円分体および 2 次体における素数の分解について

佐藤 隆

2009 年 7 月 22 日

これは，加藤和也・黒川信重・斉藤毅著「数論 2」（岩波講座現代数学の基礎）の §5.1-5.2 をまとめたものである．

1 準備

定義 1.1. K を $\mathbb{Q}$ の有限次拡大体とし，O_K をその整数環とする．O_K はデデキント環ゆえ，素数 p について，O_K のイデアル pO_K は

$$pO_K = Q_1^{e_1} Q_2^{e_2} \dots Q_g^{e_g}$$

と素イデアル分解される．このとき，$\sum_{i=1}^{g} e_i \leqq [K:\mathbb{Q}]$ となることが知られている．

- $2 \leqq e_i$ となる i があるとき，p は K において**分岐する**という．
- 分岐しないとき，p は K において**不分岐である**という．
- $g = [L:\mathbb{Q}]$ のとき（このとき，各 i について，$e_i = 1$ となるので，p は K において不分岐である）p は K において**完全分解する**という．

定理 1.2 (ガロア理論の基本定理（ガロア対応）). $K_0 \subset K$ をガロア拡大とするとき，$\mathrm{Gal}(K/K_0)$ の部分群と $K_0 \subset K$ の中間体は一対一に対応する．

2 円分体における素数の分解

各自然数 N について，素数 p が $\mathbb{Q}(\zeta_N)$ において分岐，完全分解する条件を調べる（ここで，ζ_N は 1 の原始 N 乗根である）．

命題 2.1 (不分岐であるための十分条件). $a_1, \dots, a_m$ を整数, $n_1, \dots, n_m$ を自然数とし，各 i について $\alpha_i := \sqrt[n_i]{a_i}$ とする．素数 p が $a_1, \dots, a_m, n_1, \dots, n_m$ を割らないならば，p は $\mathbb{Q}(\alpha_1, \dots, \alpha_m)$ において不分岐である．

この命題はここでは証明しない.

命題 2.2 **($\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ は $(\mathbb{Z}/N\mathbb{Z})^\times$ と見做せる).** N を自然数とする. $\sigma \in \mathbb{Q}(\zeta_N)/\mathbb{Q})$ に対し, $\sigma(\zeta_N) = \zeta_N^r$ となる整数 r が存在するので, $S_N : \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \to (\mathbb{Z}/NZ)^\times$ を, $S_N(\sigma) := \bar{r}$ として定める. ここで, $S_N(\sigma) \cdot S_N(\sigma^{-1}) = 1 \mod N$ より, S_N は well-defined であることに注意する. S_N は同形写像であることが確かめられる(「数論 2」ではフロベニウス置換の存在によって全射性を示しているが, それを待たずに簡単にわかる).

命題 2.3 (フロベニウス置換). L を $\mathbb{Q}$ の有限次アーベル拡大とし, p を L において不分岐な素数とする.

(1) ただ 1 つの $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ が存在し, 次を満たす：すべての $x \in O_L$ について, $\mathrm{Frob}_{p,L}(x) \equiv x^p \mod pO_L$. この σ を p の**フロベニウス置換**といい, $\mathrm{Frob}_{p,L}$ と表す.

(2) $\mathrm{Frob}_{p,L}$ の位数を f とすると, p は L において相違なる $[L:\mathbb{Q}]/f$ 個の素イデアルの積に分解する. ここで, $f \mid \#\mathrm{Gal}(L/\mathbb{Q}) = [L:\mathbb{Q}]$ であることに注意する.

(3) L' を $Q \subset L$ の中間体とする. $\mathbb{Q} \subset L'$ がガロア拡大であることに注意して, $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ に対して, $\sigma|_{L'} \in \mathrm{Gal}(L'/\mathbb{Q})$ となる対応を考えると, $\mathrm{Frob}_{p,L}$ は $\mathrm{Frob}_{p,L'}$ に対応する.

この命題はここでは証明しない.

命題 2.4. N を自然数とし, p を N を割らない素数とする. このとき, 命題 2.1 より p は $\mathbb{Q}(\zeta_N)$ において不分岐である. S_N を命題 2.2 のものとすると, $S_N(\mathrm{Frob}_{p,\mathbb{Q}(\zeta_N)}) = \bar{p}$ が成り立つ.

証明. まず, $\mathbb{Q}(\zeta_N)$ 係数の多項式 $T^N - 1 = \prod_{a=1}^N (T - \zeta_N^a)$ の両辺を微分して, $NT^{N-1} = \sum_{a=1}^N \prod_{i \neq a}(1 - \zeta_N^a)$ を得る. $T = 1$ を代入し, $N = \prod_{a=1}^{N-1}(1 - \zeta_N^a)$ を得る. 仮定より $N \notin pO_{\mathbb{Q}(\zeta_N)}$ なので, $a = 1, \ldots N-1$ に対して $1 - \zeta_N^a \notin pO_{\mathbb{Q}(\zeta_N)}$ である.

さて, $\mathrm{Frob}_{p,\mathbb{Q}(\zeta_N)}$ の定義より, $\mathrm{Frob}_{p,\mathbb{Q}(\zeta_N)}(\zeta_N) \equiv \zeta^p \mod pO_{\mathbb{Q}(\zeta_N)}$ であるから, $S_N(\mathrm{Frob}_{p,\mathbb{Q}(\zeta_N)}) = r$ とおくと, $\zeta_N^p \equiv \zeta_N^r \mod pO_{\mathbb{Q}(\zeta_N)}$, すなわち, $\zeta_N^{p-r} \equiv 1 \mod pO_{\mathbb{Q}(\zeta_N)}$ を得る.

よって, $N \mid p - r$, すなわち, $p = r$ を得る. □

定理 2.5 (円分体の中間体における素数 p の分解). N を自然数とし，p を N を割らない素数とする（このとき p は $\mathbb{Q}(\zeta_N)$ において不分岐である）．L を $\mathbb{Q} \subset \mathbb{Q}(\zeta_N)$ の中間体とし，L に対応する $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ の部分群を H とする．p の $(\mathbb{Z}/N\mathbb{Z})^\times/H$ での位数を f とすると，p は L において相違なる $[\mathbb{Q}(\zeta_N):\mathbb{Q}]/f$ 個の素イデアルの積に分解する．

証明. いままでの言い換えに過ぎない． □

この命題によって，p の $\mathbb{Q}(\zeta_N)$ およびその中間体における分解の様子が mod N で判定できることがわかった．

3　2 次体における素数の分解

次の定理が基本的である．

定理 3.1. m を平方因子を含まない整数とし, $N := \begin{cases} 4|m| & m \equiv 2,3 \mod 4 \\ |m| & m \equiv 1 \mod 4 \end{cases}$ とすると，$\mathbb{Q}(\sqrt{m}) \subset \mathbb{Q}(\zeta_N)$ であり，N はこれを満たす最小の自然数である．

証明は，ガウス和を計算して 1 の N 乗根たちの四則演算で $\sqrt{m}$ を表せることを示すことによる（最小性はどう示すの？）．

定義 3.2 ($\mathbb{Q}(\zeta_m)$ に対応するディリクレ指標). m, N を定理 3.1 のものとする．アーベル拡大 $\mathbb{Q} \subset \mathbb{Q}(\sqrt{m}) \subset \mathbb{Q}(\zeta_N)$ において，$\mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) \cong \{\pm 1\}$（2 元からなる群），$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q} \cong (\mathbb{Z}/N\mathbb{Z})^\times$ である．

ここで，ディリクレ指標 $\chi_m : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$ を，$\sigma \in (\mathbb{Z}/N\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ を $\sigma\,|_{\mathbb{Q}(\sqrt{m})} \in \mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) \cong \{\pm 1\}$ に対応させるものとして定義する．

すると，$\mathbb{Q}(\sqrt{m})$ に対応する $(\mathbb{Z}/N\mathbb{Z})^\times$ の部分群は $\ker \chi_m$ となることがわかる．

$\ker \chi_m$ は，多少の計算の結果，具体的に表すことができる，

定理 3.3 ($\mathbb{Q}(\sqrt{m})$ における素数 p の分解). m, N を定理 3.1 のものとするとき，以下が成り立つ．

(1) $p \mid N \iff p$ は $\mathbb{Q}(\sqrt{m})$ で分岐する．
(2) $p \not| N$ かつ $\chi_m(p) = 1 \iff p$ は完全分解.

(3) $p \not| N$ かつ $\chi_m(p) = -1 \Longleftrightarrow p$ は惰性する (すなわち，(p) は $O_{\mathbb{Q}_{\sqrt{m}}}$の素イデアル).

(1) の証明は別に考える必要があるが，(2) 以降はこれまでの言い換えである．

4　まとめ

「p が $\mathbb{Q}(\sqrt{m})$ でどのように分解するか」という問題は「$p = x^2 + my^2 (x, y \in \mathbb{Z})$ という形に表せるか」という問題と等価なのであった．それが，今回証明しなかった類体論の諸定理からの帰結として，以上のように解決した．つまり，類体論は，こういった問題を一般化して説明する理論であると言える．