第13章　第２補充法則，相互法則の証明

13.1　第２補充法則の証明

第２補充法則（定理 12.5 の後半）を証明するためには，12.2 節の最後に述べたように，奇素数 p に関する「ものすごい等式」

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

を確かめればよい．そのために，複素数

$$z = e^{\frac{2\pi i}{8}} = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{1+i}{\sqrt{2}}$$

を用いる．等式 $z + z^{-1} = \sqrt{2}$ および $z^2 + z^{-2} = 0$ を確かめるのは難しくない．はじめの等式から

$$2^{\frac{p-1}{2}} = \sqrt{2}^{p-1} = \frac{(z+z^{-1})^p}{\sqrt{2}} = \frac{1}{\sqrt{2}} \sum_{j=0}^{p} {}_pC_j z^{p-j} z^{-j} = \frac{1}{\sqrt{2}} \sum_{j=0}^{p} {}_pC_j z^{p-2j}.$$

ここで，$j = 0, 1, 2, \cdots, p$ に対する $p - 2j$ の値を見てみると，

j	0	1	2	$\cdots$	$\frac{p-1}{2}$	$\frac{p+1}{2}$	$\cdots$	$p-2$	$p-1$	p
$p-2j$	p	$p-2$	$p-4$	$\cdots$	1	-1	$\cdots$	$-(p-4)$	$-(p-2)$	$-p$

であり，${}_pC_j = {}_pC_{p-j}$ に注意して，表の左半分と右半分を真ん中で折りたたむようにしてまとめると

$$2^{\frac{p-1}{2}} = \frac{1}{\sqrt{2}} \sum_{j=0}^{\frac{p-1}{2}} {}_pC_j \left(z^{p-2j} + z^{-(p-2j)} \right)$$

を得る．よって,「ものすごい等式」は次の補題から導かれる．

補題 13.1 任意の奇数 k に対して，$z^k + z^{-k} = (-1)^{\frac{k^2-1}{8}} \sqrt{2}$ が成り立つ．

証明　$z^2 + z^{-2} = 0$ に注意すれば，任意の整数 k に対して

$$z^{k+4} + z^{-(k+4)} = (z^{k+2} + z^{-(k+2)})(z^2 + z^{-2}) - (z^k + z^{-k}) = -(z^k + z^{-k}),$$

よって，$z^{k+8}+z^{-(k+8)}=z^k+z^{-k}$ となるから，z^k+z^{-k} の値は k に関して 8 を法として定まる． さらに，$z+z^{-1}=\sqrt{2}$ からはじめて，$k=-1,1,3$ をあてはめれば，

$$z^k+z^{-k}=\begin{cases}\sqrt{2} & (k\equiv 1,7 \pmod 8 \text{ のとき}),\\ -\sqrt{2} & (k\equiv 3,5 \pmod 8 \text{ のとき})\end{cases}$$

が確かめられ，補題の等式を得る． □

以上の証明は，青木 昇 著「素数と 2 次体の整数論」共立出版 (2012) (出たばっか!) から採った．

13.2　相互法則の証明

平方剰余の相互法則（定理 12.6）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 [G. Rousseau, On the quadratic reciprocity law, J. Aust. Math. Soc. Ser. A 51(1991), 423–425(短い!)] 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 (って無意味か?)．

—— 証明はここから ——

相異なる奇素数 p,q に対する自然な写像

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

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，

$$x\equiv a \pmod p,\quad x\equiv b \pmod q,\quad 1\le x<pq$$

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 は一意的に定まるが，いま

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

とおいて，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 対応を与え，

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

となる． さらに，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 が右辺に含まれることは Λ の定義を見れば明らかであり，右辺の元の個数 $\varphi(pq)/2 = (p-1)(q-1)/2$ が，S (したがって T) の元の個数に等しいからである． よって $(\clubsuit)$ から $(\boldsymbol{Z}/p\boldsymbol{Z})^\times \times (\boldsymbol{Z}/q\boldsymbol{Z})^\times$ における等式

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

が導かれる． 以下において，$(\spadesuit)$ の両辺の積をそれぞれ計算してみよう． まず，$\boldsymbol{Z} \times \boldsymbol{Z}$ 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，

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

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，

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

一方，(♠) の右辺，すなわち

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

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，

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

であり，オイラーの規準（定理 12.4）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，

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

したがって，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．