

第13章 相互法則，補充法則の証明

13.1 補充法則の証明

この節では，定理 12.6 の証明を与える．

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，

$$(x^2 + 1)^p = \sum_{j=0}^p {}_p C_j x^{2j} = \sum_{j=0}^{\frac{p-1}{2}} {}_p C_j x^{2j} + \sum_{k=0}^{\frac{p-1}{2}} {}_p C_{p-k} x^{2(p-k)} = \sum_{j=0}^{\frac{p-1}{2}} {}_p C_j (x^{2j} + x^{2p-2j})$$

を x^p で割って得られる恒等式

$$(x + x^{-1})^p = \sum_{j=0}^{\frac{p-1}{2}} {}_p C_j (x^{p-2j} + x^{-(p-2j)})$$

を利用する．一方，1 の 8 乗根 $\beta = e^{\frac{2\pi i}{8}}$ について， $\beta + \beta^{-1} = \sqrt{2}$ ， $\beta^3 + \beta^{-3} = -\sqrt{2}$ を確かめるのは難しくない．さらに， $\beta^8 = 1$ より， $\beta^n + \beta^{-n}$ の値は n に関して 8 を法として定まるから

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

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

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

これとオイラーの規準から第 2 補充法則が得られる．

13.2 相互法則の証明

平方剰余の相互法則 (定理 12.5) は，1783 年，オイラーによって初めて提示された．その後，ルジャンドルが最初に証明を試みたが，1790 年代にガウスがその不備を指摘し完全

な証明を与えたというのが通説である. 以下の証明は, ネットで見つけた比較的新しい論文 G. Rousseau, On the quadratic reciprocity law, J. Aust. Math. Soc. Ser. A 51(1991), 423-425 を参考にしたものである.

まず, 次の補題から始めよう.

補題 13.1 p, q を相異なる奇素数とすると, $(\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times$ において

$$(\spadesuit) \quad \pm \prod_{\substack{1 \leq a < p/2 \\ 1 \leq b \leq q-1}} (\bar{a}, \bar{b}) = \prod_{\substack{1 \leq k < pq/2 \\ \gcd(k, pq) = 1}} (\bar{k}, \bar{k})$$

が成り立つ.

証明 自然な写像

$$G: (\mathbf{Z}/pq\mathbf{Z})^\times \longrightarrow (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times, \quad u + pq\mathbf{Z} \mapsto (u + p\mathbf{Z}, u + q\mathbf{Z})$$

について思い出そう. 第 7 章や第 8 章で述べたように, G は全単射, すなわち 1 対 1 の対応になっている. G の逆写像は「中国の剰余定理」によって与えられる. すなわち $(\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times$ の元 $(\bar{a}, \bar{b}) = (a + p\mathbf{Z}, b + q\mathbf{Z})$ に対して,

$$x \equiv a \pmod{p}, \quad x \equiv b \pmod{q}, \quad 1 \leq x < pq$$

をみたく $x \in \mathbf{Z}$ をとれば, $\bar{x} = x + pq\mathbf{Z} \in (\mathbf{Z}/pq\mathbf{Z})^\times$ について $G(\bar{x}) = (\bar{a}, \bar{b})$ となる. このような整数 x は (範囲を $1 \leq x < pq$ に限定しているから) 一意に定まるが, いま $\Lambda(\bar{a}, \bar{b}) \in (\mathbf{Z}/pq\mathbf{Z})^\times$ を

$$\Lambda(\bar{a}, \bar{b}) = \begin{cases} \bar{x} & \left(1 \leq x < \frac{pq}{2} \text{ のとき} \right), \\ -\bar{x} = \overline{pq - x} & \left(\frac{pq}{2} < x \leq pq - 1 \text{ のとき} \right) \end{cases}$$

と定めて, 写像

$$\Lambda: (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times \longrightarrow (\mathbf{Z}/pq\mathbf{Z})^\times$$

を定義すれば,

$$G(\Lambda(\bar{a}, \bar{b})) = G(\pm \bar{x}) = \pm G(\bar{x}) = \pm(\bar{a}, \bar{b})$$

が成り立っている. ここで, Λ 自身は単射ではない (たとえば $\Lambda(\bar{1}, \bar{1}) = \Lambda(\overline{-1}, \overline{-1})$) が, Λ を $(\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times$ の部分集合

$$S = \left\{ (\bar{a}, \bar{b}) \mid 1 \leq a < \frac{p}{2}, \quad 1 \leq b \leq q-1 \right\}$$

に制限した写像は単射であることに注意する. 実際, もし

$$\Lambda(\bar{a}, \bar{b}) = \Lambda(\bar{c}, \bar{d}), \quad 1 \leq a, c < \frac{p}{2}, \quad 1 \leq b, d \leq q-1$$

ならば,

$$(\bar{a}, \bar{b}) = \pm G(\Lambda(\bar{a}, \bar{b})) = \pm G(\Lambda(\bar{c}, \bar{d})) = \pm(\bar{c}, \bar{d})$$

であるが，ここで符号が負 $-$ とすると， $a + c \equiv 0 \pmod{p}$ かつ $0 < a + c < p$ となって矛盾するから，符号は正 $+$ ，すなわち $(\bar{a}, \bar{b}) = (\bar{c}, \bar{d})$ となり，単射性が確認できた．そこで， T を Λ による S の像

$$T = \{ \Lambda(\bar{a}, \bar{b}) \mid (\bar{a}, \bar{b}) \in S \} \subset (\mathbf{Z}/pq\mathbf{Z})^\times$$

とすれば， Λ は S から T への1対1の写像を与え，したがって

$$(\clubsuit) \quad \pm \prod_{(\bar{a}, \bar{b}) \in S} (\bar{a}, \bar{b}) = \prod_{(\bar{a}, \bar{b}) \in S} G(\Lambda(\bar{a}, \bar{b})) = \prod_{\xi \in T} G(\xi)$$

となる．ここで， T は具体的に

$$T = \left\{ \bar{k} \in (\mathbf{Z}/pq\mathbf{Z})^\times \mid 1 \leq k < \frac{pq}{2}, \gcd(k, pq) = 1 \right\}$$

で与えられる．なぜなら， T は Λ の像であり，それが右辺に含まれることは Λ の定義を見れば明らか，さらに，右辺の元の個数

$$\frac{\varphi(pq)}{2} = \frac{(p-1)(q-1)}{2}$$

が， S (したがって T) の元の個数に等しいからである．このことを用いれば， (\clubsuit) から $(\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times$ における等式 (\spadesuit) が導かれることは難しくない．

—— 相互法則の証明始まり ——

以下において (\spadesuit) の両辺それぞれの積を計算してみよう．

まず，左辺について考える． $\mathbf{Z} \times \mathbf{Z}$ において

$$\prod_{\substack{1 \leq a < p/2 \\ 1 \leq b < q-1}} (a, b) = \left(\left(\left(\frac{p-1}{2} \right)! \right)^{q-1}, ((q-1)!)^{\frac{p-1}{2}} \right)$$

であるが，

$$\begin{aligned} (p-1)! &= 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \left(p - \frac{p-1}{2} \right) \cdots (p-2) \cdot (p-1) \\ &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2} \right) \cdots (-2) \cdot (-1) \\ &= \left(\left(\frac{p-1}{2} \right)! \right)^2 (-1)^{\frac{p-1}{2}} \pmod{p} \end{aligned}$$

より

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

だから，

$$(\spadesuit) \text{ の左辺} = \pm \left(\overline{((p-1)!)^{\frac{q-1}{2}} (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}}, \overline{((q-1)!)^{\frac{p-1}{2}}} \right)$$

が得られる.

次に, (♠) の右辺, すなわち

$$1 \leq k \leq \frac{pq-1}{2}, \quad \gcd(k, pq) = 1$$

をみだすすべての k の積を計算するために, まず, 1 から $(pq-1)/2$ のうち p, q の倍数すべてがそれぞれ

$$p, 2p, \dots, \frac{q-1}{2}p \quad \text{および} \quad q, 2q, \dots, \frac{p-1}{2}q$$

であり, これらに共通部分はないことに注意する. そこで, はじめに p の倍数を除いた 1 から $(pq-1)/2$ の整数の積を考え, 次にそれを q の倍数の積で割ることで, (♠) の右辺の左成分が

$$\frac{\left(\prod_{n=1}^{p-1} n\right) \left(\prod_{n=1}^{p-1} (n+p)\right) \cdots \left(\prod_{n=1}^{p-1} \left(n + \left(\frac{q-1}{2} - 1\right)p\right)\right) \left(\prod_{n=1}^{\frac{p-1}{2}} \left(n + \frac{q-1}{2}p\right)\right)}{q \cdot (2q) \cdot (3q) \cdots \left(\frac{p-1}{2}q\right)}$$

と表わされることがわかる. p を法として分子, 分母を計算すれば,

$$\text{分子} \equiv ((p-1)!)^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!, \quad \text{分母} \equiv q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}$$

であり, オイラーの規準 (定理 12.2) を援用すれば, (♠) の右辺の左成分が

$$\prod_{\substack{1 \leq k < pq/2 \\ \gcd(k, pq) = 1}} k \equiv ((p-1)!)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}.$$

と計算される. p, q の役割を置き換えれば, 右成分も同様に計算でき,

$$\text{(♠) の右辺} = \left(\overline{((p-1)!)^{\frac{q-1}{2}} \left(\frac{q}{p}\right)}, \overline{((q-1)!)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)} \right)$$

が得られた.

そこで, 先に計算した (♠) の左辺とあわせれば, 等式 (♠) は

$$\pm(-1)^{\frac{p-1}{2} \frac{q-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}, \quad \pm 1 \equiv \left(\frac{p}{q}\right) \pmod{q} \quad (\text{複号同順})$$

と同値であることがわかる. 各項はすべて ± 1 なので合同式は等式で置き換えられ, それらから直ちに相互法則

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

が導かれる.

—— 証明終わり ——

ちょっと難しかったかな?

拙い講義を聴いてくれてありがとう.

聴いてなかった奴には「損したね」と捨て台詞を吐いておこう.