Galois 理論とその応用 [1]

市川 尚志 [2]

Galois(1811–1832) の遺言

決闘の前夜、ガロアは友人シュヴァリエに与える遺書を草した。その書に言う：

『予は解析に於て二三の新しい物を成就した。その或るものは方程式論に、又他のものは積分に関する。… 公開状を以ってヤコービ又はガウスの意見、予の定理の正否に関してでなく、それの重大性に関しての意見を求めて欲しい。予はこのごたごた (gâchis) を判読して自得するものが後に来ることを期待している』(Galois, 1832 年 5 月 29 日)

ガロアの方程式論は彼が期待したように四十年後にジョルダン (Camille Jordan) が「判読」して、厖然たる置換論 (Traité des substitutions, 1870) の述作を成した。(高木貞治「近世数学史談より)

目次

参考文献

[K] 木村 俊一, 数学のかんどころ 14 ガロア理論, 共立出版 (2012).

[T] 高木 貞治, 近世数学史談, 岩波文庫 (1995).

[vdW] B. L. van der Waerden, Algebra, Springer (2003).

[1] http://ichikawa.ms.saga-u.ac.jp/ からダウンロードできます

[2] 佐賀大学工学系研究科数理科学専攻 e-mail: ichikawn@cc.saga-u.ac.jp

§1. 体の拡大

1.1. 有理整数環.

群の定義. 空でない集合 G の元 a, b に対し、その積 $a \cdot b = ab$ が定義されて次の条件を満たすとき、G を**群**という。

(G0) G の任意の元 a, b に対し、$ab \in G$ が成り立つ。

(G1) G の任意の元 a, b, c に対し、結合律 $(ab)c = a(bc)$ が成り立つ。

(G2) G の任意の元 a に対し $ae = ea = a$ を満たす G の元 e が (ただ 1 つ) 存在する。(e を G の**単位元**という)

(G3) a を G の元とするとき、$ab = ba = e$ を満たす G の元 b が (ただ 1 つ) 存在する。(b を a の**逆元**といい、a^{-1} と書く)

さらに G の任意の元 a, b に対し交換律 $ab = ba$ が成り立つとき、G を **Abel 群**または**可換群**という。

環の定義. 空でない集合 R の元 a, b に対し、その和 $a + b$ と積 $a \cdot b = ab$ が定義されて次の条件を満たすとき、R を（乗法の単位元 1 を持つ可換）**環**という。

(R0) R の任意の元 a, b に対し、$a + b, ab \in R$ が成り立つ。

(R1) R は加法について可換群になる、すなわち R の任意の元 a, b に対し $a - b \in R$ が成り立つ（加法の単位元を 0 と書く）。

(R2) R は、任意の $a \in R$ に対し $a1 = 1a = a$ を満たす乗法の単位元 1 を含む。

(R3) 加法と乗法について、数の場合と同じ法則（交換律、結合律、分配律）が成り立つ。

注意. R の任意の元 a に対し、$a \cdot 0 = 0$ が成り立つ。

体の定義. 環 K の 0 でない元の集合 $K^\times = K - \{0\}$ が乗法について群になるとき、K を**体**という。（体 K の元 $a \neq 0$ の乗法についての逆元を a^{-1} と書く）

注意.

- 体 K の元 a, b に対し、$a \neq 0$ ならば $ax = b$ を満たす $x \in K$ はただ 1 つ存在し、$x = a^{-1}b = ba^{-1}$ で与えられる。すなわち体においては割り算ができる。
- 体は**整域**になる。すなわち K が体ならば

$$a, b \in K,\ ab = 0 \ \Rightarrow\ a = 0 \text{ または } b = 0.$$

環と体の例. 数の加法と乗法について

$$\begin{array}{ccccccc} \mathbb{Z} & \subset & \mathbb{Q} & \subset & \mathbb{R} & \subset & \mathbb{C} \\ \text{有理整数環 (整域)} & & \text{有理数体} & & \text{実数体} & & \text{複素数体} \end{array}$$

イデアルの定義. 環 R の空でない部分集合 I が次の条件

$$\begin{cases} I \text{ は加法について } R \text{ の部分群、すなわち任意の } a, b \in I \text{ に対し } a - b \in I, \\ \text{任意の } a \in I,\ r \in R \text{ に対し } ra \in I \end{cases}$$

を満たすとき、I を R の**イデアル**という。

例. 環 R の元 $a_1, ..., a_n$ に対し、

$$\{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R\}$$

は R のイデアルになる。これを $a_1, ..., a_n$ で生成されたイデアルといい、$(a_1, ..., a_n)$ と書く。特に 1 つの元 a から生成されたイデアル (a) を**単項イデアル**という

問題. 環 R の元 $a_1, ..., a_n$ に対し、$(a_1, ..., a_n)$ は R のイデアルになることを示せ。

定理 1.1.1. $\mathbb{Z}$ は単項イデアル環である。すなわち $\mathbb{Z}$ の任意のイデアルは単項イデアルになる。

応用.

(1) 自然数 a, b の最大公約数を d とするとき、$ma + nb = d$ を満たす整数 m, n が存在する。（実際は互除法で求める）

(2) 素数 p が 2 つの整数 a, b の積を割り切るとき、p は a または b を割り切る。

(3) 任意の自然数は、素数の積に（積の順序を除いて）ただ一通りに分解される。（素因数分解の一意性）

注意.

- 素数の定義と定理 1.1.1 より、p が素数ならば、(p) を含む $\mathbb{Z}$ のイデアルは (p) と $\mathbb{Z}$ に限る。
- 応用の (2) より、p が素数ならば

$$a, b \in \mathbb{Z},\ ab \in (p) \ \Rightarrow\ a \in (p) \text{ または } b \in (p).$$

問題. 素因数分解の一意性を用いて、自然数 a の正の平方根 $\sqrt{a}$ が有理数ならば、$\sqrt{a}$ は自然数になることを示せ。

極大イデアルと素イデアルの定義. 環 R のイデアル I に対し、

- I が R の**極大イデアル**であるとは、I を含む R のイデアルは I と R に限ることである。
- I が R の**素イデアル**であるとは、

$$a, b \in R,\ ab \in I \ \Rightarrow\ a \in I \text{ または } b \in I$$

が成り立つことである。

定理 1.1.2. 素数 p に対し、(p) は $\mathbb{Z}$ は極大イデアルかつ素イデアルになる。

問題. 1 より大きい自然数 n に対し、次の (1)〜(3) が同値になることを示せ：

(1) n は素数。

(2) (n) は $\mathbb{Z}$ の素イデアル。

(3) (n) は $\mathbb{Z}$ の極大イデアル。

問題. 次の問いに答えよ。

(1) $\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} \,\middle|\, a, b \in \mathbb{Z}\right\}$ は、複素数の加法と乗法によって環になることを示せ。

(2) $\mathbb{Z}\left[\sqrt{-5}\right]$ の元 $\alpha = a + b\sqrt{-5}$ $(a, b \in \mathbb{Z})$ のノルム $N(\alpha)$ を $N(\alpha) = a^2 + 5b^2$ で定義するとき、$N(\alpha)$ は 0 以上の整数で、

$$N(\alpha\beta) = N(\alpha)N(\beta)\ \left(\alpha, \beta \in \mathbb{Z}\left[\sqrt{-5}\right]\right)$$

が成り立つことを示せ。

(3) (2) を用いて、$\mathbb{Z}\left[\sqrt{-5}\right]$ のイデアル $\left(2, 1 + \sqrt{-5}\right)$ は単項イデアルにならない（従って $\mathbb{Z}\left[\sqrt{-5}\right]$ は単項イデアル環にならない）ことを示せ。

問題. p を素数とするとき、次の問いに答えよ。なお (3) を **Fermat の小定理**という。

(1) 素数の性質を用いて、$i = 1, 2, ..., p-1$ に対し、2 項係数 $\begin{pmatrix} p \\ i \end{pmatrix}$ は p で割り切れることを示せ。

(2) (1) と帰納法を用いて、任意の自然数 a に対し $a^p - a$ は p で割り切れることを示せ。

(3) (2) を用いて、任意の整数 a に対し $a^p - a$ は p で割り切れることを示せ。また a が p で割り切れないとき、$a^{p-1} - 1$ は p で割り切れることを示せ。

1.2. 整数の合同と剰余環.

余りの計算. 2^{100} を 7 と 9 で割った余りをそれぞれ求めよ $\Rightarrow$ 合同式を使うと簡単にできる

合同の定義. 自然数 n と整数 a, b に対し、

$$a, b \text{ を } n \text{ で割った余りが等しい } \Leftrightarrow \ a-b \text{ が } n \text{ で割り切れる } \Leftrightarrow \ a-b \in (n)$$

が成り立つとき、a と b は n を法として**合同**であるといい、$a \equiv b \bmod(n)$ と書く。

合同式の性質. 同じ法の下では等式のように計算してよい。すなわち

$$(*)\begin{cases} a \equiv b \bmod(n),\ c \equiv d \bmod(n) \\ \Rightarrow\ a \pm c \equiv b \pm d \bmod(n) : \text{複号同順 (以下同じ)},\ ac \equiv bd \bmod(n). \end{cases}$$

これを用いると

- $2^3 = 8 \equiv 1 \bmod(7)\ \Rightarrow\ 2^{100} = (2^3)^{33} \cdot 2 \equiv 1^{33} \cdot 2 = \underline{2} \bmod(7).$
- $2^3 = 8 \equiv -1 \bmod(9)\ \Rightarrow\ 2^{100} = (2^3)^{33} \cdot 2 \equiv (-1)^{33} \cdot 2 = -2 \equiv \underline{7} \bmod(9).$

$(*)$ の証明. (n) が $\mathbb{Z}$ のイデアルになることを用いる。仮定より $a-b, c-d \in (n)$ だから

$$\begin{cases} (a \pm c) - (b \pm d) = (a-b) \pm (c-d) \in (n), \\ ac - bd = ac - bc + bc - bd = (a-b)c + b(c-d) \in (n). \ \square \end{cases}$$

問題. 必要な場合は Fermat の小定理を用いて、3^{100} を $7, 8, 11, 13, 15$ で割った余りをそれぞれ求めよ。また 5^{100} を $3, 6, 7, 11, 15$ で割った余りをそれぞれ求めよ。

剰余環の定義.

(1) $\mathbb{Z}/(n)$ は、整数を n で割った余りの集合 $\{0, 1, ..., n-1\}$ の元 a, b に対し、

$$a+b,\ ab \text{ を } n \text{ で割った余り}$$

によって、それぞれ加法、乗法を定めて得られる環を表す。

(2) 一般の環 R とそのイデアル I に対し、I による R の**剰余環** R/I とは、剰余類の集合

$$\{\overline{a} = a + I \mid a \in R\};\ \text{ただし } a+I = b+I \ \Leftrightarrow\ a-b \in I$$

に、

$$\begin{cases} (a+I)+(b+I) &= (a+b)+I, \\ (a+I)\cdot(b+I) &= ab+I \end{cases}$$

によって、それぞれ加法と乗法を定めて得られる環のこと。$R = \mathbb{Z}$, $I = (n)$ とすると、剰余環 $\mathbb{Z}/(n)$ の各元 $\overline{a} = a + (n)$ に a を n で割った余りを対応させることにより、(1) の定義と一致することが分る。

(∗) の意味. $\mathbb{Z}/(n)$ において

$$\overline{a}=\overline{b},\ \overline{c}=\overline{d}\ \Rightarrow\ \overline{a\pm c}=\overline{b\pm d},\ \overline{ac}=\overline{bd}.$$

これは剰余環 $\mathbb{Z}/(n)$ の和、差、積の定義：

$$\overline{a}\pm\overline{c}=\overline{a\pm c},\ \overline{a}\cdot\overline{c}=\overline{ac}$$

において、右辺が剰余類の代表元 a,c のとり方によらず定まる（これを **well-defined** であるという）ことを示している。

問題. 一般の環 R とそのイデアル I に対し、剰余環 R/I の加法と乗法が well-defined になることを示せ。また

$$I\text{ が素イデアル }\Leftrightarrow\ R/I\text{ が整域、 }I\text{ が極大イデアル }\Leftrightarrow\ R/I\text{ が体}$$

が成り立つこと、従って I が極大イデアルならば素イデアルになることを示せ。

暗号への応用. 情報を安全に伝えるために必要

- 古典暗号 (特定の人間に使用を限定) : 暗号を作る ⇔ 鍵を持っている ⇔ 暗号が解ける
- 現代暗号 (不特定多数の人間が使用、例：インターネット)

  公開鍵 (⇒ 暗号が作れる) ≠ 秘密鍵 (⇒ 暗号が解ける)

  ⇒ コンピューターと代数学を用いて実現

RSA 暗号. (1977 年) 現代暗号の代表例

- $\begin{cases} p,q : \text{相異なる大きな素数 (実用上は数百桁以上)}, \\ e,d : ed-1 \text{ が } (p-1)(q-1) \text{ で割り切れる自然数} \end{cases}$ を用意する。
- 公開鍵を $n=pq$ と e、秘密鍵を d とする。
- メッセージ (平文) を n 未満の自然数 (同義数)A に置き換え、

$$A \overset{\text{暗号化}}{\longmapsto} B=A^e\text{を } n \text{ で割った余り (暗号)} \overset{\text{解読}}{\longmapsto} B^d\text{を } n \text{ で割った余り } \overset{(\sharp)}{=} A.$$

$(\sharp)\ \Leftarrow$ Fermat の小定理：素数 p で割り切れない整数 a に対し $a^{p-1}\equiv 1 \bmod(p)$.

RSA 暗号の安全性.

RSA 暗号を解くには、n と e から d を求めることが必要

⇒ d の性質より $(p-1)(q-1)$ を知る、すなわち n の素因数 p,q を知ることが必要.

しかし、大きい自然数の素因数分解は非常に難しい（と信じられている）。

P ≠ NP 問題 (賞金 100 万ドル). 自然数 n の素因数分解は、$\log(n)$ の多項式に比例する時間で行うことができないことを証明せよ。

素数判定.

- https://ja.wikipedia.org/wiki/巨大な素数の一覧（1952 年以降は電子計算機で検証）

発表年	1876	1951	1952	$\cdots$	2016	2017
素数	$2^{127}-1$	$(2^{148}+1)/17$	$2^{521}-1$	$\cdots$	$2^{74207281}-1$	$2^{77232917}-1$
桁数	39	44	157	$\cdots$	約 2234 万	約 2325 万

- 2^m-1 が素数ならば m も素数になる（逆は正しくない：$2^{11}-1=2047=23\times 89$）。よって素数 p に対し、2^p-1 が素数になることが分れば大きな素数が得られる（2^p-1 と表される素数を Mersenne 型という）。

- 大きな自然数（奇数）n が素数かどうか判定する方法：

  (1) $\sqrt{n}$ 以下の自然数で割り切れるかどうかを調べる … 非実用的
  $\Rightarrow \sqrt{n}$ に比例して時間がかかり、すべての場合をチェックする必要がある。

  (2) Fermat の小定理を用いた**確率的**判定法 … n と互いに素な自然数 a に対し

  $$(*) \qquad a^{n-1}\equiv 1 \bmod(n)$$

  が成り立つかどうかを調べる。

  注. Fermat の小定理より、n が素数ならば $(*)$ は常に成り立つので、$(*)$ が成り立たない a が 1 つでもあれば、n は素数でない。また $(*)$ が成り立たない a があれば、そのような a は全体の半分以上存在する。よって r 個のランダムに選んだ a について $(*)$ が成り立てば、$1-(1/2)^r$ 以上の確率で n が素数であると言える（ただしこのテストを常にパスする合成数（擬素数）が存在する）。

  (3) Solovay-Strassen の**確率的**判定法 (1977) … (2) より強力
  n と互いに素な自然数 a に対し、

  $$a^{\frac{n-1}{2}}\equiv \left(\frac{a}{n}\right) \bmod(n);\ \left(\frac{a}{n}\right) : \text{平方数と合同であるかどうかを表す Jacobi 記号}$$

  が成り立つかどうかを調べる（このテストでは擬素数は存在しない）。

  (4) AKS(Agrawal, Kayal, Saxena) 判定法 (2004) … 素数判定の理論的完成
  整数係数の多項式についての合同式

  $$(X+a)^n\equiv X^n+a \bmod(n)$$

  が成り立つかどうかを、n の桁数の多項式に比例する時間（**多項式時間**）で調べることにより、n が素数かどうかを**決定的に**判定できる。

1.3. 体上の多項式環.

多項式環の定義. 環 R 上の（1 変数）**多項式環**とは、R 上の多項式

$$\sum_{i=0}^{n} a_i X^i = a_n X^n + \cdots + a_1 X + a_0 \quad (a_i \in R)$$

の集合 $R[X]$ に、

$$\begin{cases} \left(\sum_{i\geq 0} a_i X^i\right) + \left(\sum_{i\geq 0} b_i X^i\right) &= \sum_{i\geq 0}(a_i + b_i)X^i, \\ \left(\sum_{i\geq 0} a_i X^i\right) \cdot \left(\sum_{i\geq 0} b_i X^i\right) &= \sum_{i\geq 0}(a_i b_0 + a_{i-1} b_1 + \cdots + a_0 b_i)X^i \end{cases}$$

によって、それぞれ和と積を定めて得られる環のこと。なお $R[X]$ の元 $f(X) = \sum_{i=0}^{n} a_i X^i$ に対し、

- $a_n \neq 0$ のとき、n を $f(X)$ の**次数**といい $\deg(f)$ と書く。
- さらに $a_n = 1$ のとき、$f(X)$ は**モニック**であるという。

注意. R が整域ならば、$R[X]$ も整域になる。特に体上の多項式環は整域になる。

定理 1.3.1 (多項式の剰余定理). 体 K 上の多項式 $f(X), g(X)$ に対し、$g(X) \neq 0$ ならば

$$f(X) = q(X)g(X) + r(X);\ \text{ただし } r(X) = 0 \text{ または } \deg(r) < \deg(g)$$

を満たす K 上の多項式 $q(X), r(X)$ がただ 1 つずつ存在する。($r(X) = 0$ のとき、$g(X)$ は $f(X)$ を割り切る、または $f(X)$ は $g(X)$ で割り切れるという)

定理 1.3.2. 体上の多項式環は単項イデアル環になる。

定理 1.3.3. 体 K 上の 0 でない多項式 $f(X)$, $g(X)$ に対し、$f(X)$, $g(X)$ を割り切る K 上のモニック多項式の中で、次数が最大になるもの（の 1 つ）を $d(X)$ とするとき、

$$(f(X), g(X)) = (d(X))$$

が成り立つ。($d(X)$ を $f(X)$, $g(X)$ の**最大公約元**という)

既約多項式の定義. 体 K 上の次数 1 以上の多項式 $f(X)$ に対し、

- $f(X)$ が K 上**可約**であるとは、

  $$f(X) = g(X)h(X),\ 0 < \deg(g), \deg(h) < \deg(f)$$

  を満たす K 上の多項式 $g(X)$, $h(X)$ が存在すること。
- $f(X)$ が K 上**既約**であるとは、$f(X)$ が K 上可約にならないこと。

注意.

- 多項式の既約性は、考えている体によって変わる。例えば代数学の基本定理 (Gauss) より、$\mathbb{C}$ 上の既約多項式は 1 次式のみになる。
- $\deg(f) = 2, 3$ のとき

$$f(X) \text{ が } K \text{ 上可約} \ \Leftrightarrow \ f(X) = 0 \text{ が } K \text{ 上の解を持つ。}$$

定理 1.3.4 (既約多項式分解の一意性). 体 K 上のモニック多項式は、K 上のモニック既約多項式の積に（積の順序を除いて）一意的に分解される。

問題. $X^4 - X^2 - 2$, $X^4 + 1$, $X^6 + 1$, $X^5 - 1$ を、それぞれ $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 上で既約多項式の積に分解せよ。

問題. 体 K 上の正次数の多項式 $f(X)$ に対し、次の (1)〜(3) が同値になることを示せ：

(1) $f(X)$ は K 上既約。

(2) $(f(X))$ は $K[X]$ の素イデアル。

(3) $(f(X))$ は $K[X]$ の極大イデアル。

1.4. 拡大体の構成.

部分体、拡大体の定義. 体 L の部分集合 K が L の加法と乗法について体になるとき、すなわち K のなかで加減乗除ができるとき、

$$\begin{cases} K \text{ を } L \text{ の部分体}, \\ L \text{ を } K \text{ の拡大体} \end{cases} \text{といい、} \begin{matrix} L \\ | \\ K \end{matrix} \text{と書く。}$$

剰余環の定義. 体 K 上の多項式 $f(X)$ が正の次数 $n = \deg(f)$ を持つとき、$K[X]/(f(X))$ は K 上の $(n-1)$ 次以下の多項式の集合

$$\{a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \mid a_i \in K\}$$

に、

$$g(X) + h(X),\ g(X)h(X) \text{ を } f(X) \text{ で割った余り}$$

によって、それぞれ加法、乗法を定めて得られる環を表す。

$R = K[X],\ I = (f(X))$ とすると、剰余環 R/I の各元 $g(X) + I$ に $g(X)$ を $f(X)$ で割った余りを対応させることにより、

$$R/I \cong K[X]/(f(X)) \ :\ \text{環として同型.}$$

定理 1.4.1. $f(X)$ が体 K 上の既約多項式ならば、$L = K[X]/(f(X))$ は K 上の拡大体で、$n = \deg(f)$ とすると、L は

$$X^{n-1}, ..., X, 1$$

を基底とする K 上の n 次元線形空間になる。

証明. 定理 1.3.2 より $K[X]$ は単項イデアル環だから、$f(X)$ が K 上既約であることより $(f(X))$ は $K[X]$ の極大イデアルとなり、L は体になる。K の各元 a に $a + (f(X))$ を対応させる写像は K から L への単射準同型写像になるから、L は K の拡大体で、上記に述べたことより L は K の n 次元線形空間になる。 □

拡大次数の定義. 体 K の拡大体 L が K 上の n 次元線形空間になるとき、L を K の n 次拡大体という。また

$$\dim_K L = n$$

を L/K の**拡大次数**といい、$[L : K]$ と書く。

環の準同型定理. $\varphi : R \to R'$ を環の準同型写像、すなわち環 R, R' の和と積について

$$\varphi(a + b) = \varphi(a) + \varphi(b),\ \varphi(ab) = \varphi(a)\varphi(b)\ (a, b \in R)$$

を満たし、かつ R の乗法の単位元を R' の乗法の単位元に写す写像とする。このとき

(1) φ の核 (kernel)

$$\mathrm{Ker}(\varphi) = \{a \in R \mid \varphi(a) = 0_{R'} :\ R' \text{ の加法の単位元 }\}$$

は R のイデアル。

(2) φ の像 (image)

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in R\}$$

は R' の部分環。

(3) 剰余環 $R/\mathrm{Ker}(\varphi)$ の各元 $a + \mathrm{Ker}(\varphi)$ に $\varphi(a)$ を対応させる写像は、環の同型写像

$$R/\mathrm{Ker}(\varphi) \xrightarrow{\sim} \mathrm{Im}(\varphi)$$

を導く。

定理 1.4.2. L を体 K の拡大体とするとき、K 上の既約多項式 $f(X)$ に対し、$f(\alpha) = 0$ を満たす L の元 α が存在すると仮定する。このとき

$$K[\alpha] = \{g(\alpha) \mid g(X) \in K[X]\} :\ L \text{ の部分環}$$

とすると

(1) $K[\alpha] \cong K[X]/(f(X))$: 環として同型。

(2) $n = \deg(f)$ とすると、$K[\alpha]$ は K の n 次拡大体。

注意.

- $K[\alpha]$ は K と α を含む最少の体になるので、K と α **で生成された体**

$$K(\alpha) = \left\{ \frac{g(\alpha)}{h(\alpha)} \;\middle|\; g(X), h(X) \in K[X],\ h(\alpha) \neq 0 \right\}$$

に等しい。特に $K[\alpha]$ の中で割り算ができることになる。

- 下記の証明から分かるように、$f(X)$ は $f(\alpha) = 0$ を満たす次数が最少の K 上の多項式になる。従って $f(X)$ は α の K 上の**最少多項式**と呼ばれる。

証明. $K[X]$ の各元 $g(X)$ に $g(\alpha)$ を対応させる写像 φ は、$K[X]$ から $K[\alpha]$ への全射準同型写像を与える。このとき $\mathrm{Ker}(\varphi) = (f(X))$ を示す。

まず任意の $(f(X))$ の元は、$K[X]$ の元 $g(X)$ を用いて $g(X)f(X)$ と表されるから、

$$\varphi\left(g(X)f(X)\right) = g(\alpha)f(\alpha) = g(\alpha)0 = 0.$$

従って $g(X)f(X) \in \mathrm{Ker}(\varphi)$ となるから、$(f(X)) \subset \mathrm{Ker}(\varphi)$ が示された。

次に $\mathrm{Ker}(\varphi) \subset (f(X))$ でないと仮定して矛盾を導く。仮定より $(f(X))$ に含まれない $\mathrm{Ker}(\varphi)$ の元 $h(X)$ が存在し、このとき定理 1.4.1 より $h(X) + (f(X))$ は $K[X]/(f(X))$ において乗法の逆元を持つから、

$$a(X)h(X) + b(X)f(X) = 1$$

を満たす $a(X), b(X) \in K[X]$ が存在する。ここで $X = \alpha$ を代入すると $0 = 1$ となり矛盾が生ずるから、$\mathrm{Ker}(\varphi) \subset (f(X))$ が成り立つ。

以上より $\mathrm{Ker}(\varphi) = (f(X))$ となるから、環の準同型定理より φ は環の同型写像

$$K[X]/(f(X)) \xrightarrow{\sim} K[\alpha]$$

を導く。従って (1) が成り立ち、定理 1.4.1 より (2) も成り立つ。 □

問題. $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2} - 1$ に対し、

$$\frac{1}{\alpha_i^2 + 2\alpha_i + 2} = a_i\alpha_i^2 + b_i\alpha_i + c_i \quad (i = 1, 2)$$

を満たす $a_i, b_i, c_i \in \mathbb{Q}$ を求めよ。

問題. a, b, c, d を有理数とするとき、$\alpha^2 + a\alpha + b = 0$, $\beta^2 + c\beta + d = 0$ を満たす複素数 α, β に対し、$\alpha\beta$ を解に持つ有理数体上の 4 次方程式を次のようにして求めよ。

(1) $\boldsymbol{a} = \begin{pmatrix} 1 \\ \alpha \\ \beta \\ \alpha\beta \end{pmatrix}$ とするとき、$(\alpha\beta)\boldsymbol{a} = A\boldsymbol{a}$ を満たし、有理数を成分に持つ 4 次の正方行列 A を求めよ。

(2) E を 4 次の単位行列とし、$f(X)$ を $XE - A$ の行列式（A の特性多項式）とする。このとき $f(X)$ を求め、$f(X) \in \mathbb{Q}[X]$ および $f(\alpha\beta) = 0$ を示せ。

問題. 有理数を係数とする代数方程式の解となる複素数を**代数的数**と呼ぶ。上記の問題を参考にして、代数的数の集合が複素数の加法と乗法について体になることを示せ。

数の体の（奥深い）系列.

$$\mathbb{Q} \subsetneqq \{\text{作図可能な数}\} \subsetneqq \{\text{4 則と巾乗根で表される数}\} \subsetneqq \{\text{代数的数}\} \subsetneqq \{\text{periods}\} \subsetneqq \mathbb{C}.$$

1.5. 多項式の既約性.

$\mathbb{Q}$ 上の多項式の既約性を考える。

原始的多項式の定義. $\mathbb{Z}$ 上の 0 でない多項式

$$f(X) = a_n X^n + \cdots + a_1 X + a_0$$

の係数 $a_n, ..., a_1, a_0 \in \mathbb{Z}$ が互いに素、すなわちこれらの最大公約数が 1 に等しいとき、$f(X)$ は**原始的**であるという。

定理 1.5.1 (Gauss の補題). $\mathbb{Z}$ 上の原始多項式 $f(X)$, $g(X)$ に対し、その積 $f(X)g(X)$ は原始的になる。

証明.

$$f(X) = a_n X^n + \cdots + a_1 X + a_0, \quad g(X) = b_m X^m + \cdots + b_1 X + b_0$$

とすると、仮定より任意の素数 p に対し

$$a_n, ..., a_1, a_0 \text{ のいずれか及び } b_m, ..., b_1, b_0 \text{ のいずれか}$$

は p で割り切れない。よって

$$\begin{cases} s &= \min\{\ 0 \le i \le n \ \mid a_i \text{ は } p \text{ で割り切れない } \}, \\ t &= \min\{\ 0 \le j \le m \mid b_j \text{ は } p \text{ で割り切れない } \} \end{cases}$$

とすると

$$\begin{cases} a_0, ..., a_{s-1} \text{ は } p \text{ で割り切れ、} a_s \text{ は } p \text{ で割り切れない}, \\ b_0, ..., b_{t-1} \text{ は } p \text{ で割り切れ、} b_t \text{ は } p \text{ で割り切れない}. \end{cases}$$

従って $f(X)g(X)$ の X^{s+t} の係数

$$\underbrace{a_0 b_{s+t} + \cdots + a_{s-1} b_{t+1}}_{p \text{ の倍数}} + \underbrace{a_s b_t}_{p \text{ の倍数でない}} + \underbrace{a_{s+1} b_{t-1} + \cdots + a_{s+t} b_0}_{p \text{ の倍数}}$$

は p で割り切れないから、$f(X)g(X)$ は原始的になる。 □

系. $\mathbb{Z}$ 上の 0 でない多項式 $f(X)$ が $\mathbb{Q}$ 上可約ならば、$\mathbb{Z}$ 上可約、すなわち

$$f(X) = g(X)h(X), \text{ ただし } 0 < \deg(g), \deg(h) < \deg(f)$$

を満たす $g(X), h(X) \in \mathbb{Z}[X]$ が存在する。言い換えると、$\mathbb{Z}$ 上既約な多項式は $\mathbb{Q}$ 上既約になる。

証明. 仮定より

$$f(X) = G(X)H(X), \text{ ただし } 0 < \deg(G), \deg(H) < \deg(f)$$

を満たす $G(X), H(X) \in \mathbb{Q}[X]$ が存在する。従って

$$G(X) = a \cdot g(X), \quad H(X) = b \cdot h(X)$$

を満たす正の有理数 a, b と $\mathbb{Z}$ 上の原始多項式 $g(X), h(X)$ が存在する。このとき $f(X) = (ab)g(X)h(X)$ となり、Gauss の補題より $g(X)h(X)$ は $\mathbb{Z}$ 上の原始多項式なので、$f(X) \in \mathbb{Z}[X]$ の係数の最大公約数を d とすると、自然数 d は ab に等しい。よって $f(X) = d \cdot g(X)h(X)$ となるから、$d \cdot g(X)$ を $g(X)$ とすればよい。 □

定理 1.5.2 (Eisenstein). $\mathbb{Z}$ 上の 0 でない多項式

$$f(X) = a_n X^n + \cdots + a_1 X + a_0 \quad (a_i \in \mathbb{Z},\ a_n \neq 0)$$

に対し、次の条件

$$\begin{cases} a_n \text{ は } p \text{ で割り切れない}, \\ a_{n-1}, ..., a_1, a_0 \text{ は } p \text{ で割り切れる}, \\ a_0 \text{ は } p^2 \text{で割り切れない} \end{cases}$$

を満たす素数 p が存在すれば、$f(X)$ は $\mathbb{Q}$ 上既約になる。

証明. Gauss の補題の系より、$f(X)$ が $\mathbb{Z}$ 上既約になることを示せばよい。結論を否定して

$$f(X) = g(X)h(X),\ 0 < \deg(g), \deg(h) < \deg(f)$$

を満たす $g(X), h(X) \in \mathbb{Z}[X]$ が存在すると仮定する。

$$\begin{cases} g(X) = b_m X^m + \cdots + b_1 X + b_0 & (b_i \in \mathbb{Z},\ b_m \neq 0), \\ h(X) = c_l X^l + \cdots + c_1 X + c_0 & (c_j \in \mathbb{Z},\ c_l \neq 0) \end{cases}$$

と書くと、$a_n = b_m c_l$ についての仮定より、b_m, c_l は共に p で割り切れないから、

$$\begin{cases} s &= \min\{\ 0 \leq i \leq m \mid b_i \text{ は } p \text{ で割り切れない }\}, \\ t &= \min\{\ 0 \leq j \leq l \mid c_j \text{ は } p \text{ で割り切れない }\} \end{cases}$$

が定義される。$a_0 = b_0 c_0$ についての仮定より、b_0, c_0 のいずれか片方のみが p で割り切れる。いま b_0 が p で割り切れないとすると、c_0 は p で割り切れるから $t > 0$ が成り立つ。t の定義より、$c_0, ..., c_{t-1}$ は p で割り切れ、c_t は p で割り切れないから、$f(X) = g(X)h(X)$ の X^t の係数

$$a_t = b_0 c_t + b_1 c_{t-1} + \cdots + b_t c_0$$

は p で割り切れない。$t \leq l < l + m = n$ だから、これは a_t についての仮定に矛盾する。c_0 が p で割り切れない場合にも同様に矛盾が生ずるので、$f(X)$ は $\mathbb{Z}$ 上既約、従って $\mathbb{Q}$ 上既約になる。 □

例.

(1) p を素数、a を p で割り切れて p^2 で割り切れない整数とするとき、任意の自然数 n に対し $X^n - a$ は $\mathbb{Q}$ 上既約。

(2) p を素数とするとき、p 次円周等分多項式

$$\frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$$

は $\mathbb{Q}$ 上既約。

問題. Eisenstein の定理の逆が成り立つかどうか答えよ。またその理由を述べよ。

問題. 1 より大きい自然数 n が素数でないとき、

$$\frac{X^n - 1}{X - 1}$$

は $\mathbb{Q}$ 上可約になることを示せ。

問題. 素数 p と自然数 d に対し、$\mathbb{Z}$ 上の多項式 $f(X)$ を

$$f(X) = \left(X^{p^{d-1}}\right)^{p-1} + \left(X^{p^{d-1}}\right)^{p-2} + \cdots + X^{p^{d-1}} + 1$$

で定めるとき、次の問いに答えよ。

(1) $f(X)\left(X^{p^{d-1}} - 1\right) = X^{p^d} - 1$ を示せ。

(2) $\mathbb{Z}[X]$ において $(X+1)^p \equiv X^p + 1 \bmod(p)$ が成り立つことを示せ。

(3) (2) を用いて

$$(X+1)^{p^d} \equiv X^{p^d} + 1 \bmod(p), \quad f(X+1) \equiv \left(X^{p^{d-1}}\right)^{p-1} \bmod(p)$$

を示せ。

(4) Eisenstein の定理を用いて、$f(X)$ が $\mathbb{Q}$ 上既約になることを示せ。

1.6. 作図問題への応用.

作図とは？定規とコンパスを有限回用いて、図形（すなわち与えられた数を長さに持つ線分）を描くこと。

ギリシャの 3 大作図問題.

$$\begin{aligned} \text{体積が 2 倍の立方体の作図} &\Leftrightarrow \sqrt[3]{2} \text{ の作図,} \\ \text{与えられた角の 3 等分の作図} &\Leftrightarrow \cos(\theta) \text{ から } \cos(\theta/3) \text{ を作図,} \\ \text{正方形と同面積の円の作図} &\Leftrightarrow \pi \text{ の作図.} \end{aligned}$$

結論. この 3 つの作図はいずれも不可能であり、ここでは上の 2 つの不可能性を示す（3 番目の不可能性は円周率の超越性から従う）。

ポイント. 作図可能な数の集合（体）の持つ構造に目をつける $\Rightarrow$ 有効な大局的アプローチ

定理 1.6.1. a, b が作図可能な実数ならば、

$$a \pm b, \quad ab, \quad 1/a \ (a \neq 0), \quad \sqrt{a} \ (a \geq 0)$$

はいずれも作図可能。

系.

(1) 作図可能な実数のなす集合 L は、数の加法と乗法によって体になる。特に L は有理数体 $\mathbb{Q}$ を含む。

(2) L の 0 以上の元 a に対し、$\sqrt{a} \in L$.

この系の “逆”

作図可能な数は、有理数に加減乗除と平方根をとる操作を有限回行って得られる

も成り立つ。すなわち

定理 1.6.2. 実数 α が作図可能になるための必要十分条件は、

$$\begin{cases} \mathbb{Q} = K_1 \subset K_2 \subset \cdots \subset K_n; \ \mathbb{R} \text{ に含まれる体の拡大列,} \\ \text{ただし、} K_{i+1} \text{ は } K_i \text{ のある元 } a_i \geq 0 \text{ によって } K_{i+1} = K_i\left(\sqrt{a_i}\right) \text{ と表される} \end{cases}$$

で、$\alpha \in K_n$ を満たすものが存在する。

証明. 定理 1.6.1 より、上の K_n の各元は作図可能になるから、作図可能な数が上のように表されることを示せばよい。

既に作図された実数の集合 S から新しく作図される実数は、S の元を用いて作図された

$$\text{直線} : ax + by = c \ (a, b, c \in S), \quad \text{円} : (x - d)^2 + (y - e)^2 = f^2 \ (d, e, f \in S)$$

の直線どうし、円どうし、直線と円の交点を結ぶ線分の長さとして表される。これらの交点の座標は、S の元から加減乗除で得られる数を係数とする 1 次方程式と 2 次方程式の実数解になるから、解の公式より、S の元に加減乗除と平方根をとる操作を行って得られる。よって三平方の定理より、これらの交点どうしの距離も同じ性質を持つ。 □

注意. 体 K_i の元 a_i に対し、$K_{i+1} = K_i\left(\sqrt{a_i}\right)$ とすると

$$\begin{array}{lllll} \sqrt{a_i} \in K_i & \Leftrightarrow & K_{i+1} = K_i & \Leftrightarrow & [K_{i+1} : K_i] = 1, \\ \sqrt{a_i} \notin K_i & \Leftrightarrow & X^2 - a_i \text{ は } K_i \text{ 上既約} & \Leftrightarrow & [K_{i+1} : K_i] = 2. \end{array}$$

問題. 体の拡大列 $K_1 \subset K_2 \subset K_3$ に対し、

$$\begin{array}{l} \alpha_1, ..., \alpha_n : \ K_2 \text{ の } K_1 \text{ 上の基底}, \ \ \beta_1, ..., \beta_m : \ K_3 \text{ の } K_2 \text{ 上の基底} \\ \Rightarrow \ \ \alpha_i\beta_j \ (1 \leq i \leq n, \ 1 \leq j \leq m) : \ K_3 \text{ の } K_1 \text{ 上の基底} \end{array}$$

が成り立ち、従って

$$[K_3 : K_1] = [K_3 : K_2]\,[K_2 : K_1]$$

となることを示せ。

問題. 次の問いに答えよ。

(1) Eisenstein の定理を用いて、$\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] = 4$ を示せ。

(2) d を自然数とするとき、

$$\left[\mathbb{Q}\left(\sqrt[4]{2}, \sqrt{-d}\right) : \mathbb{Q}\left(\sqrt[4]{2}\right)\right] = 2, \ \ \left[\mathbb{Q}\left(\sqrt[4]{2}, \sqrt{-d}\right) : \mathbb{Q}\left(\sqrt{-d}\right)\right] = 4$$

を示せ。

(3) (2) を用いて、$X^4 - 2$ が $\mathbb{Q}\left(\sqrt{-d}\right)$ 上既約になることを示せ。

系. 実数 α が作図可能ならば、$[\mathbb{Q}(\alpha) : \mathbb{Q}]$ は 2 の巾乗になる。

注意. 実はこの “逆” も成り立つ。

定理 1.6.3. $\sqrt[3]{2}$ は作図できない。

証明. $\sqrt[3]{2}$ を解に持つ多項式 $X^3 - 2$ は、Eisenstein の定理より $\mathbb{Q}$ 上既約になる。従って $\left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$ が成り立つから、定理 1.6.2 の系より $\sqrt[3]{2}$ は作図できない。 □

定理 1.6.4. $\cos 20^\circ$ は作図できない。

注意. $\cos 60^\circ = 1/2$ は作図できるから、角の 3 等分は一般には作図可能でない。

証明. 三角関数の加法定理より $\cos 20^\circ$ は $8X^3 - 6X - 1 = 0$ の解になるから、$\alpha = 2\cos 20^\circ$ は

$$f(X) = X^3 - 3X - 1 = 0$$

の解になる。よって $f(X)$ が $\mathbb{Q}$ 上既約になることが示されれば、

$$[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

となるから、定理 1.6.2 の系より $\cos 20^\circ$ が作図できないことが分る。

いま $f(X) = X^3 - 3X - 1$ が $\mathbb{Q}$ 上可約になると仮定すると、Gauss の補題の系より

$$X^3 - 3X - 1 = (aX + b)(cX^2 + dX + e)$$

を満たす整数 a, b, c, d, e が存在する。両辺の 3 次の項及び定数項を比べると $ac = 1, be = -1$ が成り立つので、a, b は 1 または -1 に等しい。従って $f(X) = 0$ は $-b/a = \pm 1$ を解に持つことになり、矛盾が生ずる。 □

定理 1.6.5 (Gauss). 素数 p に対し、

$$\begin{aligned} \text{正 } p \text{ 角形が作図可能} &\Leftrightarrow p - 1 \text{ が 2 の巾乗} \\ &\Leftrightarrow p = 3, 5, 17, 257, \ldots (\text{どれ位あるの？}) \end{aligned}$$

証明の概略. 定理 1.6.2 の系とその注意より

$$\begin{aligned} \text{正 } p \text{ 角形が作図可能} &\Leftrightarrow \zeta = e^{2\pi i/p} = \cos(2\pi/p) + i\sin(2\pi/p) \text{ が作図可能} \\ &\Leftrightarrow [\mathbb{Q}(\zeta) : \mathbb{Q}] \text{ が 2 の巾乗.} \end{aligned}$$

一方定理 1.5.2 の例 (2) より、ζ の満たす方程式

$$\frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1 = 0$$

は $\mathbb{Q}$ 上既約だから、定理 1.4.2 より $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ となり、定理が示された。 □

正 5 角形の作図. $\zeta = e^{2\pi i/5} = \cos(2\pi/5) + i\sin(2\pi/5)$ は $\zeta^5 = 1, \zeta \neq 1$ を満たすから、

$$\frac{X^5 - 1}{X - 1} = X^4 + X^3 + X^2 + X + 1 = 0$$

の解になる。よって $\alpha = \zeta + \zeta^{-1} = 2\cos(2\pi/5)$ とすると、

$$\alpha^2 + \alpha - 1 = \zeta^2 + 2 + \zeta^{-2} + \zeta + \zeta^{-1} - 1 = 0.$$

さらに $\alpha > 0$ だから $\alpha = \dfrac{-1 + \sqrt{5}}{2}$ となり、$\cos(2\pi/5) = \dfrac{-1 + \sqrt{5}}{4}$ は作図できる。従って正 5 角形は作図できる。

正 17 角形の作図 (Gauss). Galois 理論を用いるため、第 3 章の 3.1 で述べる。

§2. Galois 理論

2.1. Galois 拡大と Galois 群.

Galois 拡大の定義. 体 K の有限次拡大体 $L = K(\alpha)$ が K の **Galois 拡大**であるとは、$f(X)$ を α の K 上の最小多項式、すなわち $f(\alpha) = 0$ となる K 上の既約多項式とするとき、次の条件：

- $f(X) = 0$ が重解を持たない（分離性），
- $f(X) = 0$ のすべての解が L に含まれる（正規性）

が成り立つことである。

注意. M が K を含む L の部分体ならば、α の M 上の最小多項式は $f(X)$ を割り切るので、分離性と正規性を満たす。従って $L = M(\alpha)$ は M の Galois 拡大になる。

問題. $\mathbb{Q}\left(\sqrt{2}\right)$ は $\mathbb{Q}$ の Galois 拡大になることを示せ。また $\mathbb{Q}\left(\sqrt[3]{2}\right)$ は $\mathbb{Q}$ の Galois 拡大にならないことを示せ。

Galois 群の定義. 体 K の Galois 拡大 $L = K(\alpha)$ に対し、写像 $\sigma : L \to L$ で次の条件：

- σ は全単射,
- 任意の $x, y \in L$ に対し、$\sigma(x + y) = \sigma(x) + \sigma(y)$,
- 任意の $x, y \in L$ に対し、$\sigma(xy) = \sigma(x)\sigma(y)$,
- 任意の $a \in K$ に対し、$\sigma(a) = a$

を満たすものの集合は、写像の合成を積として群になる。これを Galois 拡大 L/K の **Galois 群**と言い、$\mathrm{Gal}(L/K)$ と書く。

問題. $\mathrm{Gal}(L/K)$ が写像の合成を積として群になることを示せ。

定理 2.1.1. $\mathrm{Gal}(L/K)$ の位数 $|\mathrm{Gal}(L/K)|$ は、体の拡大次数 $[L : K]$ に等しい。

証明. $f(X)$ を α の K 上の最小多項式とし、その次数を n とすると

$$f(X) = a_n X^n + \cdots + a_1 X + a_0,\ a_n \neq 0$$

を満たす $a_i \in K$ が存在する。$f(X) = 0$ のすべての解を $\alpha_1(= \alpha), \alpha_2, ..., \alpha_n$ とすると、$L = K(\alpha)$ は K の Galois 拡大だから、$\alpha_1, ..., \alpha_n$ は相異なる L の元である。よって任意の $\sigma \in \mathrm{Gal}(L/K)$ に対し、

$$0 = \sigma(0) = \sigma\left(f(\alpha)\right) = \sigma\left(\sum_i a_i \alpha^i\right) = \sum_i \sigma(a_i)\sigma(\alpha)^i = \sum_i a_i \sigma(\alpha)^i = f(\sigma(\alpha))$$

となるから、$\sigma(\alpha) \in \{\alpha_1, ..., \alpha_n\}$ が成り立つ。またこのとき $L = K(\alpha) = K[\alpha]$ の任意の元を $g(\alpha) = \sum_i b_i \alpha^i$ $(b_i \in K)$ と表すと、上式と同様に

$$\sigma\left(g(\alpha)\right) = \sigma\left(\sum_i b_i \alpha^i\right) = \sum_i b_i \sigma(\alpha)^i = g(\sigma(\alpha))$$

となるから、写像 σ は $\sigma(\alpha)$ によって一意的に定まる。

一方、各 $j = 1, ..., n$ に対し、$\alpha_j \in L$ だから $K(\alpha_j) \subset L = K(\alpha)$ となる。また $f(X)$ は α_j の K 上の最小多項式にもなるから、

$$[K(\alpha_j) : K] = \deg(f) = [K(\alpha) : K].$$

よって $K(\alpha_j) = K(\alpha) = L$ が成り立つ。従って定理 1.4.2 より、$K[X]$ の元 $g(X)$ に対し、

$$g(X) \mapsto g(\alpha),\ g(X) \mapsto g(\alpha_j)$$

という対応は、それぞれ環の同型写像

$$K[X]/(f(X)) \xrightarrow{\sim} K(\alpha) = L,\ K[X]/(f(X)) \xrightarrow{\sim} K(\alpha_j) = L$$

を導くから、$g(\alpha) \mapsto g(\alpha_j)$ は α を α_j に写す $\mathrm{Gal}(L/K)$ の元を与える。従って $\mathrm{Gal}(L/K)$ と $\{\alpha_1, ..., \alpha_n\}$ は $\sigma \leftrightarrow \sigma(\alpha)$ によって 1 対 1 に対応するから、

$$|\mathrm{Gal}(L/K)| = n = \deg(f) = [L : K]$$

が成り立つ。 □

系. $L = K(\alpha)$ が K の Galois 拡大ならば

$$\prod_{\sigma \in \mathrm{Gal}(L/K)} (X - \sigma(\alpha)) = \prod_{j=1}^{n} (X - \alpha_j) :\ \alpha \text{ の } K \text{ 上の最小多項式.}$$

注意. 体 K の一般の有限次拡大 $L = K(\alpha)$ に対し、拡大 L/K の自己同型群 $\mathrm{Aut}(L/K)$ を上の Galois 群と同様に定義すると、定理 2.1.1 の証明より

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

が成り立つことが分る。ここで等式が成り立つ拡大を Galois 拡大と定義することもある。

定理 2.1.2. K を標数 0 の体とする。K 上の 0 でない多項式 $f(X)$ に対し、$f(X) = 0$ のすべての解 $\alpha_1, ..., \alpha_n$ と K から生成された体 $K(\alpha_1, ..., \alpha_n)$ を L とするとき、L は K の Galois 拡大になる。(L を $f(X)$ の K 上の**分解体**という)

証明. まず L の任意の元 β の K 上の最小多項式 $g(X)$ に対し、$g(X) = 0$ は重解を持たないことを示す。$g(X)$ の導関数を $g'(X) \in K[X]$ とすると、K の標数が 0 であることより、

$\deg(g') = \deg(g) - 1$ となり、特に $g'(X) \neq 0$ が成り立つ。$g(X)$ と $g'(X)$ の最大公約元を $d(X) \in K[X]$ とすると、$g(X)$ が K 上既約であることより、$\deg(d)$ は 0 または $\deg(g)$ に等しい。もし $\deg(d) = \deg(g)$ ならば、$g(X)$ が $d(X)$、従って $g'(X)$ を割り切ることになり、$\deg(g') = \deg(g) - 1 < \deg(g)$ に矛盾する。従って $\deg(d) = 0$ となるから、定理 1.3.3 より $(g(X), g'(X)) = (d(X)) = K[X]$ が成り立ち、

$$1 = a(X)g(X) + b(X)g'(X)$$

を満たす $a(X), b(X) \in K[X]$ が存在する。もし $g(X) = 0$ が重解 β' を持つと仮定すると、β' は $g'(X) = 0$ の解にもなるから、上式より $X - \beta'$ は 1 を割り切ることになり、矛盾が生ずる。

次に $K(\alpha_1, ..., \alpha_n) = K(\delta)$ を満たす $K(\alpha_1, ..., \alpha_n)$ の元 δ が存在することを示す。帰納法により $n = 2$ の場合に示せばよい。

$$\begin{cases} h_1(X) : \ \alpha_1 \text{の } K \text{ 上の最小多項式、} \quad \beta_1 (= \alpha_1), ..., \beta_m : \ h_1(X) = 0 \text{ の解,} \\ h_2(X) : \ \alpha_2 \text{の } K \text{ 上の最小多項式、} \quad \gamma_1 (= \alpha_2), ..., \gamma_l : \ h_2(X) = 0 \text{ の解} \end{cases}$$

とすると、上で示したことより $h_1(X)$ と $h_2(X)$ は重解を持たない。K は標数が 0 なので無限集合になり、従って

$$\left\{ -\frac{\alpha_1 - \beta_j}{\alpha_2 - \gamma_j} \;\middle|\; 1 \leq i \leq m, \ 2 \leq j \leq l \right\}$$

に含まれない K の元が存在する。その 1 つを c とすると、

$$\beta_i + c\gamma_j \neq \alpha_1 + c\alpha_2 \ \ (1 \leq \forall i \leq m, \ 2 \leq \forall j \leq l)$$

が成り立つ。このとき $\delta = \alpha_1 + c\alpha_2 \in K(\alpha_1, \alpha_2)$ とおくと、$h_2(X) = 0$ の解 $\gamma_j \ (1 \leq j \leq l)$ の中で、$\delta - c\gamma_j$ が $h_1(X) = 0$ の解 $\beta_i \ (1 \leq i \leq m)$ になるのは $\gamma_1 = \alpha_2$ に限るから、$h_1(\delta - cX) = 0$ と $h_2(X) = 0$ の共通の解は α_2 のみになる。従って $K(\delta)$ 上の多項式 $h_1(\delta - cX), h_2(X)$ の最大公約元は $X - \alpha_2$ となり、定理 1.3.3 より $\alpha_2 \in K(\delta)$ が成り立つ。よって $\alpha_1 = \delta - c\alpha_2 \in K(\delta)$ となるから、$K(\alpha_1, \alpha_2) = K(\delta)$ が示された。

最後に $L = K(\alpha_1, ..., \alpha_n)$ が K の Galois 拡大になることを示す。$L = K(\delta)$ を満たす δ の K 上の最小多項式を $k(X)$ とすると、上で示したことより $k(X) = 0$ は重解を持たない。また $k(X) = 0$ の他の解を δ' とすると、定理 2.1.1 の証明より、体の同型写像 $\sigma : K(\delta) \xrightarrow{\sim} K(\delta')$ で $\sigma(\delta) = \delta'$ を満たすものが存在し、任意の $i = 1, ..., n$ に対し、$\sigma(\alpha_i)$ は $\{\alpha_1, ..., \alpha_n\} \subset L$ に含まれる。$\delta \in K(\alpha_1, ..., \alpha_n)$ より $\delta = \dfrac{F(\alpha_1, ..., \alpha_n)}{G(\alpha_1, ..., \alpha_n)}$ を満たす K 上の n 変数多項式 $F(X_1, ..., X_n), G(\alpha_1, ..., \alpha_n)$ が存在するから、

$$\delta' = \sigma(\delta) = \sigma\left(\frac{F(\alpha_1, ..., \alpha_n)}{G(\alpha_1, ..., \alpha_n)}\right) = \frac{F\left(\sigma(\alpha_1), ..., \sigma(\alpha_n)\right)}{G\left(\sigma(\alpha_1), ..., \sigma(\alpha_n)\right)} \in L.$$

従って $L = K(\delta)$ は分離性と正規性を満たすから、K の Galois 拡大になる。 □

問題. $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)=\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ を示せ。また $\sqrt{2}=f\left(\sqrt{2}+\sqrt{3}\right)$, $\sqrt{3}=g\left(\sqrt{2}+\sqrt{3}\right)$ を満たす $\mathbb{Q}$ 上の多項式 $f(X)$, $g(X)$ を求めよ。

問題. L を X^3-2 の $\mathbb{Q}$ 上の分解体とするとき、次を示せ。

$$L=\mathbb{Q}\left(\sqrt[3]{2},\sqrt{-3}\right),\quad [L:\mathbb{Q}]=6,\quad L=\mathbb{Q}\left(\sqrt[3]{2}+\sqrt{-3}\right).$$

問題. L を X^4-2 の $\mathbb{Q}$ 上の分解体とするとき、次を示せ。

$$L=\mathbb{Q}\left(\sqrt[4]{2},\sqrt{-1}\right),\quad [L:\mathbb{Q}]=8,\quad L=\mathbb{Q}\left(\sqrt[4]{2}+\sqrt{-1}\right).$$

2.2. Galois 対応の証明.

定理 2.2.1（Galois 対応）. 体 K の Galois 拡大 $L = K(\alpha)$ に対し、K を含む L の部分体を拡大 L/K の**中間体**と呼ぶ。このとき次が成り立つ。

(1) L/K の中間体の集合から $\mathrm{Gal}(L/K)$ の部分群の集合への写像 $M \mapsto \mathrm{Gal}(L/M)$ は全単射写像となり、この逆写像は

$$H \mapsto L^H := \{a \in L \mid \sigma(a) = a \ (\sigma \in H)\};\ H \text{ の}\textbf{不変体}\text{と呼ぶ}$$

で与えられる。またこのとき

$$|\mathrm{Gal}(L/M)| = [L : M],\ \left[L^H : K\right] = \frac{|\mathrm{Gal}(L/K)|}{|H|}$$

が成り立つ。さらに L/K の中間体 M_1, M_2 に対し、

$$M_1 \subset M_2 \ \Leftrightarrow\ \mathrm{Gal}(L/M_1) \supset \mathrm{Gal}(L/M_2).$$

(2) 上の対応において、

$$\begin{aligned} &\text{任意の } \sigma \in \mathrm{Gal}(L/K) \text{ に対し } \sigma(M) = M (\Leftrightarrow M/K \text{ が Galois 拡大}) \\ \Leftrightarrow\ &\mathrm{Gal}(L/M) \text{ は } \mathrm{Gal}(L/K) \text{ の正規部分群} \end{aligned}$$

が成り立ち、このとき

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \cong \mathrm{Gal}(M/K);\ \text{群として同型.}$$

証明. まず (1) を示す。$\mathrm{Gal}(L/K)$ の部分群 H に対し、$H' = \mathrm{Gal}\left(L/L^H\right)$ とすると、

$$\sigma \in H \ \Rightarrow\ \sigma(a) = a\ \left(\forall a \in L^H\right)\ \Rightarrow\ \sigma \in \mathrm{Gal}\left(L/L^H\right) = H'.$$

$$\therefore\ H \subset H' \ \cdots\cdots (\mathrm{I})$$

従って定理 2.1.1 の系より $\prod_{\sigma \in H'}(X - \sigma(\alpha))$ は α の L^H 上の最小多項式を与える。一方、

$$g(X) = \prod_{\sigma \in H}(X - \sigma(\alpha))$$

は α を解に持ち、(I) より $\prod_{\sigma \in H'}(X - \sigma(\alpha))$ を割り切る。さらに任意の $\tau \in H$ に対し、

$$\tau(g(X)) = \prod_{\sigma \in H}(X - \tau(\sigma(\alpha))) = g(X)$$

となるから、$g(X) \in L^H[X]$ が成り立つ。よって $g(X)$ は α の L^H 上の最小多項式となり、

$$\prod_{\sigma \in H}(X - \sigma(\alpha)) = g(X) = \prod_{\sigma \in H'}(X - \sigma(\alpha)).$$

従って $|H| = |H'|$ となるから、(I) より

$$H = H' = \mathrm{Gal}\left(L/L^H\right) \ \cdots\cdots (\mathrm{II}).$$

L はその部分体 M の Galois 拡大だから、定理 2.1.1 と (II) より、

$$\left[L^H : K\right] = \frac{[L:K]}{[L:L^H]} = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/L^H)|} = \frac{|\mathrm{Gal}(L/K)|}{|H|} \ \cdots\cdots (\mathrm{III}).$$

また L/K の中間体 M に対し、$H = \mathrm{Gal}(L/M)$ とすると、

$$a \in M \ \Rightarrow \ \sigma(a) = a \ (\forall \sigma \in H) \ \Rightarrow \ a \in L^H.$$

$$\therefore \ M \subset L^H \ \cdots\cdots (\mathrm{IV}).$$

L はその部分体 L^H と M の Galois 拡大だから、定理 2.1.1 と (II) より、

$$\left[L : L^H\right] = \left|\mathrm{Gal}\left(L/L^H\right)\right| = |H| = |\mathrm{Gal}(L/M)| = [L:M] \ \cdots\cdots (\mathrm{V})$$

となるから、$\left[L^H : M\right] = [L:M] \,/\, \left[L : L^H\right] = 1$ が成り立ち、(IV) より

$$M = L^H = L^{\mathrm{Gal}(L/M)} \ \cdots\cdots (\mathrm{VI}).$$

従って、(II), (III), (V), (VI) より (1) が成り立つことが示された。

次に (2) を示す。$\sigma, \tau \in \mathrm{Gal}(L/K)$ に対し、

$$\begin{aligned} \tau \in \mathrm{Gal}(L/\sigma(M)) \ &\Leftrightarrow \ \tau(\sigma(a)) = \sigma(a) \ (\forall a \in M) \\ &\Leftrightarrow \ (\sigma^{-1}\tau\sigma)(a) = a \ (\forall a \in M) \\ &\Leftrightarrow \ \sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/M) \end{aligned}$$

となるから、$\sigma^{-1} \cdot \mathrm{Gal}(L/\sigma(M)) \cdot \sigma = \mathrm{Gal}(L/M)$ が成り立つ。従って (1) より

$$\sigma(M) = M \ \Leftrightarrow \ \mathrm{Gal}(L/\sigma(M)) = \mathrm{Gal}(L/M) \ \Leftrightarrow \ \sigma \cdot \mathrm{Gal}(L/M) \cdot \sigma^{-1} = \mathrm{Gal}(L/M)$$

$$\therefore \ \sigma(M) = M \ (\forall \sigma \in \mathrm{Gal}(L/K)) \ \Leftrightarrow \ \mathrm{Gal}(L/M) \text{ は } \mathrm{Gal}(L/K) \text{ の正規部分群.}$$

またこのとき、$\sigma \in \mathrm{Gal}(L/K)$ の M への制限写像 $\sigma|_M$ は $\mathrm{Aut}(M/K)$ の元を与えるから、$\sigma \mapsto \sigma|_M$ は群の準同型写像 $\varphi : \mathrm{Gal}(L/K) \to \mathrm{Aut}(M/K)$ を導く。ここで、

$$\sigma \in \mathrm{Ker}(\varphi) \ \Leftrightarrow \ \sigma(a) = a \ (\forall a \in M) \ \Leftrightarrow \ \sigma \in \mathrm{Gal}(L/M)$$

となるから、準同型定理より φ は単射準同型写像

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

を導き、$|\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)| \leq |\mathrm{Aut}(M/K)|$ が成り立つ。一方 (1) より、

$$|\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)| = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/M)|} = \frac{[L:K]}{[L:M]} = [M:K]$$

だから、定理 2.1.1 とその注意より M/K は Galois 拡大で、この写像は同型になる。 □

2.3. Galois 対応の例. 標数 0 の体 K の Galois 拡大を調べる。

2 次拡大. $K^\times = K - \{0\}$ の元 α に対し、

$$X^2 - \alpha \text{ が } K \text{ 上既約} \ \Leftrightarrow \ \sqrt{\alpha} \notin K.$$

このとき

$$L = K\left(\sqrt{\alpha}\right) = \left\{a + b\sqrt{\alpha} \mid a, b \in K\right\}$$

は $X^2 - \alpha$ の分解体だから、定理 2.1.2 より K の 2 次 Galois 拡大となり、定理 2.1.1 より $|\mathrm{Gal}(L/K)| = 2$ が成り立つ。また $\sigma \in \mathrm{Gal}(L/K)$ は、$X^2 - \alpha = 0$ の解 $\pm\sqrt{\alpha}$ の置換を与え、

$$\sigma(\sqrt{\alpha}) = \pm\sqrt{\alpha} \ \Rightarrow \ \sigma(a + b\sqrt{\alpha}) = a \pm b\sqrt{\alpha} \ \text{（複合同順）}$$

従って

$$\mathrm{Gal}(L/K) = \{\sigma_1, \sigma_2\}; \ \begin{cases} \sigma_1(a + b\sqrt{\alpha}) = a + b\sqrt{\alpha} & (a, b \in K), \\ \sigma_2(a + b\sqrt{\alpha}) = a - b\sqrt{\alpha} & (a, b \in K). \end{cases}$$

2 次拡大の合成. $\alpha, \beta \in K^\times$ が $\sqrt{\alpha}, \sqrt{\beta}, \sqrt{\alpha\beta} \notin K$ を満たすとき、

$$\begin{aligned} & M = K(\sqrt{\alpha}) : \ K \text{ の 2 次拡大}, \ \ L = M(\sqrt{\beta}) : \ M \text{ の 2 次拡大} \\ \Rightarrow \ & [L : K] = [L : M][M : K] = 4. \end{aligned}$$

L は $(X^2 - \alpha)(X^2 - \beta)$ の分解体だから、定理 2.1.2 より K の 4 次 Galois 拡大となり、

$$\sigma \in \mathrm{Gal}(L/K) \ \Rightarrow \ \sigma(\sqrt{\alpha}) = \pm\sqrt{\alpha}, \ \sigma(\sqrt{\beta}) = \pm\sqrt{\beta}.$$

$$\therefore \ \mathrm{Gal}(L/K) = \{\sigma_1 = 1, \sigma_2, \sigma_3, \sigma_4\}; \ \begin{cases} \sigma_1 : \sqrt{\alpha} \mapsto \sqrt{\alpha}, & \sqrt{\beta} \mapsto \sqrt{\beta}, \\ \sigma_2 : \sqrt{\alpha} \mapsto \sqrt{\alpha}, & \sqrt{\beta} \mapsto -\sqrt{\beta}, \\ \sigma_3 : \sqrt{\alpha} \mapsto -\sqrt{\alpha}, & \sqrt{\beta} \mapsto \sqrt{\beta}, \\ \sigma_4 : \sqrt{\alpha} \mapsto -\sqrt{\alpha}, & \sqrt{\beta} \mapsto -\sqrt{\beta}. \end{cases}$$

σ_2 で生成される $\mathrm{Gal}(L/K)$ の部分群を $\langle\sigma_2\rangle$ と書くと、$\langle\sigma_2\rangle = \{1, \sigma_2\}$ となる。$\sigma_2\left(\sqrt{\alpha}\right) = \sqrt{\alpha}$ より σ_2 は $M = K\left(\sqrt{\alpha}\right)$ 上では恒等写像になるから、$\langle\sigma_2\rangle \subset \mathrm{Gal}(L/M)$ が成り立つ。一方定理 2.1.1 より $|\mathrm{Gal}(L/M)| = [L : M] = 2$ となるから、$\langle\sigma_2\rangle = \mathrm{Gal}(L/M)$ となる。同様に $\mathrm{Gal}(L/K)$ の部分群と対応する中間体を求めると、

$$\begin{array}{ccccccc} \mathrm{Gal}(L/K) & \supset & \langle\sigma_2\rangle, & \langle\sigma_3\rangle, & \langle\sigma_4\rangle & \supset & \{1\} \\ \updownarrow & & \updownarrow & \updownarrow & \updownarrow & & \updownarrow \\ K & \subset & K(\sqrt{\alpha}), & K(\sqrt{\beta}), & K(\sqrt{\alpha\beta}) & \subset & L. \end{array}$$

問題. 上記の Galois 対応を用いて、$K(\sqrt{\alpha} + \sqrt{\beta} + \sqrt{\alpha\beta}) = L$ を示せ。

円分拡大. 自然数 $n > 1$ に対し、$\zeta^n = 1, \zeta^m \neq 1 \ (1 \leq m \leq n-1)$ を満たす ζ を、1 の原始 n 乗根という (例：n 次円分数 $\exp(2\pi\sqrt{-1}/n)$)。このとき

$$\zeta^0 = 1, \ \zeta^1 = \zeta, \ \zeta^2, ..., \zeta^{n-1} \ : \ n \text{ 個の相異なる元}$$

は $X^n-1=0$ のすべての解を与えるから、定理 2.1.2 より

$$L=K(\zeta)$$

は X^n-1 の分解体となり、L/K は Galois 拡大になる。$\sigma\in\mathrm{Gal}(L/K)$ に対し、

$$\sigma(\zeta)^n=\sigma\left(\zeta^n\right)=\sigma(1)=1$$

となるから、$\sigma(\zeta)=\zeta^{\varphi(\sigma)}$ を満たす $\mathbb{Z}/(n)=\left\{\overline{0},\overline{1},...,\overline{n-1}\right\}$ $(\overline{a}:=a+(n))$ の元 $\varphi(\sigma)$ が定まる。このとき $\sigma,\tau\in\mathrm{Gal}(L/K)$ に対し、

$$(\sigma\tau)(\zeta)=\sigma\left(\zeta^{\varphi(\tau)}\right)=\sigma(\zeta)^{\varphi(\tau)}=\zeta^{\varphi(\sigma)\varphi(\tau)}.\quad\therefore\ \varphi(\sigma\tau)=\varphi(\sigma)\varphi(\tau).$$

よって $\varphi(\sigma)\varphi(\sigma^{-1})=\varphi\left(\sigma\sigma^{-1}\right)=\varphi(1)=\overline{1}$ となるから、

$$\varphi(\sigma)\in(\mathbb{Z}/(n))^{\times}:=\left\{\overline{a}\in\mathbb{Z}/(n)\mid a\text{ と }n\text{ は互いに素}\right\}.$$

$(\mathbb{Z}/(n))^{\times}$ は $\overline{a}\cdot\overline{b}=\overline{ab}$ を積として群になるから、群の準同型写像 $\varphi:\mathrm{Gal}(L/K)\to(\mathbb{Z}/(n))^{\times}$ が定まる。ここで

$$\sigma\in\mathrm{Ker}(\varphi)\ \Leftrightarrow\ \varphi(\sigma)=\overline{1}\ \Leftrightarrow\ \sigma(\zeta)=\zeta\ \Leftrightarrow\ \sigma=1:K(\zeta)\text{ 上の恒等写像}$$

となるから、準同型定理より φ は単射になる。

問題. $\zeta_n=e^{2\pi\sqrt{-1}/n}=\exp\left(2\pi\sqrt{-1}/n\right)$ とするとき、この単射準同型写像

$$\varphi:\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)\to(\mathbb{Z}/(n))^{\times}$$

は同型写像になることが定理 3.3.1 で示される。$n=3,4$ の場合にこのことを確かめよ。

Kummer 拡大. K が 1 の原始 n 乗根 ζ を含むとき、$K^{\times}$ の元 α に対し、$X^n-\alpha=0$ の解の 1 つを β とすると、

$$\beta,\ \beta\zeta,...,\beta\zeta^{n-1}$$

は $X^n-\alpha=0$ のすべての解を与えるから、定理 2.1.2 より

$$L=K(\beta)$$

は $X^n-\alpha$ の分解体となり、L/K は Galois 拡大になる。これを **Kummer** 拡大という。$\sigma\in\mathrm{Gal}(L/K)$ に対し、

$$\sigma(\beta)^n=\sigma\left(\beta^n\right)=\sigma(\alpha)=\alpha$$

だから $\sigma(\beta)=\beta\zeta^{\psi(\sigma)}$ を満たす $\psi(\sigma)\in\mathbb{Z}/(n)$ が定まる。また $\sigma,\tau\in\mathrm{Gal}(L/K)$ に対し、$\zeta\in K$ より

$$(\sigma\tau)(\beta)=\sigma\left(\beta\zeta^{\psi(\tau)}\right)=\sigma(\beta)\sigma(\zeta)^{\psi(\tau)}=\beta\zeta^{\psi(\sigma)}\zeta^{\psi(\tau)}=\beta\zeta^{\psi(\sigma)+\psi(\tau)}.$$

従って $\psi(\sigma\tau)=\psi(\sigma)+\psi(\tau)$ となり、群の準同型写像 $\psi:\mathrm{Gal}(L/K)\to\mathbb{Z}/(n)$ が定まる。

問題. この写像 $\psi:\mathrm{Gal}(L/K)\to\mathbb{Z}/(n)$ が単射になることを示せ。

問題. $\left[\mathbb{Q}\left(\sqrt[4]{2},\sqrt{-1}\right):\mathbb{Q}\left(\sqrt[4]{2}\right)\right]=2$、$\left[\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right]=4$ を示すことにより、$\mathbb{Q}\left(\sqrt[4]{2},\sqrt{-1}\right)$ が $\mathbb{Q}\left(\sqrt{-1}\right)$ の 4 次 Galois(Kummer) 拡大になることを示し、その中間体を求めよ。

問題. X^6-2 の $\mathbb{Q}$ 上の分解体 L が $K=\mathbb{Q}\left(\sqrt{-3}\right)$ の 6 次 Kummer 拡大になることを示し、L/K の中間体を求めよ。

注意. 以上の例においては $\mathrm{Gal}(L/K)$ が Abel 群（可換群）になる。このような Galois 拡大を **Abel 拡大**と呼ぶ。

3 次方程式の分解体. K 上のモニック 3 次多項式は、

$$\begin{aligned} X^3+a_2X^2+a_1X+a_0 &= \left(X+\frac{a_2}{3}\right)^3+a\left(X+\frac{a_2}{3}\right)+b \\ &\quad ;\ \text{ただし } a=a_1-\frac{a_2^2}{3},\ b=\frac{2a_2^2}{27}-\frac{a_1a_2}{3}+a_0 \end{aligned}$$

のように 2 次の項がない形に変形できるので、以下 K 上の既約 3 次多項式を

$$f(X)=X^3+aX+b\ \ (a,b\in K)$$

と置いて、その分解体を L とする。$\alpha_1,\alpha_2,\alpha_3$ を $f(X)=0$ の解とすると、

- $[K(\alpha_1):K]=3$、
- α_2 は $K(\alpha_1)$ 上の 2 次方程式 $f(X)/(X-\alpha_1)=0$ の解、
- $\alpha_3=-\alpha_1-\alpha_2\in K(\alpha_1,\alpha_2)$

となるから、$L=K(\alpha_1,\alpha_2)$ で、

$$[L:K]=[L:K(\alpha_1)][K(\alpha_1):K]=3[K(\alpha_1,\alpha_2):K(\alpha_1)]=3\text{ または }6.$$

$\sigma\in\mathrm{Gal}(L/K)$ は $f(X)=0$ の解 $\alpha_1,\alpha_2,\alpha_3$ の置換を与えるから、

$$S_3=\{\rho:\{1,2,3\}\to\{1,2,3\}:\ \text{全単射写像}\}:\ 3\text{ 次対称群}$$

とすると、$\sigma(\alpha_i)=\alpha_{\rho(i)}\ (i=1,2,3)$ を満たす S_3 の元 ρ_σ が定まる。$\sigma,\tau\in\mathrm{Gal}(L/K)$ に対し、

$$\alpha_i\overset{\sigma}{\longmapsto}\alpha_{\rho_\sigma(i)}\overset{\tau}{\longmapsto}\alpha_{(\rho_\tau(\rho_\sigma)(i))}$$

が成り立つから、$\rho_{\tau\sigma}=\rho_\tau\circ\rho_\sigma$ となり、従って $\sigma\mapsto\rho_\sigma$ は、群の準同型写像

$$\phi:\mathrm{Gal}(L/K)\to S_3\ ;\ \text{ただし}\phi(\sigma)=\rho_\sigma$$

を導く。さらに

$$\sigma \in \mathrm{Ker}(\phi) \ \Leftrightarrow\ \rho_\sigma(i) = i\ (\forall i) \ \Leftrightarrow\ \sigma(\alpha_i) = \alpha_i\ (\forall i) \ \Leftrightarrow\ \sigma = 1 : L \text{ 上の恒等写像}$$

となるから、ϕ は単射になる。いま

$$\Delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$$

とすると、任意の $\sigma \in \mathrm{Gal}(L/K)$ に対し $\sigma(\Delta) = \pm\Delta$、従って $\sigma(\Delta^2) = \Delta^2$ が成り立つから、$\Delta^2 \in K$ となる。実際 Δ^2 は K の元 a, b によって $\Delta^2 = -4a^3 - 27b^2$ と表され、これを $f(X)$ の**判別式**という。以下 K が 1 の原始 3 乗根 ζ を含むと仮定し、Δ の性質によって場合分けを行う。

- **Case 1**. $\Delta \notin K$ のとき

  $[L : K]$ は $[K(\Delta) : K] = 2$ の倍数になるから $[L : K] = 6$ が成り立つ。従って、写像 ϕ により $\mathrm{Gal}(L/K)$ と S_3 は同型になるから、L/K は Abel 拡大にならない。また

  $$(123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} : \Delta \mapsto \Delta, \quad (12) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} : \Delta \mapsto -\Delta,\ \alpha_3 \mapsto \alpha_3$$

  となるから、$\mathrm{Gal}(L/K) \cong S_3$ の部分群と対応する中間体は、

  $$\begin{array}{ccccccccc} S_3 & \supset & A_3 = \langle(123)\rangle, & \langle(12)\rangle, & \langle(13)\rangle, & \langle(23)\rangle & \supset & \{1\} \\ \updownarrow & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & & \updownarrow \\ K & \subset & K(\Delta), & K(\alpha_3), & K(\alpha_2), & K(\alpha_1) & \subset & L. \end{array}$$

  また 1 の原始 3 乗根 ζ に対して **Lagrange の分解式** $\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3$ を考えると、

  $$\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3 \overset{(123)}{\longmapsto} \alpha_2 + \zeta\alpha_3 + \zeta^2\alpha_1 = \zeta^2\left(\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3\right)$$

  となるから、$\left(\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3\right)^3 \in L^{\langle(123)\rangle} = K(\Delta)$ となり、計算により

  $$\left\{\left(\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3\right)^3,\ \left(\alpha_1 + \zeta^2\alpha_2 + \zeta\alpha_3\right)^3\right\} = \left\{-\frac{27}{2}b \pm \sqrt{-\frac{27}{4}}\Delta\right\}$$

  が分かる。また解と係数の関係より $\alpha_1 + \alpha_2 + \alpha_3 = 0$ となるから、

  $$\beta_1 = \sqrt[3]{-\frac{27}{2}b + \sqrt{-\frac{27}{4}}\Delta}, \quad \beta_2 = \sqrt[3]{-\frac{27}{2}b - \sqrt{-\frac{27}{4}}\Delta} \quad \left(\Rightarrow \beta_1^3\beta_2^3 = -27a^3\right)$$

  を $\beta_1\beta_2 = -3a$ を満たすように取ると、$X^3 + aX + b = 0$ の解 $\alpha_1, \alpha_2, \alpha_3$ は、

  $$\frac{1}{3}\left(\beta_1 + \beta_2\right), \quad \frac{1}{3}\left(\zeta\beta_1 + \zeta^2\beta_2\right), \quad \frac{1}{3}\left(\zeta^2\beta_1 + \zeta\beta_2\right)$$

  で与えられる。

- **Case 2**. $\Delta \in K$ のとき

  $$(123) : \Delta \mapsto \Delta, \quad (12) : \Delta \mapsto -\Delta$$

  より $\mathrm{Im}(\phi)$ は A_3 を含み (12) を含まないから、写像 ϕ により $\mathrm{Gal}(L/K)$ と A_3 は同型になる。L は K の 3 次 Kummer 拡大で、$f(X) = 0$ の解 α_i は上式で与えられる。

2.4. 代数方程式の可解性.

代数学の大問題. n 次方程式 $X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0$ の解の公式を求めよ。

- $n = 3$ のとき、Cardano(1501–1576) の公式（**2.3. 3 次方程式の分解体 Case 1**）。
- $n = 4$ のとき、Ferrari(1522–1565) の公式 (アイデア：4 次方程式の解 x_i $(1 \leq i \leq 4)$ から $(x_1 + x_2)(x_3 + x_4)$, $(x_1 + x_3)(x_2 + x_4)$, $(x_1 + x_4)(x_2 + x_3)$ を解に持つ 3 次方程式（還元方程式）を作り、3 次方程式の解法に帰着させる)。
- $n \geq 5$ のとき、解の公式が存在しないことを Ruffini(1765–1822)?, Abel(1802–1829) が証明：

  『其中の一つは一般［五次］方程式の［代数的］解法不可能の証明で、曾ってクリスチャニヤで印刷させたものよりは丁寧に証明を述べた。クレルレは、これは名誉の論文であるが、未だ十分に了解が出来ない所があるという。僕は随分骨を折って明瞭に説明した積りだけれども、何分人がこういう考え方に慣れていないから』(Abel, 1826 年 1 月 16 日)

  この論文は実際クレルレ誌第 1 巻に載せられた。有理区域又は体として知られている概念が論文の基調になっている外に、置換群の性質が用いられている。それらの新思想が当時余程分りにくかったものと見える。（高木貞治「近世数学史談」より）

解の公式とは？上の $a_0, ..., a_{n-1}$ を変数と見て、これらに四則（加減乗除）と巾乗根を取る操作を有限回施すことによって得られる、解を表す式のこと。

以下、Galois 理論と群論を用いて次の定理を示す。

定理 2.4.1. n が 5 以上のとき、n 次方程式の解の公式は存在しない。

注意. 「存在しない」≠「見つかっていない」（例：効率的な素因数分解の方法）

準備. 独立な変数 $x_1, ..., x_n$ に対し、

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = \prod_{i=1}^{n}(X - x_i) \quad \cdots\cdots (*)$$

によって a_i を定める（このとき $(-1)^{n-i}a_i$ は $x_1, ..., x_n$ の**基本対称式**と呼ばれる)。また

$$\begin{aligned} L &= \mathbb{C}(x_1, ..., x_n) = \left\{ \frac{f(x_1, ..., x_n)}{g(x_1, ..., x_n)} \;\middle|\; f, g \in \mathbb{C}[x_1, ..., x_n],\ g \neq 0 \right\} \\ &: n \text{ 変数有理関数体,} \\ K &= \mathbb{C}(a_0, ..., a_{n-1}) : L \text{ の部分体,} \\ S_n &= \{\sigma : \{1, ..., n\} \to \{1, ..., n\} : \text{全単射}\} : \text{写像の合成により群} \\ &: n \text{ 次対称群} \end{aligned}$$

とおく。

定理 2.4.2.

(1) S_n の各元 σ に対し、

$$\frac{f(x_1,...,x_n)}{g(x_1,...,x_n)} \mapsto \frac{f(x_{\sigma(1)},...,x_{\sigma(n)})}{g(x_{\sigma(1)},...,x_{\sigma(n)})}$$

は体の同型写像 $\varphi_\sigma : L \to L$ を与え、任意の $a \in K$ に対し、$\varphi_\sigma(a) = a$ が成り立つ。

(2) L は K の Galois 拡大で、$\sigma \mapsto \varphi_\sigma$ は群の同型写像 $\varphi : S_n \xrightarrow{\sim} \mathrm{Gal}\,(L/K)$ を与える。

証明. まず (1) を示す。φ_σ は体 L から L への準同型写像で、

$$x_i \overset{\varphi_\sigma}{\longmapsto} x_{\sigma(i)} \overset{\varphi_\tau}{\longmapsto} x_{\tau(\sigma(i))}$$

となるから、$\varphi_{\tau\sigma} = \varphi_\tau \circ \varphi_\sigma$ が成り立つ。よって φ_σ は $\varphi_{\sigma^{-1}}$ を逆写像として持つから、全単射になる。また

$$\varphi_\sigma\left(\prod_{i=1}^{n}(X - x_i)\right) = \prod_{i=1}^{n}(X - x_{\sigma(i)}) = \prod_{i=1}^{n}(X - x_i)$$

となるから、任意の $i = 1,...,n$ に対し $\varphi_\sigma(a_i) = a_i$ となる。従って、任意の $a \in K$ に対し $\varphi_\sigma(a) = a$ が成り立つ。

次に (2) を示す。L は $(*)$ の K 上の分解体だから、K の Galois 拡大になる。(1) の証明より $\varphi_{\tau\sigma} = \varphi_\tau \circ \varphi_\sigma$ だから、φ は群の準同型写像で、

$$\sigma \in \mathrm{Ker}(\varphi) \;\Leftrightarrow\; x_{\sigma(i)} = x_i \;\; (\forall i = 1,...,n) \;\Leftrightarrow\; \sigma(i) = i \;\; (\forall i)$$

より単射になる。また任意の $\rho \in \mathrm{Gal}(L/K)$ に対し、$\rho(a_i) = a_i$ より ρ は $(*)$ の解 $x_1,...,x_n$ の置換を与えるから、$\rho(x_i) = x_{\sigma(i)}$ $(i = 1,...,n)$ を満たす $\sigma \in S_n$ が存在し、$\varphi(\sigma) = \varphi_\sigma = \rho$ が成り立つ。従って、φ は全単射になる。 □

定理 2.4.1 の証明. $(*)$ の解の公式が存在すると仮定すると、

$$K = K_1 \subset K_2 \subset \cdots \subset K_m = L\,;\ \text{ただし } K_{i+1} = K_i(\sqrt[n_i]{\alpha_i}) \ \left(\alpha_i \in K_i^\times\right) \text{と表される}$$

を満たす L/K の中間体の増大列が存在する。よって定理 2.2.1 と 2.4.2 より

$$S_n \cong \mathrm{Gal}(L/K) \supset \mathrm{Gal}(L/K_2) \supset \cdots \supset \mathrm{Gal}(L/L) = \{1\}.$$

ここで $K \supset \mathbb{C}$ はすべての 1 の巾乗根を含むから、K_{i+1}/K_i は Kummer 拡大となり、$\mathrm{Gal}(K_{i+1}/K_i)$ は Abel 群になる。また定理 2.2.1 より、各 $i = 1,...,m-1$ に対し、

$$\mathrm{Gal}(L/K_i) \,/\, \mathrm{Gal}(L/K_{i+1}) \cong \mathrm{Gal}(K_{i+1}/K_i)$$

となるから、S_n は可解群、すなわち S_n の部分群 $H_1, ..., H_m$ で

$$(\sharp)\begin{cases} S_n = H_1 \supset H_2 \supset \cdots \supset H_m = \{1\}, \\ H_{i+1}\text{は}H_i\text{の正規部分群で、}H_i/H_{i+1}\text{は Abel 群} \end{cases}$$

を満たすものが存在する。一方次の定理 2.4.3 より、$n \geq 5$ のとき S_n は可解群にならないから、n 次方程式の解の公式は存在しない。 □

定理 2.4.3. $n \geq 5$ のとき、n 次対称群 S_n は可解群にならない。

証明. S_n が可解群になると仮定すると、$(\sharp)$ を満たす S_n の部分群 $H_1, ..., H_m$ が存在する。いま H_i が S_n のすべての 3 次巡回置換

$$(abc) = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \ ; \ a, b, c \text{ は } \{1, ..., n\} \text{ の相異なる元}$$

を含むと仮定する。$n \geq 5$ より、a, b, c 以外の $\{1, ..., n\}$ の 2 つの元 d, e が存在するから、$\sigma = (adb), \tau = (aec)$ とおくと、仮定より $\sigma, \tau \in H_i$ となり、さらに

$$\sigma^{-1}\tau^{-1}\sigma\tau = \overleftarrow{(abd)(ace)(adb)(aec)} = (abc)$$

が成り立つ。一方剰余群 H_i/H_{i+1} は Abel 群だから、その中では積が可換になる。従って、

$$(\sigma^{-1}\tau^{-1}\sigma\tau)H_{i+1} = (\tau^{-1}\sigma^{-1}\sigma\tau)H_{i+1} = (\tau^{-1}\tau)H_{i+1} = H_{i+1}$$

より $(abc) = \sigma^{-1}\tau^{-1}\sigma\tau \in H_{i+1}$ となるから、H_{i+1} もすべての 3 次巡回置換を含む。$S_n = H_1$ はすべての 3 次巡回置換を含むから、$H_m = \{1\}$ も同じ性質を満たすことになるが、これは矛盾である。 □

注意. Galois は、$n \geq 5$ のとき n 次交代群 A_n は単純群になる、すなわち $\{1\}, A_n$ 以外の正規部分群を持たない、ことを証明しており、定理 2.4.3 はこの命題から簡単に導かれる。

注意. Lagrange の分解式を用いることにより、次の定理を示すことができる：

$$\mathrm{Gal}(L/K) \text{ が可解群} \Rightarrow L \text{ は } K \text{ から Kummer 拡大を繰り返して得られる}$$

S_3 と S_4 は可解群になるので、解の公式 (Cardano, Ferrari) が存在することが分る。3 次方程式の解の公式は、2.3 の「3 次方程式の分解体」を参照せよ。また S_4 の部分群

$$N = \{(1),\ (12)(34),\ (13)(24),\ (14)(23)\} \ : \text{ 位数 4 の Abel 群}$$

は S_4 の正規部分群で $S_4/N \cong S_3$ を満たすから、3 次方程式の解の公式を用いて 4 次方程式を解くことができる。

問題. S_3, S_4 が可解群になることを示せ。

注意. 5 次方程式 $X^5 - X - 1 = 0$ の分解体の $\mathbb{Q}$ 上の Galois 群は、S_5 と同型になることが分かるので、定理 2.4.1（の証明）よりこの方程式の解である代数的数は、有理数から加減乗除と巾乗根を取る操作を繰り返して得ることはできない。

2.5. 有限体.

有限体. 有限個の元から成る体のこと。

例 **1**. 素数 p に対し、

$$\mathbb{Z}/(p) = \{\overline{a} = a + (p) \mid a \in \mathbb{Z}\} = \left\{\overline{0}, \overline{1}, ..., \overline{p-1}\right\}$$

は位数 p の体になる。これを $\mathbb{F}_p$ と書く。

証明. $\mathbb{F}_p^{\times} = \mathbb{F}_p - \left\{\overline{0}\right\}$ が乗法 $\overline{a} \cdot \overline{b} = \overline{ab}$ について群になることを示す。$\overline{a} \neq \overline{0}$ に対し、a は素数 p で割り切れないから、両者の最大公約数は 1 に等しい。よって定理 1.1.1 の応用より、

$$ma + np = 1$$

を満たす整数 m, n が存在するから、$\mathbb{F}_p$ において $\overline{m} \cdot \overline{a} = \overline{1}$ が成り立ち、$(\overline{a})^{-1} = \overline{m} \in \mathbb{F}_p^{\times}$ となる。 □

例 **2**. 定理 1.4.1 を用いて $\mathbb{F}_p$ の拡大体を作る。$f(X)$ を $\mathbb{F}_p$ 上の n 次既約多項式とすると、$L = \mathbb{F}_p[X]/(f(X))$ は $\mathbb{F}_p$ の n 次拡大体で、集合として

$$\{a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \mid a_i \in \mathbb{F}_p\}$$

と表されるから、その位数は p^n に等しい。L を $\mathbb{F}_{p^n}$ または $\mathrm{GF}(p^n)$ と書く。

疑問. 位数 p^n の体は複数個あるかも知れないのに、同じ記号で書いていいのか？
答えは**いいんです！** 理由：有限体の構造はその位数のみで決まるから（定理 2.5.1）

例 **2** の応用. $\mathbb{F}_2 = \left\{\overline{0}, \overline{1}\right\} = \{0, 1\}$ の拡大体を作る。

- $\mathbb{F}_2$ 上の 2 次既約多項式は、$X^2 + X + 1$ の唯 1 つで、

$$\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1) = \{a + bX \mid a, b \in \mathbb{F}_2\} = \{0, 1, X, X + 1\}.$$

- $\mathbb{F}_2$ 上の 3 次既約多項式は、$X^3 + X^2 + 1$, $X^3 + X + 1$ の 2 つで、

$$\begin{array}{ccccc} \mathbb{F}_8 & = & \mathbb{F}_2[X]/(X^3 + X^2 + 1) & \cong & \mathbb{F}_2[X]/(X^3 + X + 1) \\ & & g(X) & \leftrightarrow & g(X + 1). \end{array}$$

問題. 位数 9 の体を上のようにして作れ。

疑問. このやり方で全ての有限体が作れるのか？ 答えは **YES**（定理 2.5.1）

位数とその性質. G を有限 Abel 群とし、その位数を $|G|$ と書く。このとき G の元 α に対し、次が成り立つ。

(1) $\alpha^{|G|}$ は G の単位元 e に等しい。

(2) α の**位数** d を

$$d = \min\{m \in \mathbb{N} \mid \alpha^m = e\}$$

で定めるとき、$\alpha^m = e$ を満たす整数 m は d で割り切れる。

証明. まず (1) を示す。$G = \{a_1, ..., a_{|G|}\}$ とすると、αa_i $(i = 1, ..., g)$ は a_i $(i = 1, ..., g)$ を並べ替えたものになるから、

$$\alpha^{|G|} a_1 \cdots a_{|G|} = (\alpha a_1) \cdots (\alpha a_{|G|}) = a_1 \cdots a_{|G|}.$$

従って $\alpha^{|G|} = e$ が成り立つ。

次に (2) を示す。m を d で割り、$m = qd + r$, $0 \leq r < d$ を満たす整数 q, r をとると、

$$e = \alpha^m = \alpha^{qd+r} = (\alpha^d)^q \cdot \alpha^r = \alpha^r.$$

従って d の最小性より $r = 0$ が成り立つ。 □

注意. α で生成される G の部分群 $\langle \alpha \rangle$ の位数は d に等しいから、G が Abel 群でなくても、Lagrange の定理より d は $|G|$ を割り切る。従って補題は一般の有限群に対して成り立つ。

定理 2.5.1 (Galois?).

(1) 任意の有限体の位数は、ある素数の巾乗になる。

(2) 任意の素数 p と自然数 n に対し、位数 p^n の体が存在し、それらは互いに同型になる。

(3) 任意の素数 p と自然数 n に対し、$\mathbb{F}_p$ 上の n 次既約多項式 $f(X)$ が存在する。従って、このとき $\mathbb{F}_p[X]/(f(X))$ は位数 p^n の体 $\mathbb{F}_{p^n}$ になる。

証明. まず (1) を示す。K を有限体とし、K の加法における 1 の位数を p とする。すなわち

$$p = \min\{m \in \mathbb{N} \mid m \cdot 1 = 0\}.$$

このとき p が素数になることを示す。もし p が素数でないとすると、$p = l_1 l_2$ を満たす自然数 $1 < l_1, l_2 < p$ が存在するから、

$$(l_1 \cdot 1)(l_2 \cdot 1) = p \cdot 1 = 0$$

となるが、p の性質（最小性）より $l_1 \cdot 1$ と $l_2 \cdot 1$ は 0 でないから、K が体であることに矛盾する。従って p は素数になる（これを K の**標数**という）。このとき各整数 a に対し $a \cdot 1$ を対応させる写像 $\mathbb{Z} \to K$ は環の準同型写像となり、その核 (kernel) は p の倍数から成るイデアル (p) に等しいから、体の単射準同型写像

$$\mathbb{F}_p = \mathbb{Z}/(p) \to K$$

が存在し、K は $\mathbb{F}_p$ の拡大体になる。その拡大次数 $[K : \mathbb{F}_p] = \dim_{\mathbb{F}_p} K$ を n とし、$\mathbb{F}_p$ 上の線形空間 K の基底を $\{u_1, ..., u_n\}$ とすると、K の各元は

$$a_1 u_1 + \cdots + a_n u_n \ (a_i \in \mathbb{F}_p)$$

の形に一意的に表されるから、K の位数は p^n に等しい。

次に (2) を示す。K を位数 $q = p^n$ の体とすると、$K^\times = K - \{0\}$ は乗法について群となり、その位数は $q-1$ だから、「位数の性質」より $K^\times$ の各元 a は $a^{q-1} = 1$ を満たす。従って K の任意の元は $X^q - X = 0$ の解になる。一方 $\mathbb{F}_p$ 上の多項式 $X^q - X$ の導関数は

$$(X^q - X)' = qX^{q-1} - 1 = -1$$

となるから解を持たない。従って $X^q - X = 0$ は重解を持たないから、q 個の相異なる解を持ち、これが K のすべての元を与える。従って K は $X^q - X$ の分解体として（同型を除いて）一意的に構成される。

最後に (3) を示す。後述の定理 3.2.1 より乗法群 $\mathbb{F}_{p^n}^\times = \mathbb{F}_{p^n} - \{0\}$ は巡回群になるから、その生成元の 1 つを α とすると、

$$\mathbb{F}_{p^n} \supset \mathbb{F}_p(\alpha) \supset \{0, \alpha^m \mid m : \text{自然数}\} = \mathbb{F}_{p^n}^\times \cup \{0\} = \mathbb{F}_{p^n}$$

となるから、$\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ が成り立つ。よって定理 1.4.2 より、α の $\mathbb{F}_p$ の最小多項式 $f(X)$ は n 次既約多項式になり、$\mathbb{F}_{p^n} \cong \mathbb{F}_p[X]/(f(X))$ が成り立つ。 □

定理 2.5.2. q を素数 p の n 乗とする。

(1) $\mathbb{F}_q$ から $\mathbb{F}_q$ への写像 $F(a) = a^p$ は、体の同型写像を与える。（F を **Frobenius 写像**という）

(2) $\mathbb{F}_q$ は $\mathbb{F}_p$ の n 次 Galois 拡大となり、$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ は Frobenius 写像 F を生成元とする位数 n の巡回群になる。

証明. まず (1) を示す。$a, b \in \mathbb{F}_q$ に対し、

$$F(1) = 1^p = 1, \quad F(ab) = (ab)^p = a^p b^p = F(a)F(b).$$

また 2 項定理と、2 項係数 $\left(\begin{array}{c} p \\ k \end{array} \right) = \dfrac{p!}{k!(p-k)!}$ が $1 \leq k \leq p-1$ のとき p で割り切れることを用いると、

$$F(a+b) = (a+b)^p = a^p + \sum_{k=1}^{p-1} \left(\begin{array}{c} p \\ k \end{array} \right) a^{p-k} b^k + b^p = a^p + b^p = F(a) + F(b).$$

従って F は体の準同型写像になる。また定理 2.5.1 (2) の証明より、$\mathbb{F}_q$ の任意の元 a は $a^q = a$ を満たすから、

$$F^n(a) = a^{p^n} = a^q = a$$

が成り立つ。従って F は F^{n-1} を逆写像に持つから全単射になり、F は同型写像になる。

次に (2) を示す。$\mathbb{F}_p^\times$ は位数 $p-1$ の乗法群だから、「位数の性質」より

$$a \in \mathbb{F}_p^\times \;\Rightarrow\; a^{p-1} = 1 \text{ (Fermat の小定理)} \;\Rightarrow\; F(a) = a^p = a.$$

よって (1) より $F \in \mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$ となる。ここで F の位数を m とすると、F^m は $\mathbb{F}_q$ 上の恒等写像になるから、

$$\alpha \in \mathbb{F}_q \ \Rightarrow \ F^m(\alpha) = \alpha^{p^m} = \alpha.$$

従って $\mathbb{F}_q$ の各元は p^m 次の多項式 $X^{p^m} - X = 0$ の解になるから、因数定理より $q = p^n \leq p^m$ すなわち $n \leq m$ が成り立つ。一方定理 2.1.1 の注意より

$$m = \left|\{1, F, ..., F^{m-1}\}\right| \leq |\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)| \leq [\mathbb{F}_q : \mathbb{F}_p] = n$$

が成り立つから、F の位数は $m = n$ となり、$\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$ は F で生成される巡回群になる。また $|\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)| = n$ が成り立つから、$\mathbb{F}_q/\mathbb{F}_p$ は Galois 拡大になる。 □

問題. 素数 p と自然数 m, n に対し、

$$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \ \Leftrightarrow \ m \text{ は } n \text{ の約数}$$

が成り立ち、このとき $\mathrm{Gal}\,(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ は F^m で生成される位数 n/m の巡回群になることを示せ。

§3. 円分体と類体論

3.1. 正 17 角形の作図.

円分体. **円分体**とは、複素平面上の単位円 $\{z \in \mathbb{C} \mid |z| = 1\}$ を n 等分して得られる複素数

$$\zeta_n = e^{2\pi\sqrt{-1}/n} = \cos(2\pi/n) + \sqrt{-1}\sin(2\pi/n)$$

から生成される体 $\mathbb{Q}(\zeta_n)$ のこと。

$$\zeta_n^0 = 1,\ \zeta_n^1 = \zeta_n,\ \zeta_n^2,\ ...,\ \zeta_n^{n-1}$$

は $X^n - 1 = 0$ のすべての解を与えるから、$\mathbb{Q}(\zeta_n)$ は $X^n - 1$ の分解体として $\mathbb{Q}$ の Galois 拡大になる。

歴史.

- 正 17 角形の作図 (Gauss):

  1796 年 3 月 30 日の朝、十九歳の青年ガウスが目ざめて臥床から起き出でようとする刹那に正十七角形の作図法に思い付いた。

  『 … その後凡ての根の整数論的の関係を専心考究している中に休暇にブラウンシュワィヒに帰省していた時、上記の日の朝（臥床を出る前）この関係を明瞭に看破することに成功した。それを特に十七角形に適用して数値を算出することは即座に出来たのである。』(Gauss)（高木貞治「近世数学史談より）

- Fermat 予想へのアプローチ (Kummer),
- 有理数体 $\mathbb{Q}$ の類体論 (Kronecker),
- p 進円分体の p 進類体論 (岩澤).

定理 3.1.1. 素数 p に対し、$\zeta = \zeta_p = e^{2\pi\sqrt{-1}/p}$ とするとき、

(1) $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ が成り立つ。より詳しく

$$\begin{cases} 1, \zeta, \zeta^2, ..., \zeta^{p-2} \text{ は } \mathbb{Q}(\zeta) \text{ の } \mathbb{Q} \text{ 上の基底を与える,} \\ 1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0. \end{cases}$$

(2) 2.3 の「円分拡大」における写像

$$\varphi : \mathrm{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q}) \to \mathbb{F}_p^\times \ ;\ \text{ただし } \sigma \in \mathrm{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q}) \text{ に対し } \sigma(\zeta) = \zeta^{\varphi(\sigma)}$$

は群の同型写像を与える。

複素数の作図. 複素数 $\alpha = a + b\sqrt{-1} = re^{\sqrt{-1}\theta}$ に対し、

$$\begin{aligned} \alpha \text{ が複素平面上で作図可能} &\Leftrightarrow \text{実部 } a \text{ と虚部 } b \text{ が作図可能} \\ &\Leftrightarrow \text{絶対値 } r \text{ と偏角 } \theta \text{ が作図可能} \\ &\Leftrightarrow \sqrt{r} \text{ と } \theta/2 \text{ が作図可能} \\ &\Leftrightarrow \sqrt{\alpha} \text{ が複素平面上で作図可能.} \end{aligned}$$

従って、定理 1.6.2 と同様の方法で次が示される。

定理 3.1.2. 複素数 α に対し、次の (1)〜(3) は同値な条件になる。

(1) α が作図可能。

(2)
$$\begin{cases} \mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}, \\ \text{ただし } K_{i+1} \text{は } K_i \text{の元 } a_i \text{によって } K_{i+1} = K_i\left(\sqrt{a_i}\right) \text{と表される} \end{cases}$$
を満たす体の拡大列で、$\alpha \in K_n$ を満たすものが存在する。

(3) $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ が 2 の巾乗。

系 (Gauss). 素数 p に対し、

$$\text{正 } p \text{ 角形が作図可能 } (\Leftrightarrow\ e^{2\pi\sqrt{-1}/p} \text{が作図可能}) \ \Leftrightarrow\ p-1 \text{ が 2 の巾乗.}$$

Fermat 素数. 2 の巾乗 + 1 の形の素数。知られているものは次の 5 つ。

$$2^{2^0}+1 = 3,\ 2^{2^1}+1 = 5,\ 2^{2^2}+1 = 17,\ 2^{2^3}+1 = 257,\ 2^{2^4}+1 = 65537.$$

正 17 角形の作図 (Gauss). $e^{2\pi\sqrt{-1}/17}$ を平方根で表すため、Galois 理論 (の考え方) を用いて

$$\mathbb{Q} \subset K_1 \subset K_2 \subset K_3 \subset \mathbb{Q}\left(e^{2\pi\sqrt{-1}/17}\right)$$

を満たす 2 次拡大の列を求める。

$$\begin{aligned} \mathbb{F}_{17} &= \mathbb{Z}/(17) = \{\overline{a} = a + (17) \mid a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{16}\} \ :\ \text{位数 17 の体,} \\ \mathbb{F}_{17}^{\times} &= \mathbb{F} - \{\overline{0}\} \ :\ \text{位数 16 の乗法群} \end{aligned}$$

とするとき、

大切な事実. $\mathbb{F}_{17}^{\times}$ は巡回群で、$\overline{3}$ はその生成元の 1 つ。

よって $\mathbb{F}_{17}^{\times}$ の部分群は、$16 = 2^4$ の約数を位数に持つ次の 5 個になる。

$$\begin{aligned} \mathbb{F}_{17}^{\times} &\supset H_1 = \left\langle \overline{3}^2 \right\rangle = \left\langle \overline{9} \right\rangle = \left\{\overline{1}, \overline{9}, \overline{13}, \overline{15}, \overline{16}, \overline{8}, \overline{4}, \overline{2}\right\} : \text{位数 } 8 \\ &\supset H_2 = \left\langle \overline{3}^4 \right\rangle = \left\langle \overline{13} \right\rangle = \left\{\overline{1}, \overline{13}, \overline{16}, \overline{4}\right\} : \text{位数 } 4 \\ &\supset H_3 = \left\langle \overline{3}^8 \right\rangle = \left\langle \overline{16} \right\rangle = \left\{\overline{1}, \overline{16}\right\} : \text{位数 } 2 \\ &\supset \left\{\overline{1}\right\}. \end{aligned}$$

$\zeta = e^{2\pi\sqrt{-1}/17}$ とすると、定理 3.1.1 (2) より

$$\varphi : \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{F}_{17}^{\times}\ ;\ \text{ただし} \zeta^{\varphi(\sigma)} = \sigma(\zeta).$$

よって K_i を $\varphi^{-1}(H_i)$ による $\mathbb{Q}(\zeta)$ の不変体とすると、Galois 対応（定理 2.2.1）より

$$\begin{array}{ccccccccc} \mathbb{F}_{17}^{\times} & \supset & H_1 = \langle\overline{9}\rangle & \supset & H_2 = \langle\overline{13}\rangle & \supset & H_3 = \langle\overline{16}\rangle & \supset & \{\overline{1}\} \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ \mathbb{Q} & \subset & K_1 & \subset & K_2 & \subset & K_3 & \subset & \mathbb{Q}(\zeta). \end{array}$$

また $\varphi^{-1}(H_i)$ の各元 σ に対し、$\varphi(\sigma) \cdot H_i = H_i$ となるから、

$$\sigma\left(\sum_{a\in H_i} \zeta^a\right) = \sum_{a\in H_i} \sigma(\zeta)^a = \sum_{a\in H_i} \zeta^{\varphi(\sigma)a} = \sum_{a\in H_i} \zeta^a.$$

従って $\sum_{a\in H_i} \zeta^a \in K_i$ となるから、

$$\begin{cases} \alpha &= \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2 & \in K_1, \\ \beta &= \zeta + \zeta^{13} + \zeta^{16} + \zeta^4 & \in K_2, \\ \gamma &= \zeta + \zeta^{16} & \in K_3. \end{cases}$$

一方、$\sigma = \varphi^{-1}\left(\overline{3}\right) \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ は $\sigma(\zeta) = \zeta^3$ を満たすから、

$$\sigma(\alpha) = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6$$

となる。よって定理 3.1.1 より $\sigma(\alpha) \neq \alpha$ が成り立つから、$\alpha \notin \mathbb{Q}$ となる。

問題. 上の $\beta \in K_2$, $\gamma \in K_3$ に対し、$\beta \notin K_1$, $\gamma \notin K_2$ を示せ。

従って $\mathbb{Q} \subset K_1 \subset K_2 \subset K_3 \subset \mathbb{Q}(\zeta)$ が 2 次の拡大体の増大列であることから、

$$K_1 = \mathbb{Q}(\alpha),\quad K_2 = K_1(\beta) = \mathbb{Q}(\alpha, \beta),\quad K_3 = K_2(\gamma) = \mathbb{Q}(\alpha, \beta, \gamma)$$

が成り立ち、平方根を用いて下記のように α, β, γ が表される。

Step 1. $\sigma = \varphi^{-1}\left(\overline{3}\right)$ は位数 2 の群 $\mathrm{Gal}(K_1/\mathbb{Q}) \cong \mathbb{F}_{17}^{\times}/\langle\overline{9}\rangle$ の生成元を与え、$\alpha + \sigma(\alpha)$, $\alpha \cdot \sigma(\alpha)$ は σ の作用で不変となるから $\mathbb{Q}$ に属する。定理 3.1.1 (1) を用いて計算すると、

$$\sigma(\alpha) = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6 = \sum_{k=1}^{16} \zeta^k - \alpha = -1 - \alpha.$$

$$\therefore\ \sigma(\alpha) \cdot \alpha = -\alpha - \alpha^2 = -4.$$

従って α と $\sigma(\alpha)$ は $X^2 + X - 4 = 0$ の解で、

$$\alpha = \zeta + \zeta^{16} + \zeta^2 + \zeta^{15} + \zeta^4 + \zeta^{13} + \zeta^8 + \zeta^9 = 2\left(\cos\frac{2\pi}{17} + \cos\frac{4\pi}{17} + \cos\frac{8\pi}{17} + \cos\frac{16\pi}{17}\right)$$

は正だから、

$$\alpha = \frac{-1+\sqrt{17}}{2}.$$

Step 2. $\sigma = \varphi^{-1}\left(\overline{9}\right)$ は位数 2 の群 $\mathrm{Gal}(K_2/K_1) \cong \left\langle\overline{9}\right\rangle / \left\langle\overline{13}\right\rangle$ の生成元を与え、$\alpha+\sigma(\alpha)$, $\alpha\cdot\sigma(\alpha)$ は σ の作用で不変となるから K_1 に属する。定理 3.1.1 (1) を用いて計算すると、

$$\sigma(\beta) = \zeta^9+\zeta^{15}+\zeta^8+\zeta^2 = \alpha-\beta. \quad \therefore\ \sigma(\beta)\cdot\beta = \alpha\beta-\beta^2 = -1.$$

従って β と $\sigma(\beta)$ は $X^2-\alpha X-1=0$ の解で、$\beta>0$ だから

$$\beta = \frac{\alpha+\sqrt{\alpha^2+4}}{2} = \frac{1}{4}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\right).$$

Step 3. $\sigma = \varphi^{-1}\left(\overline{13}\right)$ は位数 2 の群 $\mathrm{Gal}(K_3/K_2) \cong \left\langle\overline{13}\right\rangle / \left\langle\overline{16}\right\rangle$ の生成元を与え、$\alpha+\sigma(\alpha)$, $\alpha\cdot\sigma(\alpha)$ は σ の作用で不変となるから K_2 に属する。定理 3.1.1 (1) を用いて計算すると、

$$\sigma(\gamma) = \zeta^{13}+\zeta^4 = \beta-\gamma. \quad \therefore\ \sigma(\gamma)\cdot\gamma = \beta\gamma-\gamma^2 = \frac{1}{2}(-\alpha+\beta+\alpha\beta-3).$$

従って γ と $\sigma(\gamma)$ は

$$X^2-\beta X+\frac{1}{2}(-\alpha+\beta+\alpha\beta-3)=0$$

の解で、$\gamma>\sigma(\gamma)$ を満たすから

$$\begin{aligned}\cos\frac{2\pi}{17} &= \frac{\gamma}{2}\\ &= \frac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\right)\\ &\quad+\frac{1}{16}\sqrt{68+12\sqrt{17}-6\sqrt{34-2\sqrt{17}}-2\sqrt{17(34-2\sqrt{17})}}.\end{aligned}$$

問題.

$$\alpha = \beta-\frac{1}{\beta} = \beta^3+\beta^2-5\beta-1, \quad \beta = \gamma+(\gamma^2-2)^2-2 = \gamma^4-4\gamma^2+\gamma+2$$

を示すことにより、$K_2=\mathbb{Q}(\beta)$, $K_3=\mathbb{Q}(\gamma)$ を証明せよ。

問題. 上の $\cos(2\pi/17)$ の値と Gauss が求めた値

$$\begin{aligned}\cos\frac{2\pi}{17} &= \frac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}\right)\\ &\quad+\frac{1}{8}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.\end{aligned}$$

が等しいことを示せ。

3.2. 円分体と 2 次体.

目標.

$$\text{円分体}\ \mathbb{Q}\left(e^{2\pi\sqrt{-1}/17}\right)\ \supset\ \text{2 次体}\ \mathbb{Q}\left(\sqrt{17}\right)$$

を一般の素数に拡張すること。

定理 3.2.1. 素数 p に対し、$\mathbb{F}_p^\times$ は巡回群（一般の有限体 $\mathbb{F}_q$ に対し $\mathbb{F}_q^\times$ も巡回群)。

注意. $\overline{2}$ または $\overline{3}$ が生成元になることが多い（なぜか？）

補題. p を素数、d を $p-1$ の正の約数とするとき、X^d-1 は d 個の $\mathbb{F}_p$ 上の解を持つ。

証明. $e=(p-1)/d$ とすると、

$$X^{p-1}-1=\underbrace{\left(X^d-1\right)}_{(1)}\underbrace{\left((X^d)^{e-1}+(X^d)^{e-2}+\cdots+X^d+1\right)}_{(2)}.$$

因数定理より $(1)=0$, $(2)=0$ の解の個数はそれぞれ d, $d(e-1)$ 以下になる。一方 $\mathbb{F}_p^\times$ の $p-1$ 個の元が左辺 $=0$ のすべての解を与えるから、(1) も $\mathbb{F}_p$ 上 d 個の解を持つ。 □

定理の証明. $p-1$ の素因数分解を $q_1^{e_1}q_2^{e_2}\cdots q_n^{e_n}$ とすると、補題より各 $i=1,...,n$ に対し、

$$\left\{a\in\mathbb{F}_p^\times\mid a^{q_i^{e_i-1}}=1\right\}\subset\left\{a\in\mathbb{F}_p^\times\mid a^{q_i^{e_i}}=1\right\}$$

の左辺の位数は $q_i^{e_i-1}$, 右辺の位数は $q_i^{e_i}$ となるから、位数が $q_i^{e_i}$ となる $\mathbb{F}_p^\times$ の元 α_i が存在する。このとき

$$\alpha=\alpha_1\alpha_2\cdots\alpha_n\in\mathbb{F}_p^\times$$

の位数が $p-1$ になることを示せばよい。

まず α の位数は $p-1$ の約数だから、

$$q_1^{d_1}q_2^{d_2}\cdots q_n^{d_n}\ ;\ \text{ただし}\ d_i\le e_i$$

の形に表される。このとき

$$1=\left(\alpha^{q_1^{d_1}q_2^{d_2}\cdots q_n^{d_n}}\right)^{q_2^{e_2-d_2}\cdots q_n^{e_n-d_n}}=\alpha^{q_1^{d_1}q_2^{e_2}\cdots q_n^{e_n}}=\alpha_1^{q_1^{d_1}q_2^{e_2}\cdots q_n^{e_n}}\cdot\left(\alpha_2^{q_2^{e_2}}\right)^{q_1^{d_1}q_3^{e_3}\cdots q_n^{e_n}}\cdots$$

となるが、$\alpha_i^{q_i^{e_i}}=1$ が成り立つから、

$$1=\alpha^{q_1^{d_1}q_2^{e_2}\cdots q_n^{e_n}}.$$

従って $q_1^{d_1}q_2^{e_2}\cdots q_n^{e_n}$ が α_1 の位数 $q_1^{e_1}$ の倍数になるから、$d_1=e_1$ が成り立つ。同様に任意の $i=1,...,n$ に対し $d_i=e_i$ となるから、α の位数は

$$q_1^{d_1}q_2^{d_2}\cdots q_n^{d_n}=q_1^{e_1}q_2^{e_2}\cdots q_n^{e_n}=p-1$$

に等しい。 □

系. p を奇素数とするとき、

$$\left(\mathbb{F}_p^{\times}\right)^2 = \left\{\alpha^2 \mid \alpha \in \mathbb{F}_p^{\times}\right\}$$

の位数は $(p-1)/2$ に等しい。

例. $\mathbb{F}_{17}^{\times} = \langle \overline{3} \rangle$ なので、$\mathbb{F}_{17}^{\times} = \left\langle \overline{3}^2 \right\rangle = \left\{\overline{1}, \overline{9}, \overline{13}, \overline{15}, \overline{16}, \overline{8}, \overline{4}, \overline{2}\right\}$.

Legendre 記号. p を奇素数とするとき、$\alpha \in \mathbb{F}_p$ に対し、

$$\left(\frac{\alpha}{p}\right) := \begin{cases} 1 & \left(\alpha \in \left(\mathbb{F}_p^{\times}\right)^2 \text{ のとき}\right), \\ -1 & \left(\alpha \in \mathbb{F}_p^{\times} - \left(\mathbb{F}_p^{\times}\right)^2 \text{ のとき}\right), \\ 0 & \left(\alpha = \overline{0} \text{ のとき}\right). \end{cases}$$

また $a \in \mathbb{Z}$ に対し、

$$\left(\frac{a}{p}\right) := \left(\frac{\overline{a}}{p}\right)$$

と定義し、この値が $1, -1$ のとき、a は p を法としてそれぞれ**平方剰余、平方非剰余**であるという。

定理 3.2.2. p を奇素数とする。

(1) $\alpha, \beta \in \mathbb{F}_p$ に対し、$\left(\frac{\alpha\beta}{p}\right) = \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right)$.

(2) $\alpha \in \mathbb{F}_p^{\times}$ に対し、$\left(\frac{\alpha}{p}\right) = \left(\frac{\alpha^{-1}}{p}\right)$.

(3) $\left(\frac{-1}{p}\right) = 1 \ \Leftrightarrow \ p \equiv 1 \bmod(4)$.

証明. まず (1) を示す。$\left(\mathbb{F}_p^{\times}\right)^2$ は $\mathbb{F}_p^{\times}$ の指数 2 の部分群だから、剰余群 $\mathbb{F}_p^{\times}/\left(\mathbb{F}_p^{\times}\right)^2$ は乗法群 $\{\pm 1\}$ と同型になる。従って Legendre 記号の定義より、$\alpha \in \mathbb{F}_p^{\times}$ に $\left(\frac{a}{p}\right)$ を対応させる写像は、自然な準同型写像

$$\mathbb{F}_p^{\times} \to \mathbb{F}_p^{\times}/\left(\mathbb{F}_p^{\times}\right)^2 \cong \{\pm 1\}$$

に等しい。よって (1) は $\alpha, \beta \neq 0$ のとき成り立つ。また $\alpha = 0$ または $\beta = 0$ のときも、(1) の両辺は 0 になり等しい。

次に (2) を示す。(1) より

$$\left(\frac{\alpha}{p}\right)\left(\frac{\alpha^{-1}}{p}\right) = \left(\frac{1}{p}\right) = 1$$

が成り立ち、$\left(\frac{a}{p}\right) = \pm 1$ だから、(2) が成り立つ。

最後に (3) を示す。定理 3.2.1 より $\mathbb{F}_p^\times$ は位数 $p-1$ の巡回群だから、

$$\begin{aligned}\left(\frac{-1}{p}\right)=1 \quad &\Leftrightarrow \quad \alpha^2=-1 \text{ となる元 } \alpha\in\mathbb{F}_p^\times \text{が存在する}\\ &\Leftrightarrow \quad \text{位数 } 4 \text{ の元 } \alpha\in\mathbb{F}_p^\times \text{が存在する}\\ &\Leftrightarrow \quad p-1 \text{ が } 4 \text{ で割り切れる}\\ &\Leftrightarrow \quad p\equiv 1 \bmod(4).\ \square\end{aligned}$$

Gauss の和. 奇素数 p に対し、$\zeta_p=e^{2\pi\sqrt{-1}/p}$ とするとき、

$$g_p:=\sum_{\alpha\in\mathbb{F}_p^\times}\left(\frac{\alpha}{p}\right)\zeta_p^\alpha\in\mathbb{C}.$$

定理 3.2.3. p を奇素数とする。

(1) $\overline{g_p}=\left(\dfrac{-1}{p}\right)g_p=\begin{cases} g_p & (p\equiv 1 \bmod(4)\text{ のとき}),\\ -g_p & (p\equiv 3 \bmod(4)\text{ のとき}).\end{cases}$

(2) $|g_p|^2=p$.

(3) $g_p=\begin{cases} \pm\sqrt{p} & (p\equiv 1 \bmod(4)\text{ のとき}),\\ \pm\sqrt{-p} & (p\equiv 3 \bmod(4)\text{ のとき}).\end{cases}$

注意. (3) の符号は共にプラス (Gauss)。

証明. まず (1) を示す。$\overline{\zeta_p}=\zeta_p^{-1}$ だから、定理 3.2.2 (1) より

$$\overline{g_p}=\sum_{\alpha\in\mathbb{F}_p^\times}\left(\frac{\alpha}{p}\right)\zeta_p^{-\alpha}=\sum_{\alpha\in\mathbb{F}_p^\times}\left(\frac{-1}{p}\right)\left(\frac{-\alpha}{p}\right)\zeta_p^{-\alpha}=\left(\frac{-1}{p}\right)\sum_{-\alpha\in\mathbb{F}_p^\times}\left(\frac{-\alpha}{p}\right)\zeta_p^{-\alpha}=\left(\frac{-1}{p}\right)g_p.$$

次に (2) を示す。上式と定理 3.3.2 (1), (2) より

$$g_p\overline{g_p}=\sum_{\alpha,\beta\in\mathbb{F}_p^\times}\left(\frac{\alpha\beta}{p}\right)\zeta_p^{\alpha-\beta}=\sum_{\alpha,\beta\in\mathbb{F}_p^\times}\left(\frac{\alpha\beta^{-1}}{p}\right)\zeta_p^{\alpha-\beta}.$$

ここで $\gamma=\alpha\beta^{-1}$ とおくと、$\alpha-\beta=\beta\gamma-\beta$ となるから、

$$\text{上式}=\sum_{\beta,\gamma\in\mathbb{F}_p^\times}\left(\frac{\gamma}{p}\right)\zeta_p^{\beta\gamma-\beta}=\sum_{\beta\in\mathbb{F}_p^\times}\left(\frac{1}{p}\right)+\sum_{\gamma\in\mathbb{F}_p^\times-\{1\}}\left(\frac{\gamma}{p}\right)\sum_{\beta\in\mathbb{F}_p^\times}\zeta_p^{\beta(\gamma-1)}.$$

$\gamma\neq 1$ のとき $\displaystyle\sum_{\beta\in\mathbb{F}_p}\zeta_p^{\beta(\gamma-1)}=0$ で、定理 3.3.1 の系より $\displaystyle\sum_{\gamma\in\mathbb{F}_p^\times}\left(\frac{\gamma}{p}\right)=0$ となるから、

$$\text{上式}=p-1-\sum_{\gamma\in\mathbb{F}_p^\times-\{1\}}\left(\frac{\gamma}{p}\right)=p.$$

最後に (3) は (1), (2) より従う。 □

系. 奇素数 p に対し、

$$\mathbb{Q}\left(\sqrt{\left(\frac{-1}{p}\right)p}\right) = \mathbb{Q}(g_p) \subset \mathbb{Q}(\zeta_p) = \mathbb{Q}\left(e^{2\pi\sqrt{-1}/p}\right).$$

定理 3.2.4. $\mathbb{Q}$ の任意の 2 次拡大 K に対し、$K \subset \mathbb{Q}\left(e^{2\pi\sqrt{-1}/n}\right)$ を満たす自然数 n が存在する。

この定理は次のように拡張されている：

定理 (Kronecker-Weber). $\mathbb{Q}$ の任意の **Abel 拡大** (Galois 群が Abel 群になる Galois 拡大) K に対し、$K \subset \mathbb{Q}\left(e^{2\pi\sqrt{-1}/n}\right)$ を満たす自然数 n が存在する。

3.3. 円分体と類体論.

円分体. 一般の自然数 n に対し $\zeta_n = e^{2\pi\sqrt{-1}/n}$ とおくとき、$\mathbb{Q}(\zeta_n)$ を n 次の円分体と呼ぶ。

定理 3.3.1.

(1) $\mathbb{Q}(\zeta_n)$ は有理数体 $\mathbb{Q}$ の Galois 拡大。

(2) 体の拡大次数 $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ は、**Euler の関数** $\varphi(n) = |(\mathbb{Z}/(n))^\times|$ に等しい。

(3) 2.3「円分拡大」において定義された群の準同型写像

$$\varphi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/(n))^\times \ ; \ \text{ただし } \sigma(\zeta_n) = \zeta_n^{\varphi(\sigma)}$$

は同型写像になる。

(4) n を割り切らない素数 p に対し、

$$f_p = \min\left\{k \in \mathbb{N} \;\middle|\; p^k \equiv 1 \bmod(n)\right\} = (\mathbb{Z}/(n))^\times \text{の元 } \overline{p} \text{ の位数}$$

とすると、$\mathbb{Z}$ の素イデアル (p) は、$\mathbb{Z}[\zeta_n]$ において $\varphi(n)/f_p$ 個の相異なる素イデアルの積に分解する。

注意. この定理と Kronecker-Weber の定理：

体 L が $\mathbb{Q}$ の Abel 拡大、すなわち L が $\mathbb{Q}$ の Galois 拡大で $\mathrm{Gal}(L/\mathbb{Q})$ が Abel 群ならば、$L \subset \mathbb{Q}(\zeta_n)$ を満たす自然数 n が存在する

より、$\mathbb{Q}$ の任意の Abel 拡大 L に対し、$L/\mathbb{Q}$ の Galois 群の構造と素数の分解の様子が記述できる。このように、**代数体**と呼ばれる $\mathbb{Q}$ の有限次拡大体の間の Galois 拡大 L/K に対し、

$$\begin{cases} \mathrm{Gal}(L/K) \text{ の構造}, \\ K \text{（の整数環）の素イデアルの } L \text{ における分解の様子} \end{cases}$$

を記述する理論を**類体論**という。

- L/K が Abel 拡大のとき、$\mathrm{Gal}(L/K) \cong K$ の “合同イデアル類群”（Hilbert-高木）：

  … 要するにアーベル体は類体なりということにぶつかった。当時これは、あまりにも意外なことなので、それは当然間違っていると思うた。間違いだろうと思うから、何処が間違っているんだか、専らそれを探す。その頃は、少し神経衰弱に成りかかったような気がする。よく夢を見た。夢の裡で疑問が解けたと思って、起きてやってみると、まるで違っている。何が間違いか、実例を探して見ても、間違いの実例が無い。大分長く間違いばかり探していたので、其の後理論が出来上った後にも自信が無い。どこかに一寸でも間違いがあると、理論全体が、その蟻の穴から毀われてしまう。外の科学は知らないが、数学では「大体良さそうだ」では通用しない。（高木貞治「回顧と展望」より）

- L/K が Abel 拡大でないとき、モジュラー形式を用いたプログラム (志村、Langlands 等):

  良い性質を持つ Galois 群の表現 $\Leftarrow$ モジュラー形式から作られる Galois 群の表現

  に基づき、Wiles 等により 360 年未解決であった Fermat 予想が証明された。

例. $n = 4$ のとき、定理 3.3.1 (2) より

$$\mathrm{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q}) = \mathrm{Gal}\left(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}\right) \cong (\mathbb{Z}/(4))^\times = \left\{\overline{1}, \overline{3}\right\}.$$

よって奇素数 p に対し、定理 3.3.1 (4) より

$$(p) \text{ が } \mathbb{Z}\left[\sqrt{-1}\right] \text{ で 2 つの素イデアルに分解する } \Leftrightarrow\ f_p = 1 \ \Leftrightarrow\ p \equiv 1 \bmod(4).$$

実際 Euler の定理より

$$p \equiv 1 \bmod(4) \ \Leftrightarrow\ \exists a, b \in \mathbb{Z} \text{ such that } p = a^2 + b^2, \text{ i.e., } (p) = (a + b\sqrt{-1})(a - b\sqrt{-1}).$$

問題. 定理 3.3.1 (4) を $n = 3$ の場合に適用して、3 以外の素数 p に対し、

$$p \equiv 1 \bmod(3) \ \Leftrightarrow\ \exists a, b \in \mathbb{Z} \text{ such that } p = F(a, b)$$

を満たす（と予想される）a, b の $\mathbb{Z}$ 上の 2 次式 $F(a, b)$ を求めよ。

注意. 一般には、代数体のイデアルは単項イデアルにならないため、$\mathbb{Z}$ の素イデアルの分解から素数の分解が従うとは限らない。

定理の証明. 2.3「円分拡大」の所で、(1) 及び (3) の写像が単射になることを示しており、定理 2.1.1 より

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)|$$

が成り立つので、(2) が示されれば (1)〜(3) が成り立つことが分る。

まず n が素数 p の巾乗 p^d の場合に (2) を示す。ζ_{p^d} は 1 の原始 p^d 乗根だから、

$$f(X) = \frac{X^{p^d} - 1}{X^{p^{d-1}} - 1} = \left(X^{p^{d-1}}\right)^{p-1} + \left(X^{p^{d-1}}\right)^{p-2} + \cdot + X^{p^{d-1}} + 1 = 0$$

の解になる。2 項定理と、2 項係数 $\begin{pmatrix} p \\ k \end{pmatrix} = \dfrac{p!}{k!(p-k)!}$ が $1 \le k \le p-1$ のとき p で割り切れることを用いると、$(X+1)^p \equiv X^p + 1 \bmod(p)$ が成り立つから、

$$f(X+1) \bmod(p) = \frac{(X+1)^{p^d} - 1}{(X+1)^{p^{d-1}} - 1} \bmod(p) = X^{p^{d-1}(p-1)} \bmod(p).$$

また $f(X+1)$ はモニックで定数項は p だから、素数 p について Eisenstein の定理の仮定を満たす。よって $f(X+1)$ は $\mathbb{Q}$ 上既約になるから、$f(X)$ も $\mathbb{Q}$ 上既約になる。従って $f(X)$ は ζ_{p^d} の $\mathbb{Q}$ 上の最小多項式となるから、

$$\left[\mathbb{Q}\left(\zeta_{p^d}\right):\mathbb{Q}\right]=\deg(f)=p^{d-1}(p-1).$$

一方 $\varphi(n)$ は、n と互いに素となる 0 以上 n 未満の整数の個数だから、

$$\varphi(p^d)=p^d-\left|\left\{0,p,2p,...,\left(p^{d-1}-1\right)p\right\}\right|=p^d-p^{d-1}=p^{d-1}(p-1).$$

従って $n=p^d$ のとき (2) が成り立つことが示された。

次に互いに素な自然数 m,l に対し (2)、従って (3) が成り立つと仮定する。このとき

$$H_m=\mathrm{Gal}\left(\mathbb{Q}(\zeta_{ml})/\mathbb{Q}(\zeta_m)\right),\quad H_l=\mathrm{Gal}\left(\mathbb{Q}(\zeta_{ml})/\mathbb{Q}(\zeta_l)\right)$$

は Abel 群 $G=\mathrm{Gal}\left(\mathbb{Q}(\zeta_{ml})/\mathbb{Q}\right)$ の部分群で、$\mathbb{Q}(\zeta_m,\zeta_l)=\mathbb{Q}(\zeta_{ml})$ より $H_m\cap H_l=\{1\}$ が成り立つから、$(\sigma,\tau)\in H_m\times H_l$ を $\sigma\tau$ に写す写像 ψ は、単射準同型写像 $H_m\times H_l\to G$ を導く。従って

$$|G|\geq|H_m|\times|H_l|=\varphi(m)\varphi(l).$$

一方、整数 a に $(a \bmod(m), a \bmod(l))$ を対応させる写像は、環の準同型写像

$$\mathbb{Z}\to\mathbb{Z}/(m)\times\mathbb{Z}/(l)$$

を与え、準同型定理よりこれは環の同型写像

$$\mathbb{Z}/(ml)\xrightarrow{\sim}\mathbb{Z}/(m)\times\mathbb{Z}/(l)$$

及び群の同型写像

$$(\mathbb{Z}/(ml))^\times\xrightarrow{\sim}(\mathbb{Z}/(m))^\times\times(\mathbb{Z}/(l))^\times$$

を導く（これらの事実を **Chinese Remainder Theorem** という)。従って

$$\varphi(ml)=\varphi(m)\varphi(l)$$

となるから、$|G|\geq\varphi(ml)$ が成り立つ。(3) の写像は単射になるから $|G|\leq\varphi(ml)$ となり、従って $n=ml$ に対し (2) が成り立つ。以上のことから、任意の自然数 n に対し (2) 及び (3) が成り立つことが示された。

次に (4) の略証を与える。(3) より ζ_n の $\mathbb{Q}$ 上の最小多項式は

$$\Phi_n(X)=\prod_{a\in(\mathbb{Z}/(n))^\times}(X-{\zeta_n}^a)\in\mathbb{Z}[X]:n\text{次円周等分多項式}$$

で与えられる。$\Phi_n(X) \bmod(p)$ の $\mathbb{F}_p$ 上の既約多項式への分解を

$$\phi_1(X)^{e_1}\cdots\phi_g(X)^{e_g}$$

とすると、代数的整数論の一般論より

$$\begin{cases} \varphi(n) = \sum_{i=1}^{g} e_i \cdot \deg(\phi_i), \\ (p) = P_1^{e_1} \cdots P_g^{e_g} \ : \ \mathbb{Q}(\zeta_n) \text{ における素イデアル分解.} \end{cases}$$

いま p は n を割り切らないから、$\Phi_n(X) \bmod(p)$ は重解を持たず、従って任意の $i = 1, ..., g$ に対し $e_i = 1$ が成り立つ。また $\phi_i(X)$ の $\mathbb{F}_p$ 上の分解体を $\mathbb{F}_{q_i}$ とすると、定理 2.5.2 より $\mathrm{Gal}\,(\mathbb{F}_{q_i}/\mathbb{F}_p)$ は Frobenius 写像 $F : x \mapsto x^p$ で生成され、$\varphi(\overline{p})$ は ζ_n を ζ_n^p に写すから、$\mathbb{F}_{q_i}$ 上の写像として F を導く。従って

$$f_p = |\mathrm{Gal}\,(\mathbb{F}_{q_i}/\mathbb{F}_p)| = [\mathbb{F}_{q_i} : \mathbb{F}_p] = \deg(\phi_i)$$

が成り立つ。従って $\varphi(n) = g \cdot f_p$ となるから、求める素イデアルの個数 g は $\varphi(n)/f_p$ に等しい。 □

応用. p と q を相異なる奇素数とし、$q^* = \left(\dfrac{-1}{q}\right) q = (-1)^{\frac{q-1}{2}} \cdot q$ とすると、

$$\begin{aligned} &(p) \text{ が } \mathbb{Q}(\sqrt{q^*}) \text{ で 2 つの素イデアルに分解する} \\ \Leftrightarrow \ \ &\mathbb{F}_p(\sqrt{q^*}) = \mathbb{F}_p \ \Leftrightarrow \ q^* \in \left(\mathbb{F}_p^{\times}\right)^2 \ \Leftrightarrow \ \left(\frac{q^*}{p}\right) = 1. \end{aligned}$$

一方、定理 3.2.3 の系より拡大 $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ における Galois 対応は

$$\begin{array}{ccccc} \mathbb{Q} & \subset & \mathbb{Q}\,(\sqrt{q^*}) & \subset & \mathbb{Q}(\zeta_q) \\ \updownarrow & & \updownarrow & & \updownarrow \\ \mathbb{F}_q^{\times} & \supset & (\mathbb{F}_q^{\times})^2 & \supset & \{1\} \end{array}$$

となるから、定理 3.3.1 (4) より

$$\begin{aligned} &(p) \text{ が } \mathbb{Q}(\sqrt{q^*}) \text{ で 2 つの素イデアルに分解する} \\ \Leftrightarrow \ \ &\overline{p} \text{ の } \mathbb{F}_q^{\times}/(\mathbb{F}_q^{\times})^2 \text{での位数が } 1 \ \Leftrightarrow \ \overline{p} \in \left(\mathbb{F}_q^{\times}\right)^2 \ \Leftrightarrow \ \left(\frac{p}{q}\right) = 1. \end{aligned}$$

従って

$$\left(\frac{p}{q}\right) = 1 \ \Leftrightarrow \ \left(\frac{q^*}{p}\right) = \left(\frac{(-1)^{(q-1)/2}}{p}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right) = 1$$

となり、平方剰余についての**相互法則**

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

が導かれる。

参考文献

[K] 木村 俊一, 数学のかんどころ 14 ガロア理論, 共立出版 (2012).

[T] 高木 貞治, 近世数学史談, 岩波文庫 (1995).

[vdW] B. L. van der Waerden, Algebra, Springer (2003).