代数的整数論 類体論入門

alg-d

2021-03-20

代数的整数論 類体論入門

- alg-d　twitter: https://twitter.com/alg_d
  Youtube: https://www.youtube.com/alg-dx
  WEB サイト: http://alg-d.com/
- 代表作 (?)
  選択公理と同値な命題集 http://alg-d.com/math/ac/
  常識的な圏論の PDF http://alg-d.com/math/kan_extension/
- 選択公理が専門ではない
- 圏論が専門でもない
- 専門はなんと代数的整数論
- 今日は，代数的整数論における類体論がどういう主張なのか，どういう応用があるのかを説明して，皆さんに類体論に入門してもらうのが目的です．

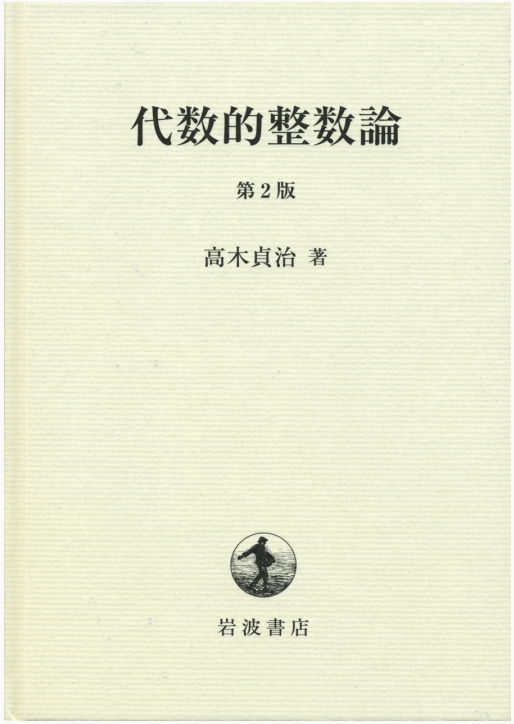
参考文献

石田 信, 代数的整数論

代数的整数論の入門書．薄めでギャップもそんなにないのでサッと読める．類体論については書いてない．

参考文献

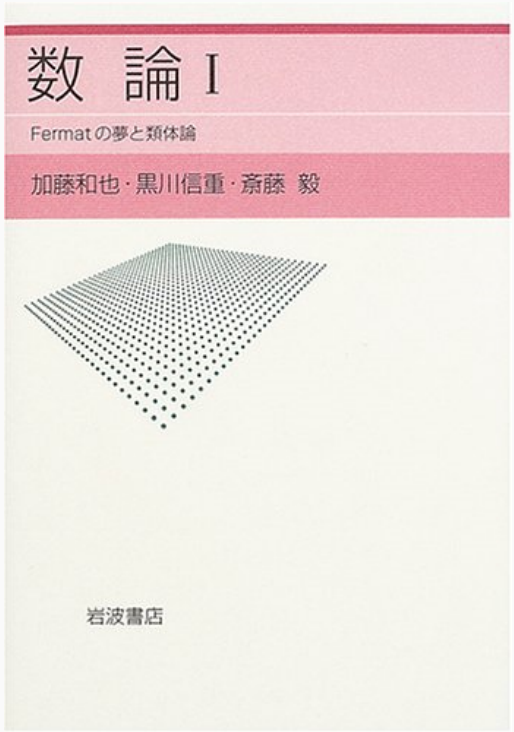
高木 貞二, 代数的整数論



類体論の教科書 1．大好き

参考文献

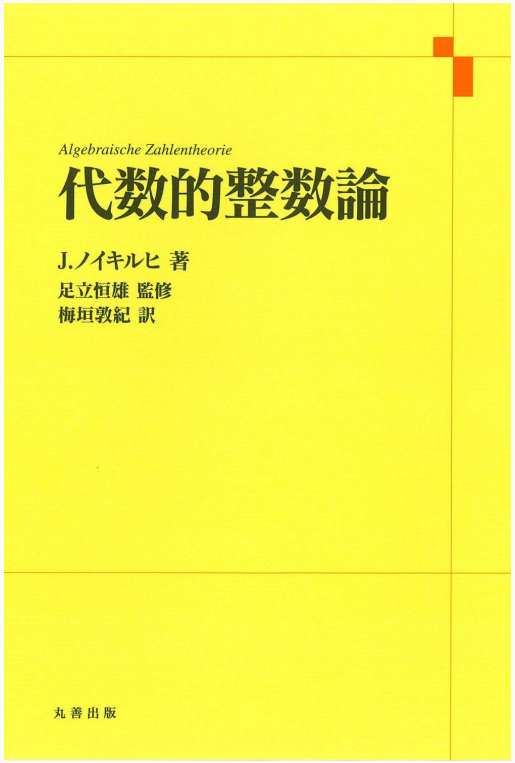
加藤 和也, 黒川 信重, 斎藤 毅, 数論 I　　Fermat の夢と類体論



類体論の教科書 2．今読むなら普通はこれなのかな?

参考文献

J. ノイキルヒ, 代数的整数論



類体論の教科書 3

代数的整数論とは

代数的整数論とは

【命題】 (Fermat の二平方和定理)

素数 $p \neq 2$ に対して

$$\text{ある } a, b \in \mathbb{Z} \text{ が存在して } p = a^2 + b^2 \Longleftrightarrow p \equiv 1 \pmod 4$$

証明.

$(\Longrightarrow)$ $p = a^2 + b^2$ と書けたとする．p は奇数だから，a を偶数 b を奇数としてよい．そこで $a = 2a'$，$b = 2b' + 1$ と書けば

$$\begin{aligned} p &= a^2 + b^2 \\ &= (2a')^2 + (2b' + 1)^2 \\ &= 4a'^2 + 4b'^2 + 4b' + 1 \\ &\equiv 1 \pmod 4. \end{aligned}$$

($\Longleftarrow$) $p \equiv 1 \pmod 4$ とする．$t^2 \equiv -1 \pmod p$ となる $t \in \mathbb{Z}$ が存在する．

> ˙.˙) Wilson の定理により $(p-1)! \equiv -1 \pmod p$ である．よって $p = 4k+1$ と書けば $\bmod p$ で
>
> $$\begin{aligned} -1 &\equiv (p-1)! \\ &= \big(1 \cdot 2 \cdots (2k)\big)\big((2k+1)(2k+2)\cdots(p-2)(p-1)\big) \\ &= \big(1 \cdot 2 \cdots (2k)\big)\big((p-2k)(p-(2k-1))\cdots(p-2)(p-1)\big) \\ &\equiv (2k)!(-1)^{2k}(2k)! = ((2k)!)^2 \end{aligned}$$

正整数 e を $(e-1)^2 < p < e^2$ となるように取る．

代数的整数論とは

$A := \{0, 1, \cdots, e-1\}$ として写像

$$A^2 \ni \langle a, b \rangle \longmapsto (a - bt \bmod p) \in \mathbb{Z}/p\mathbb{Z}$$

を考えると $|A^2| = e^2 > p$ だからこの写像は単射ではない．故に異なる二元 $\langle a, b \rangle, \langle c, d \rangle \in A^2$ が存在して $a - bt \equiv c - dt \pmod{p}$ となる．このとき

$$\begin{aligned}(a-c)^2 + (b-d)^2 &\equiv \big((a-c) - (b-d)t\big)\big((a-c) + (b-d)t\big) \\ &\equiv 0 \pmod{p}\end{aligned}$$

である．即ち $(a-c)^2 + (b-d)^2 > 0$ は p の倍数であるが，一方 $0 \leq a, b, c, d \leq e-1$ より $(a-c)^2, (b-d)^2 \leq (e-1)^2$ となる．従って $(a-c)^2 + (b-d)^2 \leq 2(e-1)^2 < 2p$ が分かるので $p = (a-c)^2 + (b-d)^2$ でなければならない． $\square$

代数的整数論とは

Fermat の二平方和定理はこのように初等的に証明できるが，少し難しい．

実はこの定理は環 $\mathbb{Z}$ で考えるのではなく，Gauss 整数環

$$\mathbb{Z}[\sqrt{-1}] := \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$$

で考えればより自然に証明できる．何故かというと $\mathbb{Z}[\sqrt{-1}]$ では $a^2 + b^2 = (a + b\sqrt{-1})(a - b\sqrt{-1})$ と書けるので，この定理は

素数 p は環 $\mathbb{Z}[\sqrt{-1}]$ でいつ"分解"するか?

という問題になるからである．(後でもう少し詳しくやります)

代数的整数論とは

$\mathbb{Z}$ における"分解"については「素因数分解の一意性」が知られている.

【定理】

任意の正整数 n は

$$n = p_1^{e_1} \cdots p_g^{e_g} \ (p_i \text{ は相異なる素数}, e_i > 0)$$

と (順番を除いて) 一意に書ける.

これを $\mathbb{Z}$ の言葉で書き直すと次のようになる.

代数的整数論とは

【定理】

任意の整数 $n \neq 0$ は

$$n = w p_1^{e_1} \cdots p_g^{e_g} \quad (w = \pm 1,\ p_i \text{ は相異なる素数},\ e_i > 0)$$

と (順番を除いて) 一意に書ける.

※ 環論の言葉で言えば「$\mathbb{Z}$ は UFD(一意分解整域) である」.

これは $\mathbb{Z}[\sqrt{-1}]$ の場合どうなるか?

代数的整数論とは

【定義】

$P \in \mathbb{Z}[\sqrt{-1}]$ が G-素数とは以下を満たすこととする．(これはここだけの用語)

(1) $P \neq 0$

(2) P は単数でない

(3) $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$ に対して「$P = \alpha\beta \Longrightarrow \alpha$ または β が単数」

(4) $\mathrm{Re}\, P > 0$

(5) $\mathrm{Im}\, P \geq 0$

※ $\alpha \in \mathbb{Z}[\sqrt{-1}]$ が単数 $\Longleftrightarrow \alpha^{-1} \in \mathbb{Z}[\sqrt{-1}]$
(つまりこの場合 $\alpha = \pm 1, \pm\sqrt{-1}$)

代数的整数論とは

【定理】

任意の $\alpha\ (\neq 0) \in \mathbb{Z}[\sqrt{-1}]$ は

$$\alpha = wP_1^{e_1} \cdots P_g^{e_g}\ (w \text{ は単数，} P_i \text{ は相異なる G-素数，} e_i > 0)$$

と (順番を除いて) 一意に書ける．

つまり $\mathbb{Z}[\sqrt{-1}]$ は UFD である．

代数的整数論とは

$\alpha \in \mathbb{Z}[\sqrt{-1}]$ に対して $N(\alpha) := \alpha\rho(\alpha)$ とする．(ρ: 複素共役)
$\alpha = a + b\sqrt{-1}$ $(a, b \in \mathbb{Z})$ と書けば

$$N(\alpha) = (a + b\sqrt{-1})(a - b\sqrt{-1}) = a^2 + b^2 \in \mathbb{Z}$$

であり

$$N(\alpha) = 1 \Longleftrightarrow a^2 + b^2 = 1 \Longleftrightarrow \alpha = \pm 1, \pm\sqrt{-1}$$

となる．$\pm 1,\ \pm\sqrt{-1}$ は G-素数でないから

$$P \text{ が G-素数} \Longrightarrow N(P) \text{ は } 2 \text{ 以上の整数}$$

が分かる．また定義から明らかに $N(\alpha\beta) = N(\alpha)N(\beta)$ である．
これらを踏まえて

代数的整数論とは

素数 p の $\mathbb{Z}[\sqrt{-1}]$ での分解が $p = wP_1^{e_1} \cdots P_g^{e_g}$ であるとすると

$$p^2 = N(p) = N(wP_1^{e_1} \cdots P_g^{e_g}) = N(w)N(P_1)^{e_1} \cdots N(P_g)^{e_g}$$

$w = \pm 1, \pm\sqrt{-1}$ だから $N(w) = 1$ である．

P_i は G-素数だから $N(P_i) > 1$ となり，$\mathbb{Z}$ での素因数分解の一意性より $N(P_i) = p^{f_i},\ f_i > 0$ と書ける．

すると $p^2 = p^{e_1 f_1 + \cdots + e_g f_g}$ となるから $2 = e_1 f_1 + \cdots + e_g f_g$ が分かる．故に

$$\begin{cases} g = 1,\ e_1 = 1,\ f_1 = 2 \\ g = 1,\ e_1 = 2,\ f_1 = 1 \\ g = 2,\ e_1 = e_2 = f_1 = f_2 = 1 \end{cases}$$

のうちのどちらかである．

代数的整数論とは

即ち，素数 p の $\mathbb{Z}[\sqrt{-1}]$ における素因数分解の仕方は次の 3 通りしかない．

(1) $p = wP_1$，$N(P_1) = p^2$ (つまりこの場合 p 自体が G-素数)

(2) $p = wP_1^2$

(3) $p = wP_1P_2$，$P_1 \neq P_2$，$N(P_1) = N(P_2) = p$

これを踏まえて Fermat の二平方和定理を証明する．

【命題】 (Fermat の二平方和定理)

素数 $p \neq 2$ に対して

$$\text{ある } a, b \in \mathbb{Z} \text{ が存在して } p = a^2 + b^2 \Longleftrightarrow p \equiv 1 \pmod 4$$

証明.

($\Longleftarrow$) 素数 p の $\mathbb{Z}[\sqrt{-1}]$ での分解を $p = wP_1^{e_1} \cdots P_g^{e_g}$ とする. このとき $P_1 = a + b\sqrt{-1}$ と書けば $p^{f_1} = N(P_1) = a^2 + b^2$ である. ここで, この分解は次の 3 通りしかない.

$$\begin{cases} g = 1,\ e_1 = 1,\ f_1 = 2 \quad (*) \\ g = 1,\ e_1 = 2,\ f_1 = 1 \\ g = 2,\ e_1 = e_2 = f_1 = f_2 = 1 \end{cases}$$

$(*)$ の場合でないことを示せば $p = N(P_1) = a^2 + b^2$ が分かる.

証明.

そこで $(*)$ の場合であると仮定する．つまり p は G-素数である．

$p \equiv 1 \pmod 4$ だから $t^2 \equiv -1 \pmod p$ なる $t \in \mathbb{Z}$ が取れる．
即ちある $m \in \mathbb{Z}$ により $t^2 + 1 = pm$ と書ける．よって

$$pm = (t + \sqrt{-1})(t - \sqrt{-1})$$

である．故に $\mathbb{Z}[\sqrt{-1}]$ での素因数分解の一意性から $t + \sqrt{-1}$ か $t - \sqrt{-1}$ は p で割り切れなければならない．しかし明らかに $\dfrac{t \pm \sqrt{-1}}{p} \notin \mathbb{Z}[\sqrt{-1}]$ であるから矛盾する． □

類体論とは

類体論とは

類体論とは

$\longrightarrow$ 代数的整数論の中で最強の理論 (個人の感想です)

類体論とは

先ほど $\mathbb{Z}[\sqrt{-1}]$ における p の分解は 3 通りしかないことを見た．
より詳しく見ると，それは次のようになっている．

$p \bmod 4$	e_i	f_i	g	分解の形	素数の例
0	$-$	$-$	$-$	$-$	$-$
1	1	1	2	$p = wP_1P_2,\ N(P_i) = p$	$5, 13, 17 \cdots$
2	2	1	1	$p = wP_1^2,\ N(P_1) = p$	2
3	1	2	1	$p = wP_1,\ N(P_1) = p^2$	$3, 7, 11 \cdots$

このように素数の分解の仕方が $\bmod$ で決まってしまうことがあり，これが類体論 (Class Field Theory) の例である．類体論の「類」とは $\bmod n$ による剰余類のことである．

類体論とは

もう一つの例として環 $\mathbb{Z}[\zeta_7]$ を見る．(定義は後でする)
この環では素数 p の分解は次のように $\bmod 7$ で判定できる．

$p \bmod 7$	e_i	f_i	g	分解の形	例
0	6	1	1	$p = wP_1^6,\ N(P_i) = p$	7
1	1	1	6	$p = wP_1P_2\cdots P_6,\ N(P_i) = p$	29
2	1	3	2	$p = wP_1P_2,\ N(P_i) = p^3$	23
3	1	6	1	$p = wP_1,\ N(P_i) = p^6$	17
4	1	3	2	$p = wP_1P_2,\ N(P_i) = p^3$	67
5	1	6	1	$p = wP_1,\ N(P_i) = p^6$	19
6	1	2	3	$p = wP_1P_2P_3,\ N(P_i) = p^2$	13

$\bmod 7$ で 0 になる素数は勿論 7 しかないが，$e_i > 1$ となるのはこの唯一つの素数 7 のみである．

類体論とは

この唯一つの"例外" 7 を除いた $\{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} = (\mathbb{Z}/7\mathbb{Z})^\times$ は乗法で群になる．各元 $\bar{a} \in (\mathbb{Z}/7\mathbb{Z})^\times$ の位数 = 「$\bar{a}$ での f_i」となる．
(位数: 初めて $a^k \equiv 1 \pmod 7$ となる $k > 0$)
更に $f_i g = |(\mathbb{Z}/7\mathbb{Z})^\times| = 6$ である．

$p \bmod 7$	e_i	f_i	g	$\bmod 7$ での位数
1	1	1	6	1
2	1	3	2	3
3	1	6	1	6
4	1	3	2	3
5	1	6	1	6
6	1	2	3	2

こうしてこの表は $(\mathbb{Z}/7\mathbb{Z})^\times$ の構造から決定できる．

類体論とは

このような「素数 p の分解の仕方が $\bmod n$ で判定できる」というのは常に起こる現象ではない．

例えば $\alpha \in \mathbb{C}$ を

$$x^6 + 3x^5 - 5x^3 + 3x + 1$$

の根としたとき，環 $\mathbb{Z}[\alpha]$ において素数 p の分解の仕方は，どのような正整数 n を使っても $\bmod\ n$ で判定することは出来ないことが知られている．
($\text{この環は } \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \text{ の整数環になる．}$)
https://math.stackexchange.com/questions/346699/

代数的整数論

【定義】

$\alpha \in \mathbb{C}$ が代数的数 $\Longleftrightarrow$ ある $f \in \mathbb{Q}[x]$ が存在して $f(\alpha) = 0$.

【定義】

代数的数 α の最小多項式とは以下を満たす $f_\alpha \in \mathbb{Q}[x]$ である.

(1) $f_\alpha(\alpha) = 0$.

(2) f_α の最高次の係数が 1.

(3) そのような多項式のうち次数が最小.

【定義】

代数的数 α が代数的整数 $\Longleftrightarrow$ $f_\alpha \in \mathbb{Z}[x]$.

【例】

$\sqrt{2}$ は代数的整数．$f_{\sqrt{2}} = x^2 - 2$

【例】

$\sqrt{-1}$ は代数的整数．$f_{\sqrt{-1}} = x^2 + 1$

【例】

$\dfrac{\sqrt{2}}{2}$ は代数的数だが代数的整数でない．$f_{\frac{\sqrt{2}}{2}} = x^2 - \dfrac{1}{2}$

【例】

$\dfrac{1+\sqrt{-3}}{2}$ は代数的整数．$f_{\frac{1+\sqrt{-3}}{2}} = x^2 - x + 1$

【定義】

$$\zeta_n := \exp\left(\frac{2\pi\sqrt{-1}}{n}\right).$$

【命題】

ζ_n は代数的整数.

【定義】

K が代数体

$\iff \mathbb{Q} \subset K \subset \mathbb{C}$ は部分体であって，$[K : Q] := \dim_{\mathbb{Q}} K < \infty$

【定義】

代数体 K に対して $\mathcal{O}_K := \{\alpha \in K \mid \alpha$ は代数的整数 $\}$ を K の整数環という．これは環になる．

(環論知ってる人向け: $\mathbb{Z}$ の K における整閉包のことである)

【定義】

K, L が体で $K \subset L$ が部分体のとき L を K の拡大体といい L/K と書く.

【定義】

L/K がアーベル拡大
$\iff L/K$ が Galois 拡大で $\mathrm{Gal}(L/K)$ がアーベル群.

【定義】

K の全ての有限次アーベル拡大の合併を K の最大アーベル拡大体といい K^{ab} と書く.

【定義】

$\alpha_1, \cdots, \alpha_s$ を複素数とするとき

(1) $\mathbb{Q}$ と $\alpha_1, \cdots, \alpha_s$ を含む最小の体を $\mathbb{Q}(\alpha_1, \cdots, \alpha_s)$ と書く.

(2) $\mathbb{Z}$ と $\alpha_1, \cdots, \alpha_s$ を含む最小の環を $\mathbb{Z}[\alpha_1, \cdots, \alpha_s]$ と書く.

【命題】

(1) $\mathbb{Z}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Z}[x]\}$

(2) $\mathbb{Q}(\alpha) = \left\{ \dfrac{f(\alpha)}{g(\alpha)} \;\middle|\; f, g \in \mathbb{Z}[x], g(\alpha) \neq 0 \right\}$

(3) $\alpha_1, \cdots, \alpha_s$ が代数的数のとき $\mathbb{Q}(\alpha_1, \cdots, \alpha_s)$ は代数体.

【例】

$\sqrt{-1}$ は代数的数だから $\mathbb{Q}(\sqrt{-1})$ は代数体．

$$\mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$$
$$\mathcal{O}_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$$

【例】

ζ_n は代数的数だから $\mathbb{Q}(\zeta_n)$ は代数体．
$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ となる．更に $n = p$ が素数のときは

$$\mathbb{Q}(\zeta_p) = \{a_{p-2}\zeta_p^{p-2} + \cdots + a_1\zeta_p + a_0 \mid a_i \in \mathbb{Q}\}$$
$$\mathbb{Z}[\zeta_p] = \{a_{p-2}\zeta_p^{p-2} + \cdots + a_1\zeta_p + a_0 \mid a_i \in \mathbb{Z}\}$$

【例】

$\sqrt{-3}$ は代数的数だから $\mathbb{Q}(\sqrt{-3})$ は代数体.

$$\mathbb{Q}(\sqrt{-3}) = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Q}\}$$

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \left\{a + b\frac{1+\sqrt{-3}}{2} \;\middle|\; a, b \in \mathbb{Z}\right\}$$

【定義】

代数体 K のイデアルとは $\mathcal{O}_K$ のイデアルのこと
($\mathcal{O}_K$ のイデアル $=$ 部分 $\mathcal{O}_K$-加群 $\mathfrak{a} \subset \mathcal{O}_K$)

$\mathfrak{a}, \mathfrak{b}$ を K のイデアルとするとき，その積 $\mathfrak{ab}$ を

$$\mathfrak{ab} := \{\alpha_1\beta_1 + \cdots + \alpha_m\beta_m \mid \alpha_i \in \mathfrak{a}, \beta_i \in \mathfrak{b}\}$$

と定める．$\mathfrak{ab}$ も K のイデアルとなる．

この積により K のイデアル全体は可換なモノイドとなる．

- 単位元は $\mathcal{O}_K$ 自身をイデアルとみなしたもの
- 逆元は無いから群にはならない．

そこでイデアルをより一般化したものを考える．

【定義】

K の分数イデアルとは次を満たす部分 $\mathcal{O}_K$-加群 $\mathfrak{a} \subset K$ のこと

ある $\gamma \in K$ が存在して $\gamma\mathfrak{a} \subset \mathcal{O}_K$.

イデアルは分数イデアルである．($\gamma = 1$ と取れるから)

【定義】

$\mathfrak{a}, \mathfrak{b}$ を K の分数イデアルとするとき

$$\mathfrak{ab} := \{\alpha_1\beta_1 + \cdots + \alpha_m\beta_m \mid \alpha_i \in \mathfrak{a}, \beta_i \in \mathfrak{b}\}$$
$$\mathfrak{a}^{-1} := \{\gamma \in K \mid \gamma\mathfrak{a} \subset \mathcal{O}_K\}$$

$\mathfrak{ab}$，$\mathfrak{a}^{-1}$ も K の分数イデアルとなる．また $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$.

K の分数イデアル全体 J_K は群をなす．

【定理】

K の分数イデアル $\mathfrak{a} \neq 0$ は

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \quad (\mathfrak{p}_i \text{ は相異なる素イデアル，} e_i \neq 0)$$

と (順番を除いて) 一意に書ける．

※ $\mathfrak{a}$ がイデアルとなるのは各番号 i について $e_i > 0$ となるときである．

【定義】

$\alpha_i \in K$ に対して

$$(\alpha_1, \ldots, \alpha_m) := \{\alpha_1\beta_1 + \cdots + \alpha_m\beta_m \mid \beta_i \in \mathcal{O}_K\}$$

は分数イデアルとなる．特に (α) の形の分数イデアルを単項分数イデアルという．

代数体 K の乗法群を $K^\times$ とすると，群準同型写像が

$$F\colon K^\times \longrightarrow J_K$$

$$\alpha \longmapsto (\alpha)$$

により定まる．これで数 $\alpha \in K^\times$ を分数イデアルと"みなす"．

この意味で分数イデアルは数を拡張したものと考える．

【例】

代数体 $\mathbb{Q}(\sqrt{-5})$ を考える．$\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ である．この整数環では

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

となり，6 は既約元の積として 2 通りに書ける．(つまり $\mathbb{Z}[\sqrt{-5}]$ は UFD ではなく"素因数分解の一意性"はない)
これらの数を単項イデアルとみなして素イデアル分解すると

$$\begin{aligned}
(2) &= (2, 1+\sqrt{-5})^2 \\
(3) &= (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) \\
(1+\sqrt{-5}) &= (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) \\
(1-\sqrt{-5}) &= (2, 1+\sqrt{-5})(3, 1-\sqrt{-5})
\end{aligned}$$

【例】

つまり 6 はイデアルとして考えれば

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

と素イデアル分解できる．

このように一般の整数環では素因数分解ができるとは限らないが，イデアルに拡張して考えることで分解ができるようになる．

数とイデアルの"ずれ"の情報として，準同型 $\alpha \mapsto (\alpha)$ の核と余核を考えることが多い．

(1) 核を E_K と書き K の単数群という．
(2) 余核を Cl_K と書き K のイデアル類群という．

E_K, Cl_K については次の定理が知られている.

【定理】 (Dirichlet の単数定理)

$E_K \cong (\mathbb{Z}/w_K\mathbb{Z}) \times \mathbb{Z}^{r_K}$.

(記号の説明は省略)

【定理】

Cl_K は有限群である.

$h_K := |Cl_K|$ を K の類数という.

$$
\begin{aligned}
h_K = 1 &\iff J_K = \{(\alpha) \mid \alpha \in K\} \\
&\iff \mathcal{O}_K \text{は PID(単項イデアル整域)} \\
&\iff \mathcal{O}_K \text{は UFD(一意分解整域)}
\end{aligned}
$$

※ PID: 全てのイデアルが単項イデアルになる整域
UFD: 全ての元が既約元の積に一意に分解できる整域
一般に PID $\Longrightarrow$ UFD

よって「$h_K = 1 \iff K$ では素因数分解が一意にできる」となり，
例えば $h_{\mathbb{Q}} = h_{\mathbb{Q}(\sqrt{-1})} = 1$，$h_{\mathbb{Q}(\sqrt{-5})} = 2$ である．

【定義】

$K/\mathbb{Q}$ を代数体，p を素数とする．p を含む最小の K のイデアル (p) を K で

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

と素イデアル分解する．このとき $g \leq [K : \mathbb{Q}]$ となることが知られている．

(1) p は L/K で完全分解する $\Longleftrightarrow$ $g = [K : \mathbb{Q}]$

(2) p は L/K で分岐する $\Longleftrightarrow$ ある i について $e_i > 1$

(3) p は L/K で不分岐 $\Longleftrightarrow$ 全ての i について $e_i = 1$

【定義】

L/K を代数体，$\mathfrak{p}$ を K の素イデアルとする．$\mathfrak{p}$ を含む最小の L のイデアルを $\mathfrak{p}\mathcal{O}_L$ と書く．これを L で

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

と素イデアル分解する．このとき $g \leq [L : K]$ となることが知られている．

(1) $\mathfrak{p}$ は L/K で完全分解する $\Longleftrightarrow$ $g = [L : K]$

(2) $\mathfrak{p}$ は L/K で分岐する $\Longleftrightarrow$ ある i について $e_i > 1$

(3) $\mathfrak{p}$ は L/K で不分岐 $\Longleftrightarrow$ 全ての i について $e_i = 1$

有理数体の類体論

まず次のような定義をしてみる.

【定義】

$n > 2$ を整数，$H \subset (\mathbb{Z}/n\mathbb{Z})^\times$ を部分群とする.
Galois 拡大 $K/\mathbb{Q}$ が H の類体
$\Longleftrightarrow$ 素数 p に対して次が成り立つ

$$\bar{p} \in H \Longleftrightarrow p \text{ は } K/\mathbb{Q} \text{ で完全分解する}$$

このとき考えられる問題として

(1) 任意の H に対して類体は存在するだろうか?

(2) 類体となるのはどのような代数体だろうか?

まず代数体 $\mathbb{Q}(\zeta_n)$ については次のことが知られている.

【定理】

$n > 2$ を整数とするとき

(1) $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. (特に $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ はアーベル拡大)

(2) $p \mid n \iff p$ は $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ で分岐する.

(3) $p \equiv 1 \pmod{n} \iff p$ は $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ で完全分解する.
より一般に, $\bar{p}$ の $(\mathbb{Z}/n\mathbb{Z})^\times$ での位数を f, $\varphi(n) = fg$ とすれば p は $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ で g 個に分解する.

特に $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ は $1 \subset (\mathbb{Z}/n\mathbb{Z})^\times$ の類体である.

例として $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ を考えると次の表になる．$(\varphi(7)=6)$

$p \bmod 7$	e_i	f	g	分解の形	例
0	6	1	1	$(p)=\mathfrak{p}_1^6$	7
1	1	1	6	$(p)=\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_6$	$29, 43, \cdots$
2	1	3	2	$(p)=\mathfrak{p}_1\mathfrak{p}_2$	$2, 23, \cdots$
3	1	6	1	$(p)=\mathfrak{p}_1$	$3, 17, \cdots$
4	1	3	2	$(p)=\mathfrak{p}_1\mathfrak{p}_2$	$11, 67, \cdots$
5	1	6	1	$(p)=\mathfrak{p}_1$	$5, 19, \cdots$
6	1	2	3	$(p)=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$13, 41, \cdots$

有理数体の類体論

より一般に，部分群 $H \subset (\mathbb{Z}/n\mathbb{Z})^\times$ が与えられたとき．Galois 理論により部分群 $(\mathbb{Z}/n\mathbb{Z})^\times \supset H \supset 1$ に対応する部分体 $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_n)$ を取る．このとき

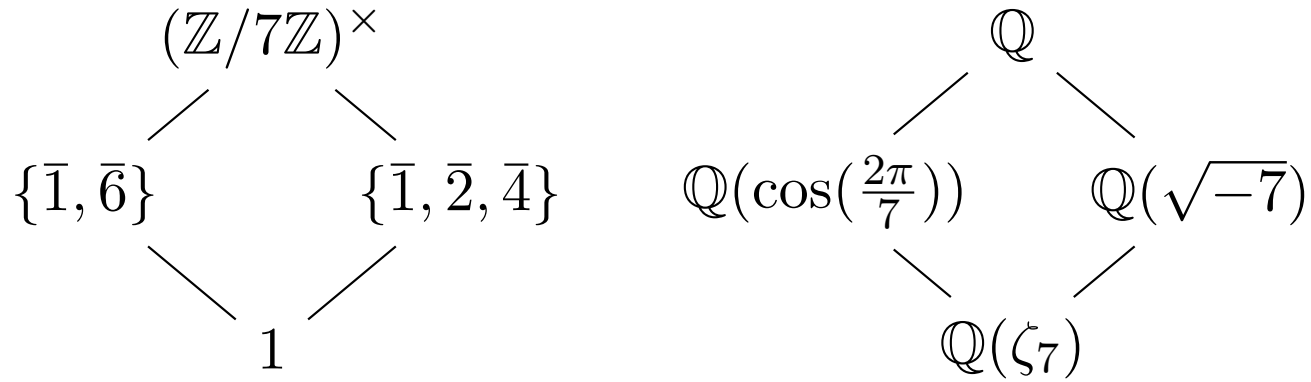
$$\bar{p} \in H \Longleftrightarrow p \text{ は } K/\mathbb{Q} \text{ で完全分解する}$$

となる．(即ちこの $K/\mathbb{Q}$ は H の類体である．)
より一般に，$\bar{p}$ の $(\mathbb{Z}/n\mathbb{Z})^\times/H$ での位数を f, $|(\mathbb{Z}/n\mathbb{Z})^\times/H| = fg$ とすれば p は $K/\mathbb{Q}$ で g 個に分解する．従って

任意の H に対して類体は存在するだろうか? $\to$ YES

【例】

$n = 7$ とする．$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ の部分群は 4 つ．
Galois 理論による対応する体は次の通り．



$\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$ は $\{\bar{1}, \bar{2}, \bar{4}\}$ の類体．
$\mathbb{Q}(\cos(\frac{2\pi}{7}))/\mathbb{Q}$ は $\{\bar{1}, \bar{6}\}$ の類体．

$\mathbb{Q}(\cos(\frac{2\pi}{7}))/\mathbb{Q}$ では次の表になる.

$p \bmod 7$	e_i	f_i	g	分解の形	例
0	3	1	1	$(p) = \mathfrak{p}_1^3$	7
1	1	1	3	$(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$29, 43, \cdots$
2	1	3	1	$(p) = \mathfrak{p}_1$	$2, 23, \cdots$
3	1	3	1	$(p) = \mathfrak{p}_1$	$3, 17, \cdots$
4	1	3	1	$(p) = \mathfrak{p}_1$	$11, 67, \cdots$
5	1	3	1	$(p) = \mathfrak{p}_1$	$5, 19, \cdots$
6	1	1	3	$(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$13, 41, \cdots$

つまり $p \equiv 1, 6 \pmod 7 \iff p$ は $\mathbb{Q}(\cos(\frac{2\pi}{7}))/\mathbb{Q}$ で完全分解する

$\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$ では次の表になる.

$p \bmod 7$	e_i	f_i	g	分解の形	例
0	2	1	1	$(p) = \mathfrak{p}_1^2$	7
1	1	1	2	$(p) = \mathfrak{p}_1\mathfrak{p}_2$	$29, 43, \cdots$
2	1	1	2	$(p) = \mathfrak{p}_1\mathfrak{p}_2$	$2, 23, \cdots$
3	1	2	1	$(p) = \mathfrak{p}_1$	$3, 17, \cdots$
4	1	1	2	$(p) = \mathfrak{p}_1\mathfrak{p}_2$	$11, 67, \cdots$
5	1	2	1	$(p) = \mathfrak{p}_1$	$5, 19, \cdots$
6	1	2	1	$(p) = \mathfrak{p}_1$	$13, 41, \cdots$

つまり $p \equiv 1, 2, 4 \pmod 7 \iff p$ は $\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$ で完全分解する

有理数体の類体論

$\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times/H$ であるから $\mathbb{Q}$ の類体は $\mathbb{Q}$ の有限次アーベル拡大である.

ところが実は逆，即ち $\mathbb{Q}$ の有限次アーベル拡大は類体であることが次の定理から分かる.

【定理】 (Kronecker-Weber の定理)

任意の有限次アーベル拡大 $K/\mathbb{Q}$ に対して，ある正整数 n が存在して $K \subset \mathbb{Q}(\zeta_n)$

K に対してこの n を取って，K に対応する部分群 $H \subset (\mathbb{Z}/n\mathbb{Z})^\times$ を取れば $K/\mathbb{Q}$ は H の類体である.

つまり，類体論とは要するに有限次アーベル拡大の理論ということになる.

代数体の類体論

代数体の類体論

有理数体の場合と同様の定理が一般の代数体に対しても成り立つ.

まず有理数体の場合でいう $(\mathbb{Z}/n\mathbb{Z})^\times$ に当たる群として $Cl_K(\mathfrak{m})$ を定義する．但し，一般の場合は事情が複雑になるため，以下では K は総虚であるとする.
(代数体 K が総虚 $=$ 準同型 $K \to \mathbb{R}$ が存在しない)

【定義】

K を代数体，$\mathfrak{m}$ を K のイデアルとする.

$$J_K(\mathfrak{m}) := \{\mathfrak{a} \subset K \mid \mathfrak{a} \text{ は分数イデアルで } \mathfrak{m} \text{ と素 }\}$$
$$P_K(\mathfrak{m}) := \{(\alpha) \mid \alpha \in K^\times,\ \alpha \equiv 1 \pmod{\mathfrak{m}}\}$$
$$Cl_K(\mathfrak{m}) := I_K(\mathfrak{m})/P_K(\mathfrak{m})$$

このとき有理数体の場合の $\mathbb{Q}(\zeta_n)$ に当たる体 $K(\mathfrak{m})$ が存在する．

【定理】

有限次アーベル拡大 $K(\mathfrak{m})/K$ が存在して以下が成り立つ．

(1) $\mathrm{Gal}(K(\mathfrak{m})/K) \cong Cl_K(\mathfrak{m})$.

(2) $\mathfrak{p} \mid \mathfrak{m} \Longleftrightarrow \mathfrak{p}$ は $K(\mathfrak{m})/K$ で分岐する．

(3) $\bar{\mathfrak{p}} = 1$ in $Cl_K(\mathfrak{m}) \Longleftrightarrow \mathfrak{p}$ は $K(\mathfrak{m})/K$ で完全分解する．
より一般に，$\mathfrak{p}$ の $Cl_K(\mathfrak{m})$ での位数を f, $|Cl_K(\mathfrak{m})| = fg$ とすれば $\mathfrak{p}$ は $K(\mathfrak{m})/K$ で g 個に分解する．

特に $\mathfrak{m} := \mathcal{O}_K$ の場合の $H := K(\mathcal{O}_K)$ を K の Hilbert 類体，もしくは絶対類体という．

$$\mathfrak{p} \mid \mathcal{O}_K \Longleftrightarrow \mathfrak{p} \text{ は } H/K \text{ で分岐する．}$$

だから，H/K では全ての素イデアルが不分岐である．

【定理】 (単項化定理)

$\mathfrak{a}$ を K のイデアルとするとき $\mathfrak{a}\mathcal{O}_H$ は単項イデアル．

【定理】 (分解定理)

K の素イデアル $\mathfrak{p}$ について

$$\mathfrak{p} \text{ が } H/K \text{ で完全分解する} \Longleftrightarrow \mathfrak{p} \text{ は単項イデアル}$$

代数体の類体論

$K_0/\mathbb{Q}$ を代数体として，K_{n+1} を K_n の絶対類体とすれば代数体の上昇列 $K_0 \subset K_1 \subset K_2 \subset \cdots$ が得られる．(類体塔という)

【問】 (類体塔問題)

任意の n について $K_n \subsetneq K_{n+1}$ となるような代数体 K_0 は存在するか?

【定理】 (Golod-Shafarevich の定理 (1964))

存在する．例えば $K_0 = \mathbb{Q}(\sqrt{-5 \cdot 11 \cdot 461})$ ならよいらしい．

応用例 (1) 整数論

応用例 (1) 整数論

【命題】

素数 $p \neq 2, 5$ に対して

ある $a, b \in \mathbb{Z}$ が存在して $p = a^2 + 5b^2 \iff p \equiv 1, 9 \pmod{20}$

Fermat の二平方和定理の場合と同様に $K := \mathbb{Q}(\sqrt{-5})$ とすれば

$$a^2 + 5b^2 = (a + b\sqrt{-5})(a - b\sqrt{-5})$$

$K \subset \mathbb{Q}(\zeta_n)$ となる最小の n は $n = 20$ であり，K に対応する $\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/\mathbb{Q}) \cong (\mathbb{Z}/20\mathbb{Z})^\times$ の部分群は $\{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ である．故に

$$K/\mathbb{Q} \text{ で } p \text{ が完全分解する} \iff p \equiv 1, 3, 7, 9 \pmod{20}$$

応用例 (1) 整数論

ここでの「$K/\mathbb{Q}$ で p が完全分解する」とは

$$(p) = \mathfrak{p}_1\mathfrak{p}_2 \quad (\mathfrak{p}_i \text{ は } K \text{ の素イデアル，} \mathfrak{p}_1 \neq \mathfrak{p}_2)$$

と書けることである．ここでもし $\mathfrak{p}_1, \mathfrak{p}_2$ が単項イデアルならば，つまり

$$\mathfrak{p}_1 = (a_1 + b_1\sqrt{-5}), \quad \mathfrak{p}_2 = (a_2 + b_2\sqrt{-5})$$

と書ければ

$$(p) = (a_1 + b_1\sqrt{-5})(a_2 + b_2\sqrt{-5})$$

となるから数として

$$\alpha p = (a_1 + b_1\sqrt{-5})(a_2 + b_2\sqrt{-5})$$

であり，Fermat の二平方和定理の時と同様の議論ができる．

応用例 (1) 整数論

ところが $K = \mathbb{Q}(\sqrt{-5})$ には単項でないイデアルが存在する．つまり p が完全分解する条件だけでは足りなくて，分解後の素イデアルが単項になる条件まで考慮する必要がある．

そこで絶対類体を応用する．H/K を絶対類体とすれば

$$\mathfrak{p} \text{ が単項イデアル} \iff \mathfrak{p} \text{ が } H/K \text{ で完全分解する}$$

である．$H = K(\sqrt{-1}) = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$ であることが知られており，$H/\mathbb{Q}$ はアーベル拡大である．$H \subset \mathbb{Q}(\zeta_n)$ となる最小の n も $n = 20$ であり，H に対応する $\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/\mathbb{Q}) \cong (\mathbb{Z}/20\mathbb{Z})^\times$ の部分群は $\{\bar{1}, \bar{9}\}$ である．

以上を踏まえて

応用例 (1) 整数論

【命題】

素数 $p \neq 2, 5$ に対して

ある $a, b \in \mathbb{Z}$ が存在して $p = a^2 + 5b^2 \iff p \equiv 1, 9 \pmod{20}$

証明.

$p = a^2 + 5b^2$ と書ける

$\iff p = (a + b\sqrt{-5})(a - b\sqrt{-5})$

$\iff K/\mathbb{Q}$ で $p = \mathfrak{p}_1\mathfrak{p}_2$ と完全分解，$\mathfrak{p}_1, \mathfrak{p}_2$ が単項イデアル

$\iff K/\mathbb{Q}$ で $p = \mathfrak{p}_1\mathfrak{p}_2$ と完全分解，H/K で $\mathfrak{p}_1, \mathfrak{p}_2$ が完全分解

$\iff p$ は $H/\mathbb{Q}$ で完全分解

$\iff p \equiv 1, 9 \pmod{20}$

□

応用例 (1) 整数論

【命題】

mod 20 で 3 か 7 になる二つの素数 p, q に対して，ある $a, b \in \mathbb{Z}$ が存在して $pq = a^2 + 5b^2$.

証明.

$p \equiv 3, 7 \pmod{20}$ だから $K := \mathbb{Q}(\sqrt{-5})$ とすると $K/\mathbb{Q}$ で

$$(p) = \mathfrak{p}_1\mathfrak{p}_2 \quad (\mathfrak{p}_i \text{ は非単項素イデアル}, \mathfrak{p}_1 \neq \mathfrak{p}_2)$$

$(q) = \mathfrak{q}_1\mathfrak{q}_2$ も同様．このとき $pq = \mathfrak{p}_1\mathfrak{q}_1\mathfrak{p}_2\mathfrak{q}_2$ であるが $h_K = 2$ だから $\mathfrak{p}_1\mathfrak{q}_1, \mathfrak{p}_2\mathfrak{q}_2$ は単項イデアルである．$\mathfrak{p}_1\mathfrak{q}_1 = (a + b\sqrt{-5})$ と書けば $\mathfrak{p}_2\mathfrak{q}_2 = (a - b\sqrt{-5})$ であり $pq = a^2 + 5b^2$ となる． □

応用例 (1) 整数論

【命題】

素数 $p \neq 2, 13$ に対して「ある $a, b \in \mathbb{Z}$ が存在して $p = a^2 + 26b^2$ と書ける」かどうかは mod では判定できない．

証明.

$K := \mathbb{Q}(\sqrt{-26})$ として H/K を Hilbert 類体とすると

$p = a^2 + 26b^2$ と書ける

$\iff K/\mathbb{Q}$ で $p = \mathfrak{p}_1\mathfrak{p}_2$ と完全分解，$\mathfrak{p}_1, \mathfrak{p}_2$ が単項イデアル

$\iff K/\mathbb{Q}$ で $p = \mathfrak{p}_1\mathfrak{p}_2$ と完全分解，H/K で $\mathfrak{p}_1, \mathfrak{p}_2$ が完全分解

$\iff p$ は $H/\mathbb{Q}$ で完全分解

となるが，$H/\mathbb{Q}$ はアーベル拡大でないことが分かる．よって p が $H/\mathbb{Q}$ で完全分解するかを mod で判定はできない． □

応用例 (1) 整数論

【命題】

素数 $p \neq 2, 13$ に対して「ある $a, b \in \mathbb{Z}$ が存在して $p = a^2 + 26b^2$ と書ける」かどうかは mod では判定できない.

証明.

$K := \mathbb{Q}(\sqrt{-26})$ として H/K を Hilbert 類体とすると

$p = a^2 + 26b^2$ と書ける

$\iff K/\mathbb{Q}$ で $p = \mathfrak{p}_1\mathfrak{p}_2$ と完全分解, $\mathfrak{p}_1, \mathfrak{p}_2$ が単項イデアル

$\iff K/\mathbb{Q}$ で $p = \mathfrak{p}_1\mathfrak{p}_2$ と完全分解, H/K で $\mathfrak{p}_1, \mathfrak{p}_2$ が完全分解

$\iff p$ は $H/\mathbb{Q}$ で完全分解

となるが，$H/\mathbb{Q}$ はアーベル拡大でないことが分かる．よって p が $H/\mathbb{Q}$ で完全分解するかを mod で判定はできない. $\square$

類体論その２

類体論その 2

(ここからは難しい話になります)

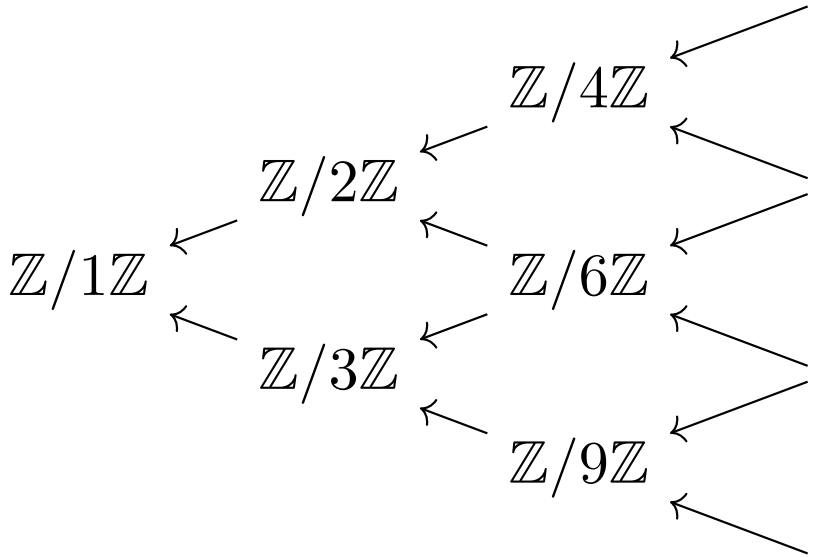
類体論とは要するにアーベル拡大の理論であり，最大アーベル拡大のガロア群 $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ を簡単な群で"近似"するという形で述べることができる.

類体論その 2

【例】 (0 次元類体論 = 有限体の類体論)

$\mathbb{F}$ を有限体とする．
$n > 0$ に対して $\mathbb{F}$ の n 次拡大体 K は唯一つで
$\mathrm{Gal}(K/\mathbb{F}) \cong \mathbb{Z}/n\mathbb{Z}$ である．よって

$$\mathrm{Gal}(\mathbb{F}^{\mathrm{ab}}/\mathbb{F}) \cong \widehat{\mathbb{Z}} := \lim(\mathbb{Z}/n\mathbb{Z}).$$



類体論その 2

【例】 (0 次元類体論 = 有限体の類体論)

$\mathbb{F}$ を有限体とする.
$n > 0$ に対して $\mathbb{F}$ の n 次拡大体 K は唯一つで
$\mathrm{Gal}(K/\mathbb{F}) \cong \mathbb{Z}/n\mathbb{Z}$ である. よって

$$\mathrm{Gal}(\mathbb{F}^{\mathrm{ab}}/\mathbb{F}) \cong \widehat{\mathbb{Z}} := \lim(\mathbb{Z}/n\mathbb{Z}).$$

無限次元 Galois 理論により次の一対一対応が得られる.

$$\mathrm{Gal}(\mathbb{F}^{\mathrm{ab}}/\mathbb{F}) \text{ の開部分群} \overset{1:1}{\longleftrightarrow} \mathbb{F} \text{ の有限次アーベル拡大}$$

【例】 (0 次元類体論)

普遍性により得られる準同型を $h\colon \mathbb{Z} \to \widehat{\mathbb{Z}}$ とする．$U \subset \widehat{\mathbb{Z}}$ を開部分群とするとき $h^{-1}(U) \subset \mathbb{Z}$ は指数有限部分群である．これにより次の一対一対応が得られる．

$$\widehat{\mathbb{Z}} \text{ の開部分群} \overset{1:1}{\longleftrightarrow} \mathbb{Z} \text{ の指数有限部分群}$$

$\rho_{\mathbb{F}}$ を合成 $\mathbb{Z} \xrightarrow{h} \widehat{\mathbb{Z}} \cong \mathrm{Gal}(\mathbb{F}^{\mathrm{ab}}/\mathbb{F})$ とする．

$$\begin{aligned} \mathbb{F} \text{ の有限次アーベル拡大} &\overset{1:1}{\longleftrightarrow} \mathrm{Gal}(\mathbb{F}^{\mathrm{ab}}/\mathbb{F}) \text{ の開部分群} \\ &\overset{1:1}{\longleftrightarrow} \widehat{\mathbb{Z}} \text{ の開部分群} \\ &\overset{1:1}{\longleftrightarrow} \mathbb{Z} \text{ の指数有限部分群} \end{aligned}$$

類体論その 2

【定義】

K が 0 次元局所体 $\Longleftrightarrow$ K が有限体

【定義】

$n > 0$ のとき，K が n 次元局所体

$\Longleftrightarrow$ K は完備離散付値体かつその剰余体が $(n-1)$ 次元局所体.

【例】

p 進数体 $\mathbb{Q}_p$ やその有限次拡大体は 1 次元局所体.

【定理】 (1 次元局所類体論)

1 次元局所体 K に対して，連続準同型 $\rho_K \colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ が存在して

(1) ρ_K により「K の有限次アーベル拡大」と「$K^\times$ の指数有限開部分群」が一対一に対応する．

(2) K の剰余体が $\mathbb{F}$ のとき次が可換

$$\begin{array}{ccc} K^\times & \xrightarrow{\rho_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ \text{付値}\downarrow & & \downarrow \\ \mathbb{Z} & \xrightarrow[\rho_{\mathbb{F}}]{} & \mathrm{Gal}(\mathbb{F}^{\mathrm{ab}}/\mathbb{F}) \end{array}$$

【定理】 (1 次元大域類体論)

代数体 K に対して，イデール類群と呼ばれる位相群 C_K と連続準同型 $\rho_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ が構成できて

(1) ρ_K により「K の有限次アーベル拡大」と「C_K の指数有限開部分群」が一対一に対応する．

(2) K の素点 $\mathfrak{p}$ に対して次が可換となる．

$$\begin{array}{ccc} K_{\mathfrak{p}}^{\times} & \xrightarrow{\rho_{K_{\mathfrak{p}}}} & \mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{ab}}/K_{\mathfrak{p}}) \\ \downarrow & & \downarrow \\ C_K & \xrightarrow[\rho_K]{} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

類体論その 2

【命題】

K のイデアル $\mathfrak{m}$ に対して，ある部分群 $C_K^{\mathfrak{m}} \subset C_K$ が存在して $C_K/C_K^{\mathfrak{m}} \cong Cl(\mathfrak{m})$ となる．更に次の一対一対応が得られる．

$$
\begin{aligned}
& C_K\text{の指数有限開部分群} \\
\overset{1:1}{\longleftrightarrow}\ & C_K\text{の部分群であって，ある } \mathfrak{m} \text{ に対する } C_K^{\mathfrak{m}}\text{を含むもの}
\end{aligned}
$$

$\rho_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ により

$$
\begin{aligned}
& \text{有限次アーベル拡大 } L/K \overset{1:1}{\longleftrightarrow} C_K\text{の指数有限開部分群} \\
& \qquad\qquad \overset{1:1}{\longleftrightarrow} Cl(\mathfrak{m}) \cong C_K/C_K^{\mathfrak{m}}\text{の部分群}
\end{aligned}
$$

という一対一対応が得られることになる．この対応で $1 \subset Cl(\mathfrak{m})$ に対応するのが $K(\mathfrak{m})/K$ である．

応用例 (2) n 乗剰余の相互法則

応用例 (2) n 乗剰余の相互法則

整数論における重要な定理として「平方剰余の相互法則」というものがある．

平方剰余とは要するに体 $\mathbb{F}_p$ の中に平方根があることをいう．

【定義】

p を奇素数，$a \in \mathbb{Z}$ が p と互いに素とするとき

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & (\exists x \in \mathbb{Z}, x^2 \equiv a \pmod{p}) \\ -1 & (\text{それ以外}) \end{cases}$$

と定める．(Legendre 記号という)
また $\left(\frac{a}{p}\right) = 1$ のとき a は p を法として平方剰余であるという．

応用例 (2) n 乗剰余の相互法則

このように定めると a の部分が積と可換になる．つまり

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

そこでより一般に，$b = p_1 \cdots p_s$ が奇数で a と b が互いに素のとき

$$\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_s}\right)$$

と定める．(Jacobi 記号という)

応用例 (2) n 乗剰余の相互法則

【定理】 (平方剰余の相互法則)

a, b を互いに素な奇数とするとき

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}(-1)^{\frac{\mathrm{sgn}(a)-1}{2}\frac{\mathrm{sgn}(b)-1}{2}}$$

また

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}, \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$$

つまり $\left(\frac{a}{b}\right)$ が分かれば $\left(\frac{b}{a}\right)$ も分かる．そこで「平方」ではなく，より一般の n 乗剰余についても相互法則は成り立つか? という問題が生まれる．これは類体論 (Artin の相互律) により解決された．

応用例 (2) n 乗剰余の相互法則

K を代数体，$\mu_n := \{x \in \mathbb{C} \mid x^n = 1\}$ として $\mu_n \subset K$ とする．
L/K，$M/K_\mathfrak{p}$ を有限次アーベル拡大とするとき

$$(-, L/K)\colon C_K \xrightarrow{\rho_K} \mathrm{Gal}(K^{\mathrm{ab}}/K) \xrightarrow{\text{制限}} \mathrm{Gal}(L/K)$$

$$(-, M/K_\mathfrak{p})\colon K_\mathfrak{p}^\times \xrightarrow{\rho_{K_\mathfrak{p}}} \mathrm{Gal}(K_\mathfrak{p}^{\mathrm{ab}}/K_\mathfrak{p}) \xrightarrow{\text{制限}} \mathrm{Gal}(M/K_\mathfrak{p})$$

とすると次は可換である．$(L_\mathfrak{p} := K_\mathfrak{p}L)$

$$\begin{array}{ccccc} K_\mathfrak{p}^\times & \xrightarrow{\rho_{K_\mathfrak{p}}} & \mathrm{Gal}(K_\mathfrak{p}^{\mathrm{ab}}/K_\mathfrak{p}) & \longrightarrow & \mathrm{Gal}(L_\mathfrak{p}/K_\mathfrak{p}) \\ \downarrow & & \downarrow & & \downarrow \\ C_K & \xrightarrow[\rho_K]{} & \mathrm{Gal}(K^{\mathrm{ab}}/K) & \longrightarrow & \mathrm{Gal}(L/K) \end{array}$$

また K のイデール α に対して $(\alpha, L/K) = \prod_\mathfrak{p} (\alpha_\mathfrak{p}, L_\mathfrak{p}/K_\mathfrak{p})$．

応用例 (2) n 乗剰余の相互法則

$a, b \in K_{\mathfrak{p}}^{\times}$ に対して $\left(\dfrac{a, b}{\mathfrak{p}}\right) \in \mu_n$ を

$$(a, K_{\mathfrak{p}}(\sqrt[n]{b})/K_{\mathfrak{p}})\sqrt[n]{b} = \left(\frac{a, b}{\mathfrak{p}}\right)\sqrt[n]{b}$$

により定める．(Hilbert 記号という)

$\mathfrak{p} \nmid n$，$a \in U_{\mathfrak{p}}$，$\pi \in K_{\mathfrak{p}}$ を素元としたとき

$$\left(\frac{a}{\mathfrak{p}}\right) := \left(\frac{\pi, a}{\mathfrak{p}}\right)$$

と定義する．これは

$$\left(\frac{a}{\mathfrak{p}}\right) = 1 \Longleftrightarrow x^n \equiv a \pmod{\mathfrak{p}}$$

を満たす．

応用例 (2) n 乗剰余の相互法則

より一般に n と素なイデアル $\mathfrak{b} = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ に対して

$$\left(\frac{a}{\mathfrak{b}}\right) := \left(\frac{a}{\mathfrak{p}_1}\right) \cdots \left(\frac{a}{\mathfrak{p}_s}\right)$$

と定めて，$\mathfrak{b} = (b)$ のとき

$$\left(\frac{a}{b}\right) := \left(\frac{a}{\mathfrak{b}}\right)$$

と書く．

【定理】 (n 乗剰余の相互法則)

$a, b \in K^\times$ を互いに素で，更に n とも素なとき

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{p}|n\infty} \left(\frac{a, b}{\mathfrak{p}}\right)$$

応用例 (3) 選択公理

応用例 (3) 選択公理

【定理】

ZFC において，PID は UFD である．

【問】

この定理は ZF で証明できるか?

$\longrightarrow$ 答え: No

$\longrightarrow$ このことは，なんと類体論を応用することで証明できる．

Wilfrid Hodges, Läuchli's algebraic closure of Q, Math. Proc. Camb. Phil. Soc. 79 (1976), 289–297

応用例 (3) 選択公理

N を ZF の推移的モデル，$L \in N$ を体とする．

【定義】

L 上の n 項関係 R が support S を持つ
$\Longleftrightarrow S \subset L$ は有限集合で，自己同型 $\sigma\colon L \to L$ が

$$x \in S \text{ ならば } \sigma(x) = x$$

を満たすならば $\sigma(R) = R$.

【例】

$\mathfrak{a} = (\alpha_1, \cdots, \alpha_s)$ を代数体 L のイデアルとして 1 項関係 $\mathfrak{a}$ を考えると，これは support $\{\alpha_1, \cdots, \alpha_s\}$ を持つ．

応用例 (3) 選択公理

【定義】

L が N-symmetric
$\Longleftrightarrow$ R が L 上の n 項関係で $R \in N$ ならば，R は support S を持つ．

【定理】

ZF の推移的モデル N で次を満たすものが存在する．

$\mathbb{Q}$ の代数閉包 L で N-symmetric なものが存在する．

PLOTKIN and JACOB MANITCEL, Generic embeddings, J. Symbolic Logic 34 (1969), 388–394.

以下，そのような N と L を取り固定する．

応用例 (3) 選択公理

$K_0 \subset L$ を Golod-Shafarevich の定理を満たす代数体とする．

K_{n+1}/K_n を K_n の絶対類体，$\mathcal{O}_n := \mathcal{O}_{K_n}$ として

$$K := \bigcup_{n\in\mathbb{N}} K_n,\ \mathcal{O} := \bigcup_{n\in\mathbb{N}} \mathcal{O}_n.$$

定義の絶対性から $K_n, K, \mathcal{O}_n, \mathcal{O} \in N$ が分かる．

応用例 (3) 選択公理

【命題】 (in N)

$\mathcal{O}$ は (体でない) 単項イデアル整域である.

証明.

$\mathfrak{a} \subset \mathcal{O}$ をイデアルとすれば，一項関係 $\mathfrak{a}$ は $\mathrm{support}\ S \subset \mathcal{O}$ を持つことが分かる.

S は有限集合だから，ある番号 n が存在して $S \subset \mathcal{O}_n$ となる.

このとき $\mathfrak{a} = \mathcal{O}(\mathfrak{a} \cap \mathcal{O}_{n+1})$ が分かる．単項化定理により K_{n+1} のイデアル $\mathfrak{a} \cap \mathcal{O}_{n+1}$ は K_{n+2} で単項イデアルになる．即ち

$$\mathcal{O}_{n+2}(\mathfrak{a} \cap \mathcal{O}_{n+1}) = x\mathcal{O}_{n+2}$$

と書ける．このとき

$$\mathfrak{a} = \mathcal{O}(\mathfrak{a} \cap \mathcal{O}_{n+1}) = \mathcal{O}\mathcal{O}_{n+2}(\mathfrak{a} \cap \mathcal{O}_{n+1}) = \mathcal{O}(x\mathcal{O}_{n+2}) = x\mathcal{O}$$

□

応用例 (3) 選択公理

【命題】 (in N)

$\mathcal{O}$ は素元を持たない．

証明.

素元 $p \in \mathcal{O}$ が存在すると仮定する．ある番号 n が存在して $p \in \mathcal{O}_n$ である．このとき $(p) = p\mathcal{O}_n$ は K_n の素イデアルである．

分解定理より (p) は K_{n+1}/K_n で完全分解する．即ち K_{n+1} の素イデアル $\mathfrak{p}_i$ が存在して

$$(p) = \mathfrak{p}_1 \dots \mathfrak{p}_s \ (s = [K_{n+1} : K_n] > 1)$$

となる．$\alpha_i \in \mathfrak{p}_i \setminus (p)$ を取れば $p \mid \alpha_1 \cdots \alpha_s$ かつ $p \nmid \alpha_i$ となり p が素元でなく矛盾する． □

応用例 (3) 選択公理

以上により次の定理が分かった.

【定理】

ZF の推移的モデル N で次を満たすものが存在する.

体でない，素元を持たない単項イデアル整域が存在する.

【定理】

ZF において「PID は UFD」は証明できない.