第14章　ガウス和，相互法則の別証明

14.1　ガウス和

前にも述べたように，平方剰余の相互法則には様々なタイプの証明があるが，この章ではガウス和による証明の概略を述べる．

自然数 n に対して，$\zeta_n = e^{\frac{2\pi i}{n}} = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$ とする．

補題 14.1 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

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

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．　□

補題 14.2 奇素数 p に対して，$\left(\dfrac{a}{p}\right) = -1$ をみたす整数 a が存在する．

証明　写像 $f:(\boldsymbol{Z}/p\boldsymbol{Z})^\times \to (\boldsymbol{Z}/p\boldsymbol{Z})^\times$ を $f(\alpha)=\alpha^2$ によって定義する．もし，すべての a $(1\leq a\leq p-1)$ に対して $\left(\dfrac{a}{p}\right)=1$ ならば，f は全射である．$(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ は有限集合なので f は単射でもあるはずだが，$f(\overline{1})=\overline{1}=f(\overline{-1})$ および $\overline{1}\neq\overline{-1}$ より矛盾である．□

補題 14.3 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，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．□

定義 14.4 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．

命題 14.5 p を奇素数とすると，$\tau_p^2 = (-1)^{\frac{p-1}{2}} p$ が成り立つ．

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，

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

ここで，補題 14.1 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 14.3 より

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

よって，第 1 補充法則（定理 12.7）より命題を得る．□

14.2　相互法則の別証明

まず，q が奇素数なので，命題 14.5 より，τ_p^{q-1} は整数であることに注意する．命題 14.5 とオイラーの規準より

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

よって，以下に示す命題 14.6 より

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

両辺とも ± 1 だから等号が成り立ち，相互法則の証明が完了する．

命題 14.6 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．

証明 集合

$$R = \{\, c_0 + c_1\zeta_p + c_2\zeta_p^2 + \cdots + c_{p-1}\zeta_p^{p-1} \mid c_0, c_1, \ldots, c_{p-1} \in \boldsymbol{Z} \,\}$$

を考える． R は次の性質をもつ．

(R1) R は和，差，積について閉じている; すなわち，$\alpha, \beta \in R \Rightarrow \alpha+\beta, \alpha-\beta, \alpha\beta \in R$.

(R2) $R \cap \boldsymbol{Q} = \boldsymbol{Z}$.

(R1) は簡単に確かめられるが，(R2) の証明はかなり難しい． ここでは，これらを認めて証明を続ける． さて，2 項定理を繰り返し用いれば，一般に

$$(x_1 + \cdots + x_n)^q = x_1^q + \cdots + x_n^q + qf(x_1, \ldots, x_n),$$

が成り立つことがわかる（ただし，$f(x_1, \ldots, x_n)$ は整数を係数とする $x_1, \ldots, x_n$ の多項式）． したがって，(R1) より，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，

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

ここで，命題 14.5 より $\tau_p^2 = \pm p$ であり，これは q と互いに素だから，$\tau_p^2 x + qy = 1$ をみたす整数 x, y がとれる． よって，

$$\tau_p^{q-1} - \left(\frac{q}{p}\right) = (\tau_p^2 x + qy)\left(\tau_p^{q-1} - \left(\frac{q}{p}\right)\right) = q\alpha\tau_p x + qy\left(\tau_p^{q-1} - \left(\frac{q}{p}\right)\right)$$

と計算され，$\beta = \alpha\tau_p x + y\left(\tau_p^{q-1} - \left(\frac{q}{p}\right)\right)$ とおけば，(R1) より $\beta \in R$ であって

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

とまとめられる． ここで，左辺は整数だから $\beta \in R \cap \boldsymbol{Q}$ であり，したがって (R2) より，$\beta \in \boldsymbol{Z}$． ゆえに示したい合同式が得られた． □

—— 相互法則の別証明終わり ——

最後の授業，記念写真を撮りました．

2017 年 1 月 13 日 北 1 号館 401 教室にて撮影

最後まで聴いてくれて，ありがとう，さんきゅー，めるしー，だんけ，ぐらっつぃえ，ぐらしあす，おぶりがーど，すぱしーば，しゅくらん，しぇしぇ，かむさはむにだ，…