平方剰余の相互法則と
二次体での素数の分解法則の例

黒木 玄

2008 年 6 月 15 日 (日) 作成

1 平方剰余の相互法則

奇素数 p と n で割り切れない整数 n に対して Legendre 記号 $\left(\frac{n}{p}\right)$ 次のように定める:

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & (x^2 \equiv n \pmod p) \text{ を満たす整数 } n \text{ が存在する}), \\ -1 & (x^2 \equiv n \pmod p) \text{ を満たす整数 } n \text{ が存在しない}), \end{cases}$$

このとき以下が成立している.

定理 1.1 互いに異なる奇素数 p, q と p で割り切れない整数 m, n に対して

1. $\displaystyle\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$ (平方剰余の相互法則),
2. $\displaystyle\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ (第一補充法則),
3. $\displaystyle\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ (第二補充法則),
4. $\displaystyle\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$. □

2 二次体の整数環

一般に平方因子を持たない $m \in \mathbb{Z}$ に対して $\mathbb{Q}(\sqrt{m})$ の整数環 $O_{\mathbb{Q}(\sqrt{m})}$ は次のようになる:

$$O_{\mathbb{Q}(\sqrt{m})} = \begin{cases} \mathbb{Z}[\sqrt{m}] & (m \equiv 2, 3 \pmod 4)), \\ \mathbb{Z}[(1+\sqrt{m})/2] & (m \equiv 1 \pmod 4)). \end{cases}$$

たとえば

$$O_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[(1+\sqrt{5})/2], \quad O_{\mathbb{Q}(\sqrt{3})} = \mathbb{Z}[\sqrt{3}], \quad O_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}],$$
$$O_{\mathbb{Q}(\sqrt{-2})} = \mathbb{Z}[\sqrt{-2}], \quad O_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[(1+\sqrt{-3})/2], \quad O_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}].$$

3 $\mathbb{Q}(\sqrt{-5})$ の整数環 $\mathbb{Z}[\sqrt{-5}]$

命題 3.1 素数 p に対して

$$\mathbb{Z}[\sqrt{-5}]/(p) \cong \begin{cases} \mathbb{F}_2[x]/((x-1)^2) & (p=2), \\ \mathbb{F}_5[x]/(x^2) & (p=5), \\ \mathbb{F}_p^2 & (p \equiv 1,3,7,9 \pmod{20}), \\ \mathbb{F}_{p^2} & (p \equiv 11,13,17,19 \pmod{20}). \end{cases}$$

証明. 平方剰余の相互法則と第一補充法則より 5 以外の奇素数 p に対して

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{5-1}{2}}\left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right).$$

さらに

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & (p \equiv 1 \pmod 4), \\ -1 & (p \equiv 3 \pmod 4), \end{cases} \qquad \left(\frac{p}{5}\right) = \begin{cases} 1 & (p \equiv 1,4 \pmod 5), \\ -1 & (p \equiv 2,3 \pmod 5). \end{cases}$$

したがって

$$\left(\frac{-5}{p}\right) = \begin{cases} 1 & (p \equiv 1,3,7,9 \pmod{20}), \\ -1 & (p \equiv 11,13,17,19 \pmod{20}). \end{cases}$$

たとえば

$$6^2 \equiv -5 \pmod{41}, \quad 1^2 \equiv -5 \pmod 3, \quad 3^2 \equiv -5 \pmod 7, \quad 13^2 \equiv -5 \pmod{29}.$$

$p \equiv 11,13,17,19 \pmod{20}$ ならば $x^2 \equiv -5 \pmod p$ を満たす整数 x は存在しない.

環の同型定理 $(R/I)/(J/I) \cong R/J$ ($I \subset J$ は環 R の両側イデアル) より

$$\mathbb{Z}[\sqrt{-5}]/(p) \cong \mathbb{Z}[x]/(p, x^2+5) \cong \mathbb{F}_p[x]/(x^2+5).$$

よって

$$\mathbb{Z}[\sqrt{-5}]/(2) \cong \mathbb{F}_2[x]/(x^2+5) \cong \mathbb{F}_2[x]/((x-1)^2).$$

同様にして

$$\mathbb{Z}[\sqrt{-5}]/(5) \cong \mathbb{F}_5[x]/(x^2+5) \cong \mathbb{F}_5[x]/(x^2).$$

奇素数 p に対して $p \equiv 1,3,7,9 \pmod{20}$ ならば $\mathbb{F}_p[x]$ において x^2+5 は二つの異なる根 $\pm a \in \mathbb{F}_p$ を持つので

$$\mathbb{Z}[\sqrt{-5}]/(p) \cong \mathbb{F}_p[x]/(x^2+5) \cong \mathbb{F}_p[x]/((x-a)(x+a)) \cong \mathbb{F}_p^2.$$

奇素数 p に対して $p \equiv 11,13,17,19 \pmod{20}$ ならば $\mathbb{F}_p[x]$ において x^2+5 は既約なので

$$\mathbb{Z}[\sqrt{-5}]/(p) \cong \mathbb{F}_p[x]/(x^2+5) \cong \mathbb{F}_{p^2}.$$

以上によって示すべきことが示された. □

4 $\mathbb{Z}[\sqrt{-3}]$ と $\mathbb{Q}(\sqrt{-3})$ の整数環 $\mathbb{Z}[(1+\sqrt{-3})/2]$

補題 4.1 3 以外の奇素数 p に対して

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & (p \equiv 1 \pmod 3), \\ -1 & (p \equiv 2 \pmod 3). \end{cases}$$

証明. 平方剰余の相互法則と第一補充法則より 3 以外の奇素数 p に対して

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & (p \equiv 1 \pmod 3), \\ -1 & (p \equiv 2 \pmod 3). \end{cases}$$

たとえば

$$2^2 \equiv -3 \pmod 7, \quad 6^2 \equiv -3 \pmod{13}, \quad 4^2 \equiv -3 \pmod{19}.$$

$p \equiv 2 \pmod 3$ ならば $x^2 \equiv -3 \pmod p$ を満たす整数 x は存在しない. □

命題 4.2 素数 p に対して

$$\mathbb{Z}[\sqrt{-3}]/(p) \cong \begin{cases} \mathbb{F}_2[x]/((x-1)^2) & (p = 2), \\ \mathbb{F}_3[x]/(x^2) & (p = 3), \\ \mathbb{F}_p^2 & (p \equiv 1 \pmod 6), \\ \mathbb{F}_{p^2} & (p \equiv 5 \pmod 6). \end{cases}$$

証明. 環の同型定理 $(R/I)/(J/I) \cong R/J$ ($I \subset J$ は環 R の両側イデアル) より

$$\mathbb{Z}[\sqrt{-3}]/(p) \cong \mathbb{Z}[x]/(p, x^2+3) \cong \mathbb{F}_p[x]/(x^2+3).$$

よって

$$\mathbb{Z}[\sqrt{-3}]/(2) \cong \mathbb{F}_2[x]/(x^2+3) \cong \mathbb{F}_2[x]/((x-1)^2).$$

同様にして

$$\mathbb{Z}[\sqrt{-3}]/(3) \cong \mathbb{F}_3[x]/(x^2+3) \cong \mathbb{F}_3[x]/(x^2).$$

素数 p が奇数でかつ $p \equiv 1 \pmod 3$ ならば, すなわち $p \equiv 1 \pmod 6$ ならば $\mathbb{F}_p[x]$ において x^2+3 は二つの異なる根 $\pm a \in \mathbb{F}_p$ を持つので

$$\mathbb{Z}[\sqrt{-3}]/(p) \cong \mathbb{F}_p[x]/(x^2+3) \cong \mathbb{F}_p[x]/((x-a)(x+a)) \cong \mathbb{F}_p^2.$$

素数 p が奇数でかつ $p \equiv 2 \pmod 3$ ならば, すなわち $p \equiv 5 \pmod 6$ ならば $\mathbb{F}_p[x]$ において x^2+3 は既約なので

$$\mathbb{Z}[\sqrt{-3}]/(p) \cong \mathbb{F}_p[x]/(x^2+3) \cong \mathbb{F}_{p^2}.$$

以上によって示すべきことが示された. □

命題 4.3 素数 p に対して

$$\mathbb{Z}[(1+\sqrt{-3})/2]/(p) \cong \begin{cases} \mathbb{F}_{2^2} & (p = 2), \\ \mathbb{F}_3[x]/((x-1)^2) & (p = 3), \\ \mathbb{F}_p^2 & (p \equiv 1 \pmod 6), \\ \mathbb{F}_{p^2} & (p \equiv 5 \pmod 6). \end{cases}$$

証明. 記号の簡単のため $\omega = (1+\sqrt{-3})/2$ とおく. ω の $\mathbb{Q}$ 上での最小多項式は x^2+x+1 である. 環の同型定理 $(R/I)/(J/I) \cong R/J$ ($I \subset J$ は環 R の両側イデアル) より

$$\mathbb{Z}[\omega]/(p) \cong \mathbb{Z}[x]/(p, x^2+x+1) \cong \mathbb{F}_p[x]/(x^2+x+1).$$

よって

$$\mathbb{Z}[\omega]/(3) \cong \mathbb{F}_3[x]/(x^2+x+1) \cong \mathbb{F}_3[x]/((x-1)^2)$$

$\mathbb{F}_2$ 上 x^2+x+1 は既約なので

$$\mathbb{Z}[\sqrt{-3}]/(2) \cong \mathbb{F}_2[x]/(x^2+x+1) \cong \mathbb{F}_{2^2}.$$

素数 p が奇数ならば $\mathbb{F}_p$ において 2 は可逆なので x^2+3 が $\mathbb{F}_p$ に根を持つことと x^2+x+1 が $\mathbb{F}_p$ に根を持つことは同値である. さらに x^2+x+1 は重根を持たないこともすぐにわかる. 素数 p が奇数でかつ $p \equiv 1 \pmod 3$ ならば, すなわち $p \equiv 1 \pmod 3$ ならば $\mathbb{F}_p[x]$ において x^2+x+1 は二つの異なる根 $a, b \in \mathbb{F}_p$ を持つので

$$\mathbb{Z}[\sqrt{-3}]/(p) \cong \mathbb{F}_p[x]/(x^2+3) \cong \mathbb{F}_p[x]/((x-a)(x-b)) \cong \mathbb{F}_p^2.$$

素数 p が奇数でかつ $p \equiv 2 \pmod 3$ ならば, すなわち $p \equiv 5 \pmod 6$ ならば $\mathbb{F}_p[x]$ において x^2+x+1 は既約なので

$$\mathbb{Z}[\sqrt{-3}]/(p) \cong \mathbb{F}_p[x]/(x^2+x+1) \cong \mathbb{F}_{p^2}.$$

以上によって示すべきことが示された. □

注意 4.4 平方因子を持たない $m \in \mathbb{Z}$ に対する二次体 $\mathbb{Q}(\sqrt{m})$ の判別式 d を次のように定める:

$$d = \begin{cases} 4m & (m \equiv 2, 3 \pmod 4), \\ m & (m \equiv 1 \pmod 4). \end{cases}$$

このとき素数 p に対して $p \mid d$ と $O_{\mathbb{Q}(\sqrt{m})}/(p) \cong \mathbb{F}_p^2$ は同値である ([1] の定理 5.15, p.291). たとえば $-5 \equiv 3 \pmod 4$ なので $2 \mid d = -20$ であり, $\mathbb{Z}[\sqrt{-5}]/(2) \cong \mathbb{F}_2^2$ である. たとえば $-3 \equiv 1 \pmod 4$ なので $2 \nmid d = -3$ であり, $\mathbb{Z}[\sqrt{-3}]/(2) \cong \mathbb{F}_{2^2} \ncong \mathbb{F}_2^2$ である. □

参考文献

[1] 高木貞治, 初等整数論講義, 第 2 版, 共立出版, 1971, pp. 416.