第13章　相互法則の証明

13.1　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．ガウスはこの法則の重要性に気付き，6 種類の異なる証明を出版し，さらに遺稿にもいくつかの異なる証明を遺している．その後も多くの数学者によって改良が重ねられ，現在 200 以上の証明が知られている．

以下の証明は，ネットで見つけた比較的新しい論文

[著者]　G. Rousseau

[題名]　On the quadratic reciprocity law

[掲載誌]　J. Aust. Math. Soc. Ser. A 51(1991), 423–425(短かっ！)

を参考にしたもので，論文の最後のコメントによれば，ガウスの第 5 証明の亜種との由．少しハードルが高いかもしれないけど，ぜひトライして数学科じゃない彼氏や彼女に自慢して欲しい (って意味ないか？)．

まず，

$$(\boldsymbol{Z}/p\boldsymbol{Z})^{\times} \times (\boldsymbol{Z}/q\boldsymbol{Z})^{\times} = \left\{ (\overline{a},\overline{b}) \mid 1 \leq a < p,\ \ 1 \leq b < q,\ \ \gcd(a,p) = \gcd(b,q) = 1 \right\}$$

のいくつかの元の積に関する次の補題を示す．

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

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

が成り立つ．

証明　自然な写像

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

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 $(\boldsymbol{Z}/p\boldsymbol{Z})^\times \times (\boldsymbol{Z}/q\boldsymbol{Z})^\times$ の元 $(\overline{a},\overline{b}) = (a+p\boldsymbol{Z}, b+q\boldsymbol{Z})$ に対して，

$$x \equiv a \pmod{p}, \qquad x \equiv b \pmod{q}, \qquad 1 \le x < pq$$

をみたす $x \in \boldsymbol{Z}$ をとれば，$\overline{x} = x + pq\boldsymbol{Z} \in (\boldsymbol{Z}/pq\boldsymbol{Z})^\times$ について

$$G(\overline{x}) = (\overline{a},\overline{b})$$

となる．このような整数 x は（範囲を $1 \le x < pq$ に限定しているから）一意的に定まるが，いま $\Lambda(\overline{a},\overline{b}) \in (\boldsymbol{Z}/pq\boldsymbol{Z})^\times$ を

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

と定めて，写像

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

を定義すれば，

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

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 $\Lambda(\overline{1},\overline{1}) = \Lambda(\overline{-1},\overline{-1})$）が，$\Lambda$ を $(\boldsymbol{Z}/p\boldsymbol{Z})^\times \times (\boldsymbol{Z}/q\boldsymbol{Z})^\times$ の部分集合

$$S = \left\{ \ (\overline{a},\overline{b}) \ \middle| \ 1 \le a < \frac{p}{2}, \ \ 1 \le b \le q-1 \ \right\}$$

に制限した写像は単射であることに注意する．実際，もし

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

ならば，

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

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 $(\overline{a},\overline{b}) = (\overline{c},\overline{d})$ となり，単射性が確認できた．そこで，T を Λ による S の像

$$T = \left\{ \ \Lambda(\overline{a},\overline{b}) \mid (\overline{a},\overline{b}) \in S \ \right\} \subset (\boldsymbol{Z}/pq\boldsymbol{Z})^\times$$

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

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

となる．ここで，T は具体的に

$$T = \left\{ \ \overline{k} \in (\boldsymbol{Z}/pq\boldsymbol{Z})^\times \ \middle| \ 1 \le k < \frac{pq}{2}, \ \gcd(k,pq) = 1 \ \right\}$$

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，(♣) から $(\boldsymbol{Z}/p\boldsymbol{Z})^\times \times (\boldsymbol{Z}/q\boldsymbol{Z})^\times$ における等式 (♠) 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 (♠) 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． $\boldsymbol{Z}\times\boldsymbol{Z}$ において

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

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

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

だから，

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

が得られる．

次に，(♠) の右辺，すなわち

$$1\le k\le\frac{pq-1}{2},\qquad \gcd(k,pq)=1$$

をみたすすべての 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

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

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，

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

であり，オイラーの規準（定理 12.4）を援用すれば，(♠) の右辺の左成分が

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

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．

以上により，等式 (♠) は

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

と同値であるが，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．