigma(2^{\frac{1}{3}})=2^{\frac{1}{3}}\omega$ で定める。一方、$[\mathbb{Q}(2^{\frac{1}{3}},\omega):\mathbb{Q}(2^{\frac{1}{3}})]=2$ なので、ω の $\mathbb{Q}$ 上の共役元は ω,ω^2 となる。$\mathbb{Q}(2^{\frac{1}{3}})$ 自己同型

$$\tau:\mathbb{Q}(2^{\frac{1}{3}},\omega)\to\mathbb{Q}(2^{\frac{1}{3}},\omega)$$

を $\tau(\omega)=\omega^2$ で定める。明らかに、

$$\sigma^3=\mathrm{id},\tau^2=\mathrm{id},\tau\sigma\tau=\sigma^2$$

となる。実際、

$$\sigma^3(2^{\frac{1}{3}})=\sigma^2(2^{\frac{1}{3}}\omega)=\sigma(2^{\frac{1}{3}}\omega^2)=2^{\frac{1}{3}}\omega^3=2^{\frac{1}{3}}$$
$$\tau^2(\omega)=\tau(\omega^2)=\omega^4=\omega$$
$$\tau\sigma\tau(2^{\frac{1}{3}})=\tau\sigma(2^{\frac{1}{3}})=\tau(2^{\frac{1}{3}}\omega)=2^{\frac{1}{3}}\omega^2=\sigma(2^{\frac{1}{3}})$$
$$\tau\sigma\tau(\omega)=\tau\sigma(\omega^2)=\tau(\omega^2)=\omega^4=\omega=\sigma^2(\omega)$$

となる。G を

$$G=<\sigma,\tau;\sigma^3=\tau^2=\mathrm{id},\tau\sigma\tau=\sigma^{-1}>$$

で定まる群とする。関係式から、G は位数 6 の非可換群になる。したがって、G は 3 次の対称群 S_3 と同型である。σ と τ は自己同型より、G は $\mathrm{Gal}(\mathbb{Q}(2^{\frac{1}{3}},\omega)/\mathbb{Q})$ の部分群になる。一方、体拡大 $\mathbb{Q}(2^{\frac{1}{3}},\omega)/\mathbb{Q}$ は 6 次である。したがって、

$$\mathrm{Gal}(\mathbb{Q}(2^{\frac{1}{3}},\omega)/\mathbb{Q})=G\cong S_3$$

となる。

定理 135.

L/K を有限次代数拡大とする。このとき、次は同値である。
(i) L/K はガロア拡大である。
(ii) $\sharp\mathrm{Aut}(L/K) = [L : K]$.

$\because$ 系 96 と命題 102 より

$$\sharp\mathrm{Aut}(L/K) \leq \sharp\mathrm{Hom}_K(L, \overline{K}) \leq [L : K]$$

が成り立つ。左の等号が正規拡大となる必要十分条件 (定理 121) で、右の等号が分離拡大になる必要十分条件 (定理 115) である。 □

9.2. **固定部分体.** 群の体への作用とガロア拡大の関係を調べる。

定義 136.

(1) 群 G の体 L への作用とは、写像

$$G \times L \to L \quad (g, a) \mapsto g(a)$$

で、以下の条件を満たすものをいう。
(i) $(gh)(a) = g(h(a))$.
(ii) $e(a) = a$. ただし、e は G の単位元を表す。
(iii) $g(a + b) = g(a) + g(b)$.
(iv) $g(ab) = g(a)g(b)$.
(2) K を体 L の部分体とする。群 G が K 上 L に作用するとは、G の L への作用で
(v) $g(a) = a\,(\forall g \in G, \forall a \in K)$
が成り立つことを言う。
(3) 群 G の体 L の作用が忠実とは
(vi) $g(a) = a\,(\forall a \in L) \Rightarrow g = e$
が成り立つことを言う。

つぎの 2 つの命題の証明は容易。

命題 137.

群 G の体 L への作用を与えることは、 群の準同型

$$G \to \mathrm{Aut}(L)$$

を与えることと同じである。作用が忠実であることと、群の準同型が単射になるのが同値である。
部分体 K 上の作用については、$\mathrm{Aut}(L)$ を $\mathrm{Aut}(L/K)$ に変えれば同様のことが成り立つ。

命題-定義 138.

群 G の体 L への作用が与えられているとする。このとき、

$$L^G = \{a \in L \,|\, g(a) = a \forall\, g \in G\}$$

は体になる。作用が部分体 K 上のときには、L^G は拡大 L/K の中間体になる。L^G のことを、G による L の固定部分体という。

定理 139.

L を体、G を L に忠実に作用する有限群、$K = L^G$ を固定部分群とする。このとき、L/K は拡大次数 $\sharp G$ のガロア拡大になり、自然な写像

$$G \to \mathrm{Aut}(L/K) = \mathrm{Gal}(L/K)$$

は同型になる。

補題 140.

定理 139 の状況を仮定し、$\alpha \in L$ とする。

(1) $G_\alpha = \{g \in G \,|\, g(\alpha) = \alpha\}$ は G の部分群である。

(2) $g \in G$ に対して、$g(\alpha)$ は G の G_α による剰余類だけで決まり、$g(\alpha)$ の値は剰余類により異なる。

(3) $f_\alpha(x) = \prod_{\overline{g} \in G/G_\alpha} (x - g(\alpha))$ は K 上の分離単多項式で、$f_\alpha(\alpha) = 0$ である。ただし、$\overline{g}$ は g を代表元とする剰余類を表す。

(4) L は $f_\alpha(x)$ の分解体である。

$\because$ (1) (2) は作用の固定化部分群に関して一般的に成り立つこと。

(3) 分離的なことは、(2) よりでる。K 上の多項式になることは、G が G/G_α に左から作用することと対称式の性質からわかる。

(4) 各 $g(\alpha) \in L$ だから。 □

$\because$ 定理 139 の証明：$\alpha \in L$ とする。$f_\alpha(x)$ を 補題 140 の K 上の多項式とする。$f_\alpha(\alpha) = 0$ なので α は K 上代数的で、分離的である。さらに、K 上の α の共役元は $f_\alpha(x)$ の根になるから、L に属する。よって、L/K はガロア拡大である。さらに、

$$[K(\alpha) : K] \leq \deg(p_{\alpha,K}(x)) \leq \deg(f_\alpha(x)) \leq \sharp G$$

となる。この不等式は、任意の $\alpha \in L$ に対して成り立つことに注意しておく。

L/K が無限次拡大とすると、ある K 上有限次の中間体 M で $[M : K]$ が $\sharp G$ より大きくなるものが存在することになる。L/K はガロア拡大なので、M/K は分離拡大、よって定理 115 から単拡大となり矛盾する。したがって、L/K は有限次拡大である。L/K は単拡大であり、

$$[L : K] \leq \sharp G$$

である。

一方、作用が忠実なので、自然な写像 $G \to \mathrm{Gal}(L/K)$ は単射である。よって、

$$[L : K] = \sharp \mathrm{Gal}(L/K) \geq \sharp G$$

である。以上より、L/K は $\sharp G$ 次になり、自然な写像 $G \to \mathrm{Gal}(L/K)$ は同型である。 □

系 141.

L/K を有限次ガロア拡大とする。このとき、

$$K = L^{\mathrm{Gal}(L/K)}$$

となる。

$\because$ $K \subset L^{\mathrm{Gal}(L/K)}$ は明らか。定理 139 から

$$[L : K] = \sharp \mathrm{Gal}(L/K) = [L : L^{\mathrm{Gal}(L/K)}]$$

なので、両者は一致する。 □

例 142.
k を体、$L = k(x_1, \cdots, x_n)$ を n 変数関数体 (n 変数多項式環 $k[x_1, \cdots, x_n]$ の商体) とする。また、

$$\begin{array}{rcl} s_1 & = & x_1 + \cdots + x_n \\ s_2 & = & \prod_{i_1 < i_2} x_{i_1} x_{i_2} \\ \vdots & & \vdots \\ s_n & = & x_1 \cdots x_n \end{array}$$

を、n 変数の基本対称式で、$K = k(s_1, \cdots, s_n)$ を L の部分体とする。$G = S_n$ を n 次対称群とし、G の L への作用を

$$G \times L \to L$$

を $\sigma(f(x_1, \cdots, x_n)) = f(x_{\sigma^{-1}(1)}, \cdots, x_{\sigma^{-1}(n)})$ で定める。このとき、

$$L^G = K$$

となり、L/K は G をガロア群に持つガロア拡大になる。

$\because$ $s_1, \cdots, s_n$ は n 次対称式であるから、G 不変である。よって、$K \subset L^G$ である。一方、G の L への作用は忠実だから、定理 139 から

$$[L : L^G] = \sharp G = n!$$

となる。したがって、以下の主張を証明すればよい。

主張. $[L : K] \leq n!$.

$\because$ n に関する帰納法で示す。$n-1$ 次対称群 $H = S_{n-1}$ を n 次対称群 S_n への自然な埋め込みで部分群と見る。帰納法の仮定から

$$L^H = k(x_n)(t_1, \cdots t_{n-1}) = K(x_n)$$

となる。ここで、$t_1, \cdots, t_{n-1}$ は $x_1, \cdots, x_{n-1}$ に関する基本対称式とする。K の多項式

$$f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n$$

に対して、$f(x_n) = 0$ である。したがって、$[L^H : K] \leq n$ となり、帰納法の仮定から

$$[L : K] = [L^H : K][L : L^H] \leq n!$$

となる。 □

9.3. **ガロアの基本定理.** ガロアの基本定理を紹介する。無限次元ガロア拡大についても、ガロア群に位相を入れることで同様の定理が成り立つ。

定理 143.

L/K を有限次ガロア拡大とする。

(1) 写像

$$\begin{array}{ccc} \{H \mid \mathrm{Gal}(L/K) \text{の部分群}\} & \to & \{M \mid M \text{ は } L/K \text{ の中間体}\} \\ H & \mapsto & L^H \\ \mathrm{Gal}(L/M) & \leftarrow\!\shortmid & M \end{array}$$

は全単射である。さらに、H_1, H_2 を $\mathrm{Gal}(L/K)$ の部分群、M_1, M_2 を中間体とするとき

$$H_1 \subset H_2 \iff M_1 \supset M_2$$

である。

(2) 上の対応において、H が $\mathrm{Gal}(L/K)$ の正規部分群となるための必要十分条件は、L^H/K がガロア拡大になることである。このとき、自然な写像

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/L^H) \to \mathrm{Gal}(L^H/K)$$

は同型である。

∵ (1) 定理 139 と系 141 から、上に上げた写像は互いに逆であることがわかる。さらに以下は、写像の定義から明らか。
(2) H が正規部分群とする。L^H/K は分離拡大だから (系 117)、正規拡大を示せばよい。$\alpha \in L^H$ とする。α の K 上の共役元は、すべて $g(\alpha)\,(g \in G)$ と表せる。これらが、H で不変であることを示せば、$g(\alpha) \in L^H$ となり、L^H/K が正規拡大になる。$\sigma \in H$ に対して、H は正規部分群だから $g^{-1}\sigma g = \tau \in H$ となる。

$$\sigma(g(\alpha)) = g(\tau(\alpha)) = g(\alpha)$$

となるので証明できた。
逆に、L^H/K がガロア拡大とする。自然な写像

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(L^H/K)$$

の核が $H = \mathrm{Gal}(L/L^H)$ なので、H は正規部分群である。次数を比較することで、$\mathrm{Gal}(L/K) \to \mathrm{Gal}(L^H/K)$ は全射になる。よって、$\mathrm{Gal}(L^H/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L^H)$ である。 □

定義 144.

ガロア群がアーベル群であるガロア拡大をアーベル拡大という。ガロア群が巡回群であるガロア拡大を巡回拡大という。

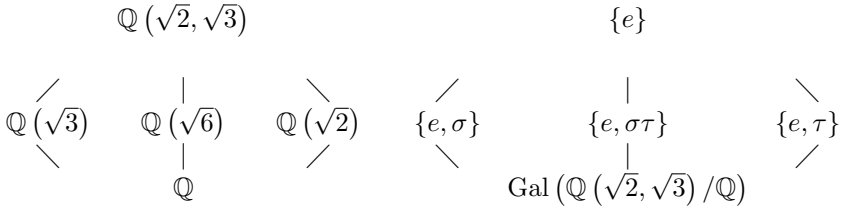
命題 145.

アーベル拡大 L/K の中間体 M は K 上のガロア拡大体である。

例 146.
4 次ガロア拡大 $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}$ の中間体の様子は以下のようになる。例 132 の記号を用いて、$\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ であり、その部分群は $\{e\}$, $\{e,\sigma\}$, $\{e,\tau\}$, $\{e,\sigma\tau\}$, $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}\right)$ の 5 つである。

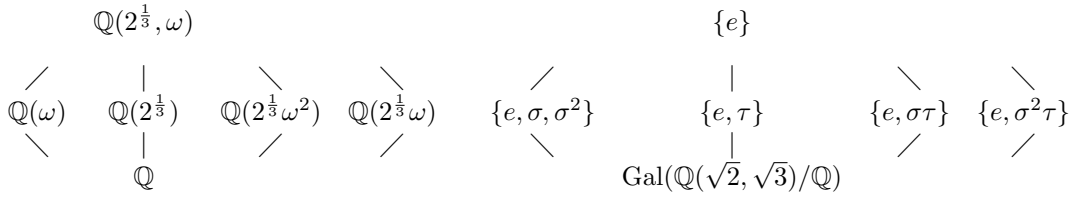
$$\sigma\tau\left(\sqrt{6}\right) = \sqrt{6}$$

なので、それぞれの群に中間体 $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$, $\mathbb{Q}\left(\sqrt{3}\right)$, $\mathbb{Q}\left(\sqrt{2}\right)$, $\mathbb{Q}\left(\sqrt{6}\right)$, $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ が対応する。



$\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}$ はアーベル拡大なので、すべての中間体が $\mathbb{Q}$ 上のガロア拡大になる。

例 147.
6 次ガロア拡大 $\mathbb{Q}(2^{\frac{1}{3}},\omega)/\mathbb{Q}$ (例 134) の中間体を求める。
$\mathrm{Gal}(\mathbb{Q}(2^{\frac{1}{3}},\omega)/\mathbb{Q}) \cong S_3$ であった。S_3 の部分群は、$\{e\},\{e,\tau\},\{e,\sigma\tau\},\{e,\sigma^2\tau\},\{e,\sigma,\sigma^2\},S_3$ である。対応する中間体は、以下の図のようになる。



正規部分群は自明な群と $\{e,\sigma,\sigma^2\}$ なので、$\mathbb{Q}$ 上 Galois 拡大である中間体は、$\mathbb{Q}, \mathbb{Q}(\omega)$ と $\mathbb{Q}(2^{\frac{1}{3}},\omega)$ である。

例 148.

8 次のガロア拡大 $\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)/\mathbb{Q}$ (例 126) のガロア群と中間体を求める。

位数 8 の群は、

$$\begin{array}{l}\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},\\ H_4\,(\text{四元数群 } H_4=\{\pm1,\pm i,\pm j,\pm k; i^2=j^2=k^2=-1, ij=-ji=k\}),\\ D_4\,(4\text{ 次の二面対群 } D_4=<\sigma,\tau;\sigma^4=\tau^2=1,\tau\sigma\tau=\sigma^{-1}>)\end{array}$$

のみで、$\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)/\mathbb{Q}\right)$ はいずれかである。

$\mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right)/\mathbb{Q}$ は正規拡大でない (例 126) ので、ガロア拡大でない (命題 144)。よって、$\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)/\mathbb{Q}$ はアーベル拡大でない。したがって、$\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)/\mathbb{Q}\right)$ は H_4 または D_4 である。

$\mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right)$ と $\mathbb{Q}\left(\sqrt{5},\sqrt{-1}\right)$ は $\mathbb{Q}$ 上 4 次の中間体なので、$\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)/\mathbb{Q}\right)$ には位数 2 の部分群は 2 つい以上ある。さて、H_4 の位数 2 の元は -1 のみなので、H_4 には位数 2 の部分群はただ一つである。したがって、

$$\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)/\mathbb{Q}\right)\cong D_4$$

である。

$\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)/\mathbb{Q}\right)$ の作用の様子をもっと具体的に見る。

$$\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)\cong\mathbb{Q}[x,y]/(x^4-4x^p-1,y^2+1)$$

だから、2 つの生成元 $\sqrt{2+\sqrt{5}},\sqrt{-1}$ がそれぞれの共役元へ勝手に移ることで $\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)$ の自己同型が与えられる。$\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)$ の自己同型 σ と τ を

$$\left\{\begin{array}{rcl}\sigma\left(\sqrt{2+\sqrt{5}}\right)&=&-\sqrt{2-\sqrt{5}}\\ \sigma\left(\sqrt{-1}\right)&=&-\sqrt{-1}\end{array}\right.\qquad\left\{\begin{array}{rcl}\tau\left(\sqrt{2+\sqrt{5}}\right)&=&\sqrt{2+\sqrt{5}}\\ \tau\left(\sqrt{-1}\right)&=&-\sqrt{-1}\end{array}\right.$$

と定める。σ と τ が 2 面体群の関係式を満たすことを調べる。$\sqrt{2+\sqrt{5}}\sqrt{2-\sqrt{5}}=\sqrt{-1}$ に注意すると、

$$\begin{array}{rcl}\sigma\left(\sqrt{2-\sqrt{5}}\right)&=&\sqrt{2+\sqrt{5}}\\ \tau\left(\sqrt{2-\sqrt{5}}\right)&=&-\sqrt{2-\sqrt{5}}\end{array}$$

となる。よって、σ を繰り返し作用させることにより

$$\begin{array}{ccccccccccc}\sqrt{2+\sqrt{5}}&\overset{\sigma}{\mapsto}&-\sqrt{2-\sqrt{5}}&\overset{\sigma}{\mapsto}&-\sqrt{2+\sqrt{5}}&\overset{\sigma}{\mapsto}&\sqrt{2-\sqrt{5}}&\overset{\sigma}{\mapsto}&\sqrt{2+\sqrt{5}}\\ \sqrt{-1}&\mapsto&-\sqrt{-1}&\mapsto&\sqrt{-1}&\mapsto&-\sqrt{-1}&\mapsto&\sqrt{-1}\end{array}$$

となる。したがって、

$$\sigma^4=\tau^2=e,\sigma^2\neq e$$

となる。また、$\tau\sigma\tau\sigma$ を作用させると

$$\begin{array}{ccccccccccc}\sqrt{2+\sqrt{5}}&\overset{\sigma}{\mapsto}&-\sqrt{2-\sqrt{5}}&\overset{\tau}{\mapsto}&\sqrt{2-\sqrt{5}}&\overset{\sigma}{\mapsto}&\sqrt{2+\sqrt{5}}&\overset{\tau}{\mapsto}&\sqrt{2+\sqrt{5}}\\ \sqrt{-1}&\overset{\sigma}{\mapsto}&-\sqrt{-1}&\overset{\tau}{\mapsto}&\sqrt{-1}&\overset{\sigma}{\mapsto}&1\sqrt{-1}&\overset{\tau}{\mapsto}&\sqrt{-1}\end{array}$$

となり、

$$\tau\sigma\tau=\sigma^{-1}$$

である。

拡大 $\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)/\mathbb{Q}$ の中間体とガロア群 $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)/\mathbb{Q}\right)\cong D_4$ の部分群との関係は、

$$\begin{array}{ccccccc} & & & \mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right) & & & \\ & & & & & & \\ \mathbb{Q}\left(\sqrt{5},\sqrt{-1}\right) & \mathbb{Q}\left(\sqrt{2-\sqrt{5}}\right) & \mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right) & & \mathbb{Q}\left(\sqrt{2+\sqrt{5}}-\sqrt{2-\sqrt{5}}\right) & \mathbb{Q}\left(\sqrt{2+\sqrt{5}}+\sqrt{2-\sqrt{5}}\right) & \\ & \mathbb{Q}\left(\sqrt{-5}\right) & \mathbb{Q}\left(\sqrt{5}\right) & & \mathbb{Q}\left(\sqrt{-1}\right) & & \\ & & \mathbb{Q} & & & & \end{array}$$

$$\begin{array}{ccccc} & & \{e\} & & \\ & & & & \\ \{e,\sigma^2\} & \{e,\sigma^2\tau\} & \{e,\tau\} & \{e,\sigma\tau\}, & \{e,\sigma^3\tau\} \\ & \{e,\sigma,\sigma^2,\sigma^3\} & \{e,\sigma^2,\tau,\sigma^2\tau\} & \{e,\sigma\tau,\sigma^2,\sigma^3\tau\} & \\ & & D_4 & & \end{array}$$

となる。例えば、

$$\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)^{\{e,\sigma\tau\}}=\mathbb{Q}\left(\sqrt{2+\sqrt{5}}-\sqrt{2-\sqrt{5}}\right)$$

を証明してみる。

$$\sigma\tau\left(\sqrt{2+\sqrt{5}}-\sqrt{2-\sqrt{5}}\right)=\sigma\left(\sqrt{2+\sqrt{5}}+\sqrt{2-\sqrt{5}}\right)=-\sqrt{2-\sqrt{5}}+\sqrt{2+\sqrt{5}}$$

であるから、

$$\mathbb{Q}\left(\sqrt{2+\sqrt{5}}-\sqrt{2-\sqrt{5}}\right)\subset\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)^{\{e,\sigma\tau\}}$$

となる。一方、

$$\sqrt{-1}=\frac{\left(\sqrt{2+\sqrt{5}}+\sqrt{2-\sqrt{5}}\right)^2-4}{2}$$

なので、

$$\mathbb{Q}\left(\sqrt{2+\sqrt{5}}-\sqrt{2-\sqrt{5}}\right)\left(\sqrt{2+\sqrt{5}}\right)=\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)$$

である。$\sqrt{2+\sqrt{5}}$ は $\mathbb{Q}\left(\sqrt{2+\sqrt{5}}-\sqrt{2-\sqrt{5}}\right)$ 上の 2 次方程式

$$x^2-\left(\sqrt{2+\sqrt{5}}-\sqrt{2-\sqrt{5}}\right)x-\sqrt{-1}=0$$

の解であるから、$\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)/\mathbb{Q}\left(\sqrt{2+\sqrt{5}}-\sqrt{2-\sqrt{5}}\right)$ は 2 次拡大で、

$$\mathbb{Q}\left(\sqrt{2+\sqrt{5}},\sqrt{-1}\right)^{\{e,\sigma\tau\}}=\mathbb{Q}\left(\sqrt{2+\sqrt{5}}-\sqrt{2-\sqrt{5}}\right)$$

となる。

D_4 の正規部分群になるのは、$\{e\},\{e,\sigma^2\},\{e,\sigma,\sigma^2,\sigma^3\},\{e,\sigma^2,\tau,\sigma^2\tau\},\{e,\sigma\tau,\sigma^2,\sigma^3\tau\},D_4$ で、対応する中間体のみが $\mathbb{Q}$ 上のガロア拡大である。

9.4. **代数学の基本定理の証明.** $\mathbb{R}$ の位相的性質から成り立つ次の 2 つの事実から出発して、代数学の基本定理を証明する。

事実.

(1) $a\geq 0$ とすると、x^2-a は $\mathbb{R}[x]$ の中で 1 次式の積に分解する。
(2) $\mathbb{R}[x]$ の奇数次の多項式は、$\mathbb{R}$ の中に少なくとも 1 つ根をもつ。

(1) は $\mathbb{R}$ の順序位相に関する完備性から成り立ち、(2) は中間値の定理である。

証明に使う群論の定理を紹介する。前者はシローの定理と呼ばれ、後者は p 群 (位数が p のべきの群) のべき零性の帰結である。代数学の基本定理の証明には、$p = 2$ のときを使う。

定理 A.

G を有限群、p を素数とする。このとき、G の p 部分群 H で $[G : H]$ が p と素になるものが存在する。H を p シロー群という。

定理 B.

G を p 群とする。このとき、G の部分群の列で

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_{r-1} \supsetneq G_r = \{e\}$$

$[G_{i-1} : G_i] = p$ $(1 \leq i \leq r)$ となるものが存在する。

主張 1.

(1) $\mathbb{C}$ には 2 次拡大が存在しない。

$\because$ 複素数の極表示と事実 1 から明らか。 □

主張 2.

(1) $\mathbb{R}$ の有限次代数拡大の次数は 2 のべきになる。
(2) $\mathbb{C}$ の有限次代数拡大の次数は 2 のべきになる。

$\because$ (1) $K/\mathbb{R}$ を位数が 2 のべきでない拡大とする。$\mathbb{R}$ は標数 0 なので (系 43)、$K/\mathbb{R}$ は分離拡大である (命題 114)。K を含む $\mathbb{R}$ 上の有限次ガロア拡大体 L をとり (定理 133)、G をそのガロア群とする。H を G の 2 シロー群とすると、$K/\mathbb{R}$ の拡大次数の仮定から $H \neq G$ である (定理 A)。H に対応する $L/\mathbb{R}$ の中間体を M とし、$M = \mathbb{R}(\alpha)$ とする (定理 115) と、α の $\mathbb{R}$ 上の最小多項式は 1 より大きい奇数次の既約多項式になる　(定理 143)。これは、事実 (2) に反する。したがって、$\mathbb{R}$ の有限次代数拡大の次数は、2 のべきになる。
(2) (1) から明らか。 □

$\because$ 代数学の基本定理の証明 : K を $\mathbb{C}$ の有限次代数拡大とする。主張 2 と K を含む $\mathbb{C}$ 上有限次のガロア閉包の存在定理から、$K/\mathbb{C}$ は次数が 2 のべきであるガロア拡大としてよい。$K \neq \mathbb{C}$ ならば、定理 B とガロアの基本定理から $\mathbb{C}$ 上に 2 次拡大が存在することになり、主張 1 に反する。したがって、$K = \mathbb{C}$ である。

したがって、命題 85 から代数学の基本定理が成り立つ。 □

問 25.

(1) $\mathbb{Q}$ 上の $\mathbb{Q}(2^{\frac{1}{4}})$ のガロア閉包を求めよ。また、そのガロア群を求めよ。
(2) $\mathbb{Q}$ 上の $\mathbb{Q}(\sqrt{3+\sqrt{11}})$ のガロア閉包を求めよ。また、そのガロア群を求めよ。

問 26.

(1) ガロア群が $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ になる $\mathbb{Q}$ 上のガロア拡大体を一つ求めよ。
(2) ガロア群が 4 元数群 H_4 になる $\mathbb{Q}$ 上のガロア拡大体を一つ求めよ。

10. 円分体

n を正の整数、$\mu_n \subset \mathbb{C}$ を 1 の n 乗根全体からなる集合とする。$\mathbb{Q}$ の拡大体 $\mathbb{Q}(\mu_n)$ を n 分体という。n 分体のように、有理数体上 1 のべき根で生成される体のことを円分体という。

この章では、円分体が有理数体上ガロア拡大であることを証明し、そのガロア群を決定する。

10.1. **オイラー関数.** オイラー関数を導入する。

定義 149.

正の整数 n に対し

$$\varphi(n) = \begin{cases} 1 & \text{if } n = 1 \\ \sharp(\mathbb{Z}/n\mathbb{Z})^\times & \text{if } n > 1 \end{cases}$$

と定める。φ をオイラー関数という。

命題 150.

n, m を互いに素な正の整数とすると

$$\varphi(mn) = \varphi(m)\varphi(n)$$

となる。

$\because$ 証明は次の中国式剰余定理から明らか。 □

命題 151.

n, m を互いに素な 2 以上の整数とすると、環準同型

$$\begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ a & \mapsto & (a \bmod m, a \bmod n) \end{array}$$

は同型である。特に、上の同型は乗法群の同型

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

を導く。

命題 152.

$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ $(r \geq 1, p_1, \cdots, p_r$ は互いに異なる素数$, e_1, \cdots, e_r \geq 1)$ とすると

$$\varphi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1)$$

である。

$\because$ 証明は、命題 150 と次補題から明らか。 □

補題 153.

p を素数、e を正の自然数とする。このとき、

$$\varphi(p^e) = p^{e-1}(p-1)$$

である。

$\because$ $(\mathbb{Z}/p^e\mathbb{Z})^\times$ は p と素な 0 から $p^e - 1$ までの元の像からなる。 □

10.2. **円分体.** この節では、円分体のガロア群を決定する。

定義 154.

n を正の整数とする。$\mathbb{Q}$ にすべての 1 の n 乗根を添加した複素数体 $\mathbb{C}$ の部分体 $\mathbb{Q}(\mu_n)$ を n 分体という。ある正の整数 n に対して、n 分体になるような $\mathbb{C}$ の部分体を円分体という。

命題 155.

K_n を n 分体とする。
(1) $2 \nmid n \implies K_n = K_{2n}$.
(2) $m \mid n \implies K_m \subset K_n$.

$\because$ (1) $\mu_{2n} = \mu_n \cup -\mu_n$ より。
(2) $\mu_m \subset \mu_n$. より。 □

命題 156.

複素数体 $\mathbb{C}$ の中で、1 の n 乗根の集合 μ_n は、乗法に関して位数 n の巡回群になる。

$\because$ $\mu_n = \{e^{\frac{2\pi ik}{n}} \mid k \in \mathbb{Z}/n\mathbb{Z}\} \cong \mathbb{Z}/n\mathbb{Z}$ となる。 □

補題 157.

$\zeta \in \mathbb{C}$ とする。以下は同値である。
(i) ζ は原始 n 乗根、すなわち、n 乗すると初めて 1 になる元である。
(ii) $\exists k \in (\mathbb{Z}/n\mathbb{Z})^\times, \zeta = e^{\frac{2\pi ik}{n}}$.

$\because$ $(\mathbb{Z}/n\mathbb{Z})^\times$ の各元が、$\mathbb{Z}/n\mathbb{Z}$ の生成元になるから。 □

よって次の命題が成り立つ。

命題 158.

K を 複素数体 $\mathbb{C}$ の部分体とする。以下は同値である。
(i) K は n 分体である。
(ii) $K = \mathbb{Q}(e^{\frac{2\pi i}{n}})$.
(iii) ある原始 n 乗根 ζ が存在して、$K = \mathbb{Q}(\zeta)$ となる。

命題-定義 159.

n を正の整数とする。

$$\Phi_n(x) = \prod_{\zeta:1\text{の原始 } n \text{ 乗根} \in \mathbb{C}} x - \zeta$$

は整係数の $\varphi(n)$ 次単多項式である。$\Phi_n(x)$ を n 等分多項式といい、総称して円分多項式という。

∵ $\Phi_n(x)$ が整係数単多項式であることを証明する。1 の n 乗根の位数は n の約数だから、

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

となる。n に関する帰納法で、$\Phi_n(x)$ が整係数単多項式であることがわかる。 □

定理 160.

K_n を n 分体とすると、$K_n/\mathbb{Q}$ はガロア拡大である。また、$\zeta \in \mathbb{C}$ を 1 の原始 n 乗根とすると、写像

$$\rho : \mathrm{Gal}(K_n/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

を $\sigma(\zeta) = \zeta^{\rho(\sigma)}$ と定める。ρ は ζ の選び方によらず、群の同型になる。

∵ 1° ガロア拡大であること：n 分体は分離多項式 $x^n - 1$ の最小分解体になっているので、例 131 からガロア拡大である。
2° ζ の取り方によらないこと：補題 157 から、任意の原始 n 乗根はある $l \in (\mathbb{Z}/n\mathbb{Z})^\times$ が存在して ζ^l とかける。

$$\sigma(\zeta^l) = \sigma(\zeta)^l = \zeta^{l\rho(\sigma)}$$

となり、l は可逆だから、ρ は 1 の原始 n 乗根の取り方によらない。
3° ρ の単射性は、ガロア群が K_n に忠実に作用することから明らか。
4° ρ の全射性：$f(x)$ を ζ の $\mathbb{Q}$ 上の最小多項式とする。ガウスの補題 (系 78) から $f(x)$ は整係数単多項式である。全射性を示すためには、任意の n と素な素数 p の対して、$f(\zeta^p) = 0$ を証明すればよい。実際、$f(\zeta^p) = 0$ ならば、系 104 より ζ を ζ^p に移す K_n の自己同型が存在する。よって、$\mathbb{Z}/n\mathbb{Z}$ の中での p の像も ρ の像に入る。$(\mathbb{Z}/n\mathbb{Z})^\times$ は n と素な素数で生成されるから、ρ は全射になる。

p を n と素な素数とする。$\Phi_n(x) = f(x)g(x)$ とおくと、$g(x)$ も整係数単多項式である。$x^n - 1$ は $F_p[x]$ 上でも分離的なので、$f(x)$ と $g(x)$ の還元射による $\mathbb{F}_p[x]$ で像 $\overline{f}(x)$ と $\overline{g}(x)$ はともに分離的である。

$\overline{\mathbb{F}}_p$ を $\mathbb{F}_p$ の代数的閉包とする。すると、環準同型 $\mathbb{Z}[\zeta] \to \overline{\mathbb{F}}_p$ が存在する。

さて、$f(\zeta^p) \neq 0$ とする。ζ^p は 1 の原始 n 乗根なので、$g(\zeta^p) = 0$ である。ζ のこの準同型 $\mathbb{Z}[\zeta] \to \overline{\mathbb{F}}_p$ による像を $\overline{\zeta}$ とすると

$$\overline{f}(\overline{\zeta}) = 0, \quad \overline{g}(\overline{\zeta}) \neq 0$$

となる。一方。$\mathbb{F}_p$ 上では

$$\overline{g}(\overline{\zeta})^p = \overline{g}(\overline{\zeta}^p) = 0$$

となる。$\overline{\mathbb{F}}_p$ は体なので、$\overline{g}(\overline{\zeta}) = 0$ となり、矛盾が生じた。したがって、$f(\zeta^p) = 0$ である。

以上で、ρ の全射性が示せた。 □

系 161.

n 等分多項式 $\Phi_n(x)$ は既約である。

∵ $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n) = \deg(\Phi_n(x))$ なので、$\Phi_n(x)$ は $\mathbb{Q}$ 上既約である。 □

例 162.

n 分体 $K_n = \mathbb{Q}(\zeta_n), \zeta_n = e^{\frac{2\pi i}{n}}$ に含まれる 2 次体 (例 73) を考察する。

(1) $K_2 = K_1 = \mathbb{Q}$ なので、2 次体は含まない。

(2) $K_6 = K_3 = \mathbb{Q}(\sqrt{-3})$ なので、円分体自身が 2 次体である。

(3) $K_4 = \mathbb{Q}(\sqrt{-1})$ なので、円分体自身が 2 次体である。

(4) $n = 5$ とする。$\mathrm{Gal}(K_5/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$ である。位数 4 の巡回群の指数 2 の部分群はただ一つだから、K_5 には 1 つだけ 2 次体が含まれる。

$$g = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 \in K_5$$

と定める。

$$\begin{aligned} g^2 &= \zeta_5^2 - \zeta_5^3 - \zeta_4 + 1 - \zeta_5^3 + \zeta_5^4 + 1 - \zeta_5 - \zeta_5^4 + 1 + \zeta_5 - \zeta_5^2 + 1 - \zeta_5 - \zeta_5^2 + \zeta_5^3 \\ &= 4 - \zeta_5 - \zeta_5^2 - \zeta_5^3 - \zeta_5^4 \\ &= 5 \end{aligned}$$

なので、

$$g = \pm\sqrt{5} \in K_5$$

となる。したがって、2 次体 $\mathbb{Q}(\sqrt{5})$ が含まれ、含まれる 2 次体はこれに限る。

(5) $n = 15$ とする。$\mathrm{Gal}(K_{15}/\mathbb{Q}) \cong (\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ である。指数 2 の部分群は、$0 \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times 2\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times 2\mathbb{Z}/4\mathbb{Z}$ となる。命題 155 から $K_3, K_5 \subset K_{15}$ だから、K_{15} に含まれる 2 次体は、$\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{-15})$ の三つである。

正 n 角形の作図に利用するので、次の命題をあげる。

命題 163.

n 分体 K_n において次は同値である。

(i) $n = 2^e p_1 p_2 \cdots p_r$. ただし、$e \geq 0$ で $p_1, \cdots, p_r$ は $1 + 2^f$ $(f \geq 1)$ となる相異なる素数とする。

(ii) $\varphi(n)$ は 2 のべきである。

(iii) 2 次拡大の列

$$\mathbb{Q} = F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_s = K_n$$

が存在する。

$\because$ (i) $\Rightarrow$ (iii) : 定理 160 より、$\mathrm{Gal}(K_n/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$ となる。$\mathbb{Z}/n\mathbb{Z}$ は位数が 2 べきのアーベル群より、ガロアの基本定理 143 から 2 次拡大の列が存在する。

(iii) $\Rightarrow$ (ii) は定理 160。

(ii) $\Rightarrow$ (i) は命題 152。 □

定理の (i) の条件を満たす 2 でない素数は、$3, 5, 17, 257, \cdots$ となる。こういう素数は無限個あると予想されているが、現在のところ未解決である。

問 27.

m, n を正の整数、l をその最大公約数とする。このとき、$K_m \cap K_n = K_l$ を証明せよ。

問 28.

7 分体、8 分体、 16 分体、60 分体に含まれる 2 次体を求めよ。

問 29.

任意の 2 次体は円分体に含まれることを証明せよ。

11. 作図とギリシアの三大作図不能問題

「定規とコンパスを使った作図」はギリシア数学から始まる由緒正しき問題である。この章では、作図と体論の関係を解説し、ギリシアの三大作図不能問題に適用する。

11.1. **作図.** 最初に、「定規とコンパスを使った作図」ということを厳密に定義する。直線は異なる 2 点で定まるから、作図というのは与えられた点から新しい点を決められた方法で得る方法である。もちろん、大きさ (長さ) を考えるためには単位の大きさ (大きさ 1) が与えられている。

定義 164.

Ω を単位の長さを表す 2 点を含む平面上の点の集合とする。

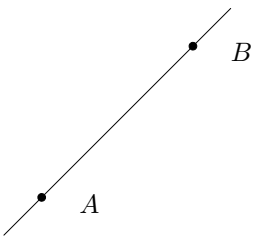
(1) $\Gamma = \Omega$ とする。 以下の (a), (b), (c) のいずれかで得た点を Γ に加える操作を行い、この操作を有限回繰り返した結果 Γ に含まれる点のことを、Ω から始めて作図可能な点という。
   (a) それぞれが Γ に属する異なる 2 点を通る 2 つの異なる直線 l, l' の交点　$l \cap l'$ を Γ に加える。
   (b) Γ に属する異なる 2 点を通る直線 l と Γ に属する異なる 2 点の一方が中心で他方が円周上にあるにある円周 π の交点 $l \cap \pi$ を Γ に加える。
   (c) それぞれが Γ に属する異なる 2 点の一方を中心に、他方が円周上にあるにある 2 つの異なる円周 π, π' の交点 $\pi \cap \pi'$ を Γ に加える。

(2) Ω から始めて作図可能な異なる 2 点を通る直線を作図可能な直線という。2 点を結ぶ線分の長さを作図可能な長さという。

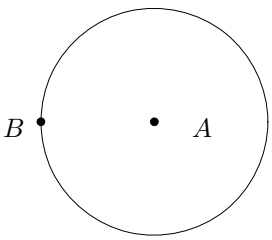
(3) Ω から始めて作図可能な 2 点を結ぶ線分の長さを作図可能な大きさという。

(4) Ω から始めて作図可能な互いに異なる 3 点 A, B, C に対して、角 ABC を作図可能な角という。単に作図可能というと、Ω が単位の大きさを与える 2 点からなる場合をいう。

定規では「与えられている 2 点を結ぶ直線を引く」ことだけができ、コンパスでは「与えられている 2 点の一方を中心に他方が円周上にある円周を描く」ことだけができる。



$A, B \in \Omega$



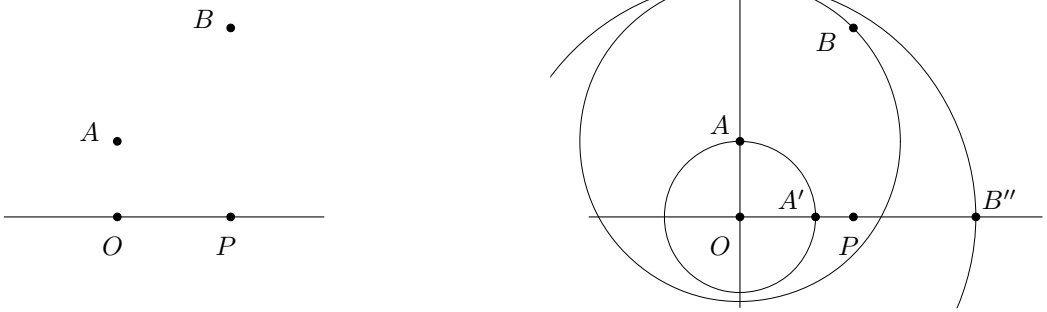
$A, B \in \Omega$

11.2. **作図の操作.** 以下の 3 つの補題では、単位の長さを与えていないが、それは本質的に必要はなく、例えば異なる 2 点をとりそれを単位の長さとすればよい。コンパスで長さを取れば、与えられた線分を移すことはできるように思えるが、定義から直ぐには明かでない。最初に、この操作が可能であることを証明する。

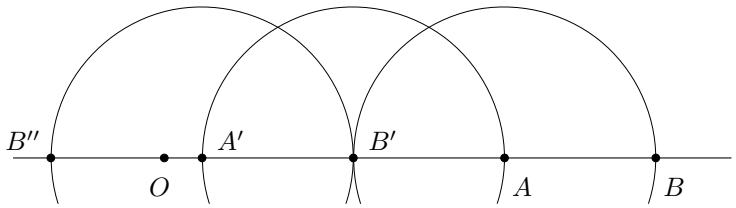
補題 165.

O, P, A, B を平面上の点とし、$O \neq P$ とする。集合 $\{O, P, A, B\}$ から始めて、直線 OP 上の点 Q で、$OQ = AB$ となるものが作図可能である。

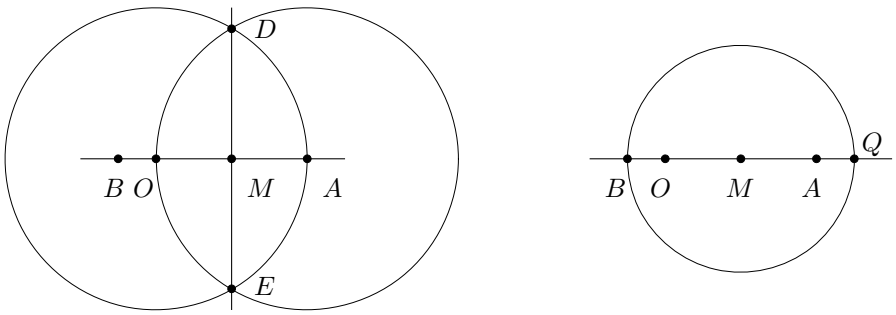
$\because$ $A = B$ のときは明らか。$A \neq B$ とする。まず、線分 AB が直線 OP 上にある場合に帰着する。点 A が直線 OP 上にないとする。A を中心とする円周と直線 OA の交点を考えることにより、操作 (b) から B は直線 OA 上にあるとしてよい。同様に、O を中心とする円周を考えることにより、A と B は直線 OP 上にあるとしてよい。



下図のように (b) を繰り返すと、点 O は線分 AB 上にあるとしてよい。



OA の 2 等分点 M は作図可能である。実際、点 O と点 A をそれぞれの中心とする半径が OA の円周の 2 つの交点 D と E は (c) より作図可能で、M は直線 DE と直線 OA の交点で、操作 (a) より作図可能である。



点 M を中心として半径が MB の円周と直線 OP の B と異なる交点を Q とすると、$OQ = AB$ となる。操作 (b) より Q は作図可能である。 □

補題 166.

直線 l と l 上にない点 P が与えられているとする。P を通り、l と平行な直線は作図可能である。

補題 167.

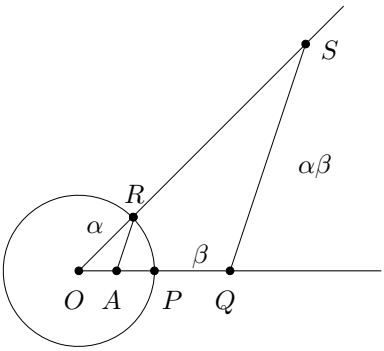
与えられた角の 2 等分線は作図可能であり、与えられた 2 つの角の和も作図可能である。

次の命題は、作図可能な大きさの加減乗除は再び作図可能であることを意味する。

命題 168.

単位の大きさを 1 とする。α, β が与えられた大きさならば、$\alpha \pm \beta, \alpha\beta, \alpha/\beta\,(\beta \neq 0)$ も作図可能な大きさである。

$\because$ 積 $\alpha\beta$ について、次の図を考える。



$AR//QS$

$OA = 1, OP = \alpha, OQ = \beta$ とする。この図が作図可能なのは、上の補題からわかる。三角形の相似より、$QS = \alpha\beta$ となる。

他の場合は省略する。 □

系 169.

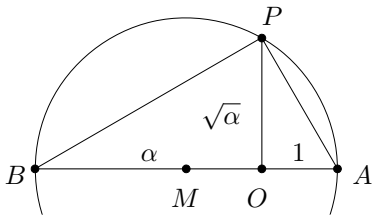
単位の大きさを 1 とする。負でない有理数は作図可能な大きさである。

平方根か作図可能であることを証明する。

命題 170.

単位の大きさを 1 とする。α が作図可能な大きさならば、$\sqrt{\alpha}$ も作図可能である。

$\because$ 次の図を考える。



$OA = 1, OB = \alpha$ とし、M は線分 AB の中点、OP と AB は直交する。この図が作図可能であることは、上のいくつかの補題からわかる。三角形の相似より、$OP = \sqrt{\alpha}$ となる。 □

11.3. **複素数と作図可能性.** 作図を考える上で、平面を複素平面として考え、作図できる点を作図できる複素数と考える方が都合がよい。単位の大きさとして、最初に与えられた複素数の集合 Ω の中に 0 と 1 は常に与えられているものとする。単に作図可能というと、$\Omega = \{0, 1\}$ の場合をいう。

命題 171.

$\alpha \in \mathbb{C}$ とする。以下は同値である。
(i) α が作図可能である。
(ii) α の実部と虚部が作図可能な大きさである。
(iii) α の大きさが作図可能な大きさであり、α の偏角が作図可能な角である。

命題 172.

(1) $\alpha, \beta \in \mathbb{C}$ が作図可能とすると、$\alpha \pm \beta, \alpha\beta, \alpha/\beta\ (\beta \neq 0)$ は作図可能である。
(2) $a, b, c \in \mathbb{C}$, $(a \neq 0)$ が作図可能とする。2 次方程式 $ax^2 + bx + c = 0$ の解は作図可能である。

$\because$ (1) 複素数の極表示に対して、前節の命題と補題を適用すればよい。
(2) (1) を用いると、方程式は $x^2 = c$ という形をしているとしてよい。複素数の極表示に、前節の命題と補題を適用すればよい。 □

定理 173.

Ω を $0, 1$ を含む複素数体 $\mathbb{C}$ の部分集合とし、$\alpha \in \mathbb{C}$ とする。このとき、以下は同値である。
(i) α が Ω から始めて作図可能である。
(ii) ある長さが有限の体拡大列

$$\mathbb{Q}(\Omega) = K_0 \subset K_1 \subset K_2 \subset \cdots K_{n-1} \subset K_n$$
$$[K_j : K_{j-1}] = 2 \quad (1 \leq j \leq n)$$

が存在して、$\alpha \in K_n$ となる。

$\because$ (ii) $\Rightarrow$ (i) は定理 172。
(i) $\Rightarrow$ (ii) の証明 : (a) 直線と直線の交点、(b) 直線と円周の交点、(c) 円周と円周の交点の 3 つの場合に、得られる点が与えられた複素数係数の高々 2 次の方程式の解になることをいえばよい。
(a) 回転は複素数倍で与えられるから、一方の直線を実軸としてよい。交点は、他方の直線を決める 2 点の実部と虚部の加減乗除で与えられる。
(b) 回転と平行移動で、円周の中心を 0、直線を虚軸と平行としてよい。円周の半径を r、直線を実部が a とすると、交点の虚部は $\pm\sqrt{r^2 - a^2}$ となる。
(c) 回転と平行移動で、一方の円周の中心を 0、他方の円周の中心を $v > 0$ とできる。それぞれの半径を r と s とすると、交点の実部は方程式 $r^2 - x^2 = s^2 - (v - x)^2$ となる。これは、1 次方程式で、(b) と合わせると交点は 2 次方程式の解になる。 □

系 174.

$\alpha \in \mathbb{C}$ が作図可能ならば $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ は 2 のべきである。

11.4. **正 n 角形の作図.** 単位円に内接する正 n 角形が 1 を一つの頂点にもつと、頂点の集合は 1 の n 乗根の集合と一致する。正 n 角形が作図可能とは、単位円に内接する 1 を一つの頂点にもつ正 n 角形が作図可能なことをいう。

定理 175.

$n \geq 3$ とする。次の条件は同値である。
(i) 正 n 角形は作図可能である。
(ii) $n = 2^e p_1 p_2 \cdots p_r$. ただし、$e \geq 0$ で $p_1, \cdots, p_r$ は $1 + 2^f\ (f \geq 1)$ となる相異なる素数とする。

$\because$ 命題 163 より。 □

例 176.

$5 = 1 + 2^2$ より、正 5 角形は作図可能である。

$\because$ $\zeta_5 = e^{\frac{2\pi i}{5}}$ とおく。$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$ なので、$f(x) = x^4 + x^3 + x^2 + x^1 + 1$ とすると $f(\zeta_5) = 0$ である。$t = x + x^{-1}$ とおくと、

$$g(t) = x^{-2} f(x) = x^2 + x + 1 + x^{-1} + x^{-2} = t^2 + t - 1$$

となる。$g(t) = 0$ とすると、$t = \frac{-1 \pm \sqrt{5}}{2}$ である。したがって、複素数列

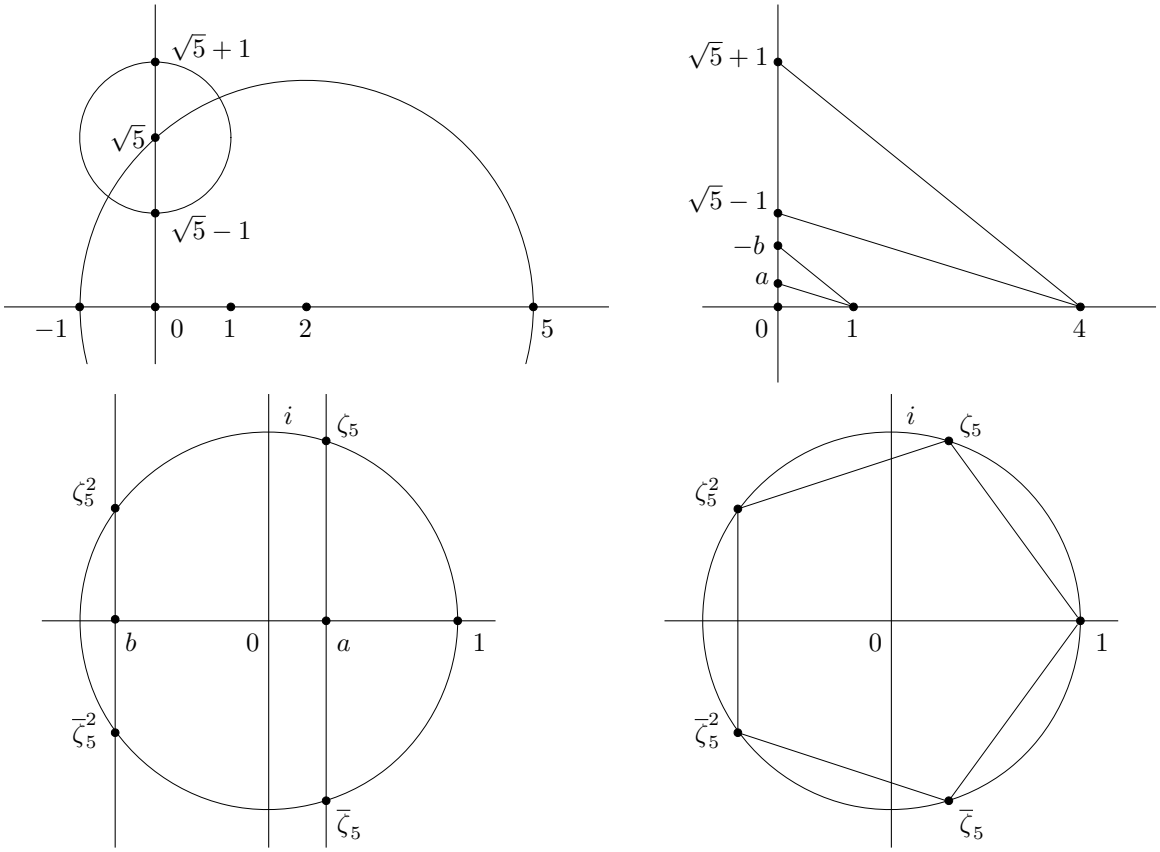
$$\mathbb{Q} \subset \mathbb{Q}(\frac{-1+\sqrt{5}}{2}) \subset \mathbb{Q}(\zeta_5)$$

が 2 次拡大列になる。 □

実際に正 5 角形を作図してみる。

$$\begin{array}{rcccl} 2\mathrm{Re}(\zeta_5) & = & \zeta_5 + \overline{\zeta}_5 & = & \frac{-1+\sqrt{5}}{2} \quad = \quad 2a \\ 2\mathrm{Re}(\zeta_5^2) & = & \zeta_5^2 + \overline{\zeta}_5^2 & = & \frac{-1-\sqrt{5}}{2} \quad = \quad 2b \end{array}$$

とおく。最初に a と b を作図し、正五角形を作図すると次のようになる。



11.5. **ギリシアの 3 大作図不能問題.** ギリシアの 3 大作図不能問題とは、

(a) 立方倍積問題：与えられた立方体の 2 倍の体積を持つ立方体一辺の作図
(b) 角の 3 等分問題：任意の角の 3 等分線の作図
(c) 円積問題：与えられた円と同じ面積の正方形の作図

のことである。以下、作図不可能であることを証明する。

(a) これは、方程式 $x^3 = 2$ の解 $x = 2^{\frac{1}{3}}$ が作図可能かを問うている問題に他ならず、

$$[\mathbb{Q}(2^{\frac{1}{3}}) : \mathbb{Q}] = 3$$

なので、作図不可能である。

(b) $e^{\frac{2\pi i}{3}}$ は 1 の 3 乗根なので、角度 $\frac{2\pi}{3}$ は作図可能である。しかし、その 3 等分である角度 $\frac{2\pi}{9}$ は作図不可能である。実際、角度 $\frac{2\pi}{9}$ が作図可能とすると、正 9 角形が作図可能になる。これは矛盾である。

(c) これは、方程式 $x^2 = \pi$ の解 $\sqrt{\pi}$ が作図可能かを問うている問題である。π は超越数なので、$\sqrt{\pi}$ は代数的でなく、作図不可能である。

問 30.
正 17 角形を作図せよ。

12. 方程式の可解性

方程式が代数的に解けるかどうかは、19 世紀までの数学において最大の問題の一つであった。4 次方程式までは代数的に解けることが知られていたが、5 次以上の方程式については、一般に不明であった。アーベルは 5 次以上の方程式が代数的に解けないことを証明した。ガロアは、彼の生み出した解の置換から定まるガロア群の言葉を用いて、方程式がいつ代数的に解けるかを判定した。

この章では、ガロアによる方程式の可解性の理論を現代風に解説する。

12.1. **最小分解体のガロア群.**

最初に、d 次方程式のガロア群が d 次対称群に埋め込めることをみておく。さらに、いくつかの例を計算する。

命題 177.

K を体、$f(x) \in K[x]$ を d 次分離多項式 $(d \geq 1)$、L を $f(x)$ の K 上の最小分解体とする。このとき、$f(x)$ の根へのガロア群 $\mathrm{Gal}(L/K)$ は、ガロア群 $\mathrm{Gal}(L/K)$ の d 次対称群 S_d への埋め込みを定める。さらに、もし $f(x)$ が K 上既約ならば、$\mathrm{Gal}(L/K)$ の根の集合への作用は推移的である。

$\because$ $\mathrm{Gal}(L/K)$ は $f(x)$ の根の集合への忠実な作用を与える。既約ならば、系 104 から作用は推移的になる。 □

定義 178.

K を体、$f(x) \in K[x]$ を d 次単多項式 $(d \geq 1)$ で、K の代数閉包 $\overline{K}$ では

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_d)$$

と分解されるとする。このとき、多項式 $f(x)$ の共役差積 Δ_f と判別式 D_f を

$$\begin{aligned} \Delta_f &= \prod_{i<j}(\alpha_i - \alpha_j) \\ D_f &= \prod_{i<j}(\alpha_i - \alpha_j)^2 \quad = \quad \Delta_f^2 \end{aligned}$$

と定める。ただし、$d=1$ のとき $D_f = \Delta_f = 1$ とする。

定義から、「$D_f = 0 \iff f(x)$ は分離的でない」となる。

例 179.

(1) $f(x) = x^2 + ax + b$ とする。このとき、

$$D_f = a^2 - 4b$$

となる。

(2) $f(x) = x^3 + ax + b$ とする。(標数が 3 でなければ一般性を失わない。) このとき、

$$D_f = -(4a^3 + 27b^2)$$

となる。

命題 180.

定義の状況で、L を既約な分離多項式 $f(x)$ の K 上の最小分解体し、$\mathrm{Gal}(L/K) \subset S_d$ を固定する。

(1) $\Delta_f \in L^\times, D_f \in K^\times$.

(2) $\Delta_f \in K^\times \iff \mathrm{Gal}(L/K) \subset A_d$.
ただし、A_d で d 次交代群を表す。

$\because$ 判別式 D_f は $\alpha_1, \cdots, \alpha_d$ の対称式で表され、共役差積 Δ_f は $\alpha_1, \cdots, \alpha_d$ の反対称式で表されるから。 □

系 181.

$f(x)=x^3+ax+b\in K[x]$ を既約分離多項式とし、L を $f(x)$ の K 上の最小分解体とする。
(1) $D_f\notin (K^\times)^2 \iff \Delta_f\notin K^\times \iff \mathrm{Gal}(L/K)\cong S_3$.
(2) $D_f\in (K^\times)^2 \iff \Delta_f\in K^\times \iff \mathrm{Gal}(L/K)\cong A_3$.

$\because$ $f(x)$ は既約だから、$[L:K]\geq 3$ となる。よって、ガロア群は A_3 を含む。したがって、いずれかの同値条件が常に成り立つ。 □

例 182.
(1) $f(x)=x^3-3x+3\in\mathbb{Q}[x]$ は、$p=3$ としてアイゼンシュタインの既約性判定法を適用すると、既約多項式であることがわかる。その判別式は

$$D_f=-(4\times(-3)^3+27\times 3^2)=-135\notin(\mathbb{Q}^\times)^2$$

となる。よって、$f(x)$ の最小分解体 L のガロア群は $\mathrm{Gal}(L/\mathbb{Q})\cong S_3$ となる。
(2) $f(x)=x^3-3x+1\in\mathbb{Q}[x]$ は、3 を法とすると　$\mathbb{F}_3[x]$ の既約多項式なので、既約多項式である。その判別式は

$$D_f=-(4\times(-3)^3+27\times 1^2)=81=9^2\in(\mathbb{Q}^\times)^2$$

となる。よって、$f(x)$ の最小分解体 L のガロア群は $\mathrm{Gal}(L/\mathbb{Q})\cong A_3\cong\mathbb{Z}/3\mathbb{Z}$ となる。

例 183.
$L(\subset\mathbb{C})$ を、$\mathbb{Q}$ 上の多項式 $f(x)=x^5-20x+5$ の最小分解体とすると、

$$\mathrm{Gal}(L/\mathbb{Q})\cong S_5$$

である。

$\because$ アイゼンシュタインの既約性判定法を、$p=5$ として適用すると $f(x)$ は既約である。よって、$\mathrm{Gal}(L/\mathbb{Q})$ の位数は 5 の倍数である。シローの定理から、$\mathrm{Gal}(L/\mathbb{Q})$ には位数が 5 の元が存在する。
　実数関数として増減を調べることにより、$f(x)$ には 3 つの相異なる実数根と 2 つの互いに共役な虚数根がある。$\mathbb{C}$ の複素共役は、$f(x)$ の根の間の置換を誘導するから、L の同型を定め、これは虚数根同士の互換になる。
　$\mathrm{Gal}(L/\mathbb{Q})$ は S_5 の部分群で、位数が 5 の巡回置換と互換をもつことがわかる。したがって、次の補題から $\mathrm{Gal}(L/\mathbb{Q})\cong S_5$ となる。 □

補題 184.

p を素数とする。p 次対称群は位数 p の巡回置換と互換で生成される。

$\because$ p は素数より、適当に位数 p の巡回置換のべきをとり、番号をつけ直して、$(123\cdots p)$ と (12) が与えられているとしてよい。

$$(123\cdots p)^i(12)(123\cdots p)^{-i}=(i+1,i+2)$$

となる。あみだくじの原理から、対称群は隣り合う互換で生成される。 □

12.2. **代数的に解けるとは.** 方程式が代数的に解ける (可解) という概念を導入する。

定義 185.

K を体、k を K の素体 ($\mathrm{char}(K)=0 \Rightarrow k=\mathbb{Q}$、$\mathrm{char}(K)=p>0 \Rightarrow k=\mathbb{F}_p$) とする。
(1) 有限次体拡大 L/K がべき根による拡大体とは、体の増加列

$$K=M_0 \subset M_1 \subset \cdots M_{r-1} \subset M_r = L$$
$$M_j = M_{j-1}(a_j^{\frac{1}{n_j}}) \quad (a_j \in M_{j-1})$$

が存在するものをいう。ここで、$a_j^{\frac{1}{n_j}}$ を添加する意味は、既約多項式 $x^{n_j}-a_j$ の根を一つ添加するという意味である。
(2) K 上の方程式 $x^n+c_1x^{n-1}+\cdots+c_n=0$ が代数的に解ける (可解) とは、ある $k(c_1,\cdots,c_n)$ 上のべき根による拡大 L が存在して、$k(c_1,\cdots,c_n)$ 上の多項式 $x^n+c_1x^{n-1}+\cdots+c_n$ の最小分解体が L に含まれることである。

定義から、次の補題が成り立つ。

補題 186.

M/K と L/M をべき根による拡大体とすると、L/K もべき根による拡大体である。

例 187.
(1) 標数が 2 でない体上の 2 次方程式 $x^2+ax+b=0$ は代数的に解ける。
(2) $\mathbb{Q}$ 上の方程式 $x^3=2$ は代数的に解ける。

$\because$ (1) $x^2+ax+b=(x+\frac{a}{2})^2-\frac{a^2-4b}{4}$ とかけるから、解は $x=\frac{-a\pm\sqrt{a^2-4b}}{2}$ となる。
(2) x^3-2 の最小分解体は $\mathbb{Q}(\sqrt{-3},2^{\frac{1}{3}})$ であり、この体は $\mathbb{Q}$ 上べき根による拡大である。 □

12.3. **クンマー理論.**

定理 188.

K は 1 の原始 n 乗根 ζ が属する体とし、L/K を n 次拡大とする。このとき以下は同値である。
(i) L/K は巡回拡大である。
(ii) $\exists a \in K,\ L=K(a^{\frac{1}{n}})$.

$\because$ (i) $\Rightarrow$ (ii) の証明 : σ を $\mathrm{Gal}(L/K)$ の生成元とする。問 18 から、ある $t \in L$ が存在して

$$\theta = t+\zeta\sigma(t)+\zeta^2\sigma^2(t)+\cdots+\zeta^{n-1}\sigma^{n-1}(t) \neq 0$$

となる。

$$\sigma(\theta)=\zeta^{-1}\theta$$

なので、θ の共役元はすべて異なる。

$$\theta^n = \pm\theta\sigma(\theta)\sigma^2(\theta)\cdots\sigma^{n-1}(\theta) \in K$$

より、$f(x)=x^n-\theta^n$ は K 上の既約多項式で、$L=K(\theta)$ である。
(ii) $\Rightarrow$ (i) は、$\sigma(a^{\frac{1}{n}})=\zeta^{\frac{1}{n}}$ となる $\mathrm{Gal}(L/K)$ の元 σ が生成元になる。 □

命題 189.

K を標数 0 の体、ζ_m を 1 の原始 m 乗根とする。$K_n=K(\zeta_1,\zeta_2,\zeta_3,\cdots\zeta_n)$ は K 上のべき根による拡大である。

∵ 補題 186 より、K_m/K_{m-1} がべき根による拡大であることを証明すればよい。制限による写像 $\mathrm{Gal}(K_m/K_{m-1}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ が単射なので (命題 129)、K_m/K_{m-1} はアーベル拡大で、その次数 h は m より小さく、$\zeta_h \in K_{m-1}$ である。アーベル群は巡回群の積なので、定理 188 が適用できる。 □

系 190.

$\mathbb{Q}$ 上の方程式 $x^n = 1$ は代数的に解ける。

12.4. **可解群.** 可解群を導入する。可解という名は、次章での方程式の可解性からきている。

定義 191.

有限群 G が可解群とは、交換子群の減少列が単位群で終わるもの、すなわち、

$$G = D_0 \supset D_1 \supset \cdots \supset D_r = \{e\}$$
$$D_j = [D_{j-1}, D_{j-1}]$$

となるものである。

命題 192.

G を有限群とする。次は同値である。

(i) G は可解群である。

(ii) G の部分群の減少列

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$$
$$G_j \text{ は } G_{j-1} \text{ の正規部分群で } G_{j-1}/G_j \text{ はアーベル群}$$

となるものが存在する。

(iii) G の部分群の減少列

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\}$$
$$G_j \text{ は } G_{j-1} \text{ の正規部分群で } G_{j-1}/G_j \text{ は巡回群}$$

となるものが存在する。

命題 193.

可解群の部分群と可解群の準同型による像は可解群である。

例 194.

(1) アーベル群は可解群である。

(2) 素数 p に対して、p 群は可解群である。(9.4 節の定理 B)

∵ 共役類の個数を考えると、自明でない p 群の中心は非自明ということがわかる。 □

(3) 3 次と 4 次の対称群 S_3, S_4 は可解群である。

∵ 剰余群がアーベル群となる減少列として

$$S_3 \supset A_3 \supset \{e\}$$
$$S_4 \supset A_4 \supset \{(12)(34), (13)(24), (14)(23), e\} \supset \{e\}$$

ただし、A_n は n 次交代群を表す。 □

定義 195.

有限群 G が単純群とは、G には自明な正規部分群 (G と $\{e\}$ のこと) しか存在しないものをいう。

命題 196.

非アーベルな単純群は、可解群でない。

定理 197.

(1) $[S_n, S_n] = A_n$.
(2) $n \geq 5$ ならば A_n は単純群である。

$\because$ 証明は省略する。群論の教科書を見よ。 □

系 198.

$n \geq 5$ ならば S_n と A_n は可解群でない。

12.5. **可解性の判定法.** ガロアによる方程式の可解性について解説する。

定理 199.

K の標数を 0 とし、L/K を有限次ガロア拡大とする。以下は同値である。
(i) L はべき根による K の拡大体に含まれる。
(ii) ガロア群 $\mathrm{Gal}(L/K)$ は可解群である。

$\because$ (i) $\Rightarrow$ (ii) の証明 : K 上のべき根による拡大

$$M = K(a_1^{\frac{1}{n_1}}, \cdots, a_r^{\frac{1}{n_r}}) \quad (\text{ただし } x^{n_j} - a_j \text{ は } K(a_1^{\frac{1}{n_1}}, \cdots, a_{j-1}^{\frac{1}{n_{j-1}}}) \text{ 上既約})$$

が L を含むとする。M の K 上のガロア閉包を $\overline{M}$ とするとき、M/K のガロア群が可解群であることを示せばよい。なぜなら、自然な全射準同型 $\mathrm{Gal}(\overline{M}/K) \to \mathrm{Gal}(L/K)$ があるからである。

$\overline{M}/K$ のガロア群が可解群であることを、r に関する帰納法で証明する。$r = 1$ のときには、$\overline{M} = K(\zeta_n, a^{\frac{1}{n}})$ とできる。ここで、ζ_n は 1 の原始 n 乗根を表す。このとき、$\overline{M}/K(\zeta_n)$ と $K(\zeta_n)/K$ はともにアーベル拡大になるので、$\mathrm{Gal}(\overline{M}/K)$ は可解群である。

$r > 1$ とする。$\overline{M}'$ を $K(a_1^{\frac{1}{n_1}}, \cdots, a_{r-1}^{\frac{1}{n_{r-1}}})$ のガロア閉包とする。$\overline{M}$ は $\overline{M}'$ を含み、$\overline{M'}(\zeta_{n_r}, a^{\frac{1}{n_r}})$ に含まれる。$r = 1$ のときと同じ論議で、$\mathrm{Gal}(\overline{M'}(\zeta_{n_r}, a^{\frac{1}{n_r}})/\overline{M}')$ は可解群であるから、$\mathrm{Gal}(\overline{M}/\overline{M}')$ も可解群になる。帰納法の仮定より、$\mathrm{Gal}(\overline{M}'/K)$ は可解群であるから、$\mathrm{Gal}(\overline{M}/K)$ は可解群である。

(ii) $\Rightarrow$ (i) の証明 : 命題 189 と補題 186 より、K には 1 の $[L : K]!$ 乗根が属するとしてよい。すると、可解群であるガロア群の各巡回群である部分商に対応する拡大に定理 188 が適用でき、L/K はべき根による拡大になる。 □

系 200.

標数 0 の体上の方程式
$$x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n = 0$$
が代数的に解ける必要十分条件は、$\mathbb{Q}(c_1, \cdots, c_n)$ 上の $x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n$ の最小分解体 L に対して、ガロア群 $\mathrm{Gal}(L/\mathbb{Q}(c_1, \cdots, c_n))$ が可解群となることである。

定理 201.

(1) $n \leq 4$ とする。複素数係数の n 次方程式 $x^n + c_1x^{n-1} + \cdots + c_n = 0$ は代数的には解ける。
(2) $n \geq 5$ とする。複素数係数の n 次方程式 $x^n + c_1x^{n-1} + \cdots + c_n = 0$ は一般には代数的には解けない。

$\because$ 命題 177 から、方程式の最小分解体の $\mathbb{Q}(c_1, \cdots, c_n)$ 上のガロア群は S_n の部分群になる。
(1) 4 次以下のときは、可解群 S_4 の部分群になるから、ガロア群は可解群である。
(2) 方程式 $x^n + c_1x^{n-1} + \cdots + c_n = 0$ の係数の体　$\mathbb{Q}(c_1, \cdots, c_n)$ が n 変数多項式環の商体と同型ならば、例 142 より最小分解体の $\mathbb{Q}(c_1, \cdots, c_n)$ 上のガロア群は n 次対称群 S_n になる。$\mathbb{C}$ は連続濃度をもつので、そういう $c_1, \cdots, c_n$ は存在する。 □

例 202.

方程式 $x^3 - 3x + 1 = 0$ を代数的に解いてみる。

複素数体 $\mathbb{C}$ の中で方程式 $x^3 - 3x + 1 = 0$ は 3 つの異なる実数解を持つので、それらを $\alpha, \beta, \gamma\ (\alpha < \beta < \gamma)$ とする。例 182 (2) から $\mathbb{Q}(\alpha)/\mathbb{Q}$ はガロア拡大でそのガロア群は $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ となる。$\zeta = \frac{-1+\sqrt{3}i}{2}$ を 1 の原始 3 乗根とする。拡大次数を考えると、$[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 6$ となり、多項式 $x^3 - 3x + 1$ は $\mathbb{Q}(\zeta)$ 上も既約で、$\mathrm{Gal}(\mathbb{Q}(\alpha, \zeta)/\mathbb{Q}(\zeta)) \cong \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ となる。
σ をガロア群の生成元で、$\sigma(\alpha) = \beta$ となるようにとる。判別式 $D = 81$ なので、共役差積
$$\Delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) = -9$$
である。定理 188 の証明をまねて、
$$\theta = \alpha + \zeta\beta + \zeta^2\gamma$$
とおく。$[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 6$ なので、
$$\theta = \alpha - \gamma + \zeta(\beta - \gamma) \neq 0$$
となる。θ は実部と虚部ともに負である。解と係数の関係を用いて、
$$\begin{aligned} \theta^3 &= \alpha^3 + \beta^3 + \gamma^3 + 3\zeta(\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha) + 3\zeta(\alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2) + 6\alpha\beta\gamma \\ &= -9 + 3\zeta\tfrac{\Delta+3}{2} - 3\zeta^2\tfrac{\Delta-3}{2} \\ &= -\tfrac{27+27\sqrt{3}i}{2} \in \mathbb{Q}(\zeta) \end{aligned}$$
となり、
$$\theta = 3\left(\frac{-1-\sqrt{3}i}{2}\right)^{\frac{1}{3}} \quad (\text{偏角は } \pi \text{ から } \tfrac{3\pi}{2} \text{ の間})$$
となる。
α を $\mathbb{Q}(\sqrt{-3})$ 上で θ を用いて表そう。
$$\alpha = l + m\theta + n\theta^2$$
とする。$\theta = \alpha + \zeta\beta + \zeta^2\gamma$ に代入して、$m = \frac{1}{3}$ を得る。$\alpha^2 + \alpha\beta + \beta^2 = -\alpha\beta + (\alpha + \beta)^2 = -\alpha\beta - \beta\gamma - \gamma\alpha = 3$ に代入して、$l = 0, n = \frac{3}{\theta^3}$ を得る。したがって、
$$\alpha = \frac{1}{3}\theta + \frac{-1+\sqrt{3}i}{18}\theta^2 \in \mathbb{Q}(\sqrt{3}i, \theta) = \mathbb{Q}(\theta)$$
と表される。 □

$n \geq 5$ ならば、有理数係数の n 次方程式でも代数的に解けないものが存在する。例えば、例 183 の $x^5 - 20x + 5 = 0$ はその最小分解体のガロア群が S_5 になるから代数的に解けない。最小分解体のガロア群が $S_n\,(n \geq 5)$ となるような有理数係数の方程式を作るには、還元による方法を用いて、有限体上のガロア理論を利用するなど、何かもう一つ必要である。

問 31.
$\mathbb{Q}$ 上 3 次の既約多項式が虚数根を持てば、その最小分解体のガロア群は S_3 と同型である。

問 32.
$f(x) = x^4 + ax^2 + bx + c \in \mathbb{K}[x]$ を 4 次既約多項式とし、D_f と Δ_f をそれぞれ $f(x)$ の判別式と共役差積とする。また、G を $f(x)$ の最小分解体 L の K 上のガロア群 $\mathrm{Gal}(L/K)$ とする。
(1) S_4 の部分群の共役類をすべて求めよ。また、そのうち G がなりうるものをはどれか。
(2) 判別式 D_f を求めよ。
(3) $D_f \in (K^\times)^2$ とする。G がなりうる S_4 の部分群の共役類はどれか。
(4) $D_f \notin (K^\times)^2$ とする。G がなりうる S_4 の部分群の共役類はどれか。
(5) $b = 0$ とする。G がなりうる S_4 の部分群の共役類はどれか。
(6) $b \neq 0$ とする。$f(x) = (x^2 - ux + s)(x^2 + ux + t)$ と K の代数閉包上で分解したときの　$s + t$ が満たす K 上の方程式を求めよ。また、G が S_3 または A_3 になる条件を求めよ。

問 33.
$f(x) = x^4 - 4x + 2 \in \mathbb{Q}[x]$ とするとき、$f(x)$ の最小分解体の $\mathbb{Q}$ 上のガロア群を求めよ。

問 34.
$\mathbb{Q}$ 上の 4 次の多項式で、その最小分解体の $\mathbb{Q}$ 上のガロア群が A_4 になるものを作れ。

問 35.
$\mathbb{Q}$ 上の方程式 $x^3 - 3x + 3 = 0$ を代数的に解け。