# 代数的整数論入門 (前期集中 特殊講義 II)

加塩朋和 *（東京理科大学 創域理工学部 数理科学科）

2025 年 8 月 25 日 (月) – 29 日 (金), 13:00 – 17:50

**概要**

代数学で学修する諸概念（群・環・体・加群・ガロア理論・群コホモロジー）を, 代数的整数論で扱う具体例を通して概説する. 具体的には代数体, 整数環, 単数群, 代数体の体拡大, 素イデアルの分岐, ガロアコホモロジー, 有限体, $p$ 進体などを予定している. また, 古典的な問題をいくつか紹介し, そのような問題解決に代数学がどのように応用されているかを学修する.

**■成績評価について**. このレジュメの問題を 3 問〜5 問解いて, 9 月 5 日 (金) 24 時までに moodle へ提出して下さい. なお, 板書, レジュメ, 他人のレポート等の丸写しは認めません.
※ 3 問の場合は最大で「可」評価, 4 問の場合は最大で「良」評価になります.

## 目次 (# は授業の進捗次第で省略)



* E-mail: tomokazu_kashio@rs.tus.ac.jp

# 記号

**定義 0.0.1.** (1) $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ をそれぞれ自然数, 整数, 有理数, 実数, 複素数全体のなす集合とする. なお, この講義では $0 \notin \mathbb{N}$.

(2) $a, b \in \mathbb{Z}$ に対し, $a \mid b \Leftrightarrow \exists c \in \mathbb{Z}$ s.t. $ac = b$.

(3) $\gcd(a, b)$ を $a, b$ の最大公約数とする.

(4) 集合 $S$ の濃度 (要素の個数) を $|S| \in \{0, 1, 2, \ldots, \infty\}$ で表す.

# 1　群・環と整数論

概略

- “演算とその逆演算” が定義されている集合を「群」, “$\pm, \times$” が定義されている集合を「環」と呼ぶ.
- 研究対象が群であれば「群論」から, 環であれば「環論」から分かることがたくさんある.
- 例として「平方剰余の相互法則」と「Pell 方程式の解法」を紹介する.

## 1.1　群論・環論 (概説)

**定義 1.1.1.** $G \neq \emptyset$ とする.

(0) $G$ 上の二項演算 $\circ\colon G \times G \to G$, $(a, b) \mapsto a \circ b$ が定義され,
(1) 結合法則: $\forall a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$.
(2) 単位元の存在: $\exists e = e_G \in G$ s.t. $\forall a \in G$, $a \circ e = e \circ a = a$.
(3) 逆元の存在: $\forall a \in G$, $\exists a'$ s.t. $a \circ a' = a' \circ a = e$.

を満たすとき, $G$ または $(G, \circ)$ を **群** と呼ぶ. さらに

(4) 交換法則: $\forall a, b \in G$, $a \circ b = b \circ a$.

を満たすとき **可換群** または **アーベル群** と呼ばれる. なお

- 演算を $\times$ や $\cdot$ で書く場合, 単位元, 逆元はそれぞれ $1 = 1_G, a^{-1}$ で表され, 演算の記号はよく省略される $(ab := a \cdot b)$.
- アーベル群の演算は $+$ で書かれる場合がある. この場合 **加法群** とも呼ばれ, 単位元, 逆元はそれぞれ $0 = 0_G, -a$ で表される. この場合, 演算の記号は省略しない.
- 群 $G$ の部分集合 $H$ が $G$ と同じ演算に関して群になるとき, $H$ は $G$ の **部分群** であるといい, 記号 $H < G$ で表す.

**例 1.1.2.** (1) $(\mathbb{Z}, +)$ はアーベル群 (加法群) になる. $(\mathbb{N}, +)$ は単位元が存在しないので群ではない.
(2) $(\mathbb{R}^\times, \times)$ $(\mathbb{R}^\times := \mathbb{R} - \{0\})$ はアーベル群になる. $(\mathbb{R}, \times)$ は 0 の逆元が存在しないの

で群ではない.

**注意 1.1.3.** おおまかにいうと, 群とは “演算とその逆演算が定義されている集合” である. 例えば

- $\mathbb{Z}$ では $+$ と $-$ が定義されている.
- $\mathbb{N}$ では $+$ は定義されているが $2-3$ は定義されていない.
- $\mathbb{R}^\times$ では $\times, \div$ が定義されている.
- $\mathbb{R}$ では $\times$ が定義されているが $\div 0$ が定義されていない.

**定義-命題 1.1.4.** (1) 部分群 $H < G$ に対し商集合

$$G/H := G/\sim, \quad g \sim g' \Leftrightarrow g^{-1}g' \in H$$

を **左剰余類集合** とよぶ. $G/H$ の元は代表元 $g \in G$ を用いて

$$\overline{g} := gH := \{x \in G \mid x \sim g\} = \{gg' \mid g' \in H\}$$

の形で表される. ただし $G$ が加法群であれば $\overline{g} = g + H$ のように表す. $|G/H|$ を ($G$ における部分群 $H$ の) **指数** と呼ぶ.

(2) 部分群 $N < G$ が **正規部分群** であるとは

$$\forall g \in G,\ gNg^{-1} = N$$

を満たすことであり, 記号 $N \triangleleft G$ で表す.

(3) 正規部分群 $N \triangleleft G$ に対して, その **商群** $(G/N, \circ)$ が

$$gN \circ g'N := gg'N$$

で定義される.

**問題 1.** $n \in \mathbb{N}$ とする.

(1) $n\mathbb{Z} \triangleleft \mathbb{Z}$ を示せ.

(2) 商群 $\mathbb{Z}/n\mathbb{Z}$ に対し

$$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid 0 \le a \le n-1\}, \quad |\mathbb{Z}/n\mathbb{Z}| = n,$$
$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a+b) + n\mathbb{Z}$$

となることを説明せよ.

(3) 商群 $\mathbb{Z}/n\mathbb{Z}$ の単位元を答えよ.

(4) $a + n\mathbb{N} \in \mathbb{Z}/n\mathbb{Z}$ の逆元を答えよ.

※ $(\mathbb{Z}/n\mathbb{Z}, +)$ は非常に重要な群である. が, 特段の名前はついていない (?). しいて言うなら位数 $n$ の **巡回群** である.

**定義 1.1.5.** 群 $(G, \circ)$, $(H, *)$ の間の写像 $f\colon G \to H$ が

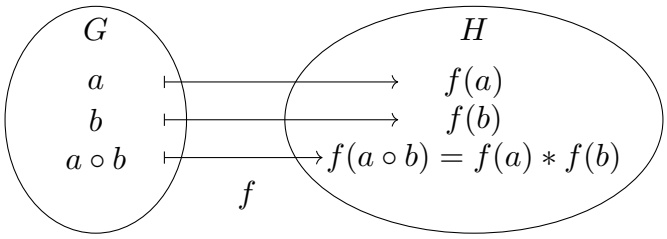
$$\forall a, b \in G,\ f(a \circ b) = f(a) * f(b)$$

を満たすとき, $f$ は **(群) 準同型写像** と呼ばれる. 全単射準同型写像は **(群) 同型写像** と呼ばれる. 同型写像 $f\colon G \to H$ が存在するとき, $G, H$ は **(群) 同型** であると言い, $G \cong H$ などと書く. 同型な群は "同一視" される. なお $f$ が準同型であれば自動的に

- $f(e_G) = e_H$ ($\because f(e_G)f(e_G) = f(e_G e_G) = f(e_G) \Rightarrow f(e_G) = f(e_G)e_H = f(e_G)f(e_G)f(e_G)^{-1} = f(e_G)f(e_G)^{-1} = e_H$).
- $f(a^{-1}) = f(a)^{-1}$ ($\because f(a^{-1})f(a) = f(a^{-1}a) = f(e_G) = e_H \Rightarrow f(a^{-1}) = f(a^{-1})e_H = f(a^{-1})f(a)f(a)^{-1} = e_H f(a)^{-1} = f(a)^{-1}$).

が成り立つ.

**注意 1.1.6.** 写像 $f\colon G \to H$ は定義域の元 $a \in G$ と終域の元 $f(a)$ の対応 ("元の対応") を与えている. さらに, 定義域での演算結果 $a \circ b$ と, 終域での演算結果 $f(a) * f(b)$ も対応している ("演算の対応") というのが準同型の意味である.




**定義 1.1.7.** $R \neq \emptyset$ とする.

(0) $R$ 上に乗法 $\cdot$ と加法 $+$ の 2 種の演算が定義され,
(1) $(R, +)$ は加法群 (演算を $+$ で表すアーベル群) である.
(2) 乗法の結合法則: $\forall a, b, c \in R$, $a(bc) = (ab)c$.
(3) 乗法の単位元: $\exists 1 = 1_R$ s.t. $\forall a \in R$, $1a = a1 = a$.
(4) 分配法則: $\forall a, b, c \in R$, $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.

を満たすとき, $R$ または $(R, +, \cdot)$ を **環** と呼ぶ. さらに

(5) 乗法の交換法則: $\forall a, b \in R,\ ab = ba$.

を満たすとき **可換環** と呼ばれる. なお

- 乗法の記号 $\cdot$ は省略されるが, 加法の記号 $+$ は省略しない.
- 乗法単位元 $1 = 1_R$ と区別し, 加法 $+$ の単位元を **零元** と呼び $0 = 0_R$ で表す.
- $R^\times := \{a \in R \mid \exists b \in R \text{ s.t. } ab = ba = 1\}$ を $R$ の **乗法群** と呼び, その元を **単元** または **可逆元** と呼ぶ. 単元 $a$ に対し $ab = ba = 1$ を満たす元 $b$ は **逆元** と呼ばれ $b = a^{-1}$ で表される. 一般に $(R^\times, \cdot)$ は群となる ($\Rightarrow$ 問題 2).

**注意 1.1.8.** おおまかにいうと, 環とは四則演算のうち "$+$, $-$, $\times$ が定義されている集合" である. 本講義では以下の場面で登場する.

- 整数全体のなす集合 $\mathbb{Z}$ は通常の和と積に関して可換環となり **有理整数環** と呼ばれる. その性質は整数論において重要である ($\Rightarrow$ 問題 4).
- 有理整数環の類似 (一般化) として代数体の整数環 ($\Rightarrow$ Section 3) が定義される.
- 加群 ($\Rightarrow$ Section 4) における係数環として. ($\mathbb{Q}, \mathbb{R}, \mathbb{C}$ などの "体係数" だけではなく, $\mathbb{Z}$ などの "環係数" で線形代数を行う.)
- 体 ($\Rightarrow$ Section 2) は環のうち特別なものである (四則演算 $+, -, \times, \div$ が全部定義される).
- 重要な群を環や体の乗法群として定義する ($\Rightarrow$ 例 1.1.9).

**問題 2.** 環 $R$ において $R^\times$ が群になることを示せ.
※ 定義 1.1.1-(0) や, 定義 1.1.1-(3) での $a' \in R^\times$ を忘れやすいので注意.

**例 1.1.9.** $n$ を自然数とする.

(1) $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ は, 演算 $\overline{a} + \overline{b} = \overline{a+b}$, $\overline{a} \cdot \overline{b} = \overline{ab}$ に関して可換環になる (整数環 $\mathbb{Z}$ のイデアル $n\mathbb{Z}$ による商環 $\Rightarrow$ 定義-命題 1.1.12-(2)).

(2) $\mathbb{Z}/n\mathbb{Z}$ の乗法群 $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ は $n$ を法とする **既約剰余類群** と呼ばれる. なお

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times &= \{\overline{a} \mid \exists x \text{ s.t. } \overline{ax} = \overline{1}\} \\ &= \{\overline{a} \mid \exists x, y \text{ s.t. } ax + ny = 1\} \\ &\overset{\text{命題 } 1.1.10}{=} \{\overline{a} \mid 0 \le a \le n-1,\ \gcd(a, n) = 1\}\end{aligned}$$

となる.

**命題 1.1.10** (ベズーの補題)**.** $a, b, c \in \mathbb{N}$ に対して以下は同値.

(1) $ax + by = c$ が整数解 $x, y$ を持つ.
(2) $\gcd(a, b) \mid c$.

**証明**. 問題 4-(1), (2) より $\{ax + by \mid x, y \in \mathbb{Z}\} = \{dn \mid n \in \mathbb{Z}\}$ $(\exists d \in \mathbb{N})$ と書ける. このとき

$$ax + by = c \text{ が整数解 } x, y \text{ を持つ} \Leftrightarrow c \in \{ax + by \mid x, y \in \mathbb{Z}\} = \{dn \mid n \in \mathbb{Z}\} \Leftrightarrow d \mid c$$

となるので $d = \gcd(a, b)$ を言えばよい. $d \mid \gcd(a, b)$ と $\gcd(a, b) \mid d$ に分けて示す.

$d \mid \gcd(a, b)$ の証明. $a = a \cdot 1 + b \cdot 0 \in \{ax + by \mid x, y \in \mathbb{Z}\} = \{dn \mid n \in \mathbb{Z}\}$ より $d \mid a$, $b = a \cdot 0 + b \cdot 1 \in \{ax + by \mid x, y \in \mathbb{Z}\} = \{dn \mid n \in \mathbb{Z}\}$ より $d \mid b$.

$\gcd(a, b) \mid d$ の証明. $d \in \{dn \mid n \in \mathbb{Z}\} = \{ax + by \mid x, y \in \mathbb{Z}\}$ より $d = ax + by$ と書ける. $a = \gcd(a, b)a_0$, $b = \gcd(a, b)b_0$ とおけば $\gcd(a, b) \mid \gcd(a, b)(a_0x + b_0y) = d$. □

**問題 3.** 一般に, 素数 $p$ に対し

$$\mathbb{Z}/(p-1)\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$$

が群同型になることが知られている $(\Rightarrow$ 補題 1.2.4). 実際に $p = 5$ のとき

$$\mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/5\mathbb{Z})^\times, \begin{cases} 0 \mapsto 1 \\ 1 \mapsto 2 \\ 2 \mapsto 4 \\ 3 \mapsto 3 \end{cases}$$

が群の同型写像になっていることを確かめよ.

**定義 1.1.11.** 環 $R$, $S$ の間の写像 $f\colon R \to S$ が

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

を満たすとき, $f$ は **(環) 準同型写像** と呼ばれる. 全単射準同型写像は **(環) 同型写像** と呼ばれる. 同型写像 $f\colon R \to S$ が存在するとき, $R, S$ は **(環) 同型** であると言い, $R \cong S$ などと書く. 同型な環は "同一視" される.

**定義-命題 1.1.12.** (1) $R$ を環とする. 空でない部分集合 $I \subset R$ $(I \neq \emptyset)$ が

$$a, b \in I \Rightarrow a - b \in I, \quad a \in I,\ r \in I \Rightarrow ar, ra \in I$$

を満たすとき, $I$ は $R$ の **(両側) イデアル** であるという.

(2) 環 $R$ のイデアル $I$ に対し, 商集合

$$R/I := R/\sim, \quad a \sim b \Leftrightarrow a - b \in I$$

上に演算

$$\overline{a} + \overline{b} := \overline{a+b}, \quad \overline{a} \cdot \overline{b} := \overline{ab}$$

を定めると **商環** と呼ばれる環になる.

(3) イデアル $I \subsetneq R$ が **素イデアル** であるとは,

$$a, b \in R,\ a \notin I,\ b \notin I \Rightarrow ab \notin I$$

を満たすことである. 一方で, 零環でない可換環 $R$ $(R \neq \{0\})$ が **整域** であるとは,

$$a, b \in R,\ a, b \neq 0 \Rightarrow ab \neq 0$$

を満たすことである. このとき, 可換環 $R$ のイデアル $I$ に対し以下は同値である.

$$I \text{ は素イデアル} \Leftrightarrow R/I \text{ は整域.}$$

(4) イデアル $I \subsetneq R$ が **極大イデアル** であるとは, 任意のイデアル $J \subset R$ に対し

$$I \subsetneq J \subset R \Rightarrow J = R$$

が成り立つことである. 一方で, 零環でない可換環 $R$ $(R \neq \{0\})$ が **体** であるとは,

$$a \in R,\ a \neq 0 \Rightarrow a \in R^\times$$

を満たすことである. このとき, 可換環 $R$ のイデアル $I$ に対し以下は同値である.

$$I \text{ は極大イデアル} \Leftrightarrow R/I \text{ は体.}$$

(5) 体は整域である. とくに (3), (4) と合わせて極大イデアルは素イデアルであることが分かる.

**問題 4.** (1) 可換環 $R$ と元 $a_1, \ldots, a_k \in R$ に対し

$$(a_1, \ldots, a_k) = \{a_1 r_1 + \cdots + a_k r_k \mid r_i \in R\}$$

は $R$ のイデアルであることを示せ. とくに $k = 1$ のとき, $aR := (a)$ の形で表されるイデアルは **単項イデアル** と呼ばれる.

(2) 整数環 $\mathbb{Z}$ は **単項イデアル整域 (PID)** であることを示せ. すなわち以下を示せ.

(a) $\mathbb{Z}$ は整域である.

(b) $\mathbb{Z}$ の任意のイデアルは単項イデアルである.

(3) $k \in \mathbb{N}$ に対し, 以下は同値であることを説明せよ.

(a) $k$ は素数である.

(b) $k$ は $\mathbb{Z}$ の **既約元** である. すなわち $k$ は 0 でも単元でもなく,

$$a, b \in \mathbb{Z},\ k = ab \Rightarrow a \in \mathbb{Z}^\times \text{ または } b \in \mathbb{Z}^\times$$

を満たす.

(c) $k$ は $\mathbb{Z}$ の **素元** である. すなわち $(k)$ は $\mathbb{Z}$ の素イデアルである.

(d) 剰余環 $\mathbb{Z}/k\mathbb{Z}$ は整域である.

(e) 剰余環 $\mathbb{Z}/k\mathbb{Z}$ は体である.

(f) $k\mathbb{Z}$ は $\mathbb{Z}$ の極大イデアルである.

ヒント: (a)$\Rightarrow \cdots \Rightarrow$(f)$\Rightarrow$(a) と回すのがコスパがよい (?). (d)$\Rightarrow$(e) には「有限整域は体」, (f)$\Rightarrow$(a) には「$(m) \subset (n) \Leftrightarrow m \in (n) \Leftrightarrow \exists l$ s.t. $m = ln$」を使うとよい.

**定理 1.1.13.** (1) $f\colon G \to H$ が群準同型であれば

$$\ker f \triangleleft G, \quad f(G) < H$$

はそれぞれ正規部分群, 部分群であり,

$$\overline{f}\colon G/\ker f \cong f(G),\ g \ker f \mapsto f(g)$$

は群同型写像となる.

(2) $f\colon R \to S$ が環準同型であれば

$$\ker f \triangleleft R, \quad f(R) \subset S$$

はそれぞれイデアル, 部分環であり,

$$\overline{f}\colon R/\ker f \cong f(R),\ r + \ker f \mapsto f(r)$$

は環同型写像となる.

**注意 1.1.14.** (1) 準同型定理は, 任意の準同型写像は射影, 同型, 単射の合成に分解できることを言っている:

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \pi\downarrow & & \uparrow\mathrm{id} \\ G/\ker f & \overset{\overline{f}}{\cong} & f(G) \end{array}$$

(2) 準同型定理の “標準的な使い方” は,

(a) うまい準同型 $f$ を構成して,

(b) その像と核を計算すると,

(c) 自動的に同型が得られる

という感じ ($\Rightarrow$ 問題 5).

**問題 5.** 群 $G_1, G_2, G_3$ が

$$G_1 \triangleright G_2,\ G_1 \triangleright G_3,\ G_2 \supset G_3$$

となっているとき,

$$G_1/G_3 \Big/ G_2/G_3 \cong G_1/G_2$$

が成り立つことを示せ.

ヒント: $f\colon G_1/G_3 \to G_1/G_2$, $gG_3 \mapsto gG_2$ が well-defined な準同型写像であることを説明し, $\ker f$, $f(G_1/G_3)$ を求めて準同型定理を使う.

## 1.2 平方剰余の相互法則

**定義 1.2.1.** $p$ を奇素数, $a \in \mathbb{Z}$ とする. このとき **ルジャンドル記号 (平方剰余記号)** を

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & (\exists b \in \mathbb{Z} \text{ s.t. } a \equiv b^2 \not\equiv 0 \mod p) \\ -1 & (\forall b \in \mathbb{Z},\ a \not\equiv b^2 \mod p) \\ 0 & (a \equiv 0 \mod p) \end{cases}$$

で定める.

**例 1.2.2.** (1) $1^2 (\equiv 4^2 \equiv 7^2 \equiv \dots) \equiv 1 \mod 3$, $2^2 (\equiv 5^2 \equiv 8^2 \equiv \dots) \equiv 1 \mod 3$ より

$$\left(\frac{1}{3}\right) = 1, \quad \left(\frac{2}{3}\right) = -1, \quad \left(\frac{0}{3}\right) = 0.$$

(2) $1^2 \equiv 1 \mod 5$, $2^2 \equiv 4 \mod 5$, $3^2 \equiv 4 \mod 5$, $4^2 \equiv 1 \mod 5$ より

$$\left(\frac{1}{5}\right) = 1, \quad \left(\frac{2}{5}\right) = -1, \quad \left(\frac{3}{5}\right) = -1, \quad \left(\frac{4}{5}\right) = 1, \quad \left(\frac{0}{5}\right) = 0.$$

**定義 1.2.3.** **群 $G$ の位数** を $|G| \in \mathbb{N} \cup \{\infty\}$ で定め, 群 $G$ の **元 $g$ の位数** を

$$\min\{n \in \mathbb{N} \mid g^n = 1_G\} \in \mathbb{N} \cup \{\infty\}$$

で定める. ただし $\forall n,\ g^n \neq 1_G$ のときは位数 $\infty$ とする. $|G| < \infty$ のとき $G$ は **有限群** であるという.

**問題 6.** $g \in G$ の位数を $d$ とおき, $d < \infty$ とする. 以下が同値であることを示せ.

$$g^n = e_G \Leftrightarrow d \mid n.$$

ヒント: $n = qd + r\ (0 \leq r < d)$ とおくと $g^n = e_G \overset{(g^d)^q = e_G}{\Leftrightarrow} g^r = e_G \overset{d \text{ の最小性}}{\Leftrightarrow} r = 0.$

**補題 1.2.4.** 群 $G$ が **巡回群** であるとは

$$\exists g \in G \text{ s.t. } G = \langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$$

を満たすことをいい, この $g$ を $G$ の **生成元** と呼ぶ.

(1) 巡回群は以下のいずれかに同型.

$$\mathbb{Z}, \quad \mathbb{Z}/d\mathbb{Z}\ (d \in \mathbb{N}).$$

(2) 体の $F$ の乗法群 $F^\times = F - \{0\}$ の有限部分群 $G$ は巡回群である.

(3) $p$ を素数とし, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ とおくとき

$$\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}.$$

**証明.** (1) $G = \langle g \rangle$ とする. このとき $f\colon \mathbb{Z} \to G,\ n \mapsto g^n$ は全射準同型写像になる. よって準同型定理より

$$\mathbb{Z}/\ker f \cong G.$$

$g$ の位数が $d$ であれば $\ker f = \{n \in \mathbb{Z} \mid g^n = e_G\} \overset{\text{問題 } 6}{=} d\mathbb{Z}$ より $G \cong \mathbb{Z}/d\mathbb{Z}$. $g$ の位数が $\infty$ であれば $\ker f = \{0\}$ より $G \cong \mathbb{Z}$.

(2) $G[d] := \{g \in G \mid g^d = e_G\}$, $G_d := \{g \in G \mid g \text{ の位数} = d\}$ とおく. まず $G[d]$ は $d$ 次方程式 $x^d = 1$ の体 $F$ の解に含まれるから

$$|G[d]| \leq d.$$

もし $G_d \neq \emptyset$ なら $g \in G_d$ を取ると

$$\{g^k \mid 1 \leq k \leq d\} \subset G[d] \overset{|G[d]| \leq d}{\Rightarrow} \{g^k \mid 1 \leq k \leq d\} = G[d].$$

さらに $G_d \subset G[d]$ より $\{g^k \mid 1 \leq k \leq d,\ \gcd(k,d) = 1\} = G_d$. とくに

$$|G_d| = \varphi(d) := |\{k \mid 1 \leq k \leq d,\ \gcd(k,d) = 1\}|.$$

一方で $G_d = \emptyset$ なら $|G_d| = 0 \leq \varphi(d)$. どちらにしても

$$|G_d| \leq \varphi(d).$$

よって $n := |G|$ に対し

$$n = |G| = |\coprod_{d|n} G_d| = \sum_{d|n} |G_d| \leq \sum_{d|n} \varphi(d) = \sum_{d|n} |\{kn/d \mid 1 \leq k \leq d,\ \gcd(k,d) = 1\}|$$
$$= |\coprod_{d|n} \{kn/d \mid 1 \leq k \leq d,\ \gcd(k,d) = 1\}| = |\{1, 2, \ldots, n\}| = n$$

となり, 途中の不等式は等号成立する: 各 $d$ で $|G_d| = \varphi(d)$. とくに $|G_n| = \varphi(n) > 0$, すなわち $G_n \neq \emptyset$. $g \in G_n$ をとれば $|\langle g \rangle| = n = |G|$ より $G = \langle g \rangle$.

(3) 問題 4 より $\mathbb{F}_p$ は (有限) 体. よって (2) より $\mathbb{F}_p^\times$ は巡回群 $\mathbb{Z}/d\mathbb{Z}$ と同型. さらに位数を数えると $d = |\mathbb{F}_p^\times| = p - 1$. □

**問題 7.** $p$ を奇素数とする.

(1) $(\mathbb{F}_p^\times)^2 := \{a^2 \mid a \in \mathbb{F}_p^\times\}$ は $\mathbb{F}_p^\times$ の正規部分群であり, 商群 $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ は $\{\pm 1\}$ と同型であることを示せ.

(2) 写像 $f\colon \mathbb{F}_p^\times \to \{\pm 1\}$ を

$$f\colon \mathbb{F}_p^\times \twoheadrightarrow \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \{\pm 1\}$$

で定める. これは準同型写像であり,

$$f(a \bmod p) = \left(\frac{a}{p}\right) \quad (p \nmid a \in \mathbb{Z})$$

を満たすことを示せ.

ヒント：補題 1.2.4 より $\mathbb{F}_p^\times$ と $\mathbb{Z}/(p-1)\mathbb{Z}$ は “同一視” できる. このとき $(\mathbb{F}_p^\times)^2 \subset \mathbb{F}_p^\times \Leftrightarrow 2\mathbb{Z}/(p-1)\mathbb{Z} = \{0, 2, \ldots, p-1\} \subset \mathbb{Z}/(p-1)\mathbb{Z}$ が対応する. $\mathbb{Z}/(p-1)\mathbb{Z}\Big/2\mathbb{Z}/(p-1)\mathbb{Z}$ には問題 5 が使える.

**補題 1.2.5.** (1) (**フェルマーの小定理**) 素数 $p$ に対し

$$a^{p-1} \equiv 1 \mod p \quad (p \nmid a \in \mathbb{Z}).$$

(2) (**オイラーの規準**) 奇素数 $p$ に対し

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p \quad (a \in \mathbb{Z}).$$

**証明**. (1) $\mathbb{F}_p^\times$ の生成元を $r$ とおく.

$$\mathbb{Z}/(p-1)\mathbb{Z} \cong \mathbb{F}_p^\times,\ b \bmod (p-1) \mapsto r^b \bmod p$$

である. とくに $\mathbb{F}_p^\times$ の一般元は $a := r^b \bmod p$ の形をしている. このとき $a^{p-1} \equiv 1 \mod p \Leftrightarrow r^{b(p-1)} \equiv 1 \mod p \Leftrightarrow b(p-1) \equiv 0 \mod (p-1)$ と言い換えることができ, 最後の主張は自明に成立.

(2) $p \mid a$ なら両辺 0 で一致. $p \nmid a$ なら (1) と同じ議論で $a^{\frac{p-1}{2}} \equiv 1 \mod p \Leftrightarrow r^{\frac{b(p-1)}{2}} \equiv 1 \mod p \Leftrightarrow \frac{b(p-1)}{2} \equiv 0 \mod (p-1) \Leftrightarrow 2 \mid b \Leftrightarrow a \in (\mathbb{F}_p^\times)^2 \Leftrightarrow \left(\frac{a}{p}\right) = 1$. □

**定理 1.2.6** (平方剰余の相互法則)**.** $p, q$ を相異なる奇素数とする.

(1) 相互法則: $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$. ただし $p^* := (-1)^{\frac{p-1}{2}} p$.
(2) 第一補充法則: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
(3) 第二補充法則: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

**注意 1.2.7.** 問題 7-(2) より $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ が成り立つことと第一補充法則より, 相互法則は

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

とも言い換えられる.

**例 1.2.8.** 平方剰余の相互法則には整数論の色んな場所で出会う.

(1) フェルマーの二平方和定理: 奇素数 $p$ に対し以下は同値.

$$\exists x, y \in \mathbb{N} \text{ s.t. } p = x^2 + y^2 \Leftrightarrow p \equiv 1 \mod 4.$$

例えば

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^4, \dots,$$
$$7 \notin \{1^2 + 1^2 = 2,\ 1^2 + 2^2 = 5,\ 2^2 + 2^2 = 8, \dots\}.$$

第一補充法則と素イデアルの分解法則から従う ($\Rightarrow$ 定理 3.1.1).

(2) オイラー・リュカの定理: フェルマー数を $F_n = 2^{(2^n)} + 1$ ($n \in \mathbb{N}$) で定める. このとき

(a) $F_n$ の素因子は $p \equiv 1 \mod 2^{n+1}$ を満たす.

(b) さらに $n \geq 2$ であれば $F_n$ の素因子は $p \equiv 1 \mod 2^{n+2}$ を満たす.

例えば

$$F_1 = 2^2 + 1 = 5,$$
$$F_2 = 2^4 + 1 = 17, \quad F_3 = 2^8 + 1 = 257, \quad F_4 = 2^{16} + 1 = 65537,$$
$$F_5 = 1 + 2^{32} = 4294967297 = 641 \cdot 6700417,$$
$$641 = 2^7 \cdot 5^1 + 1,\ 6700417 = 2^7 \cdot 3 \cdot 17449 + 1.$$

後半の証明には第二補充法則を用いる。

(3) 以下は北山氏 (2024 年度修士修了) の結果である: $n \in \mathbb{N}$, 奇素数 $q$ に対し $F_{q,n} := \frac{q^{(q^{n+1})}-1}{q^{(q^n)}-1}$ とおく. このとき $F_{q,n}$ の素因子 $p$ は

(a) $p \equiv 1 \mod 2q^{n+1}$ を満たす.

(b) さらに $q \equiv 3 \mod 4$ であれば $p \equiv 1 \mod 2^2 q^{n+1}$ を満たす.

例えば

$$F_{3,1} = 757 = 2^2 \cdot 33 \cdot 7 + 1,$$
$$F_{3,2} = 387440173 = 109 \cdot 433 \cdot 8209,$$
$$109 = 2^2 \cdot 3^3 + 1,\ 433 = 2^4 \cdot 3^3 + 1,\ 8209 = 2^4 \cdot 3^3 \cdot 19 + 1,$$
$$F_{3,3} = 581497370030476852878751 57 = 3889 \cdot 1190701 \cdot 12557612956332313,$$
$$3889 = 2^4 \cdot 3^5 + 1,\ 1190701 = 2^2 \cdot 3^5 \cdot 5^2 \cdot 7^2 + 1,$$
$$12557612956332313 = 2^3 \cdot 3^5 \cdot 11 \cdot 53 \cdot 67 \cdot 3203 \cdot 51631 + 1.$$

後半の証明には相互法則を用いる.

**定理 1.2.9** (ラグランジュの定理)**.** $G$ を有限群とし, 元 $g \in G$, 部分群 $H < G$ を考える.

(1) $|gH| = |H|$.

(2) $|G/H||H| = |G|$.

(3) $|H| \,\big|\, |G|$.

(4) $g$ の位数 $|\, |G|$.

**証明**. (1) $H \to gH$, $h \mapsto gh$ は逆写像 $g^{-1}h' \leftarrow\!\shortmid h'$ を持つので全単射.

(2) $G/H$ の完全代表系を $g_1, \ldots, g_n$ とおくと $G = g_1H \coprod g_2H \coprod \cdots \coprod g_nH$ と非交和分解できる (同値関係の一般論). 両辺の数を数えて $|G| = \sum_{i=1}^{n} |g_iH| \overset{(1)}{=} n|H| = |G/H||H|$.

(3) (2) より.

(4) $\langle g \rangle := g$ で生成される $G$ の部分群 $= \{g^n \mid n \in \mathbb{Z}\} < G$ を考えると, $g$ の位数 $|\langle g \rangle| \overset{(3)}{\mid} |G|$. □

**問題 8.** (1) 第一補充法則から二平方和定理の ($\Rightarrow$) 部分を導け.

略解：$p = x^2 + y^2$ とする. もし $p \mid x$ なら $y^2 = p - x^2 \equiv 0 \mod p \Rightarrow p \mid y$ で, とくに $p^2 \mid (x^2 + y^2) = p$ で矛盾, よって $p \nmid x$. よってフェルマーの小定理より $\exists a (:= x^{p-2})$ s.t. $ax \equiv 1 \mod p$. よって $\exists b (:= ay)$ s.t. $-1 \equiv b^2 \mod p \Rightarrow 1 = (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} \Rightarrow p \equiv 1 \mod 4$.

(2) オイラー・リュカの定理を示せ.

(a) の略解: $p \mid F_n$ とし $\overline{2} \in \mathbb{F}_p^\times$ の位数 $f$ を考える. $p \mid F_n = (2^{(2^n)}+1) \mid (2^{(2^{n+1})} - 1)$ より $f \mid 2^{n+1}$, とくに $f = 2^k$ $(k \leq n+1)$ の形. 一方で $p \mid F_n = 2^{(2^n)} + 1$ より $k \not< n$, つまり $f = 2^{n+1}$. よってラグランジュの定理より $2^{n+1} = f \mid |\mathbb{F}_p^\times| = p - 1$.

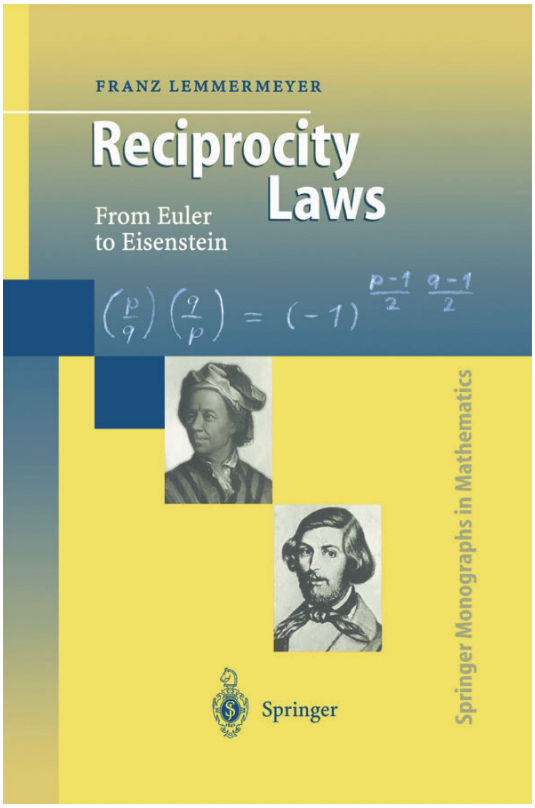
(b) のヒント: $p \equiv 1 \mod 8 \Rightarrow (\frac{2}{p}) = 1 \Rightarrow \exists a^2 \equiv 2 \mod p$. $\overline{2}$ の代わりに $\overline{a} \in \mathbb{F}_p^\times$ の位数 $d$ を考える。

(3) (余力があれば) 北山氏の結果を示せ.

**補足 1.2.10.** 相互法則の証明に関して.

(1) Gauss は 8 種類の証明を与えている.

(2) [Le, Appendix B] によれば 2000 年時点で 196 種類の証明方法が知られている.




Appendix B. Chronology of Proofs

| # | proof | year | comments |
|---|---|---|---|
| 1. | Legendre | 1788 | Quadratic forms; incomplete |
| 2. | Gauss 1 [264] | 1801 | Induction; April 8, 1796 |
| 3. | Gauss 2 [265] | 1801 | Quadratic forms; June 27, 1796 |
| 4. | Gauss 3 [266] | 1808 | Gauss' Lemma; May 6, 1807 |
| 5. | Gauss 4 [267] | 1811 | Cyclotomy; May 1801 |
| 6. | Gauss 5 [268] | 1818 | Gauss's Lemma; 1807/08 |
| 7. | Gauss 6 [269] | 1818 | Gauss sums; 1807/08 |
| 8. | Cauchy [122] | 1829 | Gauss 6 |
| 9. | Jacobi [400] | 1830 | Gauss 6 |
| 10. | Dirichlet [165] | 1835 | Gauss 4 |
| 11. | Lebesgue 1 [482] | 1838 | $N(x_1^2+\ldots+x_q^2 \equiv 1 \bmod p)$ |
| 12. | Schönemann [722] | 1839 | quadratic period equation |
| 13. | Eisenstein 1 [187] | 1844 | generalized Jacobi sums |
| 14. | Eisenstein 2 [189] | 1844 | Gauss 6 |
| 15. | Eisenstein 3 [192] | 1844 | Gauss's Lemma |
| 16. | Eisenstein 4 [197] | 1845 | Sine |
| 17. | Eisenstein 5 [198] | 1845 | infinite products |
| 18. | Liouville [549] | 1847 | Cyclotomy |
| 19. | Lebesgue 2 [485] | 1847 | Lebesgue 1 |
| 20. | Schaar [702] | 1847 | Gauss's Lemma |
| 21. | Genocchi [295] | 1852 | Gauss's Lemma |
| 22. | Dirichlet [170] | 1854 | Gauss 1 |
| 23. | Lebesgue 3 [487] | 1860 | Gauss 7, 8 |
| 24. | Kummer 1 [469] | 1862 | Quadratic forms |
| 25. | Kummer 2 [469] | 1862 | Quadratic forms |
| 26. | Dedekind 1 [174, §154] | 1863 | quadratic forms |
| 27. | Gauss 7 [270] | 1863 | quadratic periods; Sept. 1796 |
| 28. | Gauss 8 [271] | 1863 | quadratic periods; Sept. 1796 |
| 196. | Lemmermeyer [515] | | 2000 |

(3) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$ ($p^* = (-1)^{\frac{p-1}{2}}p$, $\zeta_p := \exp(\frac{2\pi i}{p})$) から得られる可換図式:

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) & \xrightarrow{\sigma \mapsto \sigma|_{\mathbb{Q}(\sqrt{p^*})}} & \mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) \\ \downarrow \wr & & \downarrow \wr \\ (\mathbb{Z}/p\mathbb{Z})^\times & \xrightarrow{a \bmod p \mapsto \left(\frac{a}{p}\right)} & \{\pm 1\} \end{array}$$

を利用した証明 (⇒ 系 5.1.4) が, 加塩の個人的な好み.

**定理 1.2.11** (**有限生成アーベル群の基本定理**). (1) アーベル群 $G$ が有限生成であれば

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$$

を満たす整数 $r \geq 0$, $s \geq 0$, $d_1, \ldots, d_s \geq 2$ が存在する. さらに $d_i \mid d_{i+1}$ という条件下でこの表示は一意的. $r$ は $G$ の **ランク** と呼ばれる.

(2) アーベル群 $G$ が有限群 (すなわち $|G| < \infty$) であれば

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$$

を満たす整数 $s \geq 0$, $d_1, \ldots, d_s \geq 2$ が存在する. さらに $d_i \mid d_{i+1}$ という条件下でこの表示は一意的.

**補足 1.2.12.** 上記定理は “有限生成アーベル群は有限個の巡回群の直積に一意的に表せる” と言っている. ただし

(1) 群 $G$ に対し $S \subset G$ が **生成系** であるとは, $G$ の部分群で $S$ を含むものは $G$ のみであること. 逆に $S$ で生成される群を $\langle S \rangle$ で現す.
(2) 群 $G$ が **有限生成** であるとは, 有限集合からなる生成系を持つこと.
(3) 群 $G, H$ に対し直積集合 $G \times H$ 上の二項演算を $(a,b)(c,d) := (ac, bd)$ で定め **直積群** と呼ぶ. 3 個以上の直積群も同様である. 自分自身との直積は $G^r := \underbrace{G \times G \times \cdots \times G}_{r \text{ 個}}$ のように書く.

## 1.3 # Pell 方程式

**定義 1.3.1.** 平方数でない自然数 $d$ (定数) に対して, $x, y$ に関する方程式

$$x^2 - dy^2 = 1$$

を **Pell 方程式** と呼ぶ. これは自明な解 $(x,y) = (1,0)$ を持つ. これ以外の解を非自明解と呼ぶことにする.

**例 1.3.2.** (1) $d = 2$ のとき, $|x|, |y| < 100$ の非自明解は

$$(x,y) = (\pm 3, \pm 2),\ (\pm 17, \pm 12),\ (\pm 99, \pm 70).$$

(2) $d = 3$ のとき, $|x|, |y| < 100$ の非自明解は

$$(x,y) = (\pm 2, \pm 1),\ (\pm 7, \pm 4),\ (\pm 26, \pm 15),\ (\pm 97, \pm 56).$$

(3) $d = 13$ のとき

$$(x,y) = (\pm 649, \pm 180)$$

が “最小解” となる.

(4) $d = 29$ のとき

$$(x,y) = (\pm 9801, \pm 1820)$$

が “最小解” となる.

**命題 1.3.3.** $d$ を平方数でない自然数とする.

(1) $\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ は通常の和と積に関して可換環となる.
(2) $P_d := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z},\ a^2 - db^2 = 1\}$ は乗法群 $\mathbb{Z}[\sqrt{d}]^\times$ の部分群となる.
(3) 以下は全単射を与える:

$$\{\text{Pell 方程式 } x^2 - dy^2 = 1 \text{ の解 } (x, y)\} \to P_d,\ (x, y) \mapsto x + y\sqrt{d}.$$

**証明**. (1), (2) は定義の各条件を確かめればよい. (3) も明らか. □

**問題 9.** $d$ を平方数でない自然数とする. 以下を確かめよ.

(1) $\mathrm{id}\colon \mathbb{Z}[\sqrt{d}]^\times \to \mathbb{Z}[\sqrt{d}]^\times,\ a + b\sqrt{d} \mapsto a + b\sqrt{d}$, $\rho\colon \mathbb{Z}[\sqrt{d}]^\times \to \mathbb{Z}[\sqrt{d}]^\times,\ a + b\sqrt{d} \mapsto a - b\sqrt{d}$ はぞれぞれ準同型写像.
(2) $\mathbb{Z}[\sqrt{d}]^\times = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z},\ a^2 - db^2 \in \{\pm 1\}\}$.
(3) $N\colon \mathbb{Z}[\sqrt{d}]^\times \to \{\pm 1\},\ a + b\sqrt{d} \mapsto a^2 - db^2$ は準同型写像 (**ノルム写像**).
(4) $P_d = \ker N$.
(5) $\frac{|\mathbb{Z}[\sqrt{d}]^\times|}{|P_d|} \in \{1, 2\}$.

(2) のヒント：$(\Leftarrow)$ は $\pm 1 = a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d}) \Rightarrow (a + b\sqrt{d})^{-1} = \pm(a - b\sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$. $(\Rightarrow)$ は $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]^\times \Rightarrow (a + b\sqrt{d})(\exists a' + \exists b'\sqrt{d}) = 1 \Rightarrow (a - b\sqrt{d})(a' - b'\sqrt{d}) = \rho(a + b\sqrt{d})\rho(a' + b'\sqrt{d}) = \rho((a + b\sqrt{d})(a' + b'\sqrt{d})) = \rho(1) = 1 \Rightarrow (a^2 - db^2)(a'^2 - db'^2) = (a + b\sqrt{d})(a' + b'\sqrt{d})(a - b\sqrt{d})(a' - b'\sqrt{d}) = 1 \cdot 1 = 1$.
よって $a^2 - db^2 \in \mathbb{Z}$ は 1 の約数なので $\pm 1$.
(5) のヒント：ノルム写像に準同型定理を使うと $\mathbb{Z}[\sqrt{d}]^\times / P_d \cong N(\mathbb{Z}[\sqrt{d}]^\times) < \{\pm 1\}$.

**定理 1.3.4.** $d$ を平方数でない自然数とする. このとき $P_d$ は有限生成アーベル群であり

$$P_d \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

となる. とくに $x_1, y_1 \in \mathbb{N}$ が存在して

$$P_d = \{\pm(x_1 + \sqrt{d}y_1)^n \mid n \in \mathbb{Z}\}$$

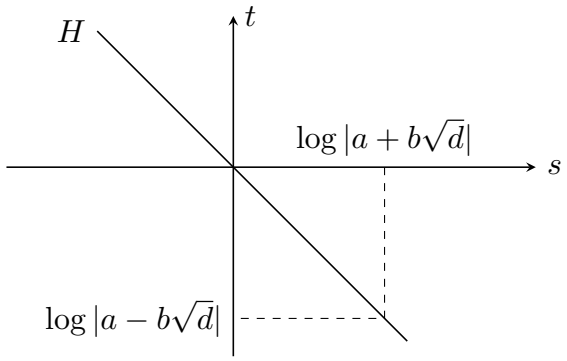
と表せる.

**証明**. 4 ステップに分けて考える.

(1) 写像

$$L\colon P_d \to \mathbb{R}^2, \quad a + b\sqrt{d} \mapsto (\log|a + b\sqrt{d}|, \log|a - b\sqrt{d}|)$$

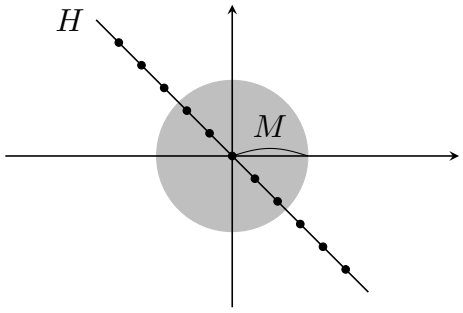
は準同型写像で, $L(P_d) < H := \{(s, t) \in \mathbb{R}^2 \mid s + t = 0\}$, $\ker L = \{\pm 1\}$.




(2) $L(P_d)$ は $\mathbb{R}^2$ の中で離散的, すなわち

$$\exists M > 0 \text{ s.t. } |L(P_d) \cap \{(s,t) \mid s^2 + t^2 < M^2\}| < \infty.$$

これと $L(P_d) < H \cong \mathbb{R}$ と併せて $L(P_d) \cong \mathbb{Z}$ または $L(P_d) = \{(0,0)\}$.




(3) $|L(P_d)| = \infty$. とくに $L(P_d) \neq \{(0,0)\}$ より $L(P_d) \cong \mathbb{Z}$.

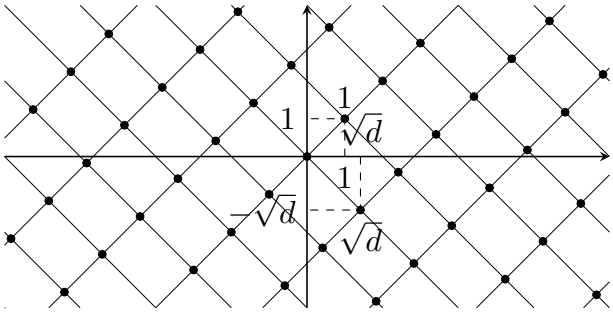
(4) 同型 $L(P_d) \cong \mathbb{Z}$ で対応する元 $L(\epsilon_0) \leftrightarrow 1$ をとると $P_d = \{\pm\epsilon_0^n \mid n \in \mathbb{Z}\}$. $x_1 + y_1\sqrt{d} = \epsilon_0$ が題意を満たす.

(1) log, id, $\rho$ が準同型よりそれらの合成で書ける $L$ も準同型. $\log|a+b\sqrt{d}| + \log|a - b\sqrt{d}| = \log(N(a+b\sqrt{d})) = \log 1 = 0$ より $L(P_d) < H$. $\ker L = \{\pm 1\}$ は $a + b\sqrt{d} \in \ker L \Leftrightarrow |a \pm b\sqrt{d}| = 1 \Rightarrow a \pm b\sqrt{d} = \pm 1 \Leftrightarrow a = \pm 1,\ b = 0$ より.

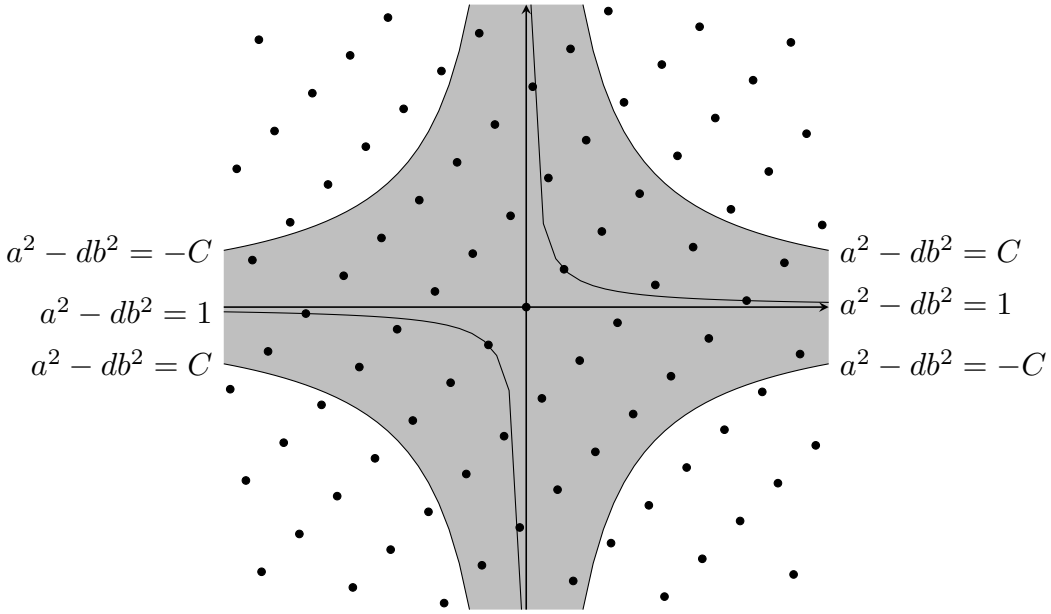
(2) $L(a+b\sqrt{d}) \in L(P_d) \cap \{(\alpha,\beta) \mid \alpha^2 + \beta^2 < M^2\} \Rightarrow |a+b\sqrt{d}||a-b\sqrt{d}| = a^2 - db^2 = 1,\ \log|a \pm b\sqrt{d}| < M \Rightarrow -M < \log|a \pm b\sqrt{d}| < M \Rightarrow e^{-M} < |a \pm b\sqrt{d}| < e^M \Rightarrow -N < a \pm b\sqrt{d} < N\ (N := \max(e^{-M}, e^M)) \Rightarrow -2N < a < 2N,\ \frac{-2N}{\sqrt{d}} < b < \frac{2N}{\sqrt{d}}$. このような $a, b \in \mathbb{Z}$ は有限個.

(3) さらに以下のステップに分ける. まず $\mathbb{Z}[\sqrt{d}]$ を $\mathbb{R}^2$ 上の "格子点" とみなす:

$$\mathbb{Z}[\sqrt{d}] \hookrightarrow \mathbb{R}^2, \quad a + b\sqrt{d} \mapsto (a + b\sqrt{d}, a - b\sqrt{d})$$




(a) $\exists C > 0$ s.t. $|\{\alpha \in \mathbb{Z}[\sqrt{d}] \mid |N(\alpha)| \leq C\}| = \infty$.




(b) $\exists c \in \mathbb{N}$, $\exists \alpha \in \mathbb{Z}[\sqrt{d}]$ s.t.

$$|\{\beta \in \mathbb{Z}[\sqrt{d}] \mid |N(\beta)| = c,\ \beta \equiv \alpha \mod c\}| = \infty.$$

(c) $|\mathbb{Z}[\sqrt{d}]^\times| = \infty$, $|P_d| = \infty$, $|L(P_d)| = \infty$.

(a) $n \in \mathbb{N}$ に対し, $\{a+b\sqrt{d} \mid 0 \leq a, b \leq n\}$ は $(n+1)^2$ 個の点をもち, 区間 $[0, n(1+\sqrt{d})]$ に含まれる. よって, ある 2 個 $a + b\sqrt{d}, a' + b'\sqrt{d}$ $(0 \leq aa', b, b' \leq n)$ は長さ $n(1+\sqrt{d})/(n+1)^2$ の区間に含まれる. よって $a_n := a_1 - a_2$, $b_n := b_1 - b_2$ とおけば

$$|a_n + b_n\sqrt{d}| \leq n(1+\sqrt{d})/(n+1)^2.$$

一方で $-n \leq a_n, b_n \leq n$ より

$$|a_n - b_n\sqrt{d}| \leq |a_n| + |b_n||\sqrt{d}| \leq n(1+\sqrt{d}).$$

併せて

$$|a_n^2 - db_n^2| = |a_n + b_n\sqrt{d}||a_n - b_n\sqrt{d}| \leq n^2(1+\sqrt{d})^2/(n+1)^2 < (1+\sqrt{d})^2.$$

よって $C := (1+\sqrt{d})^2$ とおき, $n$ をどんどん大きくとれば ($n$ の次は $n'(1+\sqrt{d})/(n'+1)^2 < |a_n + b_n\sqrt{d}|$ を満たす $n'$ をとればよい), 条件を満たし相異なる $a_n + b_n\sqrt{d}$ がいくらでもとれる.

(b) $\mathbb{Z}[\sqrt{d}] = \coprod_{c\in\mathbb{N}}\{\beta \in \mathbb{Z}[\sqrt{d}] \mid |N(\beta)| = c\}$ と分解できる. (a) より有限和 $\coprod_{c<C}$ に制限しても無限集合なので, いずれかの $c$ で

$$|\{\beta \in \mathbb{Z}[\sqrt{d}] \mid |N(\beta)| = c\}| = \infty.$$

一方で

$$\mathbb{Z}[\sqrt{d}]/(c) = \{\overline{a' + b'\sqrt{d}} \mid 0 \leq a', b' \leq c-1\}$$

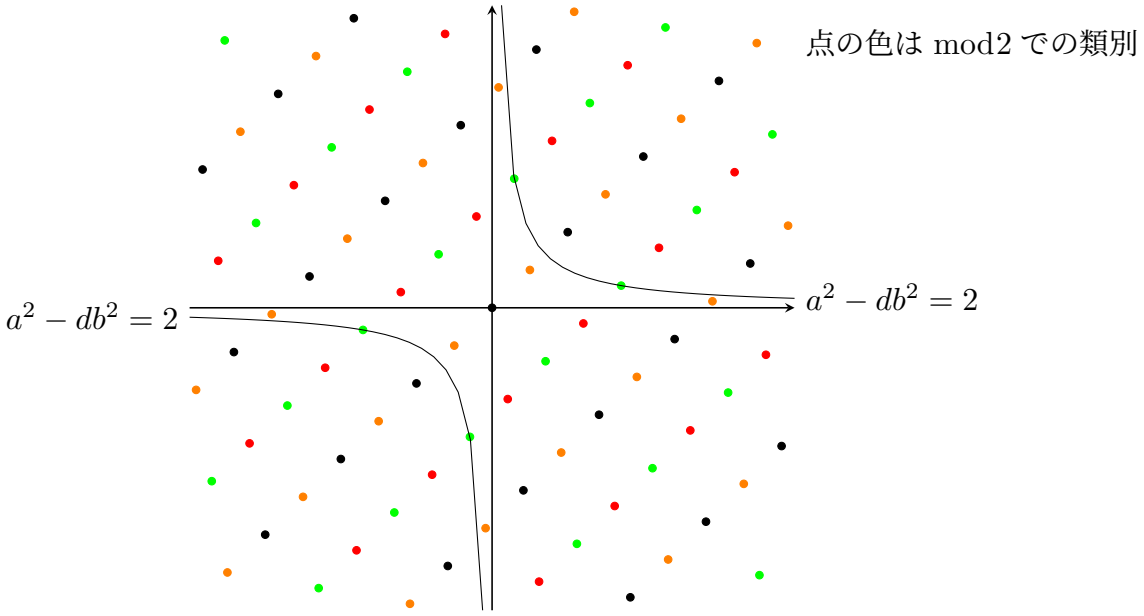
は有限集合なので, $\mathbb{Z}[\sqrt{d}]$ は $\mathrm{mod}c$ で有限個に類別できる:

$$\mathbb{Z}[\sqrt{d}] = \coprod_{0\leq a',b'\leq c-1} \{\beta \in \mathbb{Z}[\sqrt{d}] \mid \beta \equiv a' + b'\sqrt{d} \mod c\}.$$

よって

$$\begin{aligned}&\{\beta \in \mathbb{Z}[\sqrt{d}] \mid |N(\beta)| = c\}\\ &= \coprod_{0\leq a',b'\leq c-1} \{\beta \in \mathbb{Z}[\sqrt{d}] \mid |N(\beta)| = c,\ \beta \equiv a' + b'\sqrt{d} \mod c\}\end{aligned}$$

と分けたとき, いずれかの $\alpha := a' + b'\sqrt{d}$ に対し, $\{\beta \in \mathbb{Z}[\sqrt{d}] \mid |N(\beta)| = c,\ \beta \equiv \alpha \mod c\}$ は無限集合.




(c) (b) で見つけた無限集合 $\{\beta \in \mathbb{Z}[\sqrt{d}] \mid |N(\beta)| = c,\ \beta \equiv \alpha \mod c\}$ から 1 元 $\beta_0$ をとり固定する. 同じ集合から元 $\beta$ を取るごとに

$$\epsilon := \beta/\beta_0^{-1} \in \mathbb{Z}[\sqrt{d}]^\times$$

となる. 実際 $\beta \equiv \beta_0 \mod c$ だから $\beta = \beta_0 + c\beta_1$ とかける. $\beta_0\rho(\beta_0) = N(\beta_0) = \pm c$ に注意すると

$$\epsilon = \frac{\beta_0 + c\beta_1}{\beta_0} = 1 \pm \rho(\beta_0)\beta_1 \in \mathbb{Z}[\sqrt{d}].$$

さらに

$$N(\epsilon) = N(\beta)/N(\beta_0) = \pm c/c = \pm 1$$

だから, 問題 9-(2) より $\epsilon \in \mathbb{Z}[\sqrt{d}]^\times$. よって $|\mathbb{Z}[\sqrt{d}]^\times| = \infty$. 問題 9-(5) より $|P_d| < \infty$. さらに $L$ に準同型定理を使うと $\frac{|P_d|}{|L(P_d)|} = |\ker L| = 2$ が分かり, $|L(P_d)| < \infty$ を得る.

(4) 準同型定理と (3) より $P_d \twoheadrightarrow P_d/\ker L \cong L(P_d) \cong \mathbb{Z}$. $P_d$ の任意の元 $\epsilon$ をとってその像を $n \in \mathbb{Z}$ とすると $L(\epsilon) = L(\epsilon_0)^n$. $\ker L = \{\pm 1\}$ より $\epsilon = \pm\epsilon_0^n$. □

**注意 1.3.5.** 主張も証明も, ディリクレの単数定理 ($\Rightarrow$ 定理 3.3.7) の特別な場合である.

**系 1.3.6.** $d$ を平方数でない自然数とする. このとき Pell 方程式の一般解は

$$(\pm x_n, \pm y_n)\ (n \in \mathbb{Z})$$

となる. ただし $x_n, y_n$ は定理 1.3.4 の $x_1, y_1$ を用いて

$$x_n + \sqrt{d}y_n := (x_1 + \sqrt{d}y_1)^n \quad (\in \mathbb{Z}[\sqrt{d}])$$

で定義される.

**注意 1.3.7.** 以上により Pell 方程式の一般解の求解はその “最小解” $(x_1, y_1)$ の求解に帰着された.

**問題 10.** Pell 方程式 $x^2 - 2y^2 = 1$ の解で $|x|, |y| < 1000$ を満たすものをすべて求めよ.

**定義 1.3.8.** $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$ $(i = 1, 2, \dots)$ を用いて

$$[a_0; a_1, a_2, \dots, a_{n-1}, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots\, a_{n-1} + \cfrac{1}{a_n}}}}$$

の形に表される数を **(正則) 連分数** と呼ぶ. また, その極限

$$[a_0; a_1, a_2, \dots] := \lim_{n\to\infty} [a_0; a_1, a_2, \dots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

は必ず収束し, こちらも **(無限) 連分数** と呼ばれる. 与えられた (有限または無限) 連分数 $[a_0; a_1, \dots]$ に対し, $a_n$ までで止めて既約分数に表したものを $\frac{p_n}{q_n}$ で表し, **($n$ 番目の) 連分数近似** などと呼ぶ. すなわち

$$\frac{p_n}{q_n} := [a_0; a_1, \dots, a_n], \quad \gcd(p_n, q_n) = 1.$$

無限連分数の $a_n$ が循環する, すなわち

$$\exists l, m \in \mathbb{N} \text{ s.t. } n > m \Rightarrow a_n = a_{n+l}$$

のとき, **循環連分数** と呼び, 上記を満たす最小の $l$ をその **周期** と呼ぶ. またこのとき, 循環する部分 (循環節) に ‾ をつけて

$$[a_0; a_1, a_2, \dots, a_m, \overline{a_{m+1}, \dots, a_{m+l}}]$$

のように表す.

**定理 1.3.9.** (1) 任意の $\alpha \in \mathbb{R} - \mathbb{Q}$ は (無限) 連分数 $[a_0; a_1, a_2, \dots]$ の形に一意的に表される. またその表記は以下の手順で得られる: 実数 $\alpha$ の整数部分 $\lfloor \alpha \rfloor$ を $\lfloor \alpha \rfloor \in \mathbb{Z}$, $0 \leq \alpha - \lfloor \alpha \rfloor < 1$ で定める.

- $a_0 := \lfloor \alpha \rfloor$, $\alpha_1 := \frac{1}{\alpha - a_0}$.
- $a_n$ まで定まっているとき, $a_{n+1} := \lfloor \alpha_n \rfloor$, $\alpha_{n+1} := \frac{1}{\alpha_n - a_n}$.

得られた連分数 $[a_0; a_1, a_2, \dots]$ を $\alpha$ の **連分数展開** と呼ぶ.

(2) (1) の対応で, $\alpha$ が **二次無理数** ($\overset{\text{def}}{\Leftrightarrow}$ $\mathbb{Z}$ 係数の既約 2 次多項式の根) であることと, 連分数が循環連分数であることは同値.

(3) $d$ を平方数でない自然数とする. このとき $\sqrt{d}$ の連分数展開は

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \dots, a_l}]$$

の形になる. この周期を $l$ とおいたとき

$$(x_1, y_1) = \begin{cases} (q_{l-1}, p_{l-1}) & (2 \mid l), \\ (q_{2l-1}, p_{2l-1}) & (2 \nmid l) \end{cases}$$

が Pell 方程式 $x^2 - dy^2 = 1$ の最小解となる.

**補足 1.3.10.** 詳細は [木田, §8], [小野, §46] などを参照.

**問題 11.** Pell 方程式 $x^2 - 5y^2 = 1$ の最小解と一般解を求めよ.

ヒント：$\sqrt{5} = [2; \overline{4}] := 2 + \cfrac{1}{4 + \cfrac{1}{4 + \cfrac{1}{\ddots}}}$.

## 8/25 の復習 $+\alpha$

- “演算と逆元 ($\coloneqq$ 逆演算)” が定義されている集合が群. 例えば $\mathbb{Z}$ 上では “$+$ と $-$”, $\mathbb{R}^\times$ 上では “$\times$ と $\div$” が定義される.
- $+, -, \times$ まで定義された集合が環. 例えば $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$.
- $+, -, \times, \div$ (ただし $\div 0$ 以外) まで定義された集合が体. 例えば $\mathbb{R}$, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.
- 環の乗法群も重要な群. 例えば $(\mathbb{Z}/n\mathbb{Z})^\times$, $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.
- 昨日は話しそびれたが, “関数の合成” を演算とする群も重要. この場合, 逆元は逆関数となる. たとえば対称群 $S_n := \{f \colon \{1, 2, \dots, n\} \to \{1, 2, \dots, n\} \mid \text{全単射}\}$.
- ルジャンドル記号 $(\frac{*}{p}) \colon \mathbb{F}_p^\times \twoheadrightarrow \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \{\pm 1\}$.

# 2　体・ガロア理論と代数体

概略

- “四則演算 $(\pm, \times, \div)$ が定義されている集合” を「体」と呼ぶ.
- “自己同型が豊富な体の拡大” を「ガロア拡大」と呼び, そのような拡大は「ガロア群」と「ガロア理論」で調べることができる.
- ガロア理論の応用として「作図可能性」を紹介する.

## 2.1　体論 (概説)

**定義 2.1.1.** $K \neq \emptyset$ とする.

(0) $K$ 上に 2 種の演算 $\cdot, +$ が定義され,
(1) $(K, +)$ は加法群 (アーベル群であり, 演算を $+$ で表す) である.
(2) 乗法の結合法則: $\forall a, b, c \in K$, $a(bc) = (ab)c$.
(3) 乗法の単位元: $\exists 1 = 1_K$ s.t. $\forall a \in K$, $1a = a1 = a$.
(4) 分配法則: $\forall a, b, c \in K$, $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.
(5) 乗法の交換法則: $\forall a, b \in K$, $ab = ba$.
(6) $K^\times := \{a \in K \mid \exists b \in K \text{ s.t. } ab = 1\} = K - \{0\} \neq \emptyset$.

を満たすとき, $(K, +, \cdot)$ または $K$ を **体** と呼ぶ.

**注意 2.1.2.** 可換環 ($\Rightarrow$(0)$\sim$(5)) で, 0 以外での割り算ができれば ($\Rightarrow$(6)) 体である.

**例 2.1.3.** (1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は体である. それぞれ有理数体, 実数体, 複素数体と呼ばれる.
(2) 問題 4-(3) より, 各素数 $p$ に対し $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ も体になる.
(3) $\mathbb{Z}$ は $\mathbb{Z}^\times = \{\pm 1\} \subsetneq \mathbb{Z} - \{0\}$ なので体ではない ($\pm 1$ 以外での割り算ができない).

**定義 2.1.4.** (1) $K \subset L$ であり, $K, L$ は同じ演算に関して共に体であるとき, $K \subset L$ は **体拡大**, $L$ は $K$ の **拡大体**, $K$ は $L$ の **部分体** と呼ばれる. (この授業では) 記号 $L/K$, $\begin{matrix} L \\ | \\ K \end{matrix}$ などで表す.
(2) $F \subset K \subset L$ で $K/F, L/K$ がそれぞれ体拡大であるとき, $K$ は $L/F$ の **中間体** と呼ばれる. とくに $L$ は最大の中間体で $F$ は最小の中間体である.

(3) $L/K$ が体拡大であれば, $L$ は $K$ ベクトル空間となる. この次元 $\dim_K L$ を $L/K$ の **拡大次数** と呼び, 記号 $[L:K]$ で表す. $[L:K]$ が有限のとき **有限次拡大**, 無限のとき **無限次拡大** と呼ぶ. また, 体 $K$ の拡大次数 $n$ の拡大体 $L$ を**$K$ の $n$ 次拡大**である, と言い, 記号 $K \overset{n}{\subset} L$ で表す (※この授業のみの記号). すなわち, 体拡大 $L/K$ に対し, $K \overset{n}{\subset} L \Leftrightarrow K$ 上一次独立な元 $\alpha_1, \ldots, \alpha_n \in L$ が存在して

$$L = \{a_1\alpha_1 + \cdots + a_n\alpha_n \mid a_1, \ldots a_n \in K\} = K\alpha_1 \oplus \cdots \oplus K\alpha_n$$

の形に書ける.

**問題 12.** $\mathbb{C}/\mathbb{R}$ は体拡大であることを確かめよ. また $[\mathbb{C}:\mathbb{R}]$ を求めよ.

**補題 2.1.5.** 体拡大の列 $L/K/F$ に対して $[L:F] = [L:K][K:F]$.

**証明.** $L$ の $K$ 上の基底を $\{l_\lambda\}$, $K$ の $F$ 上の基底を $\{k_\kappa\}$ とおく. このとき $L = \oplus_\lambda K l_\lambda = \oplus_\lambda(\oplus_\kappa F k_\kappa)l_\lambda = \oplus_{\lambda,\kappa} F(k_\kappa l_\lambda)$ となることが示せる. □

**定義 2.1.6.** (1) 体 $K, L$ に対し, 写像 $f\colon K \to L$ が

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b), \quad f(1_K) = 1_L$$

を満たすとき, $f$ は **(体の) 準同型写像** と呼ばれる. 更に全単射であるとき **同型写像** と呼ぶ. $K$ から $K$ 自信への同型写像は **自己同型写像** と呼ばれる. 同型写像 $f\colon K \to L$ が存在するとき $K, L$ は **(体として) 同型** であると言い, 記号 $K \cong L$ で表す. $K$ から $L$ への準同型写像全体のなす集合, $K$ の自己同型写像全体のなす集合をそれぞれ

$$\begin{aligned} \mathrm{Hom}(K,L) &:= \{f\colon K \to L \mid f\text{: 体準同型}\}, \\ \mathrm{Aut}(K) &:= \{f\colon K \to K \mid f\text{: 体準同型, 全単射}\} \end{aligned}$$

で表す.

(2) $K/k$, $L/k$ は共通の部分体を持つ体拡大とする. このとき

$$\begin{aligned} \mathrm{Hom}_k(K,L) &:= \{f \in \mathrm{Hom}(K,L) \mid f|_k = \mathrm{id}_k\}, \\ \mathrm{Aut}(K/k) &:= \{f \in \mathrm{Aut}(K) \mid f|_k = \mathrm{id}_k\} \end{aligned}$$

の元を, それぞれ **$k$ 上の準同型写像**, **$k$ 上の自己同型写像** と呼ぶ. また, 同型写像 $f\colon K \overset{\cong}{\to} L$ で $f|_k = \mathrm{id}_k$ となるものを **$k$ 上の同型写像** と呼ぶ. $k$ 上の同型写像 $f\colon K \overset{\cong}{\to} L$ が存在するとき, 記号 $K \underset{k}{\cong} L$ で表す.

**命題 2.1.7.** $f\colon K \to L$ を体準同型写像とする.

(1) $f(0_K) = 0_L$, $\forall a \in K$, $f(-a) = -f(a)$, $\forall a \in K^\times$, $f(a^{-1}) = f(a)^{-1}$.
(2) $f$ は (自動的に) 単射. とくに $f$ に対し, 全射 $\Leftrightarrow$ 全単射 $\Leftrightarrow$ 同型.

**証明**. (1) 体準同型写像は加法群としての準同型でもあるので, 群準同型の一般論より最初の二つが成り立つ. 三つ目は $1_L = f(1_K) = f(aa^{-1}) = f(a)f(a^{-1})$ より.

(2) 単射でないとする. このとき $\exists a \neq \exists b$, $f(a) = f(b) \overset{c:=a-b}{\Rightarrow} c \neq 0$, $f(c) = 0$. 一方で $c \neq 0 \overset{(1)}{\Rightarrow}$ "$f(c)$ は単元" なので矛盾. □

**問題 13.** 複素共役写像

$$\rho_c\colon \mathbb{C} \to \mathbb{C}, \quad x + y\sqrt{-1} \mapsto x - y\sqrt{-1}\ (x, y \in \mathbb{R})$$

に対し $\rho_c \in \mathrm{Aut}(\mathbb{C}/\mathbb{R})$ を示せ.

**命題 2.1.8.** $\mathrm{Aut}(K), \mathrm{Aut}(K/k)$ は, それぞれ合成に関して群になる.

**証明**. 単位元は恒等写像 $\mathrm{id}_K$, $f$ の逆元は逆写像 $f^{-1}$ で与えられる. □

**定義 2.1.9.** 体拡大 $L/k$ が以下の同値な条件のいずれか (よって全部) を満たすとき, $L/k$ は **有限次ガロア拡大** である, という.

(1) $L/k$ は有限次かつ正規かつ分離拡大.
(2) $|\mathrm{Aut}(L/k)| = [L : k] < \infty$.
(3) $|\mathrm{Aut}(L/k)| \geq [L : k] < \infty$.

拡大次数が $[L : k] = n$ のときは $n$ 次ガロア拡大とも呼ぶ. 有限次ガロア拡大 $L/k$ に対し

$$\mathrm{Gal}(L/k) := \mathrm{Aut}(L/k)$$

を, 有限次ガロア拡大 $L/k$ の **ガロア群** と呼ぶ.

**補足 2.1.10.** (1) $L/k$ が代数拡大 $\overset{\mathrm{def}}{\Leftrightarrow} \forall \alpha \in L, \exists f(x) \in k[X] - \{0\}$ s.t. $f(\alpha) = 0$.
(2) 有限次拡大 $\Rightarrow$ 代数拡大.
(3) $L/k$ が正規拡大 $\overset{\mathrm{def}}{\Leftrightarrow} \forall \Omega/L$, $\forall \sigma \in \mathrm{Aut}(\Omega/k)$, $\sigma(L) = L$.
(4) $L/k$ が分離拡大 $\overset{\mathrm{def}}{\Leftrightarrow} \forall \alpha \in L, \exists f(x) \in k[x] - \{0\}$ s.t. $f(\alpha) = 0$, $f'(\alpha) \neq 0$.
(5) $\Omega$ を $k$ の任意の拡大体としたとき, 一般には

$$|\mathrm{Aut}(L/k)| \leq |\mathrm{Hom}_k(L, \Omega)| \leq [L : k] \tag{2.1}$$

が成り立つ. さらに $\Omega$ を “十分大きく” とったとき

- $L/k$ が正規拡大 $\Leftrightarrow |\mathrm{Aut}(L/k)| = |\mathrm{Hom}_k(L, \Omega)|$.
- $L/k$ が分離拡大 $\Leftrightarrow |\mathrm{Hom}_k(L, \Omega)| = [L : k]$

が成り立つ.

**例 2.1.11.** $\mathbb{C}/\mathbb{R}$ は 2 次ガロア拡大である. 実際

$$[\mathbb{C} : \mathbb{R}] = 2, \quad \mathrm{Aut}(\mathbb{C}/\mathbb{R}) \supset \{\mathrm{id}, \rho_c\}$$

が分かり,

$$|\mathrm{Aut}(\mathbb{C}/\mathbb{R})| \geq 2 = [\mathbb{C} : \mathbb{R}]$$

を得る. なお定義 2.1.9 同値 (2)⇔(3) ($\because$ Eq. (2.1)) より $|\mathrm{Aut}(\mathbb{C}/\mathbb{R})| = 2 = [\mathbb{C} : \mathbb{R}]$ となり,

$$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \rho_c\}.$$

## 2.2 二次体, 円分体, 代数体

**定義-命題 2.2.1.** (1) $\mathbb{C}/\mathbb{Q}$ の中間体 $K$ s.t. $[K : \mathbb{Q}] < \infty$ を **(有限次) 代数体** と呼ぶ.

(2) 平方数でない整数 $d$ を用いて

$$\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} = \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \sqrt{d}$$

と表される体を **二次体** ($d > 0$ のとき実二次体, $d < 0$ のとき虚二次体) と呼ぶ.

(3) $\zeta_n := e^{\frac{2\pi i}{n}}$ とおく.

$$\mathbb{Q}(\zeta_n) := \{f(\zeta_n) \mid f(x) \in \mathbb{Q}[x]\} = \sum_{i=0}^{n-1} \mathbb{Q} \cdot \zeta_n^i = \bigoplus_{i=0}^{[\mathbb{Q}(\zeta_n):\mathbb{Q}]} \mathbb{Q} \cdot \zeta_n^i$$

を **円分体** と呼ぶ.

**補足 2.2.2.** (1) $\alpha \in \mathbb{C}$ が **代数的数** $\overset{\mathrm{def}}{\Leftrightarrow} \exists f(x) \in \mathbb{Q}[x] - \{0\}$ s.t. $f(\alpha) = 0$.

(2) 任意の代数体 $K$ は, 代数的数 $\alpha$ を用いて

$$K = \mathbb{Q}(\alpha) := \{f(\alpha) \mid f(x) \in \mathbb{Q}[x]\}$$

の形で表せる. さらにこのとき, 写像

$$v_\alpha \colon \mathbb{Q}[x] \to \mathbb{C}, \ f(x) \mapsto f(\alpha)$$

は環準同型となり,

$$K = v_\alpha(\mathbb{Q}[x]), \quad \exists f_\alpha(x) \in \mathbb{Q}[x] \text{ s.t. } \ker v_\alpha = (f_\alpha(x))$$

となる. $f_\alpha(x)$ の最高次係数が 1 になるようにとったものを $\alpha$ の **最小多項式** と呼ぶ.

**命題 2.2.3.** (1) 平方数でない整数 $d$ に対して $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ は 2 次ガロア拡大であり

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{id}, \rho\} \cong \{\pm 1\}, \quad \mathrm{id} \mapsto 1,\ \rho \mapsto -1.$$

(2) $n \in \mathbb{N}$ に対して $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ は $\varphi(n)$ 次ガロア拡大であり

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma_a \mapsto \overline{a}.$$

ただし

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} = a \bmod n \mid 1 \le a \le n,\ \gcd(a,n) = 1\},\ \varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|,$$

$$\sigma_a \colon \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n),\ \sum_{i=0}^{k} c_i \zeta_n^i \mapsto \sum_{i=0}^{k} c_i \zeta_n^{ai}\ (c_i \in \mathbb{Q}).$$

**補足 2.2.4.** $\varphi(n)$ は **オイラーのトーシェント関数** と呼ばれ, 以下の公式がある:

$$\varphi(n) = n \prod_{p \mid n} (1 - p^{-1}). \tag{2.2}$$

ただし $p$ は $n$ の素因子を動く. 感覚的には

(1) $n$ と互いに素 $\Leftrightarrow$ $n$ の各素因子 $p$ と互いに素,
(2) $p$ の倍数である確率 $= p^{-1}$, $p$ と互いに素である確率 $= 1 - p^{-1}$.

でこの公式は説明できる (が証明は難しい).

**補足 2.2.5.** $\zeta_n$ の最小多項式の次数が $\varphi(n)$ となる部分 (だけ) が難しく, 初等的な証明は無いように思える. 詳細は [小野, §36], [足立, 第 13 章, §1] など参照.

## 2.3 ガロア理論 (概説)

**定理 2.3.1** (ガロア理論の基本定理)**.** 有限次ガロア拡大 $L/k$ に対し **ガロア対応** と呼ばれる, 以下の一対一対応がある.

$$\{K \mid L/K/k\} \longleftrightarrow \{H \mid H < \mathrm{Gal}(L/k)\}.$$

ただし

- 左辺は $L/k$ の中間体 $K$ 全体のなす集合.
- 右辺は $\mathrm{Gal}(L/k)$ の部分群 $H$ 全体のなす集合.

を表す. 対応は

(1) 右向きの対応は

$$\Phi\colon K \mapsto \mathrm{Gal}(L/k)_K := \{\sigma \in \mathrm{Gal}(L/k) \mid \sigma|_K = \mathrm{id}_K\}.$$

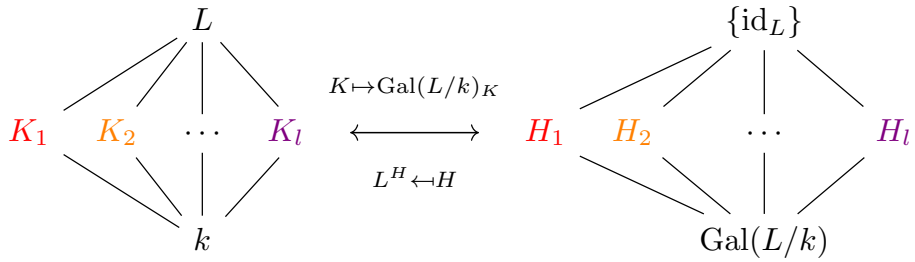
(2) 左向きの対応は

$$\Psi\colon H \mapsto L^H := \{\alpha \in L \mid \forall \sigma \in H,\ \sigma(\alpha) = \alpha\}.$$

で与えられる. これらは互いに逆の対応である:

(3) $\Psi \circ \Phi = \mathrm{id}$, すなわち $K \mapsto \mathrm{Gal}(L/k)_K \mapsto L^{\mathrm{Gal}(L/k)_K} = K$, および
$\Phi \circ \Psi = \mathrm{id}$, すなわち $H \mapsto L^H \mapsto \mathrm{Gal}(L/k)_{L^H} = H$.

イメージ図




また, ガロア対応は以下を満たす.

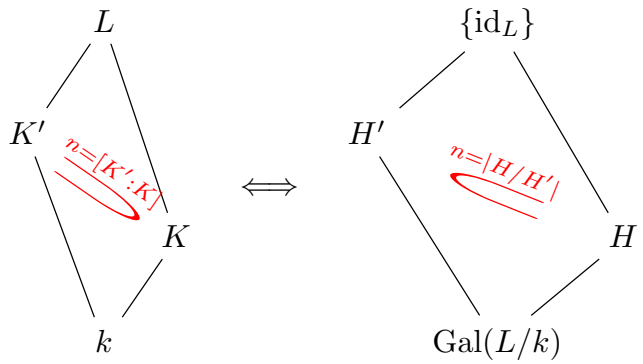
(4) ガロア対応により $K \leftrightarrow H$, $K' \leftrightarrow H'$ が対応するとき

$$K \subset K' \Leftrightarrow H \supset H'.$$

またこれらが成り立つとき

$$[K' : K] = |H/H'| \ \left(= \frac{|H|}{|H'|}\right).$$

イメージ図



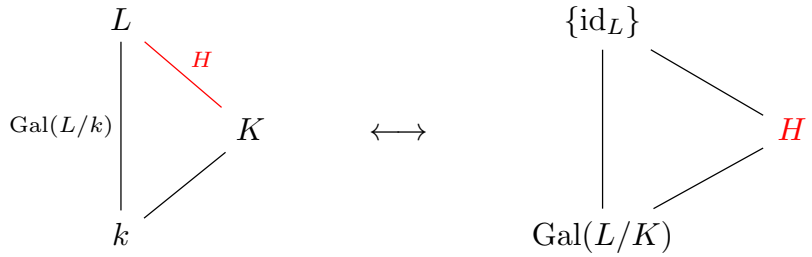

以下, ガロア対応での対応を $K \leftrightarrow H$ で表す.

(5) $k \leftrightarrow \mathrm{Gal}(L/k)$, $L \leftrightarrow \{\mathrm{id}_L\}$.

(6) $L/K/k$ のとき $L/K$ も有限次ガロア拡大であり, 自然に $\mathrm{Gal}(L/K) \subset \mathrm{Gal}(L/k)$ とみなせる. とくに

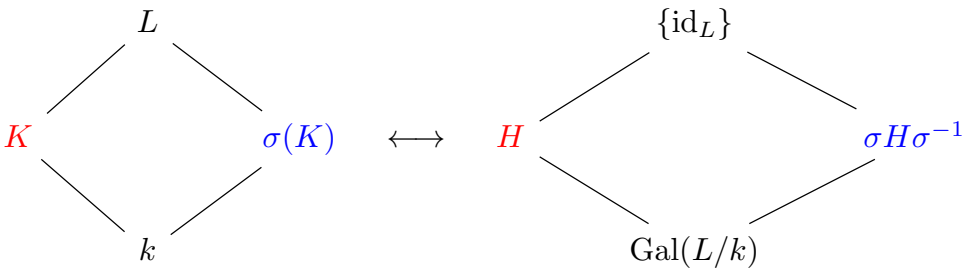
$$K \leftrightarrow H \Rightarrow \mathrm{Gal}(L/K) = H.$$

イメージ図




(7) $K \leftrightarrow H$, $\sigma \in \mathrm{Gal}(L/k) \Rightarrow \sigma(K) \leftrightarrow \sigma H \sigma^{-1}$.

イメージ図



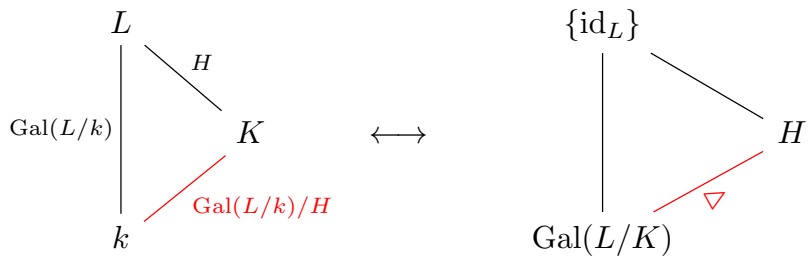
(8) $K \leftrightarrow H$ とする．このとき

$K/k$ が有限次ガロア拡大 $\Leftrightarrow$ $K/k$ が正規拡大 $\Leftrightarrow$ $H$ は $\mathrm{Gal}(L/k)$ の正規部分群．

またこれらが成り立つとき

$$\mathrm{Gal}(L/k)/H \xrightarrow[\sigma H \mapsto \sigma|_K]{\cong} \mathrm{Gal}(K/k).$$

イメージ図

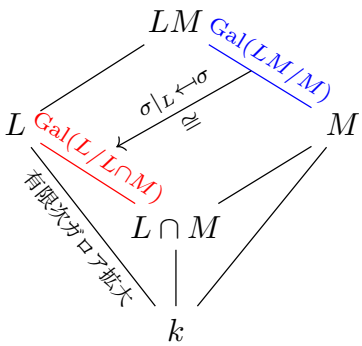



**定理 2.3.2 (推進定理).** 体拡大 $\Omega/k$ の中間体 $L, M$ を考える: $\Omega/L/k$, $\Omega/M/k$.

(9) $L/k$ を有限次ガロア拡大とする．このとき $LM/M$ も有限次ガロア拡大であり

$$\mathrm{Gal}(LM/M) \xrightarrow[\sigma \mapsto \sigma|_L]{\cong} \mathrm{Gal}(L/L \cap M).$$

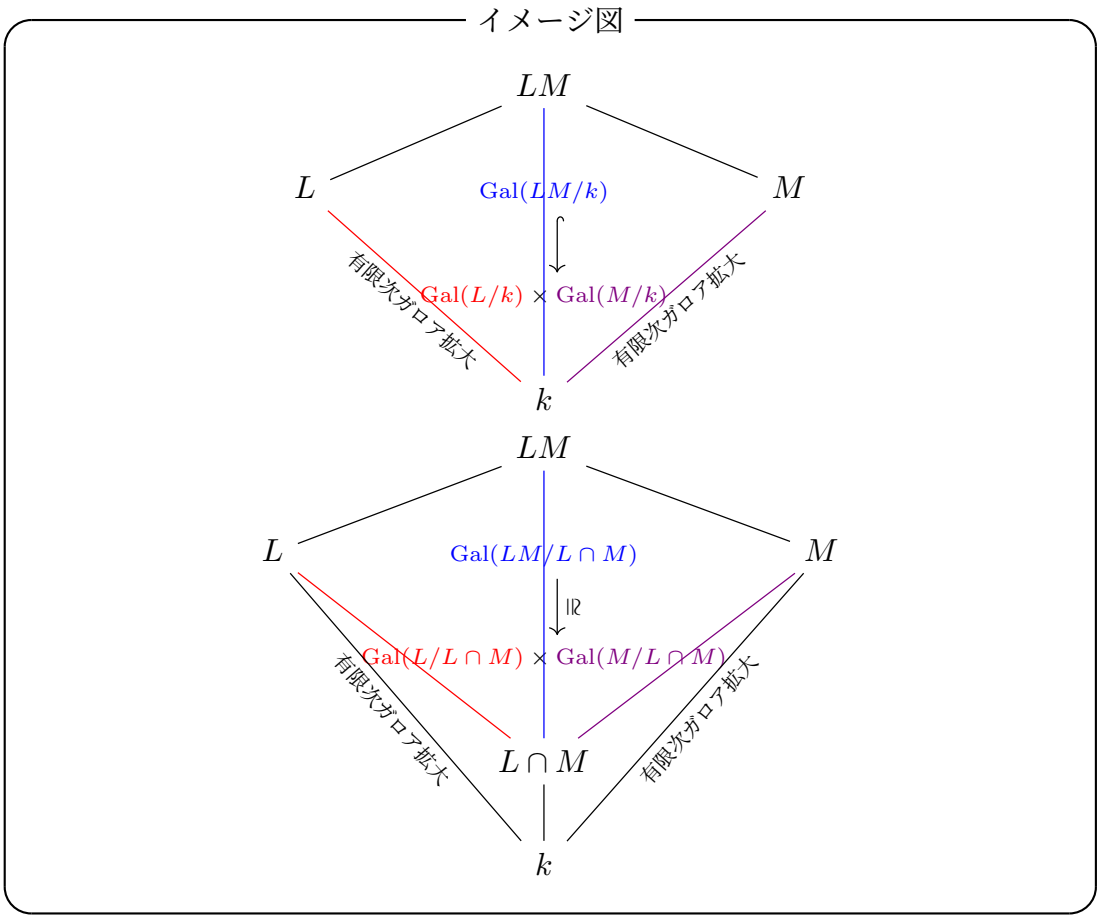
イメージ図




(10) $L/k$, $M/k$ がともに有限次ガロア拡大であるとする．このとき $LM/k$, $LM/(L \cap M)$ も有限次ガロア拡大であり

$$\mathrm{Gal}(LM/k) \xrightarrow[\sigma \mapsto (\sigma|_L, \sigma|_M)]{\cong} \{(\sigma, \tau) \in \mathrm{Gal}(L/k) \times \mathrm{Gal}(M/k) \mid \sigma|_{L\cap M} = \tau|_{L\cap M}\}$$
$$\subset \mathrm{Gal}(L/k) \times \mathrm{Gal}(M/k),$$

$$\mathrm{Gal}(LM/L\cap M) \xrightarrow[\sigma\mapsto(\sigma|_L,\sigma|_M)]{\cong} \mathrm{Gal}(L/(L\cap M))\times\mathrm{Gal}(M/(L\cap M)).$$




**例 2.3.3.** $n=5$ のとき

$$\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \overset{\text{“同一視”}}{\cong} (\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1},\overline{2},\overline{3},\overline{4}\}$$
$$\left(= \langle\overline{2}\rangle = \{\overline{2}^i \mid i=0,1,2,3\} \overset{\overline{2}^i\leftrightarrow i \bmod 4}{\cong} \mathbb{Z}/4\mathbb{Z}\right).$$

の部分群は

$$\{\overline{1}\},\qquad \{\overline{1},\overline{4}\},\qquad \mathbb{Z}/5\mathbb{Z}^\times$$

の 3 つ. ガロア対応は

$$\begin{array}{ccc} \mathbb{Q}(\zeta_5) & \leftarrow\cdots\rightarrow & \{\overline{1}\} \\ \cup\wr & & \wedge\wr \\ \mathbb{Q}(\zeta_5)^{\{\overline{1},\overline{4}\}} & \leftarrow\cdots\rightarrow & \{\overline{1},\overline{4}\} \\ \cup\wr & & \wedge\wr \\ \mathbb{Q} & \leftarrow\cdots\rightarrow & \mathbb{Z}/5\mathbb{Z}^\times \end{array}$$

となる.
※ 左辺の $\overset{n}{\subset}$ は $n$ 次拡大, 右辺の $\overset{n}{<}$ は指数 $n$ の部分群を表す (この授業のみの記法).

**補足 2.3.4.** 具体的には

$$\begin{aligned} \mathbb{Q}(\zeta_5)^{\{\overline{1},\overline{4}\}} &= \left\{c_1\zeta_5 + c_2\zeta_5^2 + c_3\zeta_5^3 + c_4\zeta_5^4 \;\middle|\; c_i \in \mathbb{Q},\ c_1 = c_4,\ c_2 = c_3\right\} \\ &= \mathbb{Q}(\zeta_5 + \zeta_5^4) \oplus \mathbb{Q}(\zeta_5^2 + \zeta_5^3) = \mathbb{Q}\frac{-1+\sqrt{5}}{2} \oplus \mathbb{Q}\frac{-1-\sqrt{5}}{2} = \mathbb{Q}(\sqrt{5}) \end{aligned}$$

が分かる.

**問題 14.** $n = 7$ のとき例 2.3.3 と同様の議論をせよ.
ヒント：$(\mathbb{Z}/7\mathbb{Z})^\times$ の部分群は $\{\overline{1}\},\ \{\overline{1},\overline{6}\},\ \{\overline{1},\overline{2},\overline{4}\},\ \mathbb{Z}/7\mathbb{Z}^\times$ の 4 つ.

## 2.4 # 作図可能性

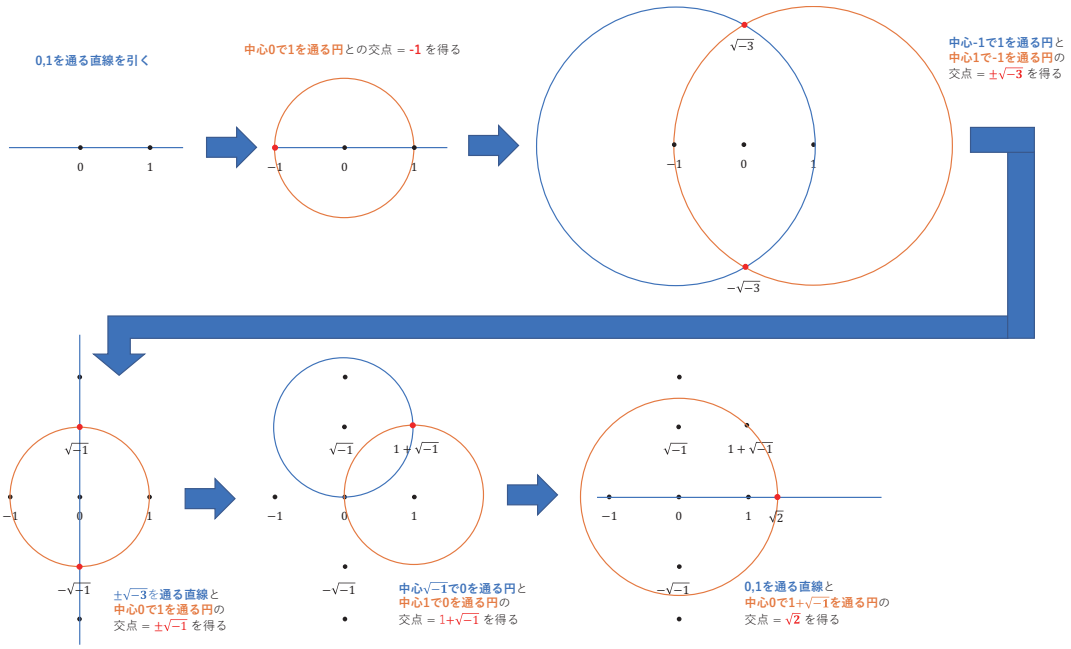
**定理 2.4.1.** $\alpha \in \mathbb{C}$ に対して以下は同値.

(1) $\alpha$ は作図可能な数である.
(2) $\mathbb{Q} =: K_0 \overset{2}{\subset} \exists K_1 \overset{2}{\subset} \exists K_2 \overset{2}{\subset} \cdots \overset{2}{\subset} \exists K_n \subset \mathbb{C}$ s.t. $\alpha \in K_n$.

**例 2.4.2.** $\sqrt{2}$ は

$$\mathbb{Q} \overset{2}{\subset} \mathbb{Q}(\sqrt{2}) \ni \sqrt{2}$$

より定理 2.4.1-(2) の条件を満たすので作図可能な数である (次図参照).




**補足 2.4.3.** 定理 2.4.1 の証明の概略:

- 直線と直線の交点 $\fallingdotseq$ 連立方程式 $\begin{cases} ax+by=c \\ dx+ey=f \end{cases}$ の解 $\Leftarrow$ 四則演算
- 直線と円の交点 $\fallingdotseq \begin{cases} ax+by=c \\ (x-d)^2+(y-e)^2=f \end{cases}$ の解 $\Leftarrow$ 二次方程式を解く
- 円と円の交点 $\fallingdotseq \begin{cases} (x-a)^2+(y-b)^2=c \\ (x-d)^2+(y-e)^2=f \end{cases}$ の解 $\Leftarrow$ 二次方程式を解く

により, $K_i$ からスタートして作図可能な点の座標は, ある二次方程式 $ax^2+bx+c=0$ $(a,b,c\in K_i)$ の解. これは $K_i$ の 2 次拡大 $K_{i+1}=K_i(\sqrt{b^2-4ac})$ に含まれる.

**定理 2.4.4.** $n\geq 3$ に対して以下は同値.

(1) 正 $n$ 角形は定規とコンパスで作図できる. すなわち, 単位円の $n$ 等分点 $\zeta_n = e^{\frac{2k\pi i\sqrt{-1}}{n}} = \cos\frac{2k\pi}{n}+\sqrt{-1}\sin\frac{2k\pi}{n}$ $(k=0,1,\dots,n-1)$ は作図可能な数である.
(2) $n$ の素因数分解は $n=2^k p_1\cdots p_r$ $(k,r\geq 0,\ p_i$ は $2^l+1$ の形の相異なる素数) の形.

**証明.** 定理 2.4.1 より

$$(1)\ \zeta_n \text{ が作図可能} \Leftrightarrow (1')\ \mathbb{Q}\overset{2}{\subset}\exists K_1\overset{2}{\subset}\cdots\overset{2}{\subset}\exists K_{l-1}\overset{2}{\subset}\exists K_l\ni\zeta_n.$$

一方で Eq. (2.2) より

(2) $n = 2^k p_1 \cdots p_r$ ($k, r \geq 0$, $p_i$ は $2^l + 1$ の形の相異なる素数) $\Leftrightarrow$ (2') $\varphi(n) = 2^{\exists k}$.

((1')⇒(2')) $[K_l : K_1] = [K_l : K_{l-1}] \dots [K_1 : \mathbb{Q}] = 2^l$. 一方で $K_l/\mathbb{Q}(\zeta_n)/\mathbb{Q}$ より $[K_l : \mathbb{Q}] = [K_l : \mathbb{Q}(\zeta_n)][\mathbb{Q}(\zeta_n) : \mathbb{Q}]$. よって $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ は 2 べキ.

((2')⇒(1')) (2') より $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ の位数は 2 べキ. よって有限生成アーベル群の基本定理より

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/2^{k_1}\mathbb{Z} \times \mathbb{Z}/2^{k_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/2^{k_s}\mathbb{Z}$$

の形に書ける. それぞれの成分で

$$\mathbb{Z}/2^{k_i}\mathbb{Z} \overset{2}{>} 2\mathbb{Z}/2^{k_i}\mathbb{Z} \overset{2}{>} 2^2\mathbb{Z}/2^{k_i}\mathbb{Z} \overset{2}{>} \cdots \overset{2}{>} 2^{k_i-1}\mathbb{Z}/2^{k_i}\mathbb{Z} \overset{2}{>} 2^{k_i}\mathbb{Z}/2^{k_i}\mathbb{Z} = \{0\}$$

という部分群列が取れるので

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \overset{2}{>} H_1 \overset{2}{>} \cdots \overset{2}{>} H_n = \{1\}$$

という部分群列も存在し, ガロア対応で (1') の体が得られる. □

**例 2.4.5.**

$$\mathbb{Q} \overset{2}{\subset} \mathbb{Q}(\zeta_5)^{\{\overline{1},\overline{4}\}} \overset{2}{\subset} \mathbb{Q}(\zeta_5) \ni \zeta_5$$

より, $\zeta_5$ や正五角形は作図可能.

**問題 15.** $\zeta_7$ や正七角形は作図不可能であることを説明せよ.
※ 問題 14 参照.

## 2.5 # 有限体

**定義 2.5.1.** $K$ を体とする.

(1) 環準同型写像 $\phi\colon \mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$ の核は素数 $p$ または 0 で生成される (∵ 準同型定理より $\mathbb{Z}/\ker\phi \cong \phi(\mathbb{Z}) \subset K$ で, 体 $K$ の部分環は整域). この生成元を $K$ の **標数** と呼ぶ.
(2) 体 $K$ の拡大体 $L$ が
   (a) $L/K$ は代数拡大.

(b) $L$ の代数拡大は $L$ のみ.

を満たすとき $L$ は $K$ の **代数閉包** であるといい, 記号 $L = \overline{K}$ で表す.

**補足 2.5.2.** (1)「任意の体 $K$ に対し, その代数閉包が同型を除いて一意に存在する」ことがツォルンの補題を用いて証明できる.

(2) $\mathbb{C}$ の代数拡大は $\mathbb{C}$ のみである ($\because$ 代数学の基本定理) ことから, $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \exists f \in \mathbb{Q}[x] - \{0\} \text{ s.t. } f(\alpha) = 0\}$ が $\mathbb{Q}$ の代数閉包となることが分かる.

**定理 2.5.3.** $K$ を体とし, $|K| = q < \infty$ とする.

(1) $K$ の標数は素数 $p$ であり, $\exists f \in \mathbb{N}$ s.t. $q = p^f$.

(2) $K^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$.

(3) $K = \{x \in \overline{K} \mid x^q - x = 0\}$.

(4) $K_n := \{x \in \overline{K} \mid x^{q^n} - x = 0\}$ は $K$ の $n$ 次ガロア拡大である. さらに

$$\begin{aligned} &\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/n\mathbb{Z}, \quad \sigma_q^k \mapsto k \bmod n, \\ &\sigma_q \colon K_n \to K_n,\ \alpha \mapsto \alpha^q. \end{aligned}$$

(5) $\overline{K}/K$ の中間体 $L$ で $[L : K] = n$ を満たすものは $K_n$ のみである.

**証明**. (1) 標数の定義に用いた環準同型写像に準同型定理を使って

$$\mathbb{Z}/\ker\phi (\cong \phi(\mathbb{Z})) \subset K$$

とみなせる. よって $|K| < \infty$ より $\ker\phi \neq (0)$ で標数は素数 $p$. さらに $\mathbb{F}_p = \mathbb{Z}/\ker\phi$ と $|K| < \infty$ より $K/\mathbb{F}_p$ は有限次拡大で, $f := [K : \mathbb{F}_p]$ とおけば ($\mathbb{F}_p$-ベクトル空間として)$K \cong \mathbb{F}_p^f$.

(2) 補題 1.2.4-(2) より.

(3) (2) より $K = K^\times \cup \{0\} \subset \{x \in \overline{K} \mid x^{q-1} = 1\} \cup \{0\} = \{x \in \overline{K} \mid x^q - x = 0\}$. 一方で $|K| = q \geq |\{x \in \overline{K} \mid x^q - x = 0\}|$ より題意を得る.

(4) 標数 $p$ より $[\sigma_p \colon \alpha \mapsto \alpha^p] \in \mathrm{Aut}(\overline{K})$ が分かり, $p^f = q$ を満たす $f$ に対して $\sigma_q = \sigma_p^f \in \mathrm{Aut}(\overline{K})$ とみなせる. また

$$K_n = \{\alpha \in \overline{K} \mid \sigma_q(\alpha) = \alpha\}$$

とも書ける. この表示から $K_n$ は四則演算で閉じていることが分かり, 従って ($\overline{K}$ の部分) 体となる, さらに (3) より $K_n \supset K$. (1) と同じ議論で $|K_n| = |K|^{[K_n:K]}$ が

分かり, $f(x) := x^{q^n} - x$ が重根を持たない ($\because f(x) = f'(x) = 0$ が解なし) ことより $|K_n| = q^n$ が分かり, あわせて $[K_n : K] = n$. $\sigma_q \in \mathrm{Aut}(K_n/K)$ の位数が $n$ なので $[K_n : K] = n \leq |\langle\sigma_q\rangle| \leq |\mathrm{Aut}(K_n/K)|$ となり, $K_n/K$ はガロア拡大で $\mathrm{Gal}(K_n/K) = \mathrm{Aut}(K_n/K) = \langle\sigma_q\rangle$.

(5) $K$ の $n$ 次拡大を $K'$ とおき, $K, q$ を $K', q^n$ に変えて (3) を適用すればよい. □

**問題 16.** $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ の単項イデアル $(3) = \{3a + 3b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ を考える. 以下を確かめよ.

(1) $\mathbb{Z}[\sqrt{2}]/(3) = \{\overline{a + b\sqrt{2}} \mid a, b = 0, 1, 2\}$.

(2) $\mathbb{Z}[\sqrt{2}]/(3)$ における掛け算の表は以下の通り (空白を埋めよ).

| | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{\sqrt{2}}$ | $\overline{1+\sqrt{2}}$ | $\overline{2+\sqrt{2}}$ | $\overline{2\sqrt{2}}$ | $\overline{1+2\sqrt{2}}$ | $\overline{2+2\sqrt{2}}$ |
|---|---|---|---|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{\sqrt{2}}$ | $\overline{1+\sqrt{2}}$ | $\overline{2+\sqrt{2}}$ | $\overline{2\sqrt{2}}$ | $\overline{1+2\sqrt{2}}$ | $\overline{2+2\sqrt{2}}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{1}$ | $\overline{2\sqrt{2}}$ | $\overline{2+2\sqrt{2}}$ | $\overline{1+2\sqrt{2}}$ | $\overline{\sqrt{2}}$ | $\overline{2+\sqrt{2}}$ | $\overline{1+\sqrt{2}}$ |
| $\overline{\sqrt{2}}$ | $\overline{0}$ | $\overline{\sqrt{2}}$ | $\overline{2\sqrt{2}}$ | $\overline{2}$ | $\overline{2+\sqrt{2}}$ | $\overline{2+2\sqrt{2}}$ | $\overline{1}$ | $\overline{1+\sqrt{2}}$ | $\overline{1+2\sqrt{2}}$ |
| $\overline{1+\sqrt{2}}$ | $\overline{0}$ | | | | | | | | |
| $\overline{2+\sqrt{2}}$ | $\overline{0}$ | | | | | | | | |
| $\overline{2\sqrt{2}}$ | $\overline{0}$ | | | | | | | | |
| $\overline{1+2\sqrt{2}}$ | $\overline{0}$ | | | | | | | | |
| $\overline{2+2\sqrt{2}}$ | $\overline{0}$ | | | | | | | | |

(3) $\mathbb{Z}[\sqrt{2}]/(3)$ は体.

(4) $\mathbb{Z}[\sqrt{2}]/(3)$ の標数は 3.

(5) $\mathbb{Z}[\sqrt{2}]/(3)$ の任意の元は $x^9 - x = 0$ を満たす.

(6) $\mathbb{Z}[\sqrt{2}]/(3)$ の元で $x^3 - x = 0$ を満たすものは□, □, □である (空白を埋めよ).

## 8/26 の復習 $+\alpha$

- $+, -, \times, \div$ (ただし $\div 0$ 以外) まで定義された集合が体. 例えば $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$.
- 体拡大 $L/k$ に対して, $k$ 上の自己同型全体のなす集合 $\mathrm{Aut}(L/k) := \{f\colon L \to L \mid f(a+b) = f(a) + f(b),\ f(ab) = f(a)f(b),\ f|_k = \mathrm{id}_k\}$ は合成に関して群となる.
- 一般に $|\mathrm{Aut}(L/k)| \leq [L:k] := \dim_k L$ が成り立つ. "上限いっぱい $|\mathrm{Aut}(L/k)| = [L:k] < \infty$" になるときが有限次ガロア拡大で $\mathrm{Gal}(L/k) := \mathrm{Aut}(L/k)$ をそのガロア群と呼ぶ.
- 有限次ガロア拡大 $L/k$ に対しガロア対応と呼ばれる一対一対応がある:

$$\begin{array}{ccc} \{K \mid L/K/k\} & \longleftrightarrow & \{H \mid H < \mathrm{Gal}(L/k)\} \\ K & \mapsto & \mathrm{Gal}(L/k)_K \\ & & \vdots\| \\ & & \{\sigma \in \mathrm{Gal}(L/k) \mid \sigma|_K = \mathrm{id}_K\} \\ L^H & \mapsfrom & H \\ \vdots\| & & \\ \{\alpha \in L \mid \forall \sigma \in H,\ \sigma(\alpha) = \alpha\} & & \end{array}$$

- 「$\exists x, y \in \mathbb{Z}$ s.t. $\gcd(x,y) = 1$, $p \mid (x^2 + y^2) \Leftrightarrow p = 2$ または $p \equiv 1 \mod 4$」は第一補充法則 (オイラーの規準) から従う.
- 「$\exists x, y \in \mathbb{Z}$ s.t. $p = x^2 + y^2 \Leftrightarrow p = 2$ または $p \equiv 1 \mod 4$」(二平方和定理) はもう一歩難しい.

# 3　代数的整数論

概略

- 有理数体 $\mathbb{Q}$ の有限次拡大体を「代数体」と呼び, その適切な部分環を「整数環」と呼ぶ. 体より環の方が「倍数・約数」に関する情報が豊富である.
- 整数論の諸問題のいくつかは, 整数環上での「イデアル」や「単数群」の言葉に翻訳できる.
- 例として「素数の二次体における素イデアル分解」と「二平方和定理」や「平方剰余の相互法則」との関係を紹介する.

## 3.1　フェルマーの二平方和定理

二平方和 $x^2+y^2$ $(x,y\in\mathbb{Z})$ で表される整数の性質を考えてみる. まず "$x^2+y^2$ の素因数分解" の表を書いてみる:

| $y \backslash x$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | … |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 5 | $2\cdot5$ | 17 | $2\cdot13$ | 37 | $2\cdot5^2$ | $5\cdot13$ | … |
| 2 | 5 | $2^3$ | 13 | $2^2\cdot5$ | 29 | $2^3\cdot5$ | 53 | $2^2\cdot17$ | … |
| 3 | $2\cdot5$ | 13 | $2\cdot3^2$ | $5^2$ | $2\cdot17$ | $3^2\cdot5$ | $2\cdot29$ | 73 | … |
| 4 | 17 | $2^2\cdot5$ | $5^2$ | $2^5$ | 41 | $2^2\cdot13$ | $5\cdot13$ | $2^4\cdot5$ | … |
| 5 | $2\cdot13$ | 29 | $2\cdot17$ | 41 | $2\cdot5^2$ | 61 | $2\cdot37$ | 89 | … |
| 6 | 37 | $2^3\cdot5$ | $3^2\cdot5$ | $2^2\cdot13$ | 61 | $2^3\cdot3^2$ | $5\cdot17$ | $2^2\cdot5^2$ | … |
| 7 | $2\cdot5^2$ | 53 | $2\cdot29$ | $5\cdot13$ | $2\cdot37$ | $5\cdot17$ | $2\cdot7^2$ | 113 | … |
| 8 | $5\cdot13$ | $2^2\cdot17$ | 73 | $2^4\cdot5$ | 89 | $2^2\cdot5^2$ | 113 | $2^7$ | … |
| 9 | $2\cdot41$ | $5\cdot17$ | $2\cdot3^2\cdot5$ | 97 | $2\cdot53$ | $3^2\cdot13$ | $2\cdot5\cdot13$ | $5\cdot29$ | … |
| 10 | 101 | $2^3\cdot13$ | 109 | $2^2\cdot29$ | $5^3$ | $2^3\cdot17$ | 149 | $2^2\cdot41$ | … |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | |

※ $p\mid\gcd(x,y)$ であれば $p\mid(x^2+y^2)$ は自明である.

**問題 17.** 素数 $p$ に対し, 以下は同値であることを示せ.

(1) $\exists x, y \in \mathbb{Z}$ s.t. $\gcd(x, y) = 1$, $p \mid (x^2 + y^2)$.
(2) $p = 2$ または [$p$ は奇素数で $\left(\frac{-1}{p}\right) = 1$].
(3) $p = 2$ または $p \equiv 1 \mod 4$.

ヒント：(1)⇒(2): $p = 2$ なら示すことはない. $p$ は奇素数とし $p \mid (x^2 + y^2)$ とする. もし $p \mid x$ なら $0 \equiv x^2 + y^2 \equiv y^2 \mod p$ より $p \mid y$, よって $\gcd(x, y) = 1$ に矛盾. $p \nmid x \overset{a:=x^{p-2}}{\Rightarrow} \exists ax \equiv 1 \mod p \Rightarrow p \mid a^2(x^2 + y^2) \equiv 1 + (ay)^2 \mod p \overset{b:=ay}{\Rightarrow} -1 \equiv \exists b^2 \Rightarrow \left(\frac{-1}{p}\right) = 1$.
(1)⇐(2): $\left(\frac{-1}{p}\right) = 1 \Rightarrow \exists a^2 \equiv -1 \mod p \Rightarrow p \mid (a^2 + 1)$. $x = a$, $y = 1$ とおけばよい.
(2)⇔(3) には第一補充法則を使ってよい.

次に “$x^2 + y^2$ が素数” となる場合の表を書いてみる:

| $y \backslash x$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | … |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 5 | | 17 | | 37 | | | | 101 | … |
| 2 | 5 | | 13 | | 29 | | 53 | | | | … |
| 3 | | 13 | | | | | | 73 | | 109 | … |
| 4 | 17 | | | | 41 | | | | 97 | | … |
| 5 | | 29 | | 41 | | 61 | | 89 | | | … |
| 6 | 37 | | | | 61 | | | | | | … |
| 7 | | 53 | | | | | | 113 | | 149 | … |
| 8 | | | 73 | | 89 | | 113 | | | | … |
| 9 | | | | 97 | | | | | | 181 | … |
| 10 | 101 | | 109 | | | | 149 | | 181 | | … |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | |

問題 17 より

素数 $p$ が $p = x^2 + y^2$ の形に書ける ⇒ $p = 2$ または [$p$ は奇素数で $\left(\frac{-1}{p}\right) = 1$]

が分かる. 次のフェルマーの二平方和定理は, これが同値条件であることを保証する

**定理 3.1.1** (フェルマーの二平方和定理)**.** 素数 $p$ に対し, 以下は同値.

(1) $\exists x, y \in \mathbb{Z}$ s.t. $p = x^2 + y^2$.
(2) $p = 2$ または [$p$ は奇素数で $\left(\frac{-1}{p}\right) = 1$].

一つの証明のアイデアは, 数の世界を $\mathbb{Z}$ から $\mathbb{Z}[\sqrt{-1}]$ に拡大し, 素数 $p = x^2 + y^2$ を $\mathbb{Z}[\sqrt{-1}]$ の世界で $p = (x + \sqrt{-1}y)(x - \sqrt{-1}y)$ と分解することである:

$$\begin{array}{ccc} \mathbb{Z}[\sqrt{-1}] & \ni & p = (x + \sqrt{-1}y)(x - \sqrt{-1}y) \text{ と分解} \\ \cup & & \Uparrow \\ \mathbb{Z} & \ni & p = x^2 + y^2 \text{ は素数} \end{array}$$

## 3.2 素数の分解法則と二平方和定理の証明

**注意 3.2.1.** (お気持ち) 整数の世界 $\mathbb{Z}$ において

$$a \mid b \Leftrightarrow b = a\exists c \Leftrightarrow (a) \ni b \Leftrightarrow (a) \supset (b)$$

というように, 割る割られるの関係がイデアルの包含関係に翻訳できる. より一般の状況で同様の議論を行うために, 少し環論から用語を準備する.

**定義 3.2.2.** $R$ を整域とする.

(1) $a \in R - (R^\times \cup \{0\})$ が既約元 $\Leftrightarrow$ $a = bc$, $b, c \in R$ なら $b \in R^\times$ または $c \in R^\times$.
(2) $a \in R - (R^\times \cup \{0\})$ が素元 $\Leftrightarrow$ $(a)$ が素イデアル.
(3) $a, b \in R$ が同伴 $\Leftrightarrow$ $\exists u \in R^\times$ s.t. $a = ub$.
(4) $R$ が UFD $\Leftrightarrow$ $R - (R^\times \cup \{0\})$ の任意の元が既約元の積に同伴を除いて一意的に表せる.
(5) $R$ が PID $\Leftrightarrow$ $R$ の任意のイデアルは単項イデアル.

**命題 3.2.3.** $R$ を整域とし, $a, b \in R$ とする.

(1) $a$ が素元である $\Rightarrow$ $a$ が既約元である.
(2) $a, b \in R$ が同伴 $\Leftrightarrow$ $(a) = (b)$.
(3) $R$ において素元分解は (必ずできるとは限らないが) もしできれば同伴を除いて一意的. すなわち $R$ の素元 $p_*, q_*$ に対して

$$p_1 \dots p_r = q_1 \dots q_s \Rightarrow r = s \text{ かつ } \exists \sigma \in S_r \text{ s.t. } \forall i,\ (p_i) = (q_{\sigma(i)}),$$

(4) $R$ が PID であればイデアルの昇鎖列は必ず止まる. すなわちイデアル $I_*$ に対して

$$\forall I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots,\ \exists n \in \mathbb{N} \text{ s.t. } n \geq N \Rightarrow I_n = I_N.$$

(5) $R$ が PID, $a \in R$ が既約元であれば $(a)$ は極大イデアル.
(6) $R$ が PID であれば, 素元 $\Leftrightarrow$ 既約元.

**証明**. (1) $a$ を素元とし, $a = bc$ と書けたとする. このとき

$$(a) \text{ が素イデアル}, bc = a \in (a) \Rightarrow b \in (a) \text{ または } c \in (a)$$

となる. $b \in (a)$ なら $b = ad$ と書け, $a = bc$ に代入して

$$a = adc \Rightarrow a(1 - cd) = 0 \Rightarrow 1 = cd \Rightarrow c \in R^\times$$

を得る. ただし $R$ が整域と, 素元より $a \neq 0$ を使った. $c \in (a)$ の場合も同様.

(2) $(\Rightarrow)$ は $u \in R^\times$ に対して $a = ub \Rightarrow (a) \ni \forall ac = buc \in (b)$, $b = u^{-1}b \Rightarrow (b) \ni \forall bc = au^{-1}c \in (a)$ より従う. $(\Leftarrow)$ は, $a = 0$ のとき両辺 $a = b = 0$ で成り立ち, $a \neq 0$ のときは

$$a \in (a) = (b) \Rightarrow a = b\exists c, \qquad b \in (b) = (a) \Rightarrow b = a\exists d$$

を合わせて

$$a = bc = acd \Rightarrow a(1 - cd) = 0 \Rightarrow cd = 1 \Rightarrow u, d \in R^\times$$

から従う.

(3) $p_1$ が素元より

$$p_1 | p_1 \dots p_r = q_1 \dots q_s \Rightarrow \exists j (=: \sigma(1)) \text{ s.t. } p_1 \mid q_j \Rightarrow q_j = p_1 \exists a_1.$$

$q_j$ は既約元でもある ($\because$ (1)) より $a \in R^\times$ で, $p_1$ と $q_j$ は同伴. また最初の式に代入して

$$\begin{aligned} p_1 \dots p_r = q_1 \dots q_{j-1}(p_1 a_1) q_{j+1} \dots q_s &\Rightarrow p_1(p_2 \dots p_r - a_1 q_1 \dots q_{j-1} q_{j+1} \dots q_s) = 0 \\ &\Rightarrow p_2 \dots p_r = a_1 q_1 \dots q_{j-1} q_{j+1} \dots q_s \end{aligned}$$

を得る. $p_2$ 以降にも同様の議論を行って題意を得る.

(4) $\cup_n I_n$ もイデアルになるので, PID より $\cup_n I_n = (\exists \alpha)$ と書ける. とくに

$$\alpha \in (\alpha) = \cup_n I_n \Rightarrow \exists N \text{ s.t. } \alpha \in I_N.$$

よって

$$\forall n,\ I_n \subset \cup_n I_n = (\alpha) \subset I_N$$

であり, とくに $n \geq N$ なら $I_N \subset I_n \subset I_N$ で一致する.

(5) 一般に, $a$ が単元 $\Leftrightarrow (a) = R$. 既約元は単元でないので $(a) \neq R$. $(a) \subset I \subset R$ とすると PID より $I = (\exists b)$, すなわち

$$a \in (a) \subset (b) \Rightarrow a = b\exists c$$

と書ける. $a$ は既約元なので $b \in R^\times$ または $c \in R^\times$. 前者なら $I = R$, 後者なら $I = (a)$ なので題意が従う.

(6) (1) より ($\Leftarrow$) のみ示せばよい. $a$ を既約元とすると $(a)$ は極大イデアル ($\because$ (5)) で, よって素イデアル ($\because$ 定義-命題 1.1.12-(5)). □

**問題 18.** (1) 整域 $R$ で, 既約元だが素元でない元が存在する例を挙げよ.
(2) 整域 $R$ で, 無限に続くイデアルの昇鎖列が存在する例を挙げよ.

**命題 3.2.4.** $R$ を整域とする.

(1) $R$ が PID であれば UFD である.
(2) $R$ が UFD であれば, 素元 $\Leftrightarrow$ 既約元.

**証明**. (1) $R$ を PID とする. 命題 3.2.3-(6) より, UFD の定義の [既約元] を [素元] に取り替えて示せばよい. 一意性も命題 3.2.3-(3) より従うので,

$$R - (R^\times \cup \{0\}) \text{ の任意の元 } a \text{ が有限個の素元の積に表せる}$$

を示せばよい. なお

$$\text{任意のイデアル } I \subsetneq R \text{ を含む極大イデアルが存在する}$$

ことを認める ($\because$ ツォルンの補題). $a \notin R^\times$ と $R$ が PID であることと定義-命題 1.1.12-(5) より

$$(a) \supset (\pi_1), \text{ すなわち } a = \pi_1 \exists a_1$$

を満たす素元 $\pi_1$ が存在する. 同様の議論を繰り返して, $a_{n-1} \notin R^\times$ である限り,

$$a_{n-1} = \pi_n a_n \ (\pi_n \text{ は素元})$$

と書ける. もしこの作業が無限に続けられるなら, $(a_k) = (\pi_{k+1} a_{k+1}) \subset (a_{k+1})$ よりこれはイデアルの昇鎖列で, 命題 3.2.3-(4) より

$$\exists N \text{ s.t. } n \geq n \Rightarrow (a_N) = (a_n), \quad \text{とくに } (\pi_{N+1} a_{N+1}) = (a_N) = (a_{N+1})$$

と書ける. これは $\pi_{N+1} \in R^\times$ を意味するので矛盾. すなわち $\exists N$ s.t. $a_N \in R^\times$ である. $\pi_N$ を $\pi_N a_N$ に取り直せば, $a$ を有限個の素元の積

$$a = \pi_1 \dots \pi_N$$

に表せたことになる.

(2) 命題 3.2.3-(1) より ($\Leftarrow$) のみ示せばよい. $a$ を既約元とし, $bc \in (a)$ とする. すなわち

$$bc = a\exists d.$$

UFD より $b, c, d$ を既約元分解でき,

$$b = b_1 \dots b_r,\ c = c_1 \dots c_s,\ d = d_1 \dots d_t$$

とかける. 代入して

$$b_1 \dots b_r \cdot c_1 \dots c_s = a \cdot d_1 \dots d_t$$

となる. 両辺全て既約元なので, 一意性より $a$ は $b_*$ または $c_*$ のいずれかと同伴で, よって

$$b = b_1 \dots b_r \in (b_*) = (a) \text{ または } c = c_1 \dots c_s \in (c_*) = (a)$$

のいずれかが成り立つ. □

**問題 19.** (1) 素数の定義を調べ, それが素元と既約元のどちらを意味しているか答えよ.

(2) 素数は (1) と逆 ((1) の答えが素元だったら既約元, 既約元だったら素元) でもあるかどうか説明せよ.
※ 問題 4-(2) 参照.

**例 3.2.5.** $\mathbb{Z}[\sqrt{-1}]$ での素数 $p = 2, 3, 5, 7, 11, 13$ の分解の様子を見てみる.

(1) $2 = (1+\sqrt{-1})(1-\sqrt{-1}) = \sqrt{-1}(1-\sqrt{-1})^2$ であり, $1-\sqrt{-1}$ は既約元. 実際, $1-\sqrt{-1} = (a+b\sqrt{-1})(c+d\sqrt{-1})$ なら両辺の絶対値の 2 乗をとって

$$2 = (a^2+b^2)(c^2+d^2) \quad (a, b, c, d \in \mathbb{Z})$$

と書ける. 2 は素数なので $(a^2+b^2, c^2+d^2) = (1, 2)$ または $(2, 1)$. もし $a^2+b^2 = 1$ なら $a+b\sqrt{-1} \in \{\pm 1, \pm\sqrt{-1}\} = \mathbb{Z}[\sqrt{-1}]^\times$ で, 逆も同様.

(2) 3 は既約元. 実際, (1) と同様の議論で

$$3 = (a+b\sqrt{-1})(c+d\sqrt{-1}) \Rightarrow (a^2+b^2, c^2+d^2) \in \{(1, 9), (3, 3), (9, 1)\}$$

となるが, $*^2 + *^2 = 3$ は解がなく, $(a^2+b^2, c^2+d^2) = (1, 3)$ または $(3, 1)$. 残りの議論も (1) と同じ.

(3) $5 = (2+\sqrt{-1})(2-\sqrt{-1})$ であり, $2+\sqrt{-1}, 2-\sqrt{-1}$ は同伴でない既約元. 実際, (1) と同様に既約元であることが分かり, 同伴でないのは $(2-\sqrt{-1})\mathbb{Z}[\sqrt{-1}]^\times = \{\pm(2-\sqrt{-1}), \pm(1+2\sqrt{-1})\}$ より従う.

(4) $7, 11$ は既約元. 証明は (2) と同じ.

(5) $13 = (3+2\sqrt{-1})(3-2\sqrt{-1})$ であり, $3+2\sqrt{-1}, 3-2\sqrt{-1}$ は同伴でない既約元. 証明は (3) と同じ.

**定理 3.2.6.** (1) $\mathbb{Z}[\sqrt{-1}]$ は PID. とくに UFD でもあり, 各素数 $p$ は既約元の積に表せる.

(2) 素数 $p$ の既約元分解は以下の 3 パターンしかない.

(a) $p$ は **分解** する, すなわち, $p = \pi_1\pi_2$, $\pi_1, \pi_2$ は同伴でない既約元.

(b) $p$ は **惰性** する, すなわち, $p$ は既約元.

(c) $p$ は **分岐** する, すなわち, $p = u\pi^2$. $u \in \mathbb{Z}[\sqrt{-1}]^\times$, $\pi$ は既約元.

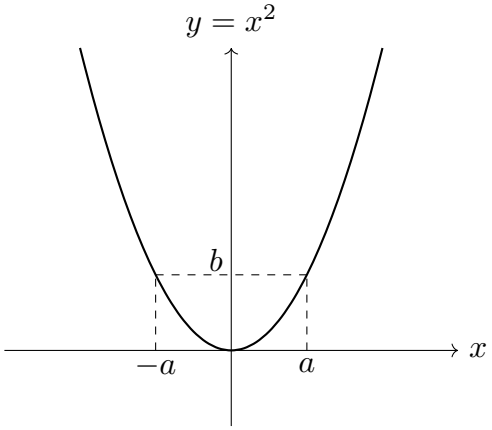
(3) (2) の各パターンの必要十分条件が以下で与えられる.

(a) 分解 $\Leftrightarrow p \neq 2$ であり $(\frac{-1}{p}) = 1$.

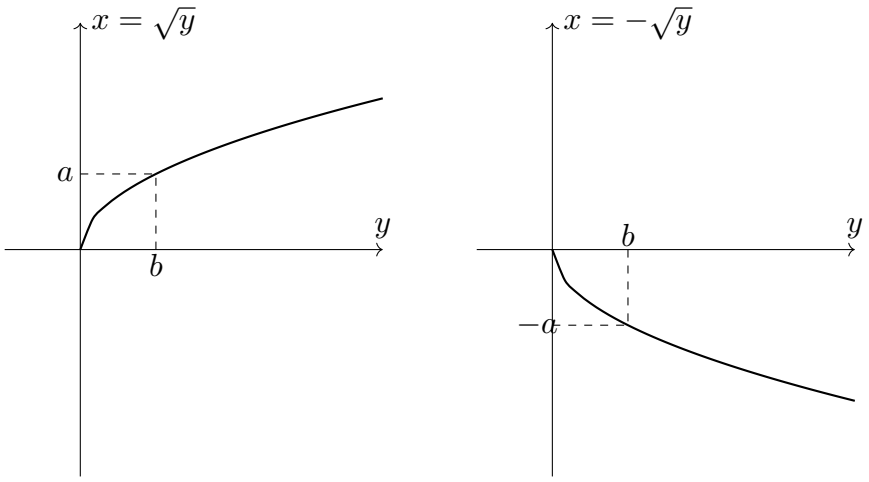
(b) 惰性 $\Leftrightarrow p \neq 2$ であり $(\frac{-1}{p}) = -1$.

(c) 分岐 $\Leftrightarrow p = 2$.

**補足 3.2.7.** 分岐という用語は幾何由来である (?). 例として $y = f(x) := x^2$ のグラフを考えてみる.




この逆関数は次のようになる.




$y = b = 0$ 付近だと, 逆関数の取り方が, $x = \sqrt{y}$ と $x = -\sqrt{y}$ の 2 種類ある (分岐している!) ことが分かる.

この現象を, 素イデアルの言葉でも観察することができる. 以下の対応を考える:

- $x$ 軸上の点 $x = a \Leftrightarrow \mathbb{R}[x]$ の素イデアル $(x - a)$
- $y$ 軸上の点 $y = b \Leftrightarrow \mathbb{R}[y]$ の素イデアル $(y - b)$
- 写像 $f$: $x$ 軸 $\to y$ 軸 $\Leftrightarrow \iota_f \colon \mathbb{R}[y] \hookrightarrow \mathbb{R}[x]$, $F(y) \mapsto F(y)|_{y=x^2} = F(x^2)$.
- 対応 $f(a) = b \Leftrightarrow$ ($\iota_f$ で $\mathbb{R}[y] \subset \mathbb{R}[x]$ とみなして) $(x-b) \cap \mathbb{R}[y] = (y-b) \Leftrightarrow (y-b)$ の $\mathbb{R}[x]$ での素イデアル分解に $(x - a)$ が現れる

$$\begin{array}{ccccc|c:c:c} x^2 \in & \mathbb{R}[x] & \supset & (y-b)\mathbb{R}[x] = (x^2-b) & (x+1)(x-1) & (x^2+1) & (x)^2 \\ \updownarrow & \cup & & \Uparrow & \Uparrow & \Uparrow & \Uparrow \\ y \in & \mathbb{R}[y] & \supset & (y-b) & (y-1) & (y+1) & (y-0) \end{array}$$

とくに, $y = b$ に対応している素イデアル $(y - b)$ は

- $b > 0$ なら $\mathbb{R}[x]$ で分解
- $b < 0$ なら $\mathbb{R}[x]$ で惰性
- $b > 0$ なら $\mathbb{R}[x]$ で分岐

していることが分かる. なお.

- $x$ 軸上の点 $x = a \Leftrightarrow \mathbb{R}[x]$ の素イデアル $(x-a) \Rightarrow$ 写像 $\mathbb{R}[x] \twoheadrightarrow (\mathbb{R}[x]/(x-a) \cong)\mathbb{R}$, $x \mapsto a$

を拡張して, $x^2 + b$ $(b > 0)$ も "点" だと思うと,

- $x$ 軸上の “点” $x^2+b$ $\Rightarrow$ 写像 $\mathbb{R}[x] \twoheadrightarrow \mathbb{R}[x]/(x^2+b) \cong \mathbb{C}$

となり, 惰性しているときは, 剰余体が拡大していることが分かる.

**補足 3.2.8.** 定理 3.2.6 の主張は以下のように一般化される.

(1) 代数体 $K$ (すなわち $\mathbb{C}/K/\mathbb{Q}$ s.t. $[K:\mathbb{Q}]<\infty$) に対し, その **整数環** と呼ばれる部分環 $\mathcal{O}_K$ が定義される ($\Rightarrow$ 定義 3.3.1-(1)). 例えば $\mathcal{O}_{\mathbb{Q}}=\mathbb{Z}$, $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})}=\mathbb{Z}[\sqrt{-1}]$ となる.

(2) 一般の整数環は必ずしも PID でない ($\Rightarrow$ 補足 3.4.7-(2)). その場合は **素イデアル分解** を考える ($\Rightarrow$ 定理 3.4.3).

$$\begin{array}{ccl} \mathcal{O}_K & \supset & p\mathcal{O}_K=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}\text{: 素イデアル } \mathfrak{p}_i \text{ 達のイデアル積} \\ \cup & & \uparrow\uparrow \\ \mathbb{Z} & \ni & p\text{: 素数} \end{array}$$

(3) 一般の場合の素数の分解のパターンは **基本等式** ($\Rightarrow$ 定理 3.4.8) を満たす:

$$[K:\mathbb{Q}]=\sum_{i=1}^{g} e_i[\mathcal{O}_K/\mathfrak{p}_i:\mathbb{F}_p].$$

(4) 一般の場合に素数の分解パターンの判別法がある ($\Rightarrow$ 定理 3.4.10). また, 二次体の場合 ($\Rightarrow$ 定理 3.4.16) や素数分体の場合 ($\Rightarrow$ 定理 5.1.1) などは, より詳細に分かる.

**定理 3.2.6$\Rightarrow$ 定理 3.1.1 の証明.** (1)$\Rightarrow$(2) は問題 17 より. 以下 (1)$\Leftarrow$(2) を示す.

(2) を仮定する. $p=2$ なら $p=1^2+1^2$ より明らか. $(\frac{-1}{p})=1$ のとき定理 3.2.6 より

$$p=(a+b\sqrt{-1})(c+d\sqrt{-1})\ (a,b,c,d\in\mathbb{Z},\ a+b\sqrt{-1},c+d\sqrt{-1}\notin\mathbb{Z}[\sqrt{-1}]^\times=\{\pm1,\pm\sqrt{-1}\}$$

と書ける. 両辺の複素絶対値の 2 乗を取って

$$p^2=(a^2+b^2)(c^2+d^2)$$

を得る. よって

$$(a^2+b^2,c^2+d^2)\in\{(1,p^2),(p,p),(p^2,1)\}$$

であるが, $a+b\sqrt{-1},c+d\sqrt{-1}\notin\mathbb{Z}[\sqrt{-1}]^\times=\{\pm1,\pm\sqrt{-1}\}$ より

$$a^2+b^2=c^2+d^2=p$$

以外は不適. □

## 3.3 # 代数体, 整数環, 単数群, 無限素点

**定義 3.3.1.** $K$ を代数体, すなわち $\mathbb{C}/K/\mathbb{Q}$, $[K:\mathbb{Q}]<\infty$ とする. 先頭項係数が 1 である多項式を **monic 多項式** と呼ぶ. 整数係数 monic 多項式のなす集合を

$$\mathbb{Z}[x]_m := \left\{ \sum_{i=0}^{n} a_i x^i \mid n\in\mathbb{N},\ a_i\in\mathbb{Z},\ a_n=1 \right\}$$

で定める. ※ $\mathbb{Z}[x]_m$ はこの授業オリジナルの記号.

(1) $K$ の **整数環** を以下で定める.

$$\mathcal{O}_K := \{\alpha\in K \mid \exists f\in\mathbb{Z}[x]_m \text{ s.t. } f(\alpha)=0\}.$$

$\mathcal{O}_K$ は整域で, その商体は $K$ になる.

(2) $K$ の **単数群** を以下で定める.

$$E_K := \mathcal{O}_K^\times$$

(3) $K$ に含まれる 1 のベキ根のなす集合を以下で表す.

$$\mu_K := \{\zeta\in K \mid \exists n\in\mathbb{N} \text{ s.t. } \zeta^n=1\}.$$

$\mu_K$ は $E_K$ の部分群になる. また, $\mu_K$ は巡回群になる ($\Rightarrow$ 補題 1.2.4-(2)).

(4) $\mathrm{id}\colon \mathbb{R}\hookrightarrow\mathbb{C}$ を用いて,

$$\mathrm{Hom}(K,\mathbb{R})\subset\mathrm{Hom}(K,\mathbb{C}),\ \sigma\mapsto \mathrm{id}\circ\sigma$$

の包含関係があるとみなす. また, 複素共役写像 $\rho_c\colon\mathbb{C}\to\mathbb{C}$ を用いて, 同値関係

$$\sigma,\tau\in\mathrm{Hom}(K,\mathbb{C}),\ \sigma\sim\tau\Leftrightarrow\sigma=\overline{\tau}:=\rho_c\circ\tau$$

を考える. このとき

(a) $\mathrm{Hom}(K,\mathbb{R})$ の要素を **実素点** と呼び, 実素点の個数を $r_1$ で表す.

(b) $(\mathrm{Hom}(K,\mathbb{C})-\mathrm{Hom}(K,\mathbb{R}))/\sim$ の要素を **複素素点** と呼び, 複素素点の個数を $r_2$ で表す.

(c) 実素点, 複素素点をまとめて **無限素点** と呼ぶ.

**補足 3.3.2.** 環は英語だと ring であり, その語源は「べき乗が一次結合に戻ってくるから」らしい (?). 例えば $R := \mathbb{Z}[\sqrt{2}]$ において $a = 1 + \sqrt{2}$ のべき乗は

$$a = 1 + \sqrt{2},\ a^2 = 3 + 2\sqrt{2},\ a^3 = 7 + 5\sqrt{2},\ a^4 = 17 + 12\sqrt{2},\ \cdots \in \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \sqrt{2}$$

と書ける. この現象は $a = 1 + \sqrt{2}$ の最小多項式 $x^2 - 2x - 1$ が整数係数 monic 多項式であることが効いている. 実際, $x^k$ を $x^2 - 2x - 1$ で割った余りは $m_k x + n_k$ $(m_k, n_k \in \mathbb{Z})$ の形になり ($\because x^2 - 2x - 1$ が整数係数 monic 多項式),

$$\begin{aligned} x^k &= \exists q_k(x)(x^2 - 2x - 1) + m_k x + n_k \\ &\overset{x:=a}{\Rightarrow} a^k = q_k(a) \cdot 0 + m_k a + n_k = (m_k + n_k) + m_k\sqrt{2} \end{aligned}$$

となる. 一方で $\mathbb{Z}[\frac{1}{\sqrt{2}}]$ も環ではあるが $a := \frac{1}{\sqrt{2}}$ のべき乗は

$$a = \frac{1}{\sqrt{2}},\ a^2 = \frac{1}{2},\ a^3 = \frac{1}{2} \cdot \frac{1}{\sqrt{2}}, \dots$$

となり, $\mathbb{Z}$ 係数の一次結合とはならない.

**例 3.3.3.** $K = \mathbb{Q}$ のとき:

(1) $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
(2) $\mu_{\mathbb{Q}} = E_{\mathbb{Q}} = \{\pm 1\}$.
(3) $\mathrm{Hom}(\mathbb{Q}, \mathbb{R}) = \mathrm{Hom}(\mathbb{Q}, \mathbb{C}) = \{\mathrm{id}\}$, $r_1 = 1$, $r_2 = 0$.

**問題 20.** 例 3.3.3 の内容に証明をつけよ.
(1) のヒント：$\frac{a}{b} \in \mathcal{O}_{\mathbb{Q}}$, $a \in \mathbb{Z}$, $b \geq 2$, $\gcd(a, b) = 1$ として矛盾を導く. 素数 $p \mid b$ をとり $f(\frac{a}{b}) = 0$ を満たす $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ $(a_i \in \mathbb{Z})$ をとると $f(\frac{a}{b})b^n = a^n + p(a_{n-1}a^{n-1}\frac{b}{p} + \cdots + a_0\frac{b^n}{p}) \equiv a^n \neq 0 \mod p$ より $f(\frac{a}{b}) = 0$ に矛盾.
(3) のヒント：$\sigma \in \mathrm{Hom}(\mathbb{Q}, \mathbb{C})$ に対して $\sigma(1) = 1 \Rightarrow \sigma(n) = n$ $(n \in \mathbb{N}) \Rightarrow \sigma(n) = n$ $(n \in \mathbb{Z}) \Rightarrow \sigma(\frac{m}{n}) = \frac{m}{n}$ $(m \in \mathbb{Z},\ n \in \mathbb{N})$ を順番に示す.

**定義-命題 3.3.4.** (1) $R$ を環, $S$ をその部分環とする. $S$ 上 $\alpha \in R$ で生成される環を

$$S[\alpha] := \{f(\alpha) \in R \mid f(x) \in S[x]\}$$

で定める. これは $S, \alpha$ を含む最小の $R$ の部分環となる.

(2) $K$ を体, $k$ をその部分体とする. $k$ 上 $\alpha \in K$ で生成される体を

$$k(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \in K \mid f(x), g(x) \in k[x],\ g(\alpha) \neq 0 \right\}$$

で定める. これは $k, \alpha$ を含む最小の $K$ の部分体となる.

※ Section 2.2 での記法と矛盾しない.

**例 3.3.5.** (1) $K = \mathbb{Q}(\sqrt{2})$ のとき:

(a) $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$.

(b) $\mu_{\mathbb{Q}(\sqrt{2})} = \{\pm 1\}$, $E_{\mathbb{Q}(\sqrt{2})} = \{\pm(1+\sqrt{2})^n \mod n \in \mathbb{Z}\}$.

(c) $\mathrm{Hom}(\mathbb{Q}(\sqrt{2}), \mathbb{R}) = \mathrm{Hom}(\mathbb{Q}(\sqrt{2}), \mathbb{C}) = \{\mathrm{id}, \rho\}$, $r_1 = 2$, $r_2 = 0$.

(2) $K = \mathbb{Q}(\sqrt{-3})$ のとき:

(a) $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

(b) $\mu_{\mathbb{Q}(\sqrt{-3})} = E_{\mathbb{Q}(\sqrt{-3})} = \langle \frac{1+\sqrt{-3}}{2} \rangle = \{\pm 1, \pm\frac{1+\sqrt{-3}}{2}, \pm\frac{-1+\sqrt{-3}}{2}\}$.

(c) $\mathrm{Hom}(\mathbb{Q}(\sqrt{-3}), \mathbb{R}) = \emptyset$, $\mathrm{Hom}(\mathbb{Q}(\sqrt{-3}), \mathbb{C}) = \{\mathrm{id}, \rho\}$, $r_1 = 0$, $r_2 = 1$.

**例 3.3.6.** $K = \mathbb{Q}(\zeta_5)$ のとき:

(1) $\mathcal{O}_{\mathbb{Q}(\zeta_5)} = \mathbb{Z}[\zeta_5]$.

(2) $\mu_{\mathbb{Q}(\zeta_5)} = \langle -\zeta_5 \rangle = \{\pm\zeta_5^m \mid m = 0, 1, 2, 3, 4\}$, $E_{\mathbb{Q}(\zeta_5)} = \times\{\pm\zeta_5^m(1+\zeta_5)^n \mid m = 0, 1, 2, 3, 4,\ n \in \mathbb{Z}\}$.

(3) $\mathrm{Hom}(\mathbb{Q}(\zeta_5), \mathbb{R}) = \mathrm{Hom}(\mathbb{Q}(\zeta_5), \mathbb{C}) = \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times$, $r_1 = 0$, $r_2 = 2$.

**定理 3.3.7** (ディリクレの単数定理)**.** 代数体 $K$ に対し

$$E_K \cong \mu_K \times \mathbb{Z}^{r_1+r_2-1}.$$

**補足 3.3.8.** 基本的には定理 1.3.4 と同様の議論で示せる. “無限素点” なるものが導入されたのは, 定理 1.3.4 の証明中の写像 $L$ の対応物を作るとき, 何次元空間への埋め込みがあるか ($\coloneqq$ 自由度) を測っている. 詳細は [小野, §33], [足立, 第 9 章, §5] などを参照.

**問題 21.** 例 3.3.3, 例 3.3.5, 例 3.3.6 でディリクレの単数定理が成り立っていることを確かめよ.

## 3.4 # 素イデアルの分解・惰性・分岐

**補足 3.4.1** (お気持ち)**.** $\mathbb{Z}$ も $\mathbb{Q}$ も, それぞれの利点がある. 前者は「倍数」「約数」の概念がある:

$$a, b \in \mathbb{Z},\ a \mid b \Leftrightarrow \exists c \in \mathbb{Z} \text{ s.t. } ac = b.$$

後者は「割り算」ができる:

$$a, b \in \mathbb{Q},\ b \neq 0 \Rightarrow \frac{a}{b} \in \mathbb{Q}.$$

そして $\mathbb{Q}$ では任意の $a, b$ $(a \neq 0)$ が $a \mid b$ を満たす $(\because a\frac{b}{a} = b)$ し, $\mathbb{Z}$ では割り算の結果がない場合 $(\frac{1}{2} \notin \mathbb{Z})$ がある.

そこで, 代数体 $K$ に対しても, $\mathbb{Q}$ に対して $\mathbb{Z}$ があったように, 整数環 $\mathcal{O}_K$ $(\Rightarrow$ 定義 3.3.1-(1)) を考え, そこれ「倍数」「約数」の概念を考えたい. その際, $\mathbb{Z}$ における言い換え:

$$a \mid b \Leftrightarrow a\mathbb{Z} \ni b \Leftrightarrow a\mathbb{Z} \supset b\mathbb{Z} \quad (a, b \in \mathbb{Z})$$

に倣って, イデアルの言葉で議論を行った方が見通しがよくなる.

**定義 3.4.2.** 可換環 $R$ のイデアル $I, J$ に対し, その **積 (イデアル)** を

$$IJ := \left\{ \sum_{k=1}^{n} i_k j_k \mid n \in \mathbb{N},\ i_k \in I,\ j_k \in J \right\}$$

で定める. $IJ$ も $R$ のイデアルとなる.
※ $I$ または $J$ どちらかが $R$ のイデアルではない場合も同様の定義をする.

**問題 22.** 可換環 $R$ に対して以下を示せ.

(1) $a_i \in R$ $(i = 1, \ldots, s)$ に対し

$$(a_i \mid i = 1, \ldots, s) = (a_1, \ldots, a_s) := \left\{ \sum_{i=1}^{s} r_i a_i \mid r_i \in R \right\}$$

とおくと $R$ のイデアルとなる. なお $(a_1, \ldots, a_s)$ を $a_1, \ldots, a_r$ で生成されたイデアル, $a_1, \ldots, a_r$ を $(a_1, \ldots, a_s)$ の生成系, と呼ぶ.

(2) $a_i, b_j \in R$ $(i = 1, \ldots, s,\ j = 1, \ldots, t)$ に対し

$$\begin{aligned}(a_i \mid i = 1, \ldots, s)(b_j \mid j = 1, \ldots, t) &= (a_i b_j \mid i = 1, \ldots, s,\ j = 1, \ldots, t) \\ &:= (a_1 b_1, a_1 b_2, \ldots, a_1 b_t, a_2 b_1, \ldots, a_s b_t).\end{aligned}$$

**定理 3.4.3.** 代数体 $K$ の整数環 $\mathcal{O}_K$ の任意の非零イデアル $\mathfrak{a} \neq (0)$ は素イデアルの積に順番を除いて一意的に書ける. すなわち

$$0 \leq \exists r \in \mathbb{Z},\ \exists \mathfrak{p}_i\text{: } \mathcal{O}_K \text{ の素イデアル},\ \exists n_i \in \mathbb{N}\ (i = 1, \ldots, r) \text{ s.t. } \mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}.$$

この表記を **素イデアル分解** と呼ぶ.

**補足 3.4.4.** 証明は **デデキント環論** を必要とし, 全容は紹介できないが, 関連事項をいくつか紹介しておく.

(1) 代数体 $K$ の整数環 $\mathcal{O}_K$ の非零イデアル $\mathfrak{a}$ に対して, 剰余環の位数

$$N\mathfrak{a} := |\mathcal{O}_K/\mathfrak{a}|$$

は有限になり, その値を **(イデアル) ノルム** と呼ぶ.

(2) 代数体 $K$ の整数環 $\mathcal{O}_K$ において, 素イデアルであることと極大イデアルであることは同値.

(3) 代数体 $K$ の整数環 $\mathcal{O}_K$ の非零イデアル $\mathfrak{a}, \mathfrak{b}$ に対し

$$\mathfrak{a} \mid \mathfrak{b} \Leftrightarrow \exists \mathfrak{c}\text{: 非零イデアル s.t. } \mathfrak{b} = \mathfrak{a}\mathfrak{c}$$

と定義する. これは以下の各々と同値になる.

- $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}}$, $\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ と素イデアル分解したとき $\forall \mathfrak{p}$, $m_{\mathfrak{p}} \leq n_{\mathfrak{p}}$,
- $\mathfrak{a} \supset \mathfrak{b}$.

また, 最大公約イデアルや最小公倍イデアルが自然な方法で定義できる.

**例 3.4.5** ($K = \mathbb{Q}$ の場合)**.** $\mathbb{Z}$ は PID なので

$$\mathbb{Z} \text{ の非零イデアル } \mathfrak{a} \overset{\mathfrak{a}=(a)}{\leftrightarrow} a \in \mathbb{N}, \quad \mathbb{Z} \text{ の素イデアル } \mathfrak{p} \overset{\mathfrak{p}=(p)}{\leftrightarrow} \text{素数 } p$$

を対応させることにより,

$$\text{素イデアル分解 } \mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r} \leftrightarrow \text{素因数分解 } a = p_1^{n_1} \cdots p_r^{n_r}$$

が対応する.

**例 3.4.6** ($K = \mathbb{Q}(\sqrt{-5})$ の場合)**.** (1) $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ では素因数分解 (正確には既約元分解) の一意性は成り立たない. 実際

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

であり, $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ は互いに同伴ではない既約元である.

(2) (お気持ち) 6 の分解を完遂するためには “ 2 と $(1 + \sqrt{-5})$ の共通の因子” のようなもの達が必要になる.

(3) 一方で $\mathbb{Z}[\sqrt{-5}]$ での素イデアル分解は可能である:

$$(6) = (2, 1+\sqrt{5}) \cdot (2, 1-\sqrt{5}) \cdot (3, 1+\sqrt{5}) \cdot (3, 1-\sqrt{5})$$

で, $(2, 1+\sqrt{5}), (3, 1+\sqrt{5}), (3, 1-\sqrt{5})$ は相異なる素イデアルで, $(2, 1+\sqrt{5}) = (2, 1-\sqrt{5})$ である.

(4) $(2) = (2, 1+\sqrt{5})(2, 1-\sqrt{5})$, $(3) = (3, 1+\sqrt{5})(3, 1-\sqrt{5})$, $(1+\sqrt{5}) = (2, 1+\sqrt{5})(3, 1+\sqrt{5})$, $(1-\sqrt{5}) = (2, 1-\sqrt{5})(3, 1-\sqrt{5})$ である. とくに

$$(2, 1+\sqrt{5}) = \gcd((2), (1+\sqrt{-5}))$$

等となる ($\Rightarrow$ (2)).

**問題 23.** 例 3.4.6 の主張 ((2) 以外) を証明せよ.

**補足 3.4.7.** (1) 素イデアル分解が可能であるのには, 整数環であることが効いている ($\Rightarrow$ デデキント環論). 例えば $\mathbb{Z}[\sqrt{-3}] \subsetneq \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ において

$$\mathfrak{a} := (2, 1+\sqrt{-3})$$

とおくと

$$\mathfrak{a}^2 = (4, 2+2\sqrt{-3}, -2+2\sqrt{-3}) = (4, 2+2\sqrt{-3}) = (2)\mathfrak{a}$$

となる. もし素イデアル分解の一意性が成り立てば

$$\mathfrak{a} \stackrel{?}{=} (2)$$

となるハズだが, $\mathfrak{a} \ni 1+\sqrt{-3} \notin (2)$ よりこれは成り立たない.

(2) 一般の代数体 $K$(の整数環 $\mathcal{O}_K$) において, (素イデアル分解は可能だが) 素因数分解はできない理由は, 単項イデアルでないイデアルが存在することにある. 関連して

$$[\text{イデアルの個数: 単項イデアルの個数}] \text{ の比}$$

を表す指標として **類数** と呼ばれる値が定義できる. 具体的には

(a) $K$ の分数イデアルを $\alpha\mathfrak{a}$ ($\alpha \in K^\times$, $\mathfrak{a}$ は $\mathcal{O}_K$ の非零イデアル) で定義する.

(b) $I_K := \{\text{分数イデアル全体}\}$ はイデアル積に関して可換群になる.

(c) 単項分数イデアル全体 $P_K := \{\alpha\mathcal{O}_K \mid \alpha \in k^\times\}$ は $I_K$ の部分群となる.

(d) イデアル類群を商群 $Cl_K := I_K/P_K$ で定義すると有限群となる.

(e) 類数を $h_K := |Cl_K|$ で定義する.

とくに $h_K = 1$ であれば $I_K = P_K$ であり, 任意のイデアルが単項イデアル (つまり $\mathcal{O}_K$ が PID) である.

(3) 類数が 1 となる虚二次体は

$$\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-7}),\ \mathbb{Q}(\sqrt{-11}),$$
$$\mathbb{Q}(\sqrt{-19}),\ \mathbb{Q}(\sqrt{-43}),\ \mathbb{Q}(\sqrt{-67}),\ \mathbb{Q}(\sqrt{-163})$$

のみであることが知られている. 一方で類数が 1 の実二次体は無限個あると予想されているが, 未解決である ($\Rightarrow$ ガウスの類数問題).

**定理 3.4.8.** $K$ を代数体, $p \in \mathbb{Z}$ を素数とし, $(p) = p\mathcal{O}_K$ の $\mathcal{O}_K$ での素イデアル分解を考えると

$$\begin{array}{ccccc} K & \supset & \mathcal{O}_K & \supset & (p) = p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g} \\ \cup & & \cup & & | \\ \mathbb{Q} & \supset & \mathbb{Z} & \supset & (p) = p\mathbb{Z} \end{array}$$

の形になる. ただし

(1) $g \in \mathbb{N}$ であり, $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ は $\mathcal{O}_K$ の素イデアル $\mathfrak{p}$ で $p \in \mathfrak{p}$ を満たすもの全体であり, $p$ **の上の素イデアル** と呼ばれる.

(2) $e_i \in \mathbb{N}$ であり, $\mathfrak{p}_i/p$ の **分岐指数** と呼ばれる. $e_i = 1$ のとき $\mathfrak{p}_i/p$ は **不分岐** である, $e_i > 1$ のとき $\mathfrak{p}_i/p$ は **分岐** する, という. いずれかの $\mathfrak{p}_i$ が分岐するとき $p$ は $K/\mathbb{Q}$ で分岐する, 全ての $\mathfrak{p}_i$ が不分岐のとき $p$ は $K/\mathbb{Q}$ で不分岐である, という,

(3) 剰余環 $\mathcal{O}_K/\mathfrak{p}_i$ は $\mathbb{Z}/p\mathbb{Z}$ の体拡大となり, その拡大次数 $f_i := [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$ は $\mathfrak{p}_i/p$ の **剰余次数** と呼ばれる.

$$\begin{array}{ccccc} \mathfrak{p}_i & \subset & \mathcal{O}_K & \twoheadrightarrow & \mathcal{O}_K/\mathfrak{p}_i \\ \cup & & \cup & & \cup \\ p\mathbb{Z} & \subset & \mathbb{Z} & \twoheadrightarrow & \mathbb{Z}/p\mathbb{Z} \end{array} \qquad f_i \text{ 次拡大}$$

このとき

$$|\mathcal{O}_K/\mathfrak{p}_i| = p^{f_i}$$

を満たす.

(4) **基本等式**

$$[K : \mathbb{Q}] = \sum_{i=1}^{g} e_i f_i$$

が成立する.

(5) $K/\mathbb{Q}$ がガロア拡大であれば $e := e_i$, $f := f_i$ はそれぞれ一定になり, 基本等式は

$$[K : \mathbb{Q}] = efg$$

と表される.

**問題 24.** $[K : \mathbb{Q}] = 2$ のとき, 素数 $p$ の $\mathcal{O}_K$ での分解の様子は, 基本等式により

(1) $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1 \neq \mathfrak{p}_2$.
(2) $p\mathcal{O}_K = \mathfrak{p}$
(3) $p\mathcal{O}_K = \mathfrak{p}^2$

の 3 通りに絞られることを説明せよ ($\mathfrak{p}_*$ ($* = \emptyset, 1, 2$) は $\mathcal{O}_K$ の素イデアル). また, それぞれの分岐/不分岐, 分岐指数, 剰余次数を答えよ.
※ (1), (2), (3) の $p$ の $K$ における状態は, それぞれ (完全) 分解, 惰性, 分岐と呼ばれる.

**定義 3.4.9.** 素数 $p$ と $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ に対し, $\overline{f}(x) \in \mathbb{F}_p[x]$ ($\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$) を

$$\overline{f}(x) := \sum_{i=0}^{n} (a_i \bmod p) x^i$$

で定める.

**定理 3.4.10** (デデキント・クンマーの定理)**.** $K$ を代数体, $K = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}_K$ とし, $\alpha$ の最小多項式を $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]_m$ とおく. 素数 $p$ が

$$p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$$

を満たすと仮定し, $\overline{f}(x) \in \mathbb{F}_p[x]$ の既約 (多項式) 分解が

$$\overline{f}(x) = \overline{f}_1(x)^{e_1} \cdots \overline{f}_g(x)^{e_g}$$

で与えられるとする. ただし $f_i(x) \in \mathbb{Z}[x]_m$ であり, $\overline{f}_i$ は相異なる $\mathbb{F}_p[x]$ の既約多項式で $e_i \in \mathbb{N}$ である. このとき $(p) = p\mathcal{O}_K$ の素イデアル分解は

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \ \mathfrak{p}_i := (p, f_i(\alpha))$$

となる.

**証明**. (概略) $\mathbb{Z}[\alpha]$ のイデアルとして

$$p\mathbb{Z}[\alpha] \supset (p, f_1(\alpha))^{e_1} \cdots (p, f_g(\alpha))^{e_g} \tag{3.1}$$

となることを示せば, 他の部分は基本等式等より従う. 右辺の生成系を問題 22-(2) を用いて書き下したとき, $p\cdots$ の形にならない生成元は

$$f_1(\alpha)^{e_1}\cdots f_g(\alpha)^{e_g} \equiv f(\alpha) = 0 \mod p$$

のみであり, 結局これも $(p)$ の元となり, 必要な包含関係が得られる. □

**問題 25.** (定理 3.4.10 の証明に必要な事柄を羅列する. 挑戦できそうなところを証明してみよ.) $K$ を代数体, $K = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}_K$ とし, $\alpha$ の最小多項式を $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]_m$ とおく. 素数 $p$ に対し, $\overline{f}(x) \in \mathbb{F}_p[x]$ の既約 (多項式) 分解が

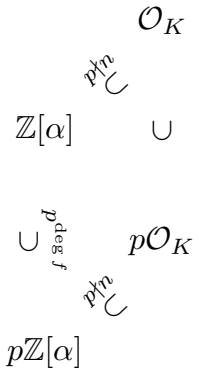
$$\overline{f}(x) = \overline{f}_1(x)^{e_1}\cdots\overline{f}_g(x)^{e_g}$$

で与えられるとする. だし $f_i(x) \in \mathbb{Z}[x]_m$ であり, $\overline{f}_i$ は相異なる $\mathbb{F}_p[x]$ の既約多項式で $e_i \in \mathbb{N}$ である.

(1) $\mathbb{Z}[\alpha]$ の 2 元生成イデアル $\mathfrak{p}_i^0 = (p, f_i(\alpha))$ に関して以下を示せ.
  (a) $\mathfrak{p}_i^0$ は $p$ を含む極大イデアルである.
  (b) $\mathbb{Z}[\alpha]$ の $p$ を含む任意の極大イデアル $\mathfrak{p}^0$ は $\exists i$ s.t. $\mathfrak{p}_i^0$ と一致する.
  (c) $|\mathbb{Z}[\alpha]/\mathfrak{p}_i^0| = p^{\deg f_i}$.

(2) さらに $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ を仮定する.
  (a) $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \to \mathcal{O}_K/p\mathcal{O}_K$, $\alpha \bmod p\mathbb{Z}[\alpha] \mapsto \alpha \bmod p\mathcal{O}_K$ は環同型. とくに $\mathbb{Z}[\alpha]$ の $p$ を含む極大イデアルと $\mathcal{O}_K$ の $p$ を含む極大イデアルは 1 対 1 対応し, $\mathfrak{p}_i^0$ と対応するものは $\mathfrak{p}_i = \mathfrak{p}_i^0\mathcal{O}_K$ となる. さらに $\mathbb{Z}[\alpha]/\mathfrak{p}_i^0 \cong \mathcal{O}_K/\mathfrak{p}_i$.
  (b) $p\mathcal{O}_K \supset \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$.
  (c) $p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$.

ヒント：(1)-(a) $\mathbb{Z}[\alpha]/(p, f_i(\alpha)) \cong \mathbb{F}_p[x]/\overline{f}_i(x)$ が体.
(1)-(b) $\mathbb{F}_p[x] \to \mathbb{Z}[\alpha]/\mathfrak{p}$, $x \mapsto \alpha \bmod \mathfrak{p}$ の核の生成元が $\overline{f}_i$.
(1)-(c) $(\mathbb{Z}[\alpha]/\mathfrak{p}_i)/\mathbb{F}_p$ の拡大次数が $\deg f_i$.
(2)-(a) (色んな示し方があると思うが例えば) $n := [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ とおけば




となり, $[\mathbb{Z}[\alpha] \cap p\mathcal{O}_K : p\mathbb{Z}[\alpha]] = 1$, すなわち $\mathbb{Z}[\alpha] \cap p = p\mathbb{Z}[\alpha]$ が従い単射が言える. 全射性は $p \nmid n \Rightarrow \exists m$ s.t. $mn \equiv 1 \mod p \Rightarrow \forall \alpha \in \mathcal{O}_K,\ \mathbb{Z}[\alpha] \ni m(n\alpha) \equiv \alpha \mod p$ より従う.
(2)-(b) Eq. (3.1) の両辺に $\mathcal{O}_K$ をかける.
(2)-(c) 基本等式より.

**補足 3.4.11.** (1) 任意の代数体は $K = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}_K$ の形でかける. 一方で $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$ とできるとは限らない ($\Rightarrow$ 冪整基底問題).

(2) $L/K$ を代数体の体拡大とする. このとき, $\mathcal{O}_K$ の素イデアル $\mathfrak{p}$ の $\mathcal{O}_L$ での素イデアル分解の様子

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

を考えることにより, (相対) 分岐指数 $e_i$, (相対) 剰余次数 $f_i := [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ 等が定義できる. 基本等式 (の相対版)

$$[L : K] = \sum_{i=1}^{g} e_i f_i$$

も成り立つ ($\Rightarrow$ $\mathfrak{p}\mathcal{O}_L$ の定義は定義 3.4.2 の※参照). 定理 3.4.10 の一般化も存在する.

**補足 3.4.12.** 詳細は [小野, §25], [足立, 第 11 章] などを参照.

**系 3.4.13.** $K$ を代数体, $K = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}_K$ とし, $\alpha$ の最小多項式を $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]_m$ とおく.

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i)$$

と書いて, 多項式 $f$ の判別式を

$$d_f := \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2 \in \mathbb{Z}$$

で定義する. このとき, 素数 $p$ に対して

$$p \nmid d_f \Rightarrow p \text{ は } K \text{ で不分岐}$$

が成り立つ.

**証明**. $\mathcal{O}_K$ の full-rank (すなわち, 階数が $n = [K : \mathbb{Q}]$ と一致) の $\mathbb{Z}$-自由部分加群 $M$ に対し, その $\mathbb{Z}$-加群としての基底を $m_1, \ldots, m_n$ とおき,

$$d(M) := \det \begin{bmatrix} \sigma_1(m_1) & \sigma_1(m_2) & \cdots & \sigma_1(m_n) \\ \sigma_2(m_1) & \sigma_2(m_2) & \cdots & \sigma_2(m_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(m_1) & \sigma_n(m_2) & \cdots & \sigma_n(m_n) \end{bmatrix}^2$$

とおく. ただし $\mathrm{Hom}(K, \mathbb{C}) =: \{\sigma_1, \ldots, \sigma_n\}$. このとき, $K$ のガロア閉包 $\tilde{K}$ に対して

$$d(\mathcal{O}_K) \in \mathcal{O}_{\tilde{K}}^{\mathrm{Gal}(\tilde{K}/\mathbb{Q})} = \mathbb{Z}$$

が分かる. さらに, もし

$$M \supset N$$

のとき, $M$ の基底 $m_1, \ldots, m_n$ と $N$ の基底 $n_1, \cdots, n_n$ の間には整数係数正則行列 $A$ を用いて

$$A[m_1 \ \cdots \ m_n] = [n_1 \ \cdots \ n_n]$$

の関係があり, ゆえに

$$\det A^2 d(M) = d(N)$$

となる. 単因子論 (掃き出し法) により $[M : N] = \det A$ が分かるので, 併せて

$$[M : N]^2 d(M) = d(N)$$

を得る. さらにヴァンデルモンド行列式の公式より

$$d(\mathbb{Z}[\alpha]) = \det \begin{bmatrix} \sigma_1(1) & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha^{n-1}) \\ \sigma_2(1) & \sigma_2(\alpha) & \cdots & \sigma_2(\alpha^{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(1) & \sigma_n(\alpha) & \cdots & \sigma_n(\alpha^{n-1}) \end{bmatrix}^2 = d_f$$

が従う. よって, 仮定より

$$p \nmid d_f = d(\mathbb{Z}[\alpha]) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 d(\mathcal{O}_K)$$

だから, 定理 3.4.10 の成立条件 $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ が従う. さらに $p \nmid d_f$ より $f(x) \bmod p$ は重根を持たないので, 定理 3.4.10 中の各 $e_i = 1$, すなわち不分岐となる. □

**注意 3.4.14.** 実際は

$$p \nmid d(\mathcal{O}_K) \Leftrightarrow p \text{ は } K \text{ で不分岐}$$

が成り立つ.

**例 3.4.15.** $\mathcal{O}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[\sqrt{-1}]$ において素数 $p$ は以下の分解法則を満たす.

(1) $p \equiv 1 \mod 4$ のとき $p\mathbb{Z}[\sqrt{-1}] = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1, \mathfrak{p}_2$ は相異なる素イデアル. 具体的には, $-1 \equiv a^2 \mod p$ を満たす $a \in \mathbb{Z}$ を用いて $\mathfrak{p}_1 := (p, \sqrt{-1} - a)$, $\mathfrak{p}_2 := (p, \sqrt{-1} + a)$ とかける.
(2) $p \equiv 3 \mod 4$ のとき $p\mathbb{Z}[\sqrt{-1}]$ は素イデアル.
(3) $p = 2$ のとき $2\mathbb{Z}[\sqrt{-1}] = \mathfrak{p}^2$, $\mathfrak{p}$ は素イデアル. 具体的には $\mathfrak{p} = (1 + \sqrt{-1})$.

**問題 26.** デデキント・クンマーの定理を使って例 3.4.15 の内容を示せ.
ヒント：$\alpha = \sqrt{-1}$, $f(x) = x^2 + 1$ に対し

- $f(x) \bmod p$ が既約 $\Leftrightarrow$ $f(x) \bmod p$ が一次式に分解しない $\Leftrightarrow$ $f(x) \equiv 0 \mod p$ が解を持たない $\Leftrightarrow$ $\forall a \in \mathbb{Z}$, $f(a) = a^2 + 1 \not\equiv 0 \mod p \Leftrightarrow \left(\frac{-1}{p}\right) = -1$.
- $\exists a, b \in \mathbb{Z}$ s.t. $f(x) \equiv (x - a)(a - b) \mod p$, $a \not\equiv b \mod p \Leftrightarrow \exists a \in \mathbb{Z} - p\mathbb{Z}$ s.t. $f(a) = a^2 + 1 \equiv 0 \mod p \Leftrightarrow \left(\frac{-1}{p}\right) = 1$.
- $\exists a \in \mathbb{Z}$ s.t. $f(x) \equiv (x - a)^2 \mod p \Leftrightarrow \exists a \in \mathbb{Z}$ s.t. $f(a) \equiv f'(a) \equiv 0 \mod p \Leftrightarrow p = 2$.

**定理 3.4.16.** $K = \mathbb{Q}(\sqrt{d})$ ($d$ は平方因子を持たない整数) において素数 $p$ は以下の分解法則を満たす. $d_K := \begin{cases} d & (d \equiv 1 \mod 4) \\ 4d & (d \equiv 2, 3 \mod 4) \end{cases}$ とおき, 平方剰余記号を

$$\left(\frac{a}{2}\right) := \begin{cases} 1 & (a \equiv \pm 1 \mod 8) \\ -1 & (a \equiv \pm 3 \mod 8) \\ 0 & (a \equiv 0 \mod 2) \end{cases}$$

で拡張しておく.

(1) $\left(\frac{d_K}{p}\right) = 1$ のとき $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1, \mathfrak{p}_2$ は相異なる素イデアル.
(2) $\left(\frac{d_K}{p}\right) = -1$ のとき $p\mathcal{O}_K$ は素イデアル.
(3) $\left(\frac{d_K}{p}\right) = 0$ のとき $p\mathcal{O}_K = \mathfrak{p}^2$, $\mathfrak{p}$ は素イデアル.

**補足 3.4.17.** 詳細は [小野, §25], [足立, 第 11 章, §6] などを参照

## 8/27 の復習 $+\alpha$

- 代数体 $K$ ($\mathbb{Q}$ の有限次拡大体) の “適切な” 部分環 $\mathcal{O}_K$ が定義でき, $K$ の整数環と呼ばれる. 具体的には $\mathcal{O}_K := \{\alpha \in K \mid \exists \text{monic 整数係数多項式} f(x) \text{ s.t. } f(\alpha) = 0\}$.
- デデキント環論 (難) より, 素数 $p$ の素イデアル分解

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \quad (\mathfrak{p}_i \text{は } p \text{ を含む相異なる } \mathcal{O}_K \text{ の素イデアル})$$

  が定まる. $e_i$ は分岐指数, $f_i := [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$ は剰余次数と呼ばれる.
- 基本等式: $[K : \mathbb{Q}] = \sum_{i=1}^{g} e_i f_i$.
- より詳しく, 分解の様子の判定法 (デデキント・クンマーの定理など) がある.
- 判定法を $K = \mathbb{Q}(\sqrt{-1})$ に適応することで以下を得る:

$$\begin{array}{lllll} p\mathbb{Z}[\sqrt{-1}] = \mathfrak{p}_1\mathfrak{p}_2,\ \mathfrak{p}_1 \neq \mathfrak{p}_2 & \Leftrightarrow & (\frac{-1}{p}) = 1 & \Leftrightarrow & p \equiv 1 \mod 4 \\ p\mathbb{Z}[\sqrt{-1}] = \mathfrak{p} & \Leftrightarrow & (\frac{-1}{p}) = -1 & \Leftrightarrow & p \equiv 3 \mod 4 \\ p\mathbb{Z}[\sqrt{-1}] = \mathfrak{p}^2 & \Leftrightarrow & p = 2. & & \end{array}$$

  また, これより二平方和定理が従う.
- $[K : \mathbb{Q}] = 2$ の場合に一般化できる $\Rightarrow$ 定理 3.4.16.
- $n$ 次巡回拡大 $K/k$ ($\zeta_n \in k$) を調べるのが “クンマー理論”. $n$ が素数なら分解の様子も分かる.
- 今日のプラン: 定理 4.4.1 (クンマー理論) $\Rightarrow$ 補足 3.4.11-(2) $\Rightarrow$ 定義-命題 4.5.1 $\Rightarrow$ 定理 4.5.2 (分解の様子) $\Rightarrow$ “$R$-加群” と “群コホモロジー” (クンマー理論の証明)

# 4　加群・群コホモロジーとクンマー理論

概略

- 体上の線形空間の類似として「環上の加群」が定義される.
- 群環 $\mathbb{Z}[G]$ 上の加群を調べる道具として「群コホモロジー」がある.
- 群コホモロジーの応用例として「ピタゴラス数」や「クンマー理論」を紹介する.

## 4.1　加群と完全系列

**定義 4.1.1.** $R$ を環, $M$ を加法群とする. $M$ が **(左)$R$-加群** であるとは

(0) $R \times M \to M$, $(r, m) \mapsto rm$ が定義され,
(1) $\forall r \in R$, $\forall m, n \in M$, $r(m+n) = rm + rn$.
(2) $\forall r, s \in R$, $\forall m \in M$, $(r+s)m = rm + sm$.
(3) $\forall r, s \in R$, $\forall m \in M$, $(rs)m = r(sm)$.
(4) $\forall m \in M$, $1m = m$. ただし $1 = 1_R$.

を満たすことである.

**注意 4.1.2.**　(1) $R$ が体 $K$(例えば $\mathbb{R}$) のとき,

$$M \text{ が } K\text{-加群} \Leftrightarrow M \text{ が } K\text{-線形空間}$$

である.

(2) $R = \mathbb{Z}$ の場合, 任意の加法群 $M$ は $n \in \mathbb{Z}$, $m \in M$ に対し

$$nm := \begin{cases} \overbrace{m + \cdots + m}^{n \text{ 個}} & (n \in \mathbb{N}) \\ 0_M & (n = 0) \\ -(\overbrace{m + \cdots + m}^{|n| \text{ 個}}) & (-n \in \mathbb{N}) \end{cases}$$

により $\mathbb{Z}$-加群となる.

**定義 4.1.3.** $R$ を環とし, $A, B, C$ は $R$-加群とする.

(1) $f\colon A \to B$ が **$R$-準同型写像** であるとは

$$\forall a, a', \in A,\ r \in R,\ f(a+a') = f(a) + f(a'),\ f(ra) = rf(a)$$

を満たすことである. $A$ から $B$ への $R$-準同型写像全体を $\mathrm{Hom}_R(A,B)$ で表す. とくに $\mathrm{Hom}(A,B) := \mathrm{Hom}_{\mathbb{Z}}(A,B)$ は $A$ から $B$ への群準同型写像全体となる ($\Rightarrow$ 注意 4.1.2-(2)).

(2) $R$-準同型写像 $f\colon A \to B$, $g\colon B \to C$ が **完全 (系列)** であるとは,

$$f(A) = \ker g$$

を満たすことである. またこのとき

$$A \xrightarrow{f} B \xrightarrow{g} C \text{ (完全)}$$

等のように表す.

(3) $R$-準同型写像の族 $f_i\colon A_i \to A_{i+1}$ に対し, 各 $i$ で $f_i\colon A_i \to A_{i+1}$, $f_{i+1}\colon A_{i+1} \to A_{i+2}$ がそれぞれ完全系列であることを

$$\cdots \to A_{i-1} \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \xrightarrow{f_{i+1}} A_{i+2} \to \cdots \text{ (完全)}$$

等のように表す.

**補足 4.1.4.** (1) 加法群 $M$ に対し

$$\mathrm{End}(M) := \mathrm{Hom}(M,M) = \{f\colon M \to M \mid f \text{ は群準同型写像}\}$$

は, 演算

$$(f+g)(m) := f(m) + g(m), \quad fg := f \circ g$$

により環になる. このとき, $R$-加群の定義 4.1.1-(0), (1) は

$$\phi\colon R \to \mathrm{End}(M),\ r \mapsto \text{“}r \text{ 倍写像”}\colon [m \mapsto rm]$$

が well-defined であることを言い, (2), (3) は $\phi$ が環準同型写像となることを言い, (4) は $\phi$ による乗法単位元 $1_R$ の像が乗法単位元 $\mathrm{id}_M$ であることを言っている.

(2) $A \xrightarrow{f} B \xrightarrow{g} C$ に対し

- $f(A) \subset \ker g \Leftrightarrow a \in A$ が右に二歩進むと零 ($g(f(a)) = 0$) となる.
- $f(A) \supset \ker g \Leftrightarrow b \in B$ が右に一歩進むと零 ($g(b) = 0$) となるなら, それは左から来た元 ($b = f(\exists a)$) である.

**問題 27.** 零元のみからなる $R$-加群 $\{0\}$ を記号 0 で表す. また, 任意の $R$-加群 $M$ に対し

- $0 \to M$ は $\{0\}$ から $M$ への唯一の群準同型 $\{0\} \to M$, $0 \mapsto 0_M$ を表す.
- $M \to 0$ は $M$ から $\{0\}$ への唯一の群準同型 $M \to \{0\}$, $\forall m \mapsto 0$ を表す.

こととする. $R$-準同型 $f\colon A \to B$ を考える. (1)〜(3) の同値と (4)〜(5) の主張を示せ.

(1) $0 \to A \xrightarrow{f} B$ が完全 $\Leftrightarrow$ $f$ が単射.
(2) $A \xrightarrow{f} B \to 0$ が完全 $\Leftrightarrow$ $f$ が全射.
(3) $0 \to A \xrightarrow{f} B \to 0$ が完全 $\Leftrightarrow$ $f$ が全単射 (つまり同型).
(4) $0 \to \ker f \xrightarrow{\iota} A \xrightarrow{f} f(A) \to 0$ は完全. ただし $\iota\colon \ker f \to A$, $k \mapsto k$ は自然な単射.
(5) $0 \to \ker f \xrightarrow{\iota} A \xrightarrow{f} B \xrightarrow{\pi} \operatorname{coker} f \to 0$ は完全系列. ただし $\pi\colon B \to \operatorname{coker} f := B/f(A)$, $b \mapsto b + f(A)$ は自然な射影.

**例 4.1.5.** (1) $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ の形の完全系列を **短完全系列** と呼ぶ. これは

$$f \text{ が単射 かつ } g \text{ が全射 かつ } f(A) = \ker g$$

を意味する. 特に, 準同型定理より

$$B/f(A) = B/\ker g \cong g(B) = C$$

が成り立つ.

(2) (1) の "逆" も成り立つ. すなわち, $R$-加群 $B$ の部分 $R$-加群 $A$ に対し, 商加群 $B/A$ を考えると

$$0 \to A \xrightarrow{\mathrm{id}} B \xrightarrow{\pi} B/A \to 0$$

は完全である. ただし $\pi\colon B \to B/A$ は自然な射影 $b \mapsto b + A$ である.

(3) $\mathbb{Z}$-加群として

$$0 \to \mathbb{Z} \xrightarrow{2\cdot} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \to 0$$

は完全である. ただし $2\cdot\colon \mathbb{Z} \to \mathbb{Z}$ は 2 倍写像 $n \mapsto 2n$ であり, $\pi\colon \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ は自然な射影 $n \mapsto n + 2\mathbb{Z}$ を表す.

**注意 4.1.6.** (お気持ち)

(1) 例 4.1.5-(3) は, ほとんど $\mathbb{Z}/2\mathbb{Z}$ の "定義" である. 同様に, 多くの $R$-加群が完全系

列で “定義” される. 例えば位数 $n$ の巡回群 $C_n = \langle g \rangle$ は

$$0 \to \mathbb{Z} \overset{n\cdot}{\to} \mathbb{Z} \overset{1 \mapsto g}{\to} C_n \to 0 \text{ (完全)}$$

で “定義” できる. また, 補足 3.4.7-(2) のイデアル類群 $Cl_K$ は

$$0 \to \mathcal{O}_K^\times \to K^\times \overset{\alpha \mapsto (\alpha)}{\to} I_K (\cong \bigoplus_{\mathfrak{p}} \mathbb{Z}) \to Cl_K \to 0 \text{ (完全)}$$

で “定義” できる.

(2) 数学の議論では, 加群たちへ何らかの “一斉操作” ($\Rightarrow$ 関手) を行うことがある. 例えば, $\mathbb{Z}$-加群 $M$ 達の $\mathrm{Hom}(\mathbb{Z}, M) = \{f \colon \mathbb{Z} \to M \mid f \text{ は群準同型}\}$ をとる操作を考える. 簡単な議論で

- $\mathrm{Hom}(\mathbb{Z}, M) \cong M$, $f \mapsto f(1)$, $[n \mapsto nm] \hookleftarrow m$.
- $f \colon A \to B$ が群準同型 $\Rightarrow$ $f_* \colon \mathrm{Hom}(\mathbb{Z}, A) \to \mathrm{Hom}(\mathbb{Z}, B)$, $\phi \mapsto f \circ \phi$ も群準同型.

が分かる. さらに, $\mathrm{Hom}(\mathbb{Z}, M)$ を例 4.1.5-(3) に施しても

$$\begin{array}{ccccc} 0 \to & \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) & \overset{(2\cdot)_*}{\to} & \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) & \overset{\pi_*}{\to} & \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \to 0 \\ & \cong \mathbb{Z} & & \cong \mathbb{Z} & & \cong \mathbb{Z}/2\mathbb{Z} \end{array}$$

は完全系列のままである. 一方で, 今度は $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, M) := \{f \colon \mathbb{Z}/2\mathbb{Z} \to M \mid f \text{ は群準同型}\}$ をとる操作を考える. すると

- $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = \{0\}$ ($\because \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \ni f \Rightarrow 2f(1) = f(2) = f(0) = 0 \Rightarrow f(1) = 0$).
- $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, $f \mapsto f(1)$, $[n \mapsto na] \hookleftarrow a$.
- $f \colon A \to B$ が群準同型 $\Rightarrow$ $f_* \colon \mathrm{Hom}(\mathbb{Z}/\mathbb{Z}, A) \to \mathrm{Hom}(\mathbb{Z}/\mathbb{Z}, B)$, $\phi \mapsto f \circ \phi$ も群準同型.

である. $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, M)$ を例 4.1.5-(3) に施すと

$$\begin{array}{ccccc} 0 \to & \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) & \overset{(2\cdot)_*}{\to} & \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) & \overset{\pi_*}{\to} & \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \to 0 \\ & = 0 & & = 0 & & \cong \mathbb{Z}/2\mathbb{Z} \end{array}$$

となり, 完全性が崩れる ($\because \pi_* \colon 0 \to \mathbb{Z}/2\mathbb{Z}$ は全射でない). 加群論では, この “崩れ方の計算” が重要になる ($\Rightarrow$ 導来関手).

**定義-命題 4.1.7.** $G$ を有限群とする.

(1) 集合 $\mathbb{Z}[G] := \left\{ \sum_{g\in G} n_g g \mid n_g \in \mathbb{Z} \right\}$ 上に演算

$$\sum_{g\in G} n_g g + \sum_{g\in G} m_g g = \sum_{g\in G} (n_g + m_g) g,$$

$$\sum_{g\in G} n_g g \cdot \sum_{g\in G} m_g g = \sum_{g\in G} \left( \sum_{g_1 g_2 = g} n_{g_1} m_{g_2} \right) g$$

を定義すると環となる. **群環** などと呼ばれる.

(2) 加法群 $M$ が **$G$-加群** である, とは

$$\exists G \times M \to M,\ (g, m) \mapsto gm$$

s.t.

$$\forall g, g' \in G,\ m, n \in M,\ (gg')m = g(g'm),\ e_G m = m,\ g(m+n) = gm + gn$$

となる事である. これは $M$ が $\mathbb{Z}[G]$-加群となることと同値である. 実際

(a) $\mathbb{Z}[G]$-加群 $M$ に対し, $gm := (1g)m$ と定めると $G$-加群になる.

(b) $G$-加群 $M$ に対し, $\sum_{g\in G}(n_g g)m := \sum_{g\in G} n_g(gm)$ と定めると $G$-加群になる.

(3) $G$-加群 $M$, すなわち, $\mathbb{Z}[G]$-加群 $M$ に対して

$$M^G := \{m \in M \mid \forall g \in G,\ gm = m\},$$

$$N_G M := \left\{ \sum_{g\in G} gm \mid m \in M \right\}$$

とおく. これは ($\mathbb{Z}[G]$-加群ではなく)$\mathbb{Z}$-加群 (加法群) であり, $N_G M \subset M^G$ を満たす.

(4) $\mathbb{Z}[G]$-準同型写像 $f\colon A \to B$ に対し,

$$f\colon A^G \to B^G,\ a \mapsto f(a)$$

も同じ $f$ で表すこととする. これは $\mathbb{Z}$-準同型写像 (すなわち群準同型写像) となる.

**例 4.1.8.** $G = \mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \rho_c\}$ ($\rho_c$ は複素共役写像) とおく ($\Rightarrow$ 問題 13, 例 2.1.11). このとき

$$\mathbb{Z}[G] = \{m \cdot \mathrm{id} + n \cdot \rho_c \mid m, n \in \mathbb{Z}\}$$

であり,

$$\begin{aligned}(m\cdot\mathrm{id}+n\cdot\rho_c)(p\cdot\mathrm{id}+q\cdot\rho_c) &= mp\cdot\mathrm{idid}+np\cdot\rho_c\mathrm{id}+mq\cdot\mathrm{id}\rho_c+nq\cdot\rho_c\rho_c\\ &= (mp+nq)\cdot\mathrm{id}+(np+mq)\cdot\rho_c\end{aligned}$$

となる. また加法群 $\mathbb{C}$ は

$$\sigma\in G,\ \alpha\in\mathbb{C}\Rightarrow\sigma\alpha:=\sigma(\alpha)=\begin{cases}\alpha & (\sigma=\mathrm{id})\\ \overline{\alpha} & (\sigma=\rho_c)\end{cases}$$

と定義すると $G$-加群となり,

$$m\cdot\mathrm{id}+n\cdot\rho_c\in\mathbb{Z}[G],\ \alpha\in\mathbb{C}\Rightarrow(m\cdot\mathrm{id}+n\cdot\rho_c)\alpha:=m\alpha+n\overline{\alpha}$$

で $\mathbb{Z}[G]$-加群とみなせる.

**問題 28.** 例 4.1.8 の $G$, $\mathbb{C}$ に対し $\mathbb{C}^G$, $N_G\mathbb{C}$ を求めよ.

## 4.2 有限巡回群の群コホモロジー

この小節では

$G$ は $\sigma$ を生成元とする位数 $n$ の巡回群 $\langle\sigma\rangle=\{e,\sigma,\sigma^2,\dots,\sigma^{n-1}\}$ である

とする.

**定理 4.2.1.** $\mathbb{Z}[G]$-加群 $A$ に対し, 2 種類の $\mathbb{Z}[G]$-準同型写像

$$\begin{aligned}N=N_A\colon A\to A,\ a\mapsto\sum_{i=0}^{n-1}\sigma^i a,\\ \Delta=\Delta_A\colon A\to A,\ a\mapsto(\sigma-1)a.\end{aligned}$$

を考え,

$$\hat{H}^n(G,A):=\begin{cases}\ker\Delta_A/N_A(A)=A^G/N_A(A) & (n=0)\\ \ker N_A/\Delta_A(A) & (n=1)\end{cases}$$

と定義する. このとき, $\mathbb{Z}[G]$-加群の短完全系列

$$0\to A\xrightarrow{f}B\xrightarrow{g}C\to 0$$

に対して, 群準同型写像

$$\delta^0\colon \hat{H}^0(G,C) \to \hat{H}^1(G,A),\ c+N_C(C) \mapsto f^{-1}(\Delta_B(g^{-1}(c))) + \Delta_A(A),$$
$$\delta^1\colon \hat{H}^1(G,C) \to \hat{H}^0(G,A),\ c+\Delta_C(C) \mapsto f^{-1}(N_B(g^{-1}(c))) + N_A(A)$$

が定まり,

$$\begin{array}{ccccc} \hat{H}^0(G,A) & \overset{\hat{H}^0(f)}{\to} & \hat{H}^0(G,B) & \overset{\hat{H}^0(g)}{\to} & \hat{H}^0(G,C) \\ {\scriptstyle\delta^1}\uparrow & & & & \downarrow{\scriptstyle\delta^0} \\ \hat{H}^1(G,C) & \overset{\hat{H}^1(g)}{\leftarrow} & \hat{H}^1(G,B) & \overset{\hat{H}^1(f)}{\leftarrow} & \hat{H}^1(G,A) \end{array} \tag{4.1}$$

が完全系列になる. ただし

- $\hat{H}^0(f)(a+N_A(A)) := f(a)+N_B(B)$, $\hat{H}^1(f)(a+\Delta_A(A)) := f(a)+\Delta_B(B)$. $\hat{H}^*(g)$ $(*=0,1)$ も同様.
- $f^{-1}(*)$ や $g^{-1}(*)$ は, $*$ の逆像から 1 元選んで取る.

**証明**. 群コホモロジーの一般論 ($\Rightarrow$ 定理 4.6.2) から従う. 差分は, 定義-命題 4.6.1 での定義との整合性で, 以下の議論で示せる: $G$ が巡回群のとき

$$\cdots \overset{\Delta_{\mathbb{Z}[G]}}{\to} \mathbb{Z}[G] \overset{N_{\mathbb{Z}[G]}}{\to} \mathbb{Z}[G] \overset{\Delta_{\mathbb{Z}[G]}}{\to} \mathbb{Z}[G] \overset{N_{\mathbb{Z}[G]}}{\to} \mathbb{Z}[G]$$

が $\mathbb{Z}[G]$-自由完全列となる. このとき

$$K^i(A) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \cong A,\ \phi \mapsto \phi(e_G),\ [\sum_{g\in G} n_g g \mapsto \sum_{g\in G} n_g g a] \leftarrow\!\shortmid a$$

により $K^i(A)$ と $A$ を同一視すれば, 複体は

$$A \overset{N_A}{\to} A \overset{\Delta_A}{\to} A \overset{N_A}{\to} A \overset{\Delta_A}{\to} \cdots$$

となり, 定理 4.2.1 での定義と定義-命題 4.6.1 での定義が一致する. ただし $\delta^1\colon \hat{H}^1(G,C) \to \hat{H}^2(G,A) \overset{\text{同一視}}{=} \hat{H}^0(G,A)$ とみなす. □

**問題 29.** $\mathbb{Z}[G]$-加群 $A$ に対し, 以下を確認せよ.

(1) $\ker \Delta_A = A^G$.
(2) $\ker \Delta_A \supset N_A(A)$.
(3) $\ker N_A \supset \Delta_A(A)$.

(4) $A$ が自明な $\mathbb{Z}[G]$-加群 (すなわち, $\forall g \in G,\ a \in A,\ ga = a$) であれば

$$\hat{H}^1(G, A) = \ker N_A \Delta_A(A) = A[n] := \{a \in A \mid na = 0\} \overset{a \mapsto [\sigma^k \to ka]}{\cong} \mathrm{Hom}(G, A).$$

**注意 4.2.2.** $\mathbb{Z}[G]$-加群 $A$ 達に対する操作

$$A \Rightarrow \ker \Delta_A (= A^G)$$

は, 短完全系列を崩す:

$$0 \to A \overset{f}{\to} B \overset{g}{\to} C \to 0 \text{ (完全)} \Rightarrow 0 \to A^G \overset{f|_{A^G}}{\to} B^G \overset{g|_{B^G}}{\to} C^G \text{ (完全)}$$
だが $g|_{B^G}$ が全射とは限らない.

別の操作

$$A \Rightarrow A^G / N_A(A)$$

は更に

$$0 \to A \overset{f}{\to} B \overset{g}{\to} C \to 0 \text{ (完全)} \Rightarrow A^G/N_A(A) \overset{\overline{f}}{\to} B^G/N_B(B) \overset{\overline{g}}{\to} C^G/N_C(C) \text{ (完全)}$$
だが $\overline{f}$ が単射, $\overline{g}$ が全射とは限らない.

群コホモロジーを使うことで, この「ずれ」を測ることができる. 詳細は [足-三, 付録 A.1], [小野, §20] などを参照.

**問題 30.** $G = \{\pm 1\}$ (2 元からなる乗法群) とする. $G$ の $\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ への作用を

$$\pm 1 \cdot n := \pm n,\ (n \in \mathbb{Z})$$
$$\pm 1 \cdot \overline{n} := \overline{n} \text{ (自明な作用) } (\overline{n} = n + 2\mathbb{Z} \in \mathbb{Z}/2\mathbb{Z})$$

で定める. 以下を確認せよ.

(1) 例 4.1.5-(3) で与えた $0 \to \mathbb{Z} \overset{2\cdot}{\to} \mathbb{Z} \overset{\pi}{\to} \mathbb{Z}/2\mathbb{Z} \to 0$ は $\mathbb{Z}[G]$-加群としても完全系列.
(2) $\mathbb{Z}^G = N_{\mathbb{Z}}(\mathbb{Z}) = \{0\}$, $\ker N_{\mathbb{Z}} = \mathbb{Z}$, $\Delta_{\mathbb{Z}}(\mathbb{Z}) = 2\mathbb{Z}$.
(3) $(\mathbb{Z}/2\mathbb{Z})^G = \mathbb{Z}/2\mathbb{Z}$, $N_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}) = \{0\}$, $\ker N_{\mathbb{Z}/2\mathbb{Z}} = \mathbb{Z}/2\mathbb{Z}$, $\Delta_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}) = \{0\}$.
(4) $0 \to \mathbb{Z}^G \overset{2\cdot}{\to} \mathbb{Z}^G \overset{\pi}{\to} (\mathbb{Z}/2\mathbb{Z})^G \to 0$ や $0 \to \mathbb{Z}^G/N_{\mathbb{Z}}(\mathbb{Z}) \overset{2\cdot}{\to} \mathbb{Z}^G/N_{\mathbb{Z}}(\mathbb{Z}) \overset{\pi}{\to} (\mathbb{Z}/2\mathbb{Z})^G/N_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}) \to 0$ は ($\mathbb{Z}$-加群として) 完全系列でない.
(5) 以下は完全系列.

$$\begin{array}{ccccc} \hat{H}^0(G,\mathbb{Z}) & \overset{\hat{H}^0(2\cdot)}{\to} & \hat{H}^0(G,\mathbb{Z}) & \overset{\hat{H}^0(\pi)}{\to} & \hat{H}^0(G,\mathbb{Z}/2\mathbb{Z}) \\ \delta^1 \uparrow & & & & \downarrow \delta^0 \\ \hat{H}^1(G,\mathbb{Z}/2\mathbb{Z}) & \overset{\hat{H}^1(\pi)}{\leftarrow} & \hat{H}^1(G,\mathbb{Z}) & \overset{\hat{H}^1(2\cdot)}{\leftarrow} & \hat{H}^1(G,\mathbb{Z}) \end{array}$$

## 4.3 ヒルベルトの定理 90 とピタゴラス数

$L/k$ が有限次ガロア拡大であるとき, $L^\times$ は

$$\sigma \in \mathrm{Gal}(L/k),\ \alpha \in L^\times \Rightarrow \sigma\alpha := \sigma(\alpha)$$

$\mathbb{Z}[\mathrm{Gal}(L/k)]$-加群とみなせる. ただし $L^\times$ 上の掛け算を加法として加法群とみなしているので, 記法上でいくつか注意が必要. 例えば

- 一般に加法群 $M$ に対し $3m$ $(m \in M)$ は

  $$3 \cdot m = m + m + m$$

  と定めるが, $\alpha \in L^\times$ に対しては

  $$3 \cdot \alpha = \alpha \times \alpha \times \alpha = \alpha^3$$

  と考える. 同様に

  $$n \in \mathbb{Z},\ \alpha \in L^\times \Rightarrow n \cdot \alpha = \alpha^n.$$

- $\sum_{\sigma \in \mathrm{Gal}(L/k)} n_\sigma \sigma \in \mathbb{Z}[\mathrm{Gal}(L/k)]$, $\alpha \in L^\times$ に対し

  $$\left( \sum_{\sigma \in \mathrm{Gal}(L/k)} n_\sigma \sigma \right)(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/k)} \sigma(\alpha)^{n_\sigma}.$$

- $G = \langle \sigma \rangle$ が位数 $n$ の巡回群のとき

  $$N_{L^\times} \colon L^\times \to L^\times,\ \alpha \mapsto \prod_{i=0}^{n-1} \sigma^i(\alpha),$$
  $$\Delta_{L^\times} \colon L^\times \to L^\times,\ \alpha \mapsto \frac{\sigma(\alpha)}{\alpha}.$$

**定理 4.3.1** (ヒルベルトの定理 90)**.** ガロア拡大 $L/k$ に対して

$$\hat{H}^1(\mathrm{Gal}(L/k), L^\times) = 0.$$

※ 群コホモロジーは一般の (副) 有限群に対して定義でき, この定理の主張も一般のガロア拡大に対して成立する.

**証明**. ここでは $\mathrm{Gal}(L/k)$ が位数 $n$ の巡回群 $=\langle\sigma\rangle$ である場合に限定して証明を与える. $\ker N_{L^\times} = \Delta_{L^\times}(L^\times)$ を示せばよい. $(\supset)$ は問題 29-(2) より従うので

$$\ker N_{L^\times} := \{\alpha \in L^\times \mid N_{L^\times}(\alpha) = 1\} \subset \Delta_{L^\times}(L^\times) := \left\{ \frac{\sigma(\alpha)}{\alpha} \mid \alpha \in L^\times \right\},$$

すなわち

$$\alpha \in L^\times,\ N_{L^\times}(\alpha) = 1 \Rightarrow \exists \beta \in L^\times \text{ s.t. } \alpha = \frac{\sigma(\beta)}{\beta}$$

を示せばよい.

$N_{L^\times}(\alpha) = 1$ を満たす $\alpha \in L^\times$ に対し, 写像

$$T\colon L \to L,\ \beta \mapsto \frac{\sigma(\beta)}{\alpha}$$

を考える. このとき, $T$ は $k$-線形写像であり

(1) $\exists \beta \in L^\times$ s.t. $\alpha = \frac{\sigma(\beta)}{\beta} \Leftrightarrow \exists \beta \neq 0$ s.t. $T(\beta) = \beta \Leftrightarrow T$ が固有値 1 を持つ.

が分かる. $L/k$ が有限次ガロア拡大より,

(2) $L = k(\gamma)$ の形に書け, $\gamma$ の最小多項式 $f$ は $(x-\gamma)(x-\sigma(\gamma))$ と分解できるので

$$\bigoplus_{i=0}^{n-1} k \cdot \gamma^i = L = k(\gamma) \cong k[x]/(f) = k[x]/(x-\gamma)(x-\sigma(\gamma)),$$

$$\bigoplus_{i=0}^{n-1} L \cdot \gamma^i = L \otimes_k L \cong L[x]/(x-\gamma)(x-\sigma(\gamma))\cdots(x-\sigma^{n-1}(\gamma))$$

$$\overset{x \mapsto \gamma \oplus \sigma(\gamma) \oplus \cdots \oplus \sigma^{n-1}(\gamma)}{\cong} \bigoplus_{i=0}^{n-1} L$$

と書ける.

$k$-線形写像 $T\colon L \to L$ を $L$-線形写像 $\tilde{T} := T \otimes \mathrm{id}_L\colon L \otimes_k L \to L \otimes_k L$ に拡張すると,

(3) $T$ の基底 $\gamma^i$ $(i = 0, \ldots, n-1)$ に関する表現行列と $\tilde{T}$ の基底 $\gamma^i$ $(i = 0, \ldots, n-1)$ に関する表現行列が一致する. とくに

$$T \text{ が固有値 } 1 \text{ を持つ} \Leftrightarrow \tilde{T} \text{ が固有値 } 1 \text{ を持つ}.$$

一方で, $\tilde{T}$ を $\bigoplus_{i=0}^{n-1} L$ 上で明示すると

(4) $\tilde{T}\colon \bigoplus_{i=0}^{n-1} L \to \bigoplus_{i=0}^{n-1} L$, $\delta_0 \oplus \delta_1 \oplus \cdots \oplus \delta_{n-1} \mapsto \alpha^{-1}(\delta_{n-1} \oplus \delta_0 \oplus \cdots \oplus \delta_{n-2}) = \alpha^{-1}\delta_{n-1} \oplus \sigma(\alpha)^{-1}\delta_0 \oplus \cdots \oplus \sigma^{n-1}(\alpha)^{-1}\delta_{n-2}$

となっている. よって, $\tilde{\beta} := 1 \oplus \sigma(\alpha)^{-1} \oplus (\sigma(\alpha)\sigma^2(\alpha))^{-1} \oplus \cdots \oplus (\sigma(\alpha)\ldots\sigma^{n-1}(\alpha))^{-1} \in \bigoplus_{i=0}^{n-1} L, \neq 0$ に対し

(5) $\tilde{T}(\tilde{\beta}) = N_{L^\times}(\alpha)^{-1} \oplus \sigma(\alpha)^{-1} \oplus \cdots \oplus (\sigma(\alpha)\ldots\sigma^{n-1}(\alpha))^{-1} = \tilde{\beta}$

と計算でき, $\tilde{T}$ は固有値 1 を持ち, 題意が従う. □

**例 4.3.2** (ピタゴラス数)**.** $K = \mathbb{Q}(\sqrt{-1})$, $k = \mathbb{Q}$ のとき, $\mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}) = \{\mathrm{id}, \rho_c\}$ ($\rho_c$ は素共役写像) は巡回群なので

$$H^1(\mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}), \mathbb{Q}(\sqrt{-1})^\times) = \frac{\ker N\colon \mathbb{Q}(\sqrt{-1})^\times \to \mathbb{Q}(\sqrt{-1})^\times}{\Delta(\mathbb{Q}(\sqrt{-1})^\times)}$$

となる. さらに

$$\ker N = \ker[\alpha \mapsto \alpha\rho_c(\alpha)] = \left\{x + y\sqrt{-1} \mid x, y \in \mathbb{Q},\ x^2 + y^2 = 1\right\},$$
$$\Delta(\mathbb{Q}(\sqrt{-1})^\times) = \left[\alpha \mapsto \frac{\rho(\alpha)}{\alpha}\right] \text{の像} = \left\{\frac{m - n\sqrt{-1}}{m + n\sqrt{-1}} \mid m, n \in \mathbb{Q},\ (m, n) \neq (0, 0)\right\}$$

となる. すなわち, ヒルベルト 90 はこの場合

$$x^2 + y^2 = 1\ (x, y \in \mathbb{Q}) \Leftrightarrow x = \frac{m^2 - n^2}{m^2 + n^2},\ y = \frac{2mn}{m^2 + n^2}\ (m, n \in \mathbb{Q},\ (m, n) \neq (0, 0))$$

を言っている. このことから, ピタゴラス数の一般形

$$\begin{aligned} &a^2 + b^2 = c^2\ (a, b, c \in \mathbb{N}), \gcd(a, b, c) = 1 \\ &\Leftrightarrow a = m^2 - n^2,\ b = 2mn,\ c = m^2 + n^2\ (m, n \in \mathbb{N},\ m > n, \gcd(m, n) = 1) \\ &\quad (\text{または } a, b \text{ の取り換え}) \end{aligned}$$

が得られる.

## 4.4 クンマー理論

**定理 4.4.1.** $n \in \mathbb{N}$ を固定し, $\zeta_n := e^{\frac{2\pi i}{n}}$, $\mu_n := \langle \zeta_n \rangle$ とおく. $k$ は代数体で $\zeta_n \in k$ とする.

(1) 有限次ガロア拡大 $L/k$ に対し

$$((L^\times)^n \cap k^\times)/(k^\times)^n \cong \mathrm{Hom}(\mathrm{Gal}(L/k), \mu_n),\ \alpha \bmod (k^\times)^n \mapsto [\sigma \mapsto \frac{\sigma(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}}].$$

(2) $k$ の任意の $n$ 次巡回拡大 $K$ は

$$K = k(\sqrt[n]{\alpha})\ (\alpha \in k^\times)$$

の形に書ける. さらに, 2 つの $n$ 次巡回拡大 $k(\sqrt[n]{\alpha_i})\ (\alpha_i \in k^\times,\ i = 1, 2)$ に対し

$$k(\sqrt[n]{\alpha_1}) = k(\sqrt[n]{\alpha_2}) \Leftrightarrow \exists a \text{ s.t. } \gcd(a, n) = 1,\ \alpha_1 \equiv \alpha_2^a \mod (k^\times)^n.$$

**証明**. (1) $\mathrm{Gal}(L/k)$ が巡回群の場合の証明を演習問題とする ($\Rightarrow$ 問題 31). 一般の場合も (群コホモロジーの定義さえすれば) 同様に示せる.

(2) $K/k$ を $n$ 次巡回拡大とし, $L := K$ とおくと, $\mathrm{Hom}(\mathrm{Gal}(L/k), \mu_n)$ に位数 $n$ の元 $\phi\colon \mathrm{Gal}(L/k) \cong \mu_n$ が存在する. よって (1) より

$$\exists \gamma \in K^\times \text{ s.t. } \alpha := \gamma^n \in k^\times,\ \phi = [\mathrm{Gal}(L/k) \ni \sigma \mapsto \frac{\sigma(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}} \in \mu_n].$$

よって $\sigma(\sqrt[n]{\alpha}) = \sqrt[n]{\alpha} \Leftrightarrow \phi(\sigma) = 1 \overset{\phi \text{ は同型}}{\Leftrightarrow} \sigma = \mathrm{id}$, すなわち $\sqrt[n]{\alpha}$ は $K$ の生成元である.

次に $K_i := K(\sqrt[n]{\alpha_i})$, $L := K_1K_2 = K(\sqrt[n]{\alpha_1}, \sqrt[n]{\alpha_2})$, $\pi_i\colon \mathrm{Gal}(L/k) \to \mathrm{Gal}(K_i/k) \cong \mu_n$ とおくと, (1) より

$$((L^\times)^n \cap k^\times)/(k^\times)^n \cong \mathrm{Hom}(\mathrm{Gal}(L/k), \mu_n),\ \alpha_i \bmod (k^\times)^n \leftrightarrow \pi_i.$$

よって $K_1 = K_2 \Leftrightarrow \mathrm{Gal}(L/K_1) = \mathrm{Gal}(L/K_2) \Leftrightarrow \ker \pi_1 = \ker \pi_2 \Leftrightarrow \pi_1 = \pi_2^{\exists a}\ (\gcd(a, n) = 1) \Leftrightarrow \alpha_1 \bmod (k^\times)^n = \alpha_2^a \bmod (k^\times)^n$. □

**問題 31.** 以下の手順で定理 4.4.1-(1) を証明せよ.

(1) $0 \to \mu_n \to L^\times \overset{x \mapsto x^n}{\to} (L^\times)^n \to 0$ は $\mathbb{Z}[\mathrm{Gal}(L/k)]$-加群の短完全系列となることを示せ.

(2) (1) の短完全系列から導かれる Eq. (4.1) の完全系列を書き下せ：

$$\begin{array}{ccccc} \boxed{???} & \to & \boxed{???} & \overset{\hat{H}^0(x \mapsto x^n)}{\to} & \boxed{???} \\ \uparrow & & & & \downarrow \delta^0 \\ \boxed{???} & \leftarrow & \boxed{???} & \leftarrow & \boxed{???} \end{array}$$

(3) 以下を (2) に代入せよ.

- ガロア対応により $(L^\times)^{\mathrm{Gal}(L/k)} = k^\times$, $((L^\times)^n)^{\mathrm{Gal}(L/k)} = (L^\times)^n \cap k^\times$.
- ヒルベルト 90 により $\hat{H}^1(\mathrm{Gal}(L/k), L^\times) = 0$,
- 問題 29-(4) より $\hat{H}^1(\mathrm{Gal}(L/k), \mu_n) = \mathrm{Hom}(\mathrm{Gal}(L/k), \mu_n)$

(4) (3) の $\delta^0$ に準同型定理を使って得られる同型写像を書け.

(5) 右上の項の完全性 ($\hat{H}(x \mapsto x^n)$ の像 $= \ker \delta^0$) から得られる式を (4) に代入し, 定理 4.4.1-(1) を導け.

**問題 32.** 以下の中で $\mathbb{Q}(\zeta_3)(\sqrt[3]{2})$ と一致する体を全て答えよ.

$$\mathbb{Q}(\zeta_3)(\sqrt[3]{4}), \quad \mathbb{Q}(\zeta_3)(\sqrt[3]{8}), \quad \mathbb{Q}(\zeta_3)(\sqrt[3]{\tfrac{1}{2}}), \quad \mathbb{Q}(\zeta_3)(\sqrt[3]{54}), \quad \mathbb{Q}(\zeta_3)(\sqrt[3]{-6\sqrt{-3}}).$$

## 4.5 # 素数次クンマー拡大での分岐理論

**定義-命題 4.5.1.** 代数体 $k$ の素イデアル $\mathfrak{p}$ を考える.

(1) $\alpha \in \mathcal{O}_k$ に対し

$$v_\mathfrak{p}(\alpha) := \max\{n \mid \alpha \in \mathfrak{p}^n\} \in \{0, 1, 2, \ldots, \infty\},$$

$\alpha/\beta \in k$, $\alpha \in \mathcal{O}_k$, $\beta \in \mathcal{O}_k - \{0\}$ に対し

$$v_\mathfrak{p}(\alpha/\beta) := v_\mathfrak{p}(\alpha) - v_\mathfrak{p}(\beta)$$

と定める.

(2) $\mathcal{O}_{k(\mathfrak{p})} := \{\alpha/\beta \in k \mid \alpha \in \mathcal{O}_k,\ \beta \in \mathcal{O}_k - \mathfrak{p}\}$ を <u>局所化</u> と呼ぶ. さらに

(a) $\mathcal{O}_{k(\mathfrak{p})}$ はただ一つの極大イデアル

$$\mathfrak{p}\mathcal{O}_{k(\mathfrak{p})} = \{\alpha \in k \mid v_\mathfrak{p}(\alpha) \geq 1\}$$

をもつ局所環となる.

(b) $\mathcal{O}_{k(\mathfrak{p})}$ の極大イデアル $\mathfrak{p}\mathcal{O}_{k(\mathfrak{p})}$ は単項イデアルとなる. その生成元 $\pi_\mathfrak{p}$ は

$$v_\mathfrak{p}(\pi_\mathfrak{p}) = 1$$

で特徴づけられる.

(c) 剰余体 $\mathbb{F}_\mathfrak{p} := \mathcal{O}_k/\mathfrak{p}$, $\mathcal{O}_{k(\mathfrak{p})}/\mathfrak{p}\mathcal{O}_{k(\mathfrak{p})}$ は以下で同一視できる (同型になる)

$$\begin{aligned} \mathbb{F}_\mathfrak{p} = \mathcal{O}_k/\mathfrak{p} &\xrightarrow{\cong} \mathcal{O}_{k(\mathfrak{p})}/\mathfrak{p}\mathcal{O}_{k(\mathfrak{p})}, \\ \alpha \bmod \mathfrak{p} &\mapsto \alpha \bmod \mathfrak{p}\mathcal{O}_{k(\mathfrak{p})}, \\ \frac{\alpha}{\beta} \bmod \mathfrak{p} := \frac{\alpha \bmod \mathfrak{p}}{\beta \bmod \mathfrak{p}} &\mapsfrom \frac{\alpha}{\beta} \bmod \mathfrak{p}\mathcal{O}_{k(\mathfrak{p})}. \end{aligned}$$

**定理 4.5.2.** $q$ を素数とし, 代数体 $k, K$ が

$$\zeta_q \in k, \quad K = k(\sqrt[q]{\mu})\ (\mu \in k^\times - (k^\times)^q)$$

を満たしているとする. このとき以下が成り立つ.

(1) $k$ の素イデアル $\mathfrak{p} \nmid q$ に対し
  (a) $\mathfrak{p}$ が $K/k$ で不分岐 $\Leftrightarrow v_\mathfrak{p}(\mu) \equiv 0 \mod q$.
  (b) $\mathfrak{p}$ が $K/k$ で完全分解 $\Leftrightarrow \exists \alpha \in k$ s.t. $\frac{\mu}{\alpha^q} \in \mathcal{O}_{k(\mathfrak{p})}$, $\frac{\mu}{\alpha^q} \equiv 1 \mod \mathfrak{p}$.

(2) $k$ の素イデアル $\mathfrak{q} \mid q$ に対し
  (a) $\mathfrak{q}$ が $K/k$ で不分岐 $\Leftrightarrow \exists \alpha \in k$ s.t. $\frac{\mu}{\alpha^q} \in \mathcal{O}_{k(\mathfrak{q})}$, $\frac{\mu}{\alpha^q} \equiv 1 \mod \mathfrak{q}^{qe_{\mathfrak{q}/(1-\zeta_q)}}$.
  (b) $\mathfrak{q}$ が $K/k$ で完全分解
    $\Leftrightarrow$ (a) を満たす $\alpha \in k$ に対して $\mathrm{tr}_{\mathbb{F}_\mathfrak{q}/\mathbb{F}_q}(\frac{\frac{\mu}{\alpha^q}-1}{q(1-\zeta_q)} \bmod \mathfrak{q}) = 0$.
    とくに $\exists \alpha \in k$ s.t. $\frac{\mu}{\alpha^q} \in \mathcal{O}_{k(\mathfrak{q})}$, $\frac{\mu}{\alpha^q} \equiv 1 \mod \mathfrak{q}^{qe_{\mathfrak{q}/(1-\zeta_q)}+1}$ は十分条件.

**補足 4.5.3.** 体 $K$ を変えずに $\mu \in \mathcal{O}_K$ とできる. このとき $\sqrt[q]{\mu}$ の最小多項式 $x^q - \mu$ の mod$\mathfrak{p}$ (または mod$\mathfrak{q}$) での分解の様子が, 基本的には $\mathfrak{q}$ (または $\mathfrak{p}$) の分解の様子を知っている ($\Rightarrow$ 補足 3.4.11-(2)). 完全な証明は少し準備が必要. 詳細は [Gr, Chap.I, §6, Theorem 6.3] などを参照.

**問題 33.** $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ において分岐している素イデアル (素数) を全て答えよ.

## 4.6 # 有限群の群コホモロジー

(Section 4.2 では有限巡回群だけを扱ったが) この小節では

$$G \text{ は巡回群とは限らない有限群}$$

とする. また $\mathbb{Z}_{\geq 0} := \{0, 1, 2, \dots\}$ とおく.

**定義-命題 4.6.1.** 各 $n \in \mathbb{Z}_{\geq 0}$ に対し,

- $\mathbb{Z}[G]$-加群 $A$ に対し, 加法群 $H^n(G, A)$ (**群 $G$ の $A$ 係数 $n$ 次コホモロジー群**).
- $f \in \mathrm{Hom}_{\mathbb{Z}[G]}(A, B)$ に対し, $H^n(f) \in \mathrm{Hom}(H^n(G, A), H^n(G, B))$.
- $\mathbb{Z}[G]$-加群の完全列 $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ に対し, **連結準同型写像** $\delta^n \in \mathrm{Hom}(H^n(G, C), H^{n+1}(G, A))$.

を, 以下の手順で定義する.

(1) $\mathbb{Z}[G]$ のいくつかの直和と同型な $\mathbb{Z}[G]$-加群を **$\mathbb{Z}[G]$-自由加群** と呼ぶ.

(2) $\mathbb{Z}[G]$-自由加群 $P_i$ からなる完全列

$$\cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 (= \mathbb{Z}[G])$$

を **$\mathbb{Z}[G]$-自由完全列** と呼ぶ. $\mathbb{Z}[G]$-自由完全列が必ず存在するので 1 つ取る.

(3) 加法群 $K_i$ と群準同型写像 $d^i$ の列

$$\cdots \xrightarrow{d^{i-2}} K^{i-1} \xrightarrow{d^{i-1}} K^i \xrightarrow{d^i} K^{i+1} \xrightarrow{d^{i+1}} \cdots$$

が $\forall i,\ d^i \circ d_{i-1} = 0$ を満たすとき **複鎖体** と呼ばれる.

(4) (2) の $P_i$ に対し, $K^i(A) := \mathrm{Hom}_{\mathbb{Z}[G]}(P_i, A)$, $d^i := [\phi \mapsto d_{i+1}\phi]$ とおいて

$$K^0(A) \xrightarrow{d^0} K^1(A) \xrightarrow{d^1} K^2(A) \xrightarrow{d^2} \cdots$$

を考えると複鎖体となる. とくに $d^i \circ d^{i-1} = 0$ であるが, 完全とは限らない.

(5) (4) の複鎖体の完全性との “差” が **群コホモロジー** である:

$$\begin{aligned} Z^n(G, A) &:= \ker d^n, \\ B^n(G, A) &:= \begin{cases} 0 & (n = 0), \\ d^{n-1}(K^{n-1}(A)) & (n > 0), \end{cases} \\ H^n(G, A) &:= Z^n(G, A)/B^n(G, A). \end{aligned}$$

(6) $f \in \mathrm{Hom}_{\mathbb{Z}[G]}(A, B)$ に対し,

$$\begin{aligned} f^n &\colon K^n(A) \to K^n(B),\ \phi \mapsto f \circ \phi, \\ H^n(f) &\colon H^n(G, A) \to H^n(G, B),\ \phi + B^n(G, A) \mapsto f^n(\phi) + B^n(G, C). \end{aligned}$$

(7) $\mathbb{Z}[G]$-加群の完全列

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

に対して

$$\begin{array}{ccccccccc} 0 \to & K^n(A) & \xrightarrow{f^n} & K^n(B) & \xrightarrow{g^n} & K^n(C) & \to 0 \\ & d_n \downarrow & & d_n \downarrow & & d_n \downarrow & \\ 0 \to & K^{n+1}(A) & \xrightarrow{f^{n+1}} & K^{n+1}(B) & \xrightarrow{g^{n+1}} & K^{n+1}(C) & \to 0 \end{array}$$

の横の列は加法群の完全列となる ($\because$ 自由 $\Rightarrow$ 射影的). さらに

$$\begin{aligned}&\delta^n\colon H^n(G,C)\to H^{n+1}(G,A),\\&\quad \phi+B^n(G,C)\mapsto ((f^{n+1})^{-1}\circ d^n\circ(g^n)^{-1})(\phi)+B^{n+1}(G,A).\end{aligned}$$

は well-defined になる ($\because$ 蛇の補題). ただし $g^n$ は単射ではないので $(g^n)^{-1}(\phi)$ は逆像から 1 元を選んで取る.

**定理 4.6.2.** (1) $H^0(G,A)\cong A^G$, $H^0(f)=f|_{A^G}$.

(2) $\mathbb{Z}[G]$-加群 $A,B,C$ の間の完全列 $0\to A\xrightarrow{f}B\xrightarrow{g}C\to 0$ に対し, $\mathbb{Z}$-加群としての完全列

$$\begin{array}{lllll}0\to & H^0(G,A) & \xrightarrow{H^0(f)} & H^0(G,B) & \xrightarrow{H^0(g)} & H^0(G,C)\\ \xrightarrow{\delta^0} & H^1(G,A) & \xrightarrow{H^1(f)} & H^1(G,B) & \xrightarrow{H^1(g)} & H^1(G,C)\\ \xrightarrow{\delta^1} & H^2(G,A) & \xrightarrow{H^2(f)} & \cdots & & \end{array}$$

が成り立つ. **長完全列** などと呼ばれる.

(3) $f\in\mathrm{Hom}_{\mathbb{Z}[G]}(A,B)$, $g\in\mathrm{Hom}_{\mathbb{Z}[G]}(B,C)$ に対し $H^n(f\circ g)=H^n(f)\circ H^n(g)$.

(4) 二つの $\mathbb{Z}[G]$-加群としての完全列

$$\begin{array}{ccccccccc}0 & \to & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \to & 0\\ & & \downarrow\alpha & & \downarrow\beta & & \downarrow\gamma & & \\ 0 & \to & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \to & 0\end{array}$$

が "可換" ならば

$$\begin{array}{ccc}H^n(G,C) & \xrightarrow{\delta^n} & H^{n+1}(G,A)\\ \downarrow{\scriptstyle (\gamma)^H_n} & & \downarrow{\scriptstyle (\alpha)^H_{n+1}}\\ H^n(G,C') & \xrightarrow{\delta^n} & H^{n+1}(G,A')\end{array}$$

も "可換" である.

(5) 加法群 $M$ を用いて

$$cI_G(M):=\mathrm{Hom}(\mathbb{Z}[G],M)\ni\phi,\ (\sigma\phi)\left(\sum_{g\in G}n_g g\right):=\phi\left(\sum_{g\in G}n_g\sigma^{-1}g\right)\ (\sigma\in G)$$

で表される $\mathbb{Z}[G]$-加群 $cI_G(M)$ を **(余) 誘導加群** と呼ぶ. $A$ が余誘導加群と同型なら, $H^n(G,A)=0$ $(n\geq 1)$.

**補足 4.6.3.** (1) 群コホモロジーの定義は何通りもあり, いずれも同値である.

(2) “標準的な $\mathbb{Z}[G]$-自由完全列” を使った計算で

$$\begin{aligned}
&H^0(G,A) := A^G,\ H^0(f) := f|_{A^G}\colon A^G \to B^G,\\
&H^1(G,A) := Z^1(G,A)/B^1(G,A),\\
&Z^1(G,A) := \{\text{写像 } \phi\colon G \to A \mid \phi(\sigma\tau) = \sigma\phi(\tau) + \phi(\sigma)\},\\
&B^1(G,A) := \{\phi_a\colon G \to A,\ \sigma \mapsto \sigma a - a \mid a \in A\},\\
&H^1(f)(\phi + B^1(G,A)) := f \circ \phi + B^1(G,B)
\end{aligned}$$

と明示的に書ける. $Z^1(G,A)$ の元は **コサイクル**, $B^1(G,A)$ の元は **コバウンダリ**, 条件 $\phi(\sigma\tau) = \sigma\phi(\tau) + \phi(\sigma)$ は **コサイクル条件** と呼ばれる. とくに $G$ が $A$ に自明に作用するとき

$$H^1(G,A) = Z^1(G,A) = \mathrm{Hom}(G,A)$$

となる.

(3) 群コホモロジーは, 定理 4.6.2 の (1)∼(5) を満たすだだけでなく, これらで特徴づけることもできる. これには, 一般の $\mathbb{Z}[G]$-加群 $A$ に対して, $A$ は余誘導加群 $cI_G(A)$ の部分 $\mathbb{Z}[G]$-加群となることが効いている:

$$A \hookrightarrow cI_G(A),\ m \mapsto [\sum_{g\in G} n_g g \mapsto \sum_{g\in G} n_g(g^{-1}m)].$$

実際, これから導かれる短完全系列

$$0 \to A \to cI_G(A) \xrightarrow{\pi} cI_G(A)/A \to 0$$

に定理 4.6.2-(2) の長完全系列を使い, 定理 4.6.2-(1), (5) を代入すると, 完全系列

$$cI_G(A)^G \xrightarrow{\pi} (cI_G(A)/A)^G \to H^1(G,A) \to 0$$

を得る. 特に

$$H^1(G,A) \cong cI_G(A)/A)^G/\pi(cI_G(A)^G).$$

(2) の $H^1$ の表示は,

$$\begin{aligned}
&(cI_G(A)/A)^G \to Z^1(G,A)/B^1(G,A),\\
&\phi + A \mapsto [g \mapsto \phi(g^{-1}) - \phi(e_G)] + B^1(G,A)
\end{aligned}$$

が全射準同型であり, その核が $\pi(cI_G(A)^G) \subset (cI_G(A)/A)^G$ と一致することからも導くことができる. $H^2$ 以降も同様に帰納的に計算できる.

(4) $H^0(G,A)$ だけ修正して, Tate (群) コホモロジー

$$\hat{H}^n(G,A) := \begin{cases} A^G/NG & (n=0) \\ H^n(G,A) & (n \geq 1) \end{cases}$$

を考えることも多い. この場合, 長完全系列は

$$\begin{array}{cccccc} & \hat{H}^0(G,A) & \overset{\hat{H}^0(f)}{\to} & \hat{H}^0(G,B) & \overset{\hat{H}^0(g)}{\to} & \hat{H}^0(G,C) \\ \overset{\delta^0}{\to} & \hat{H}^1(G,A) & \overset{\hat{H}^1(f)}{\to} & \hat{H}^1(G,B) & \overset{\hat{H}^1(g)}{\to} & \hat{H}^1(G,C) \\ \overset{\delta^1}{\to} & \hat{H}^2(G,A) & \overset{\hat{H}^2(f)}{\to} & \cdots & & \end{array}$$

に変化する ($H^0(f)$ の単射性だけなくなる).

**例 4.6.4.** 群 $G = \{\pm 1\}$ に対し, 以下の $\mathbb{Z}[G]$-加群を考える.

- $\mathbb{Z}$ に群作用 $\pm 1 \cdot n := \pm n$ を考えたもの. $\mathbb{Z}_{\pm}$ で表す.
- $\mathbb{Z}$ に自明な作用 $\pm 1 \cdot n := n$ を考えたもの. $\mathbb{Z}_0$ で表す.
- $\mathbb{Z}/2\mathbb{Z}$ に自明な作用を考えたもの. $\mathbb{Z}/2\mathbb{Z}$ で表す.
- 余誘導加群 $cI_G(A) = \mathrm{Hom}(\mathbb{Z}[G], A)$ の一般元は $\phi_{a,b} \colon \mathbb{Z}[G] \to A$, $n \cdot 1 + m \cdot (-1) \mapsto an + bm$ $(a, b \in A)$ で表される.

(1) $\mathbb{Z}[G]$-加群としての短完全列

$$0 \to \mathbb{Z}_{\pm} \overset{n \mapsto \phi_{n,-n}}{\to} cI_G(\mathbb{Z}) \overset{\phi_{a,b} \mapsto a+b}{\to} \mathbb{Z}_0 \to 0$$

が取れる. $\hat{H}^n(G, I_G(\mathbb{Z})) = 0$ に注意すると, 長完全系列 (Tate 版) の最初の方は

$$\mathbb{Z}_{\pm}^G/N_G\mathbb{Z}_{\pm} \to 0 \to \mathbb{Z}_0^G/N_G\mathbb{Z}_0 \to H^1(G, \mathbb{Z}_{\pm}) \to 0$$

を与えてくれる. よって

$$H^1(G, \mathbb{Z}_{\pm}) \cong \mathbb{Z}_0^G/N_G\mathbb{Z}_0 = \mathbb{Z}/2\mathbb{Z}.$$

(2) 同様に, $\mathbb{Z}[G]$-加群の短完全列

$$0 \to \mathbb{Z}/2\mathbb{Z} \overset{n \mapsto \phi_{n,-n}}{\to} cI_G(\mathbb{Z}/2\mathbb{Z}) \overset{\phi_{a,b} \mapsto a+b}{\to} \mathbb{Z}/2\mathbb{Z} \to 0$$

から導かれる長完全列の一部

$$0 \to \mathbb{Z}/2\mathbb{Z}^G/N_G\mathbb{Z}/2\mathbb{Z} \to H^1(G, \mathbb{Z}/2\mathbb{Z}) \to 0$$

より

$$H^1(G,\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}^G/N_G\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$$

が分かる.

(3) $\mathbb{Z}[G]$-加群としての短完全列

$$0 \to \mathbb{Z}_{\pm} \xrightarrow{2\cdot} \mathbb{Z}_{\pm} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \to 0$$

から導かれる長完全系列は

$$\begin{array}{ccccccc}
0 \to & H^0(G,\mathbb{Z}_{\pm}) & \to & H^0(G,\mathbb{Z}_{\pm}) & \to & H^0(G,\mathbb{Z}/2\mathbb{Z}) \\
 & = 0 & & = 0 & \to & = \mathbb{Z}/2\mathbb{Z} \\
\to & H^1(G,\mathbb{Z}_{\pm}) & \to & H^1(G,\mathbb{Z}_{\pm}) & \to & H^1(G,\mathbb{Z}/2\mathbb{Z}) \\
 & = \mathbb{Z}/2\mathbb{Z} & & = \mathbb{Z}/2\mathbb{Z} & & = \mathbb{Z}/2\mathbb{Z} \\
\to & \cdots & & & &
\end{array}$$

となる (Tate 版の完全列は問題 30).

## 8/28 の復習 $+\alpha$

- 加法群 $M$ が $R$-加群 $\Leftrightarrow R \to \mathrm{End}(M)$ が乗法単位元を保環準同型.
- $A \xrightarrow{f} B \xrightarrow{g} C$ が完全 $\Leftrightarrow f(A) = \ker g$.
- 重要な数学的対称が完全系列で “定義” されている. 例えば「$C$ が位数 $n$ の巡回群 $\Leftrightarrow 0 \to \mathbb{Z} \xrightarrow{n\text{ 倍写像}} \mathbb{Z} \to C \to 0$ が完全」
- $\mathbb{Z}[G]$-加群 $A$ 達への “一斉操作”
  (1) $A \Rightarrow A^G$
  (2) $A \Rightarrow A^G/NA$
  での完全系列のズレが
  (1) $H^n(G, A)$: 群コホモロジー.
  (2) $\hat{H}^n(G, A)$: Tate コホモロジー.
- 群コホモロジーの応用: ヒルベルト 90, クンマー理論.
- 素数次クンマー拡大の分岐理論.

# 5 $q$ 乗剰余の第二補充法則

概略

- 平方剰余記号は “$\mathbb{Q}$ 上の類対論の明示化” であったので, 合同条件で記述できた.
- 平方剰余記号の類似として「$q$ 乗剰余記号」が定義できる.
- $q$ 乗剰余記号はもうちょっと複雑. 共同研究成果を紹介する. (山口大学・平川義之輔氏, 島根大学・山本修司氏, 東京電機大学・関川隆太郎氏, 東京理科大学・加塩, 高田直明氏との共同研究)

## 5.1 # 平方剰余記号と $\mathbb{Q}$ 上の類体論

### 5.1.1 ガロア理論 $(+\alpha)$ から分かること

**定理 5.1.1.** $p$ を素数とし, 円分体 $\mathbb{Q}(\zeta_p)$ $(\zeta_p := e^{\frac{2\pi i}{p}})$ を考える. $d$ を $p-1$ の約数とする.

(1) $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ は $p-1$ 次巡回拡大である:

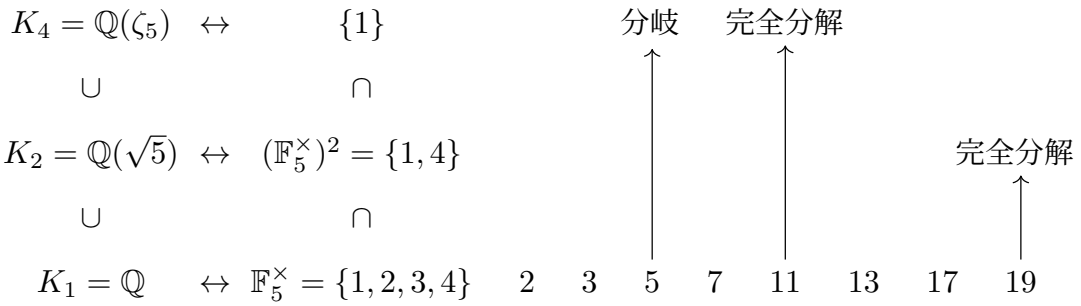
$$\begin{array}{ccccc} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) & \cong & (\mathbb{Z}/p\mathbb{Z})^\times & \cong & \mathbb{Z}/(p-1)\mathbb{Z}, \\ \cup & & \cup & & \\ [\zeta_p \mapsto \zeta_p^a] & \mapsfrom & a \bmod p. & & \end{array}$$

(2) ガロア対応により, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ の中間体 $K_d$ で $[K_d : \mathbb{Q}] = d$ を満たすものがただ一つ定まる:

$$\begin{array}{ccccccc} \mathbb{Q}(\zeta_p) & \leftrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p)) & \cong & \{1\} & \cong & \{0\} \\ \cup & & \cap & & \cap & & \cap \\ K_d & \leftrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_p)/K_d) & \cong & ((\mathbb{Z}/p\mathbb{Z})^\times)^d & \cong & d\mathbb{Z}/(p-1)\mathbb{Z} \\ \cup & & \cap & & \cap & & \cap \\ \mathbb{Q} & \leftrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) & \cong & (\mathbb{Z}/p\mathbb{Z})^\times & \cong & \mathbb{Z}/(p-1)\mathbb{Z} \end{array}$$

(3) $K_2 = \mathbb{Q}(\sqrt{p^*})$, $p^* := (-1)^{\frac{p-1}{2}} p$.

**例 5.1.2.** $p = 5$ のとき, $p - 1 = 4$ の約数は $d = 1, 2, 4$ のみであり, $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ の中間体は 3 つある ($\Rightarrow$ 例 2.3.3, 補足 2.3.4). さらに, それらの体で “完全分解する素数” または “分岐する素数” は




となる. これを定理 3.4.10 を使って確かめてみる:

- $\mathcal{O}_{\mathbb{Q}(\zeta_5)} = \mathbb{Z}[\zeta_5]$, $\zeta_5$ の最小多項式は $x^4 + x^3 + x^2 + x + 1$.
- $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} \supsetneq \mathbb{Z}[\sqrt{5}]$, $[\mathcal{O}_{\mathbb{Q}(\sqrt{5})} : \mathbb{Z}[\sqrt{5}]] = 2$ で, $\sqrt{5}$ の最小多項式は $x^2 - 5$.

であり,

- $x^4 + x^3 + x^2 + x + 1 \equiv (x - 1)^4 \mod 5$ より

  $$5\mathbb{Z}[\zeta_5] = (5, \zeta_5 - 1)^4.$$

  より詳しく

  $$5 = (1 - \zeta_5)(1 - \zeta_5^2)(1 - \zeta_5^3)(1 - \zeta_5^4) = u(1 - \zeta_5)^4,\ u = \zeta_5^3 - \zeta_5 - 1 \in \mathbb{Z}[\zeta_5]^\times$$

  が計算で分かる.
- $x^4 + x^3 + x^2 + x + 1 \equiv (x - 5)(x - 4)(x - 3)(x - 9) \mod 11$ より

  $$11\mathbb{Z}[\zeta_5] = (11, \zeta_5 - 5)(11, \zeta_5 - 4)(11, \zeta_5 - 3)(11, \zeta_5 - 9).$$

  より詳しく

  $$11 = (2\zeta_5 + 1)(2\zeta_5^2 + 1)(2\zeta_5^3 + 1)(2\zeta_5^4 + 1)$$

  が計算で分かる.
- $x^2 - 5 \equiv (x - 10)(x - 9) \mod 19$ より

  $$19\mathbb{Z}[\sqrt{5}] = (19, \sqrt{5} - 10)(19, \sqrt{5} - 9).$$

  より詳しく

  $$19 = (8 + 3\sqrt{5})(8 - 3\sqrt{5})$$

  が計算で分かる.

**問題 34.** 例 5.1.2 の各主張に証明を付けよ.

### 5.1.2 類体論 (アルティンの相互律写像) から分かること

**定理 5.1.3.** $k$ を代数体とし, $L/k$ を有限次アーベル拡大とする.

(1) $k$ の素イデアル $\mathfrak{p}$ が $L/k$ で不分岐であると仮定する.

(a) $\mathfrak{p}$ の上の $L$ の素イデアル $\mathfrak{P}$ に対し

$$\left[\left(\frac{L/k}{\mathfrak{p}}\right) : L \to L\right] \in \mathrm{Gal}(L/k)$$
$$\text{s.t. } \forall \alpha \in \mathcal{O}_L,\ \left(\frac{L/k}{\mathfrak{p}}\right)(\alpha) \equiv \alpha^{N\mathfrak{p}} \mod \mathfrak{P}$$

を満たすものが唯一つ定まり $\mathfrak{p}$ **のフロベニウス元** と呼ばれる. これは $\mathfrak{P}$ の取り方によらない.

(b) $L/k$ の中間体 $K$ に対し

$$\left(\frac{L/k}{\mathfrak{p}}\right)\Big|_K = \left(\frac{K/k}{\mathfrak{p}}\right).$$

(c) $\mathfrak{p}$ が $L/k$ で完全分解する ($\overset{\text{定義}}{\Leftrightarrow}$ 分岐指数も剰余次数も $= 1$) $\Leftrightarrow$ $(\frac{L/k}{\mathfrak{p}}) = \mathrm{id}_L$.

(2) $I_{k,\mathrm{ram}(L/k)}$ を $k$ の分数イデアルで $L/k$ で分岐している素イデアル達と互いに素なもの全体のなす群とする:

$$I_{k,\mathrm{ram}(L/k)} := \left\{ \prod_{i=1}^{t} \mathfrak{p}_i^{n_i} \;\middle|\; \mathfrak{p}_i \text{ は } L/k \text{ で不分岐な } k \text{ の素イデアル},\ n_i \in \mathbb{Z} \right\}.$$

このとき **アルティンの相互律写像**

$$\left(\frac{L/k}{\cdot}\right) : I_{k,\mathrm{ram}(L/k)} \to \mathrm{Gal}(L/k),\ \mathfrak{a} = \prod_{i=1}^{t} \mathfrak{p}_i^{n_i} \mapsto \left(\frac{L/k}{\mathfrak{a}}\right) := \prod_{i=1}^{t} \left(\frac{L/k}{\mathfrak{p}_i}\right)^{n_i}$$

は全射準同型写像で, その核 $H_{L/k} < I_{k,\mathrm{ram}(L/k)}$ を "明示的に書く" ことができる. すなわち, アルティンの相互律写像は, 同型

$$I_{k,\mathrm{ram}(L/k)}/H_{L/k} \cong \mathrm{Gal}(L/k)$$

を誘導する.

(3) $L/k = \mathbb{Q}(\zeta_n)/\mathbb{Q}$ のとき,

$$\begin{array}{ccccc} (\mathbb{Z}/n\mathbb{Z})^\times & \cong & I_{\mathbb{Q},\mathrm{ram}(\mathbb{Q}(\zeta_n)/\mathbb{Q})}/H_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} & \overset{(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{\cdot})}{\cong} & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}), \\ \cup & & \cup & & \cup \\ a \bmod n\ (a \in \mathbb{N}) & \mapsto & \overline{(a)} & \mapsto & [\zeta_n \mapsto \zeta_n^a] \end{array}$$

となる.

### 5.1.3 二次体で素数の分解法則 (定理 3.4.16 の再掲)

$K = \mathbb{Q}(\sqrt{d})$ ($d$ は平方因子を持たない整数) において素数 $p$ は以下の分解法則を満たす. $d_K := \begin{cases} d & (d \equiv 1 \mod 4) \\ 4d & (d \equiv 2, 3 \mod 4) \end{cases}$ とおき, 平方剰余記号を

$$\left(\frac{a}{2}\right) := \begin{cases} 1 & (a \equiv \pm 1 \mod 8) \\ -1 & (a \equiv \pm 3 \mod 8) \\ 0 & (a \equiv 0 \mod 2) \end{cases}$$

で拡張しておく.

(1) $\left(\frac{d_K}{p}\right) = 1$ のとき $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{p}_1, \mathfrak{p}_2$ は相異なる素イデアル.
(2) $\left(\frac{d_K}{p}\right) = -1$ のとき $p\mathcal{O}_K$ は素イデアル.
(3) $\left(\frac{d_K}{p}\right) = 0$ のとき $p\mathcal{O}_K = \mathfrak{p}^2$, $\mathfrak{p}$ は素イデアル.

### 5.1.4 平方剰余の相互法則の証明

**系 5.1.4.** 定理 3.4.16, 定理 5.1.1, 定理 5.1.3 より平方剰余の相互法則が従う.

**証明.** $(\frac{q}{p}) = 1 \overset{\text{定義 } 1.2.1}{\Leftrightarrow} q \bmod p \in (\mathbb{F}_p^\times)^2 \overset{\text{定理 } 5.1.1\text{-}(1),\,(2),\,(3)}{\Leftrightarrow} [\zeta_p \mapsto \zeta_p^q]|_{\mathbb{Q}(\sqrt{p^*})} = \mathrm{id}_{\mathbb{Q}(\sqrt{p^*})} \overset{\text{定理 } 5.1.3-(3),(1)-(b)}{\Leftrightarrow} (\frac{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}}{(q)}) = \mathrm{id}_{\mathbb{Q}(\sqrt{p^*})} \overset{\text{定理 } 5.1.3-(1)-(c)}{\Leftrightarrow} q$ が $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ で完全分解 $\overset{\text{定理 } 3.4.16}{\Leftrightarrow} (\frac{p^*}{q}) = 1.$ □

**補足 5.1.5.** 証明など, 詳細は [小野, §29] などを参照.

## 5.2 数値実験 (PARI/GP)

**定義 5.2.1.** 素数 $p, q$ と $a \in \mathbb{Z}$ に対し, $q$ 乗剰余記号を

$$\left(\frac{a}{p}\right)_q := \begin{cases} 1 & (a \bmod p \in (\mathbb{F}_p^\times)^q) \\ -1 & (a \bmod p \in \mathbb{F}_p^\times - (\mathbb{F}_p^\times)^q) \\ 0 & (a \equiv 0 \mod p) \end{cases}$$

で定める. ただし

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}, \quad \mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}.$$

とくに $p \equiv 1 \mod q$ で無ければ $\mathbb{F}_p^\times = (\mathbb{F}_p^\times)^q$ であり, $(\frac{a}{p})_q$ は常に 1 (か 0) となる.

**補足 5.2.2.** $\mathbb{Z}[\zeta_q]$ の元 $\alpha$ と素イデアル $\mathfrak{p}$ に対し

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_q \in \{0\} \cup \langle \zeta_q \rangle, \quad \left(\frac{\alpha}{\mathfrak{p}}\right)_q \equiv \alpha^{\frac{N(\mathfrak{p})-1}{q}} \mod \mathfrak{p}.$$

で定める方が一般的. $p \equiv 1 \mod q$ の場合, $N(\mathfrak{p}) = p$ となる素イデアル $\mathfrak{p}$ と, $\alpha \bmod \mathfrak{p} = a \bmod p$ となる $a \in \mathbb{Z}$ に対して

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_q = 1 \Leftrightarrow \left(\frac{a}{p}\right)_q = 1$$

が成立する.

以下, PARI/GP で実験してみる. PARI/GP はブラウザでも動かせる (以下の URL).
`https://pari.math.u-bordeaux.fr/gpwasm.html`

$(\frac{a}{p})_q$ の表を出すプログラム

```
q=3
A=10
P=10

isqpr(a,p)={
if(a%p==0,return(0));
for(b=1,p-1,if((a-b^q)%p==0,return(1)));
return(-1)};

M=matrix(A+3,P+1);M[1,1]="";for(i=2,A+3,M[i,1]=i-3);
{p=0;for(j=2,P+1,p=nextprime(p+1);while(p%q<>1,p=nextprime(p+1));
M[1,j]=p;for(i=2,A+3,M[i,j]=isqpr(i-3,p));
)};

printp(M)
```

出力

```
[""  7 13 19 31 37 43 61 67 73 79]

[-1  1  1  1  1  1  1  1  1  1  1]

[ 0  0  0  0  0  0  0  0  0  0  0]

[ 1  1  1  1  1  1  1  1  1  1  1]

[ 2 -1 -1 -1  1 -1  1 -1 -1 -1 -1]

[ 3 -1 -1 -1 -1 -1 -1  1  1  1 -1]

[ 4 -1 -1 -1  1 -1  1 -1 -1 -1 -1]

[ 5 -1  1 -1 -1 -1 -1 -1  1 -1 -1]

[ 6  1 -1 -1 -1  1 -1 -1 -1 -1 -1]

[ 7  0 -1  1 -1 -1 -1 -1 -1  1 -1]

[ 8  1  1  1  1  1  1  1  1  1  1]

[ 9 -1 -1 -1 -1 -1 -1  1  1  1 -1]
```

以下は $a = -1 \sim 10$, $p \equiv 1 \mod q$ を満たす素数 10 個に対する $(\frac{a}{p})_q$ の表.

**例 5.2.3** $(q = 2)$**.**

| $a \diagdown p$ | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|
| $-1$ | $-1$ | 1 | $-1$ | $-1$ | 1 | 1 | $-1$ | $-1$ | 1 | $-1$ |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | $-1$ | $-1$ | 1 | $-1$ | $-1$ | 1 | $-1$ | 1 | $-1$ | 1 |
| 3 | 0 | $-1$ | $-1$ | 1 | 1 | $-1$ | $-1$ | 1 | $-1$ | $-1$ |
| 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 5 | $-1$ | 0 | $-1$ | 1 | $-1$ | $-1$ | 1 | $-1$ | 1 | 1 |
| 6 | 0 | 1 | $-1$ | $-1$ | $-1$ | $-1$ | 1 | 1 | 1 | $-1$ |
| 7 | 1 | $-1$ | 0 | $-1$ | $-1$ | $-1$ | 1 | $-1$ | 1 | 1 |
| 8 | $-1$ | $-1$ | 1 | $-1$ | $-1$ | 1 | $-1$ | 1 | $-1$ | 1 |
| 9 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 10 | 1 | 0 | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ | 1 |

**例 5.2.4** $(q = 3)$**.**

| $a \diagdown p$ | 7 | 13 | 19 | 31 | 37 | 43 | 61 | 67 | 73 | 79 |
|---|---|---|---|---|---|---|---|---|---|---|
| $-1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | $-1$ | $-1$ | $-1$ | 1 | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ |
| 3 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | 1 | 1 | $-1$ |
| 4 | $-1$ | $-1$ | $-1$ | 1 | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ |
| 5 | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ |
| 6 | 1 | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 7 | 0 | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ |
| 8 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 9 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | 1 | 1 | $-1$ |
| 10 | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | 1 | 1 |

**例 5.2.5** ($q = 5$)**.**

| $a \backslash p$ | 11 | 31 | 41 | 61 | 71 | 101 | 131 | 151 | 181 | 191 |
|---|---|---|---|---|---|---|---|---|---|---|
| $-1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ |
| 3 | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 4 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ |
| 5 | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 |
| 6 | $-1$ | 1 | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | 1 |
| 7 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ |
| 8 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ |
| 9 | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 10 | 1 | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ |

**例 5.2.6** ($q = 7$)**.**

| $a \backslash p$ | 29 | 43 | 71 | 113 | 127 | 197 | 211 | 239 | 281 | 337 |
|---|---|---|---|---|---|---|---|---|---|---|
| $-1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 3 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 4 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 5 | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 6 | $-1$ | 1 | $-1$ | $-1$ | $-1$ | 1 | $-1$ | 1 | $-1$ | $-1$ |
| 7 | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ |
| 8 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 9 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 10 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ |

**例 5.2.7** ($q = 11$)**.**

| $a \backslash p$ | 23 | 67 | 89 | 199 | 331 | 353 | 397 | 419 | 463 | 617 |
|---|---|---|---|---|---|---|---|---|---|---|
| $-1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 3 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 4 | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 5 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 6 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | 1 |
| 7 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | 1 | $-1$ | $-1$ |
| 8 | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 9 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |
| 10 | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ | $-1$ | $-1$ |

次に $q, a$ を固定して, 素数 $p \equiv 1 \mod q$ を動かし, $(\frac{a}{p})_q = 1$ となるもののリスト (= PR) と $(\frac{a}{p})_q = -1$ となるもののリスト (= NPR) を表示する.

$(\frac{a}{p})_q = \pm 1$ のリストを出すプログラム

```
q=2
A=-1
P=100

isqpr(a,p)={
if(a%p==0,return(0));
for(b=1,p-1,if((a-b^q)%p==0,return(1)));
return(-1)
};

PR=Set([]);NPR=Set([]);
{p=0;for(j=2,P+1,p=nextprime(p+1);while(p%q<>1,p=nextprime(p+1));
if(isqpr(A,p)==1,PR=setunion(PR,[p]),
if(A%p<>0,NPR=setunion(NPR,[p])));
)};

print(PR)
print(NPR)
```

出力

```
[5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149,
157, 173, 181, 193, 197, 229, 233, 241, 257, 269, 277, 281, 293, 313,
317, 337, 349, 353, 373, 389, 397, 401, 409, 421, 433, 449, 457, 461,
509, 521, 541]

[3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131,
139, 151, 163, 167, 179, 191, 199, 211, 223, 227, 239, 251, 263, 271,
283, 307, 311, 331, 347, 359, 367, 379, 383, 419, 431, 439, 443, 463,
467, 479, 487, 491, 499, 503, 523, 547]
```

以下, 各 $q, a$ に対して, $p \equiv 1 \mod q$ となる素数 $p$ を

- $(\frac{a}{p})_q = 1$ となるもののリスト (= PR)
- と $(\frac{a}{p})_q = -1$ となるもののリスト (= NPR)

を並べる. さらにそれらを mod$n$ したときに差があるか (すなわち $p \bmod n$ で $q$ 乗剰余が判定できるか) を見ていく.

**例 5.2.8** ($q = 2$)**.** (1) $a = -1$:

$$\begin{aligned}\mathrm{PR} &= \{5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, \dots\},\\ \mathrm{NPR} &= \{3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131, 139, \dots\}.\end{aligned}$$

$$\begin{aligned}\mathrm{PR} \bmod 2 &= \{1\}, & \mathrm{PR} \bmod 4 &= \{1\}, & \mathrm{PR} \bmod 8 &= \{1, 8\},\\ \mathrm{NPR} \bmod 2 &= \{1\}, & \mathrm{NPR} \bmod 4 &= \{3\}, & \mathrm{NPR} \bmod 8 &= \{3, 7\}.\end{aligned}$$

(2) $a = 2$:

$$\begin{aligned}\mathrm{PR} &= \{7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, 103, 113, 127, 137, 151, 167, \dots\},\\ \mathrm{NPR} &= \{3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83, 101, 107, 109, 131, 139, \dots\}.\end{aligned}$$

$$\begin{aligned}\mathrm{PR} \bmod 2 &= \{1\}, & \mathrm{PR} \bmod 4 &= \{1, 3\}, & \mathrm{PR} \bmod 8 &= \{1, 7\},\\ \mathrm{NPR} \bmod 2 &= \{1\}, & \mathrm{NPR} \bmod 4 &= \{1, 3\}, & \mathrm{NPR} \bmod 8 &= \{3, 5\}.\end{aligned}$$

(3) $a = 3$:

$$\begin{aligned}\mathrm{PR} &= \{11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, 107, 109, 131, 157, 167, 179, \dots\},\\ \mathrm{NPR} &= \{5, 7, 17, 19, 29, 31, 41, 43, 53, 67, 79, 89, 101, 103, 113, 127, 137, 139, \dots\}.\end{aligned}$$

$$\begin{aligned}\mathrm{PR} \bmod 3 &= \{1.2\}, \quad \mathrm{PR} \bmod 6 = \{1, 5\}, \quad \mathrm{PR} \bmod 12 = \{1, 11\},\\ \mathrm{NPR} \bmod 3 &= \{1, 2\}, \quad \mathrm{NPR} \bmod 6 = \{1, 5\}, \quad \mathrm{NPR} \bmod 12 = \{5, 7\}.\end{aligned}$$

(4) $a = 5$:

$$\begin{aligned}\mathrm{PR} &= \{11, 19, 29, 31, 41, 59, 61, 71, 79, 89, 101, 109, 131, 139, 149, 151, 179, \dots\},\\ \mathrm{NPR} &= \{3, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97, 103, 107, 113, 127, 137, \dots\}.\end{aligned}$$

$$\begin{aligned}\mathrm{PR} \bmod 3 &= \{1, 2\}, \quad \mathrm{PR} \bmod 4 = \{1, 3\}, \quad \mathrm{PR} \bmod 5 = \{1, 4\},\\ \mathrm{NPR} \bmod 3 &= \{0, 1, 2\}, \quad \mathrm{NPR} \bmod 4 = \{1, 3\}, \quad \mathrm{NPR} \bmod 5 = \{2, 3\}.\end{aligned}$$

**例 5.2.9** ($q = 3$)**.** (1) $a = -1$:

$$\begin{aligned}\mathrm{PR} &= \{7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, 103, 109, 127, 139, 151, 157, \dots\},\\ \mathrm{NPR} &= \{\}.\end{aligned}$$

(2) $a = 2$:

$$\begin{aligned}\mathrm{PR} &= \{31, 43, 109, 127, 157, 223, 229, 277, 283, 307, 397, 433, 439, 457, \dots\},\\ \mathrm{NPR} &= \{7, 13, 19, 37, 61, 67, 73, 79, 97, 103, 139, 151, 163, 181, 193, 199, 211, \dots\}.\end{aligned}$$

$$\begin{aligned}\mathrm{PR} \bmod 5 &= \{1, 2, 3, 4\}, \quad \mathrm{PR} \bmod 8 = \{1, 3, 5, 7\}, \quad \mathrm{PR} \bmod 12 = \{1, 7\},\\ \mathrm{NPR} \bmod 5 &= \{1, 2, 3, 4\}, \quad \mathrm{NPR} \bmod 8 = \{1, 3, 5, 7\}, \quad \mathrm{NPR} \bmod 12 = \{1, 7\}.\end{aligned}$$

(3) $a = 3$:

$$\begin{aligned}\mathrm{PR} &= \{61, 67, 73, 103, 151, 193, 271, 307, 367, 439, 499, 523, 547, 577, 613, \dots\},\\ \mathrm{NPR} &= \{7, 13, 19, 31, 37, 43, 79, 97, 109, 127, 139, 157, 163, 181, 199, 211, \dots\}.\end{aligned}$$

$$\begin{aligned}\mathrm{PR} \bmod 5 &= \{1, 2, 3, 4\}, \quad \mathrm{PR} \bmod 8 = \{1, 3, 5, 7\}, \quad \mathrm{PR} \bmod 12 = \{1, 7\},\\ \mathrm{NPR} \bmod 5 &= \{1, 2, 3, 4\}, \quad \mathrm{NPR} \bmod 8 = \{1, 3, 5, 7\}, \quad \mathrm{NPR} \bmod 12 = \{1, 7\}.\end{aligned}$$

(4) $a = 5$:

$$\begin{aligned}\mathrm{PR} &= \{13, 67, 127, 163, 181, 199, 211, 241, 313, 337, 367, 379, 409, 457, \dots\},\\ \mathrm{NPR} &= \{7, 19, 31, 37, 43, 61, 73, 79, 97, 103, 109, 139, 151, 157, 193, 223, 229, \dots\}.\end{aligned}$$

$$\begin{aligned}\mathrm{PR} \bmod 8 &= \{1, 3, 5, 7\}, & \mathrm{PR} \bmod 20 &= \{1, 3, 7, 9, 11, 13, 17, 19\},\\ \mathrm{NPR} \bmod 8 &= \{1, 3, 5, 7\}, & \mathrm{NPR} \bmod 20 &= \{1, 3, 7, 9, 11, 13, 17, 19\}.\end{aligned}$$

## 5.3 オイラー予想 (3 乗剰余)

**注意 5.3.1.** (お気持ち) $a \in \mathbb{Z}$ を固定したとき, $q = 2$ の場合, $\left(\frac{a}{p}\right)_2$ の値は $p$ に関する合同条件で表せる:

$$\begin{aligned}\left(\frac{-1}{p}\right)_2 &= 1 \Leftrightarrow p \equiv 1 \mod 4,\\ \left(\frac{2}{p}\right)_2 &= 1 \Leftrightarrow p \equiv 1, 7 \mod 8,\\ \left(\frac{3}{p}\right)_2 &= 1 \Leftrightarrow p \equiv 1, 11 \mod 12,\\ \left(\frac{5}{p}\right)_2 &= 1 \Leftrightarrow p \equiv 1, 4 \mod 5.\end{aligned}$$

一方で $q \geq 3$ の場合はそう単純ではない

**問題 35.** 注意 5.3.1-(1) の各同値を証明せよ.
※ 平方剰余の相互法則とその補充法則を使ってよい.

**定理 5.3.2** (オイラー・ヤコビ・レーマー)**.** $p \equiv 1 \mod 3$ のとき $4p = L^2 + 27M^2$ $(L, M \in \mathbb{Z})$ と表せて, 以下の各同値が成り立つ.

(1) $(\frac{2}{p})_3 = 1 \Leftrightarrow LM \equiv 0 \mod 4$ $(\Leftrightarrow M \equiv 0 \mod 2)$.
(2) $(\frac{3}{p})_3 = 1 \Leftrightarrow LM \equiv 0 \mod 3$ $(\Leftrightarrow M \equiv 0 \mod 3)$.
(3) $(\frac{5}{p})_3 = 1 \Leftrightarrow LM \equiv 0 \mod 5$.
(4) $(\frac{6}{p})_3 = 1 \Leftrightarrow LM \equiv 0, \pm 1 \mod 12$.
(5) $(\frac{7}{p})_3 = 1 \Leftrightarrow LM \equiv 0 \mod 7$.

## 5.4 主結果 ($q$ 乗剰余の第二補充法則)

**定義 5.4.1.** (負 index の) ポリログ関数を以下で定義する:

$$\mathrm{Li}_{-n}(x) := \left(x\frac{d}{dx}\right)^n \frac{x}{1-x} \in \mathbb{Q}(x)\ (n \in \mathbb{N}).$$

**定理 5.4.2.** 以下を仮定する:

- $q$ は奇素数.
- $p$ は $p = \sum_{i=0}^{q-1} m^i n^{q-1-i}$ $(m, n \in \mathbb{Z})$ の形に表せる $q$ 以外の素数.

このとき以下は同値.

(1) $\left(\frac{q}{p}\right)_q = 1$.
(2) $\mathrm{Li}_{1-q}(\frac{n}{m}) \equiv 0 \mod q^2$.

ただし, 有理数 $\frac{a}{b}$ $(a, b \in \mathbb{Z},\ b \neq 0,\ \gcd(a, b) = 1)$ に対し, $\frac{a}{b} \equiv 0 \mod q^2 \Leftrightarrow a \equiv 0 \mod q^2$ と定める.

**例 5.4.3.** $q = 3, 5, 7$ に対し

- $\mathrm{Li}_{1-q}(x)$
- $T_q := \{\frac{n}{m} \bmod q^2 \mid \mathrm{Li}_{1-q}(\frac{n}{m}) \equiv 0 \mod q^2\}$, ただし $\frac{n}{m} \bmod q^2 = \infty$ は $\frac{m}{n} \equiv 0 \mod q^2$ を意味する
- 素数 $p = \Phi_q(n/m)m^{q-1}$ で $(\frac{q}{p})_q = 1$ を満たすもの (の一部)

を計算してみる.

(1) $q = 3$.
  - $\mathrm{Li}_{1-3}(x) = x(x+1)/(1-x)^3$
  - $T_3 = \{0, 8, \infty\}$
  - $p = 61, 67, 73, 103, 151, 193, 271, 307, 367, 439, 499, 523, 547, 577, 613, \ldots$

(2) $q = 5$.
  - $\mathrm{Li}_{1-5}(x) = x(x+1)(x^2+10x+1)/(1-x)^5$
  - $T_5 = \{0, 2, 13, 24, \infty\}$
  - $p = 31, 19141, 30941, 48871, 114641, 125591, 141961, 170101, 225241, \ldots$

(3) $q = 7$.

- $\mathrm{Li}_{1-7}(x) = x(x+1)(x^4 + 56x^3 + 246x^2 + 56x + 1)/(1-x)^7$
- $T_7 = \{0, 9, 11, 24, 47, 48, \infty\}$
- $p = 43, 10501, 3692053, 109894303, 115928821, 138520537, 141903217, \ldots$

**問題 36.** $(\frac{3}{61})_3 = 1$, $(\frac{5}{31})_5 = 1$, $(\frac{7}{43})_7 = 1$ が正しいことを (定理 5.4.2 を使わずに) チェックしてみよ.

**問題 37.** $p \equiv 1 \mod 11$, $(\frac{11}{p})_{11} = 1$ となる素数 $p$ を見つけてみよ. 定理 5.4.2 を使ってもよいし, 手計算でもよいし, 計算機を使ってもよい.

## 5.5 証明の概略

■Step0. Lemmermeyer **の手法**. 素数 $p, q$ が $p \equiv 1 \mod q$ を満たすとする. このとき, 定理 5.1.1-(3) より

$$(\tfrac{q}{p})_q = 1 \Leftrightarrow q \text{ が } K_q/\mathbb{Q} \text{ で完全分解}$$

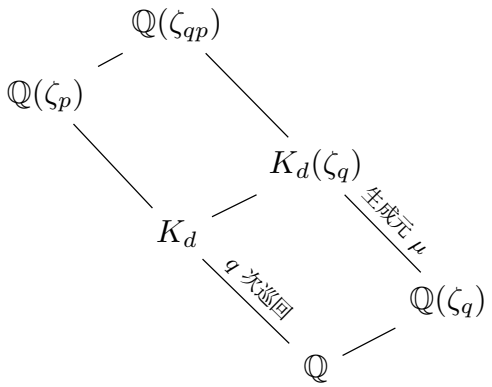
が成り立つ. さらに “分岐指数や剰余次数の基本的な性質” により

$$\Leftrightarrow (1-\zeta_q) \text{ が } K_q(\zeta_q)/\mathbb{Q}(\zeta_q) \text{ で完全分解}$$

と言い換えられる. よって定理 4.5.2-(2)-(b) より

$$\Leftrightarrow \exists \xi \in \mathbb{Z}[\zeta_q] \text{ s.t. } \mu \equiv \xi^q \mod (1-\zeta_q)^{q+1} - (\star)$$

と言い換えられる.



■Step1. **クンマー理論による生成元の決定**. $K_q(\zeta_q)/\mathbb{Q}(\zeta_q)$ が $q$ の外不分岐であることと, $K_q(\zeta_q)/\mathbb{Q}$ がアーベル拡大であることから, $K_q(\zeta_q)$ の生成元 (すなわち $K_q(\zeta_q) = \mathbb{Q}(\zeta_q)(\sqrt[q]{\mu})$ を満たす $\mu$) が

$$\mu := \zeta_q^{-n(m-n)^*} \prod_{j=1}^{q-1} (m - n\zeta_q^j)^{j^*} \in \mathbb{Z}[\zeta_q] \text{ – } (\star\star)$$

と具体的に書ける. ただし $a^*$ は $aa^* \equiv 1 \mod q$, $1 \leq a \leq q-1$ を満たす整数.

■Step2. **合同条件**. $(\star\star)$ の $\mu$ は

$$\mu \equiv \left(\frac{m-n}{q}\right)_2 = \pm 1 \mod (1-\zeta_q)^2$$

を満たしてることが計算で分かる. これが効いて, $(\star)$ の条件から更に

$$\Leftrightarrow \log_q \mu \equiv 0 \mod (1-\zeta_q)^{q+1} \text{ – } (\star\star\star)$$

と言い換えられる. ただし

$$\begin{aligned} \log_q \colon & \pm 1 + (1-\zeta_q)\mathbb{Z}[\zeta_q] \to \mathbb{Z}[\zeta_q]/(1-\zeta_q)^{q+1}\mathbb{Z}[\zeta_q], \\ & \pm(1+x) \mapsto \sum_{t=1}^{q} \frac{-(-x)^t}{t} \mod (1-\zeta_q)^{q+1} \quad (x \in (1-\zeta_q)\mathbb{Z}[\zeta_q]) \end{aligned}$$

と定める.

■Step3. $q$ **進計算**. $\log_q$ の性質も使って計算を頑張ると

$$\begin{aligned} \log_q \mu &= \log_q \left( \zeta_q^{-n(m-n)^*} \cdot \left(\frac{-n}{m-n}\right)^{\frac{(q-1)q}{2}} \cdot \prod_{j=1}^{q-1} \left(1 + \frac{n}{m-n}(1-\zeta_q^j)\right)^{j^*} \right) \\ &\equiv \sum_{1 \leq j \leq q-1} \sum_{1 \leq t \leq q} \frac{-j^*(\frac{-n}{m-n}(1-\zeta_q^j))^t}{t} \mod (1-\zeta_q)^{q+1} \\ &\equiv \sum_{1 \leq t \leq q,\ 1 \leq j \leq q-1,\ 0 \leq k \leq t} \frac{-(-1)^k j^* \binom{t}{k} (\frac{-n}{m-n})^t \zeta_q^{jk}}{t} \\ &\equiv \cdots \\ &\equiv (1-\zeta_q) \left( \sum_{j=1}^{q-1} jj^* \right) \mathrm{Li}_{1-q}(\tfrac{n}{m}) \mod (1-\zeta_q)^{q+1}. \end{aligned}$$

が分かる. すなわち $(\star\star\star)$ は

$$\mathrm{Li}_{1-q}(\tfrac{n}{m}) \mod (1-\zeta_q)^{q+1} \equiv 0 \mod q^2$$

と同値になり, 定理 5.4.2 の主張を得る.

**注意 5.5.1.** 例えば $\log_3(2)$ の “厳密な値” を知りたければ,

$$\log_3(-(1-3)) = \sum_{k=1}^{\infty} \frac{-3^k}{k}$$

の値に “意味” を持たせればよい. より一般に, 素数 $p$ に対して

$$\mathbb{Z}_p := \left\{ (a_n)_n \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \;\middle|\; \forall n,\ a_n \bmod p^{n-1} = a_{n-1} \right\}$$

に, 直積環 $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ の部分環としての環構造と, 直積位相の相対位相をいれたものを $p$ **進整数環** と呼ぶ. これは “$p$ 進無限級数全体のなす集合” と同一視できる:

$$\begin{array}{ccc} \left\{ \sum_{k=0}^{\infty} a_k p^k \;\middle|\; a_k \in \{0,1,\dots,p-1\} \right\} & = & \mathbb{Z}_p \\ \sum_{n=k}^{\infty} a_k p^k \mapsto & \leftrightarrow & \left( \sum_{k=0}^{n-1} a_k p^k \bmod p^n \right)_n . \end{array}$$

$\mathbb{Z}_p$ は整域で, その商体は

$$\mathbb{Q}_p = \mathbb{Z}[1/p]$$

で与えられる. 例えば $\log_3(2)$ の値は

$$\begin{aligned} &\log_3(-(1-3)) \\ &= \left( \sum_{k=1}^{n-1} \frac{-3^k}{k} \bmod p^n \right)_n \\ &= \left( 0 \bmod 3, -3 \bmod 3^2, \frac{-15}{2} \bmod 3^3, \frac{-33}{2} \bmod 3^4, \frac{-147}{4} \bmod 3^5, \dots \right) \\ &= \left(0 \bmod 3, 6 \bmod 3^2, 6 \bmod 3^3, 24 \bmod 3^4, 24 \bmod 3^5, \dots\right) \in \mathbb{Z}_3 \subset \prod_{n\in\mathbb{N}} \mathbb{Z}/3^n\mathbb{Z} \\ &= 0\cdot 3^0 + 2\cdot 3^1 + 2\cdot 3^2 + 0\cdot 3^3 + 0\cdot 3^4 + \cdots \end{aligned}$$

で well-defined になる. 一般に, $\mathbb{Q}_p$ の代数閉包の完備化を $\mathbb{C}_p$ とおいたとき, $p$ 進対数関数は, 連続写像かつ群準同型写像

$$\log_p \colon \mathbb{C}_p^{\times} \to \mathbb{C}_p$$

となる.

# 参考文献


[Gr] G. Gras, Class field theory: From theory to practice, Springer Monogr. Math. (2003).

[Le] F. Lemmermeyer, Reciprocity Laws: From Euler to Eisenstein, Springer Monogr. Math. (2000).

[足立] 足立 恒雄, 類体論へ至る道 改訂新版: 初等数論からの代数入門, 日本評論社 (2010).

[足-三] 足立 恒雄, 三宅 克哉, 類体論講義, 日本評論社 (1998).

[木田] 木田 雅成, 連分数, 大学数学スポットライト・シリーズ 第 9 巻 (2022).

[小野] 小野 孝, 数論序説, 裳華房 (2001).