第12章　補充法則と相互法則の証明

12.1　補充法則の証明

この節では，補充法則 (定理 11.7) を証明する． まず，第 1 補充法則はオイラーの規準から直ちに導かれる． 第 2 補充法則を示すために，恒等式

$$(x^2+1)^p = \sum_{j=0}^{p} {}_pC_j x^{2j} = \sum_{j=0}^{\frac{p-1}{2}} {}_pC_j x^{2j} + \sum_{k=0}^{\frac{p-1}{2}} {}_pC_{p-k} x^{2(p-k)} = \sum_{j=0}^{\frac{p-1}{2}} {}_pC_j (x^{2j} + x^{2p-2j})$$

が成り立つことに注目する（ここで，${}_pC_{p-j} = {}_pC_j$ を用いた）． これを x^p で割れば

$$(\heartsuit) \qquad \left(x+x^{-1}\right)^p = \sum_{j=0}^{\frac{p-1}{2}} {}_pC_j \left(x^{p-2j} + x^{-(p-2j)}\right).$$

一方，1 の 8 乗根 $\eta = e^{\frac{2\pi i}{8}}$ について，$\eta + \eta^{-1} = \sqrt{2}$, $\eta^3 + \eta^{-3} = -\sqrt{2}$ を確かめるのは難しくない． さらに，$\eta^8 = 1$ より，

$$\eta^n + \eta^{-n} = \begin{cases} \eta + \eta^{-1} = \sqrt{2} & (n \equiv \pm 1 \pmod 8 \text{ のとき}), \\ \eta^3 + \eta^{-3} = -\sqrt{2} & (n \equiv \pm 3 \pmod 8 \text{ のとき}). \end{cases}$$

すなわち，任意の奇数 n に対して，$\eta^n + \eta^{-n} = (-1)^{\frac{n^2-1}{8}}\sqrt{2}$ が成り立つ． そこで，η を恒等式 ($\heartsuit$) の x に代入し，両辺を $\sqrt{2}$ で割れば，

$$2^{\frac{p-1}{2}} = \sum_{j=0}^{\frac{p-1}{2}} {}_pC_j (-1)^{\frac{(p-2j)^2-1}{8}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod p.$$

これとオイラーの規準から第 2 補充法則が得られる．

12.2　ガウス和

平方剰余の相互法則 (定理 11.6) には様々なタイプの証明があるが，どれもちょっとずつ難しい． ここではガウス和による証明の概略を述べる． 前節の補充法則の証明では複素数 η (= 1 の 8 乗根) が使われたが，ここでは，奇素数 p に対して，1 の p 乗根

$$\zeta_p = e^{\frac{2\pi i}{p}} = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

を用いる．

定義 12.1 奇素数 p に対して，

$$\tau_p = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a$$

と定め，これを p に関する**ガウス和**という．

ガウス和 τ_p は，定義だけ見てもどうもよくわからない複素数だが，平方すると簡単な整数になっちゃうというのが次の定理である． これって，ちょっとびっくりだよね．

定理 12.2 p を奇素数とすると，$\tau_p^2 = (-1)^{\frac{p-1}{2}} p$ が成り立つ．

この定理の証明がこの節の目標だが，その前にいくつかの補題を準備する．

補題 12.3 奇素数 p に対して，$\left(\frac{a}{p}\right) = -1$ をみたす整数 a が存在する．

証明 $f(\alpha) = \alpha^2$ によって定義された写像 $f : (\boldsymbol{Z}/p\boldsymbol{Z})^\times \to (\boldsymbol{Z}/p\boldsymbol{Z})^\times$ は，$f(\overline{1}) = \overline{1} = f(\overline{-1})$ より単射ではないから，全射でもない． これから補題はすぐに導かれる． □

補題 12.4 p を奇素数とすると，$\displaystyle\sum_{t=1}^{p-1} \left(\frac{t}{p}\right) = 0$ が成り立つ．

証明 前補題のような整数 a をとれば，とくに a は p と素だから，$t = 1, 2, \ldots, p-1$ のとき，at の $\boldsymbol{Z}/p\boldsymbol{Z}$ における剰余類は，$\overline{1}, \overline{2}, \ldots, \overline{p-1}$ 全体にわたる． したがって，

$$\sum_{t=1}^{p-1} \left(\frac{t}{p}\right) = \sum_{t=1}^{p-1} \left(\frac{at}{p}\right) = \left(\frac{a}{p}\right) \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) = -\sum_{t=1}^{p-1} \left(\frac{t}{p}\right).$$

よってこの和は 0 であり，示したい等式を得る． □

補題 12.5 奇素数 p と整数 s に対して

$$\sum_{a=0}^{p-1} \zeta_p^{as} = \begin{cases} 0, & p \nmid s \text{ のとき}, \\ p, & p \mid s \text{ のとき} \end{cases}$$

が成り立つ．

証明 $p \mid s$ のときは明らかだから，以下，$p \nmid s$ を仮定して，和が 0 になることを示す． 恒等式 $x^p - 1 = (x-1)(x^{p-1} + \cdots + x^2 + x + 1)$ に $x = \zeta_p^s$ を代入して

$$(\zeta_p^s - 1) \left(\sum_{a=0}^{p-1} \zeta_p^{as} \right) = \zeta_p^{sp} - 1 = 0.$$

s が p の倍数ではないから $\zeta_p^s - 1 \neq 0$ であり，示したい式を得る． □

定理 12.2 の証明　まず，

$$\tau_p^2 = \left(\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^a\right)\left(\sum_{b=1}^{p-1}\left(\frac{b}{p}\right)\zeta_p^b\right) = \sum_{a=1}^{p-1}\left(\sum_{b=1}^{p-1}\left(\frac{ab}{p}\right)\zeta_p^{a+b}\right)$$

の最右辺内側の和について，$b = at$ とおけば，$b = 1, 2, \ldots, p-1$ のとき，t の $\boldsymbol{Z}/p\boldsymbol{Z}$ における剰余類は $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ 全体にわたるから，

$$\tau_p^2 = \sum_{a=1}^{p-1}\sum_{t=1}^{p-1}\left(\frac{a^2t}{p}\right)\zeta_p^{a+at} = \sum_{t=1}^{p-1}\left(\frac{t}{p}\right)\sum_{a=1}^{p-1}\zeta_p^{a(t+1)}.$$

ここで，補題 12.5 から

$$\sum_{a=1}^{p-1}\zeta_p^{a(t+1)} = \begin{cases} p-1, & t = p-1 \text{ のとき}, \\ -1, & 1 \leq t < p-1 \text{ のとき} \end{cases}$$

がわかるから，補題 12.4 より

$$\tau_p^2 = \sum_{t=1}^{p-2}\left(\frac{t}{p}\right)(-1) + \left(\frac{p-1}{p}\right)(p-1) = -\sum_{t=1}^{p-1}\left(\frac{t}{p}\right) + \left(\frac{p-1}{p}\right)p = \left(\frac{-1}{p}\right)p.$$

よって，第 1 補充法則（定理 11.7）より定理を得る． □

12.3　もっとガウス和

前節ではひとつの奇素数 p についてのガウス和 τ_p の性質を見てきたが，この節では別の奇素数 q をとって、τ_p と q がどのように絡むのかを調べる． 実際には，次の定理の証明がこの節での目標である．

定理 12.6 p, q を相異なる奇素数とすると，

$$\tau_p^{q-1} \equiv \left(\frac{q}{p}\right) \pmod{q}$$

が成り立つ．

ここで注意すべきことは，$q-1$ が偶数になるので，定理 12.2 より，$\tau_p^{q-1} \in \boldsymbol{Z}$ となることである (だって，そうじゃないと合同式の意味がわかんなくなっちゃうもん)．

さて，定理 12.6 の証明の前に，集合

$$R = \{\, f(\zeta_p) \mid f(x) \text{ は整数係数の多項式} \,\}$$

を考える． たとえば $\tau_p \in R$ である． R は和，差，積について閉じている． すなわち，R の任意の 2 元 α, β に対して $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ は R に属する． また，明らかに $\boldsymbol{Z} \subset R \cap \boldsymbol{Q}$ であるが，次の補題は逆の包含関係が成り立つことを主張している．

補題 12.7 $R \cap \boldsymbol{Q} = \boldsymbol{Z}$.

証明は少しばかり厄介なので（補遺を参照），以下，これを認めて定理 12.6 を証明する．

定理 12.6 の証明　まず，フェルマーの定理と二項定理を繰り返し用いれば，任意の整数係数多項式 $f(x)$ に対して

$$f(x)^q = f(x^q) + qg(x)$$

をみたす整数係数多項式 $g(x)$ がとれることがわかる． よって，ある $\alpha \in R$ があって

$$\tau_p^q = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^{aq} + q\alpha$$

と書くことができる． さらに，

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^{aq} = \sum_{a=1}^{p-1} \left(\frac{aq^2}{p}\right) \zeta_p^{aq} = \left(\frac{q}{p}\right) \sum_{a=1}^{p-1} \left(\frac{aq}{p}\right) \zeta_p^{aq} = \left(\frac{q}{p}\right) \tau_p$$

と変形できるから，

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

両辺に τ_p をかければ，定理 12.2 より

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

を得る． 左辺は整数だから $\alpha\tau_p \in \boldsymbol{Q}$ であるが，一方で $\alpha\tau_p \in R$ だから補題 12.7 より $\alpha\tau_p \in \boldsymbol{Z}$． よって合同式

$$\pm p \left(\tau_p^{q-1} - \left(\frac{q}{p}\right)\right) \equiv 0 \pmod q$$

が成り立つが，p, q が相異なる素数なので示したい合同式が得られる． □

12.4　相互法則の証明

定理 12.6，定理 12.2，およびオイラーの規準を順に用いて

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

を得るが，両端の辺は ± 1 だから等しくなければならず，相互法則の証明が完了する．

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆
☆　これで，この講義は終わりです　☆
☆　最後まで付き合ってくれた諸君に感謝の言葉を捧げます　☆
☆ ありがとう，Thank you，Merci，Danke schön，Grazie，Gracias，Obrigado ☆
☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆