Gauss 和を用いた
平方剰余の相互法則の証明

MATHEMATICS.PDF

2015-10-27

目次

1　有限群の指標

定義 1.1　有限群 G から乗法群 $\mathbb{C}^\times$ への準同型写像のことを G の**指標**という.

G を有限群, χ を G の指標とする. G の単位元を 1_G で表し, $n = |G|$ とおく. このとき, 任意の $g \in G$ に対して, χ が準同型写像であることを用いて計算すると,

$$\chi(g)^n = \chi(g^n) = \chi(1_G) = 1.$$

ゆえに, $\chi(g)$ は 1 の n 乗根である. また,

$$|\chi(g)|^n = |\chi(g)^n| = |1| = 1$$

より, $|\chi(g)| = 1$. さらに, 複素数の絶対値の定義より

$$\chi(g)\overline{\chi(g)} = |\chi(g)|^2 = 1$$

であるから, $\chi(g)^{-1} = \overline{\chi(g)}$ である.

$a \in G$ に対して $\varepsilon(a) = 1$ とおくことによって写像 $\varepsilon : G \to \mathbb{C}^\times$ を定義する. ε は G の指標になる.

定義 1.2　ε を **自明な指標** という. また, G の指標 χ が**自明**であるとは, $\chi = \varepsilon$ が成り立つことをいう.

命題 1.1　G を有限群, χ を G の指標とする. このとき,

$$\sum_{g\in G}\chi(g)=\begin{cases}0, & \chi\neq\varepsilon \text{ のとき},\\ |G|, & \chi=\varepsilon \text{ のとき}\end{cases}$$

が成り立つ.

証明　$\chi\neq\varepsilon$ のとき, ある $h\in G$ が存在して, $\chi(h)\neq 1$ が成り立つ. g が G のすべての元を動くとき, gh も G のすべての元を動くから,

$$\chi(h)\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(g)\chi(h)=\sum_{g\in G}\chi(gh)=\sum_{g\in G}\chi(g).$$

よって,

$$(\chi(h)-1)\sum_{g\in G}\chi(g)=0.$$

$\chi(h)\neq 1$ だったから, 求める等式が得られる.

$\chi=\varepsilon$ のとき,

$$\sum_{g\in G}\varepsilon(g)=\sum_{g\in G}1=|G|$$

となる. □

有限群 G の指標 χ と $a\in G$ に対して

$$\overline{\chi}(a)=\overline{\chi(a)}$$

とおくことによって写像 $\overline{\chi}: G\to\mathbb{C}^\times$ を定義する. $\overline{\chi}$ もまた G の指標になる.

2 Gauss 和

p を素数とする．$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ を p 個の元からなる有限体とし，$\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$ をその乗法群とする．

$\mathbb{F}_p$ の各元は法 p に関する剰余類である．表記を簡単にするため，剰余類をその代表元で表す．例えば，1 を代表元とする剰余類 $1+p\mathbb{Z}$ のことを単に 1 と書くといった具合である．

$\zeta_p = \exp(2\pi\sqrt{-1}/p)$ $(\in \mathbb{C}^\times)$ とおく．また，$x \in \mathbb{F}_p$ に対し，x_0 を x の代表元とするとき，

$$\zeta_p^x = \zeta_p^{x_0}$$

とおく．この定義は well-defined である．すなわち，代表元 x_0 の選び方に依存しない．なぜなら，x の別の代表元 x_1 をとると，$x_0 \equiv x_1 \pmod{p}$ と $\zeta_p^p = 1$ より $\zeta^{x_0} = \zeta^{x_1}$ が成り立つからである．

$\mathbb{F}_p^\times$ の自明な指標を ε で表す．ε は $\varepsilon(0) = 1$ として定義域を $\mathbb{F}_p$ へ延長する．それ以外の $\mathbb{F}_p^\times$ の指標 χ は $\chi(0) = 0$ として定義域を $\mathbb{F}_p$ へ延長する．

些細な注意であるが，$\mathbb{F}_p^\times$ の任意の指標 χ に対して，

$$\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1.$$

また，$\chi(-1) = \pm 1 \in \mathbb{R}$ である．

乗法群 $\mathbb{F}_p^\times$ の指標 χ と $a \in \mathbb{F}_p$ に対し，

$$\tau_a(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x)\zeta_p^{ax} = \sum_{i=0}^{p-1} \chi(i)\zeta_p^{ai}$$

とおく．

定義 2.1 $\tau_a(\chi)$ を **Gauss 和**という．$\tau_1(\chi)$ のことを $\tau(\chi)$ と書く．

命題 2.1　χ を $\mathbb{F}_p^\times$ 上の指標とし, $a \in \mathbb{F}_p^\times$ とする. このとき,

$$\tau_a(\chi) = \chi(a)^{-1}\tau(\chi)$$

が成り立つ.

証明　定義から計算すると,

$$\tau_a(\chi) = \sum_{i=0}^{p-1} \chi(i)\zeta_p^{ai} = \chi(a)^{-1} \sum_{i=0}^{p-1} \chi(ai)\zeta_p^{ai}.$$

i が $\mathbb{F}_p$ のすべての元を動くとき, ai も $\mathbb{F}_p$ のすべての元を動く. よって,

$$\sum_{i=0}^{p-1} \chi(ai)\zeta_p^{ai} = \sum_{i=0}^{p-1} \chi(i)\zeta_p^{i} = \tau(\chi).$$

したがって, 求める等式が得られる. □

命題 2.2　$a \in \mathbb{F}_p^\times$ とする. このとき,

$$\tau_a(\varepsilon) = 0$$

が成り立つ.

証明　定義から直接計算すると,

$$\tau_a(\varepsilon) = \sum_{i=0}^{p-1} \varepsilon(i)\zeta_p^{ai} = \sum_{i=0}^{p-1} \zeta_p^{ai} = \frac{1-\zeta_p^{ap}}{1-\zeta_p^{a}} = 0$$

となる. □

命題 2.3 χ を $\mathbb{F}_p^\times$ 上の指標とする. このとき,

$$\tau_0(\chi) = \begin{cases} 0, & \chi \neq \varepsilon \text{ のとき}, \\ p, & \chi = \varepsilon \text{ のとき} \end{cases}$$

が成り立つ.

証明 $\chi \neq \varepsilon$ のとき, $\chi(0) = 0$ である. これと命題 1.1 より,

$$\tau_0(\chi) = \sum_{i=0}^{p-1} \chi(i) = \sum_{i=1}^{p-1} \chi(i) = 0.$$

$\chi = \varepsilon$ のとき, $\varepsilon(0) = 1$ であるから,

$$\tau_0(\varepsilon) = \sum_{i=0}^{p-1} \varepsilon(0) = \sum_{i=0}^{p-1} 1 = p.$$

□

命題 2.4 χ を $\mathbb{F}_p^\times$ 上の指標とする. このとき,

$$\overline{\tau(\chi)} = \chi(-1)\tau(\overline{\chi})$$

が成り立つ.

証明 計算すると,

$$\overline{\tau(\chi)} = \sum_{i=0}^{p-1} \overline{\chi(i)\zeta_p} = \sum_{i=0}^{p-1} \overline{\chi(i)}\zeta_p^{-i}.$$

i が $\mathbb{F}_p$ のすべての元を動くとき, $-i$ も $\mathbb{F}_p$ のすべての元を動く. よって,

$$\sum_{i=0}^{p-1} \overline{\chi(i)}\zeta_p^{-i} = \sum_{i=0}^{p-1} \overline{\chi(-i)}\zeta_p^{i} = \chi(-1)\sum_{i=0}^{p-1} \overline{\chi(i)}\zeta_p^{i}.$$

ここで, $\chi(-1) = \pm 1 \in \mathbb{R}$ であることを用いた. また,

$$\sum_{i=0}^{p-1} \overline{\chi(i)}\zeta_p^{i} = \sum_{i=0}^{p-1} \overline{\chi}(i)\zeta_p^{i} = \tau(\overline{\chi}).$$

したがって, 求める等式が得られる. □

命題 2.5 χ を $\mathbb{F}_p^\times$ 上の自明でない指標とする. このとき,

$$|\tau(\chi)| = \sqrt{p}$$

が成り立つ.

証明 $\tau(\chi)\overline{\tau(\chi)} = p$ を示せばよい. なぜなら,

$$\tau(\chi)\overline{\tau(\chi)} = p \Longrightarrow |\tau(\chi)|^2 = p \Longrightarrow |\tau(\chi)| = \sqrt{p}$$

だからである. さて,

$$\begin{aligned}\tau(\chi)\overline{\tau(\chi)} &= \left(\sum_{i=0}^{p-1} \chi(i)\zeta_p^{i}\right)\left(\sum_{j=0}^{p-1} \overline{\chi(j)\zeta_p^{j}}\right) \\ &= \left(\sum_{i=0}^{p-1} \chi(i)\zeta_p^{i}\right)\left(\sum_{j=0}^{p-1} \overline{\chi(j)}\,\overline{\zeta_p^{j}}\right).\end{aligned}$$

χ は自明な指標ではないので, $\chi(0) = 0$ である. よって,

$$\begin{aligned}\tau(\chi)\overline{\tau(\chi)} &= \left(\sum_{i=1}^{p-1}\chi(i)\zeta_p^i\right)\left(\sum_{j=1}^{p-1}\chi(j)^{-1}\zeta_p^{-j}\right)\\ &= \sum_{i=1}^{p-1}\sum_{j=1}^{p-1}\chi(ij^{-1})\zeta_p^{i-j}.\end{aligned}$$

$k = ij^{-1}$ とおくと,

$$\tau(\chi)\overline{\tau(\chi)} = \sum_{k=1}^{p-1}\sum_{j=1}^{p-1}\chi(k)\zeta_p^{(k-1)j} = \sum_{k=1}^{p-1}\chi(k)\sum_{j=1}^{p-1}\zeta_p^{(k-1)j}.$$

一方, $k = 1$ のとき

$$\sum_{j=1}^{p-1}\zeta_p^{(k-1)j} = \sum_{j=1}^{p-1}1 = p-1.$$

であり, $k \neq 1$ のとき

$$\sum_{j=0}^{p-1}\zeta_p^{(k-1)j} = \frac{1-\zeta_p^{(k-1)p}}{1-\zeta_p^{k-1}} = 0$$

より

$$\sum_{j=1}^{p-1}\zeta_p^{(k-1)j} = -1$$

であるから,

$$\tau(\chi)\overline{\tau(\chi)} = (p-1)\chi(1) - \sum_{k=2}^{p-1}\chi(k) = p - \sum_{k=1}^{p-1}\chi(k).$$

命題 1.1 と合わせれば, 求める等式が得られる. □

命題 2.6　χ を $\mathbb{F}_p^\times$ 上の自明でない指標とする．このとき，

$$\tau(\chi)\tau(\overline{\chi}) = \chi(-1)p$$

が成り立つ．

証明　命題 2.4 と命題 2.5 より，

$$p = |\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)} = \chi(-1)\tau(\chi)\tau(\overline{\chi}).$$

よって，$\chi(-1)^2 = 1$ を用いれば，

$$\chi(-1)p = \chi(-1)^2\tau(\chi)\tau(\overline{\chi}) = \tau(\chi)\tau(\overline{\chi}).$$

□

3　Legendre 記号

定義 3.1　p を奇素数，a を $p \nmid a$ なる整数とする．合同式

$$x^2 \equiv a \pmod{p}$$

が解を持つとき a を p の**平方剰余**といい，解を持たないとき**平方非剰余**という．

命題 3.1　p を奇素数とする．p の平方剰余は

$$1^2,\quad 2^2,\quad \ldots,\quad \left(\frac{p-1}{2}\right)^2$$

のいずれかに p を法として合同である．

証明　p の平方剰余 a は $1, 2, \ldots, p-1$ の平方のいずれかと p を法として合同である．ところが，

$$x^2 \equiv (p-x)^2 \pmod{p}$$

であるから，a は $1^2, 2^2, \ldots, \big((p-1)/2\big)^2$ のいずれかに p を法として合同である．　□

命題 3.2　p を奇素数とする．$1, 2, \ldots, p-1$ のうち，p の平方剰余，平方非剰余はそれぞれ $(p-1)/2$ 個ずつある．

証明　p の平方剰余の個数がちょうど $(p-1)/2$ であることを示せば十分である．命題 3.1 より，$1^2, 2^2, \ldots, \big((p-1)/2\big)^2$ がどの 2 つも p を法として合同ではないことをいえばよい．

$S = \{1, 2, \ldots, (p-1)/2\}$ とおく．任意の $a, b \in S$ に対して，

$$\begin{aligned} a^2 \equiv b^2 \pmod{p} &\Longrightarrow (a-b)(a+b) \equiv 0 \pmod{p} \\ &\Longrightarrow a-b \equiv 0 \pmod{p} \ \text{または}\ a+b \equiv 0 \pmod{p}. \end{aligned}$$

$a, b \in S$ より $0 < a + b < p$ であるから,

$$\begin{aligned} a^2 \equiv b^2 \pmod{p} &\Longrightarrow a - b \equiv 0 \pmod{p} \\ &\Longrightarrow a \equiv b \pmod{p} \\ &\Longrightarrow a = b. \end{aligned}$$

ゆえに, 1^2, 2^2, …, $\big((p-1)/2\big)^2$ はどの 2 つも p を法として合同ではない. □

奇素数 p と整数 a に対して,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & p \nmid a \text{ かつ } a \text{ が平方剰余のとき}, \\ -1, & p \nmid a \text{ かつ } a \text{ が平方非剰余のとき}, \\ 0, & p \mid a \text{ のとき} \end{cases}$$

と定める. ここで,

$$p \nmid a \Longleftrightarrow \gcd(p, a) = 1$$

であることを注意しておく.

定義 3.2 $\left(\frac{a}{p}\right)$ を **Legendre 記号**あるいは**平方剰余記号**と呼ぶ.

命題 3.3 p を奇素数, a, b を整数とする. このとき,

$$a \equiv b \pmod{p} \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

が成り立つ. 特に, p の平方剰余と合同なものはまた平方剰余であり, 平方非剰余と合同なものはまた平方非剰余である.

証明　奇素数 p と整数 a, b について, $a \equiv b \pmod{p}$ ならば, 合同式 $x^2 \equiv a \pmod{p}$ が解を持つことと合同式 $x^2 \equiv b \pmod{p}$ が解を持つこととは同値である. □

命題 3.4（Wilson の定理）　p を素数とする. このとき,

$$(p-1)! \equiv -1 \pmod{p}$$

が成り立つ.

証明　$p = 2$ の場合は明らかである. 以下, $p \neq 2$ の場合について証明する.

$S = \{1, 2, \ldots, p-1\}$ とおく. 各 $x \in S$ に対して, $\gcd(x, p) = 1$ より, ある $x^* \in S$ がただ 1 つ存在して,

$$xx^* \equiv 1 \pmod{p} \tag{1}$$

が成り立つ. このとき,

$$\begin{aligned} x = x^* &\Longrightarrow x \equiv x^* \pmod{p} \\ &\Longrightarrow x^2 \equiv xx^* \pmod{p} \\ &\Longrightarrow x^2 \equiv 1 \pmod{p} \\ &\Longrightarrow (x+1)(x-1) \equiv 0 \pmod{p} \\ &\Longrightarrow x+1 \equiv 0 \text{ または } x-1 \equiv 0 \pmod{p} \\ &\Longrightarrow x \equiv \pm 1 \pmod{p} \\ &\Longrightarrow x = 1 \text{ または } x = p-1. \end{aligned}$$

よって, 1, 2, ..., $p-1$ のうち, 1, $p-1$ 以外の $p-3$ 個の整数は 2 つずつ合同式 (1) を満たすような対 x, x^* $(x \neq x^*)$ になっている. ゆえに,

$$(p-1)! \equiv 1 \cdot (p-1) \cdot 1^{\frac{p-3}{2}} \equiv -1 \pmod{p}$$

となる. □

命題 3.5（Euler の規準） p を奇素数，a を整数とし，$\gcd(a, p) = 1$ とする．このとき，

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

が成り立つ.

証明 $S = \{1, 2, \ldots, p-1\}$ とおく．任意の $x \in S$ に対して，$\gcd(x, p) = 1$ より，ある $x^* \in S$ がただ 1 つ存在して，

$$xx^* \equiv a \pmod{p} \tag{2}$$

が成り立つ．このとき，

$$\begin{aligned} x^2 \equiv a \pmod{p} &\iff x^2 \equiv xx^* \pmod{p} \\ &\iff x \equiv x^* \pmod{p} \\ &\iff x = x^*. \end{aligned}$$

よって，

$$\begin{aligned} \left(\frac{a}{p}\right) = 1 &\iff \text{ある } x \in S \text{ が存在して, } x^2 \equiv a \pmod{p} \\ &\iff \text{ある } x \in S \text{ が存在して, } x = x^* \end{aligned}$$

が成り立つ.

$\left(\frac{a}{p}\right) = 1$ のとき，ある $x_0 \in S$ が存在して $x_0^2 \equiv a \pmod{p}$ を満たす．こ

のとき, 任意の $x \in S$ に対して,

$$\begin{aligned} x = x^* &\Longrightarrow x \equiv x^* \pmod{p} \\ &\Longrightarrow x^2 \equiv x x^* \pmod{p} \\ &\Longrightarrow x^2 \equiv a \pmod{p} \\ &\Longrightarrow x^2 \equiv x_0^2 \pmod{p} \\ &\Longrightarrow (x + x_0)(x - x_0) \equiv 0 \pmod{p} \\ &\Longrightarrow x + x_0 \equiv 0 \text{ または } x - x_0 \equiv 0 \pmod{p} \\ &\Longrightarrow x \equiv \pm x_0 \pmod{p} \\ &\Longrightarrow x = x_0 \text{ または } x = p - x_0. \end{aligned}$$

よって, 1, 2, ..., $p-1$ のうち x_0, $p - x_0$ 以外の $p-3$ 個の整数は 2 つずつ合同式 (2) を満たすような対 x, x^* $(x \neq x^*)$ になっている. ゆえに,

$$\begin{aligned} (p-1)! &\equiv x_0 \, (p - x_0) \, a^{\frac{p-3}{2}} \\ &\equiv -x_0^2 \, a^{\frac{p-3}{2}} \\ &\equiv -a^{\frac{p-1}{2}} \pmod{p}. \end{aligned}$$

Wilson の定理と合わせれば,

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

したがって, 求める等式が得られる.

$\left(\dfrac{a}{p}\right) = -1$ のとき, 任意の $x \in S$ に対して $x \neq x^*$ である. よって, 1, 2, ..., $p-1$ は 2 つずつ式 (2) を満たすような対 x, x^* $(x \neq x^*)$ になっている. その対の個数は $(p-1)/2$ なので,

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Wilson の定理と合わせれば,

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

したがって, 求める等式が得られる. □

系 3.5.1（第 1 補充法則） p を奇素数とする. このとき,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1 \pmod 4 \text{ のとき}, \\ -1, & p \equiv 3 \pmod 4 \text{ のとき} \end{cases}$$

が成り立つ.

証明 Euler の規準における $a = -1$ の場合を考えると,

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

p は奇素数であり, 両辺とも値が ± 1 であるから,

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

がいえる. □

系 3.5.2 p を奇素数, a, b を整数とし, $\gcd(a, p) = \gcd(b, p) = 1$ とする. このとき,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

が成り立つ.

証明 Euler の規準により,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p .$$

p は奇数であり, 両辺とも ± 1 であるから, 等号が成り立つ. □

命題 3.6（Gauss の補題） p を奇素数, a を整数とし, $\gcd(a, p) = 1$ とする. このとき,

$$1 \cdot a, \quad 2 \cdot a, \quad \ldots, \quad \frac{p-1}{2} \cdot a$$

を p で割ったときの剰余の中に $p/2$ よりも大きいものが n 個あったとすれば,

$$\left(\frac{a}{p}\right) = (-1)^n$$

が成り立つ.

証明 $p-1$ 個の整数

$$\pm 1, \quad \pm 2, \quad \ldots, \quad \pm\frac{p-1}{2}$$

は法 p に関する既約剰余系である. $\gcd(a, p) = 1$ だから,

$$\pm 1 \cdot a, \quad \pm 2 \cdot a, \quad \ldots, \quad \pm\frac{p-1}{2} \cdot a$$

も法 p に関する既約剰余系である.

一方, 任意の $x \in \{1, 2, \ldots, (p-1)/2\}$ に対して, xa を p で割ったときの剰余が $p/2$ より大きいことは, xa が $-1, -2, \ldots, -(p-1)/2$ のいずれかと p を法として合同なことと同値である.

よって, $1 \cdot a, 2 \cdot a, \ldots, (p-1)/2 \cdot a$ のうち $-1, -2, \ldots, -(p-1)/2$ のいずれかと合同なものの個数を n とすると,

$$(1 \cdot a) \cdot (2 \cdot a) \cdot \cdots \cdot \left(\frac{p-1}{2} \cdot a\right) \equiv (-1)^n \cdot 1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2} \pmod{p}.$$

$1\cdot 2\cdot\cdots\cdot(p-1)/2$ と p とは互いに素であるから, 両辺を $1\cdot 2\cdot\cdots\cdot(p-1)/2$ で割ると,

$$a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}.$$

Euler の規準と合わせれば, 求める等式が得られる. □

系 3.6.1（第 2 補充法則） p を奇素数とする. このとき,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \text{ のとき}, \\ -1, & p \equiv \pm 3 \pmod 8 \text{ のとき} \end{cases}$$

が成り立つ.

証明 Gauss の補題における $a = 2$ の場合を考える.

$$1\cdot 2, \quad 2\cdot 2, \quad \ldots, \quad \frac{p-1}{2}\cdot 2 = p-1$$

のうち $p/2$ より大きいものの個数を n とする.

n は, 奇数 1, 3, 5, ..., $p-2$ のうち $p/2$ より小さいものの個数に一致する. 実際,

$$1 = p - \frac{p-1}{2}\cdot 2, \quad 3 = p - \frac{p-3}{2}\cdot 2, \quad 5 = p - \frac{p-5}{2}\cdot 2,$$
$$\ldots, \quad p-4 = p-2\cdot 2, \quad p-2 = p-1\cdot 2$$

のうち $p/2$ より小さいものの個数に一致する.

よって, $(p-1)/2$ が奇数のとき,

$$n \equiv 1+3+5+\cdots+\frac{p-1}{2} \pmod 2.$$

$(p-1)/2$ が偶数のとき,

$$n \equiv 1+3+5+\cdots+\frac{p-3}{2} \pmod 2.$$

いずれにせよ,

$$\begin{aligned} n &\equiv 1+2+3+\cdots+\frac{p-1}{2} \pmod 2 \\ &= \frac{1}{2}\cdot\frac{p-1}{2}\left(\frac{p-1}{2}+1\right) = \frac{p^2-1}{8}. \end{aligned}$$

したがって, Gauss の補題から求める式を得る. □

定理 3.7（平方剰余の相互法則） p, q を奇素数とし, $p \neq q$ とする. このとき,

$$\begin{aligned} \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \\ &= \begin{cases} 1, & p \equiv 1 \pmod 4 \text{ または } q \equiv 1 \pmod 4 \text{ のとき}, \\ -1, & p \equiv q \equiv 3 \pmod 4 \text{ のとき} \end{cases} \end{aligned}$$

が成り立つ.

証明 Gauss 和を用いた証明を第 5 節にて行う. □

4 整域 $\mathbb{Z}[\zeta_p]$ について

p を素数とする. $\zeta_p = \exp(2\pi\sqrt{-1}/p)$ $(\in \mathbb{C}^\times)$ とおく. 集合

$$\mathbb{Z}[\zeta_p] = \{f(\zeta_p) \mid f(X) \in \mathbb{Z}[X]\}$$

は円の p 分体 $\mathbb{Q}(\zeta_p)$ の部分整域になる. また, $\overline{\mathbb{Z}}$ を代数的整数の全体からなる環とすると, $\zeta_p \in \overline{\mathbb{Z}}$ より $\mathbb{Z}[\zeta_p] \subseteq \overline{\mathbb{Z}}$ が直ちにいえる. したがって,

$$\mathbb{Z}[\zeta_p] \subseteq \mathbb{Q}(\zeta_p) \cap \overline{\mathbb{Z}}$$

が成り立つ (実は等号が成り立つ).

補題 4.1 p, q を素数とする．このとき，

$$q\mathbb{Z}[\zeta_p] \cap \mathbb{Z} = q\mathbb{Z}$$

が成り立つ．

証明 まず，$1 \notin q\mathbb{Z}[\zeta_p]$ を示す．もし仮に $1 \in q\mathbb{Z}[\zeta_p]$ とすると，ある $x \in \mathbb{Z}[\zeta_p]$ が存在して，

$$1 = qx.$$

$K = \mathbb{Q}(\zeta_p)$ とおくと，1, q, x はすべて K の元なので，ノルム $N_{K/\mathbb{Q}}$ をとることができて，

$$1 = N_{K/\mathbb{Q}}(1) = N_{K/\mathbb{Q}}(qx) = N_{K/\mathbb{Q}}(q)N_{K/\mathbb{Q}}(x).$$

q, x はともに代数的整数だから，$N_{K/\mathbb{Q}}(q)$, $N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$．ゆえに，

$$N_{K/\mathbb{Q}}(q) = \pm 1.$$

ところが，

$$N_{K/\mathbb{Q}}(q) = q^{[K:\mathbb{Q}]} > 1.$$

これは矛盾である．

さて，$I = q\mathbb{Z}[\zeta_p] \cap \mathbb{Z}$ とおく．I は $\mathbb{Z}$ のイデアルである．$1 \notin q\mathbb{Z}[\zeta_p]$ より $I \neq \mathbb{Z}$ であるから，

$$q\mathbb{Z} \subseteq I \subsetneq \mathbb{Z}.$$

一方，$q\mathbb{Z}$ は $\mathbb{Z}$ の極大イデアルである．したがって，$I = q\mathbb{Z}$ となる． □

系 4.1.1 p, q を素数とする．任意の $a, b \in \mathbb{Z}$ に対して，

$$a \equiv b \pmod{q\mathbb{Z}[\zeta_p]} \iff a \equiv b \pmod{q\mathbb{Z}}$$

が成り立つ．

証明 $a, b \in \mathbb{Z}$ とし，$a \equiv b \pmod{q\mathbb{Z}[\zeta_p]}$ と仮定する．補題 4.1 により，

$$a - b \in q\mathbb{Z}[\zeta_p] \cap \mathbb{Z} = q\mathbb{Z}.$$

ゆえに，$a \equiv b \pmod{q\mathbb{Z}}$．逆は明らか． □

補題 4.2 p, q を素数とする．任意の $a_1, \ldots, a_n \in \mathbb{Z}[\zeta_p]$ に対して，

$$(a_1 + \cdots + a_n)^q \equiv a_1^q + \cdots + a_n^q \pmod{q\mathbb{Z}[\zeta_p]}$$

が成り立つ．

証明 n に関する数学的帰納法により証明する．

$n = 1$ のときは明らか．$n = 2$ のとき，二項定理より

$$(a_1 + a_2)^q = \sum_{i=0}^{q} \binom{q}{i} a_1^i a_2^{q-i}.$$

一方，$i = 1, 2, \ldots, q-1$ に対して，$\binom{q}{i}$ は q の倍数である．ゆえに，求める合同式が得られる．

一般に，$n-1$ のとき正しいと仮定すると，$n = 2$ のときの結果を用いれば

$$(a_1 + \cdots + a_n)^q \equiv (a_1 + \cdots + a_{n-1})^q + a_n^q \pmod{q\mathbb{Z}[\zeta_p]}$$

がいえるから，帰納法の仮定により n のときも正しいことがいえる． □

5　平方剰余の相互法則の証明

さて, いよいよ Gauss 和を用いて平方剰余の相互法則を証明するが, その前に, 定理の主張を再記しておく.

定理 5.1（平方剰余の相互法則, 定理 3.7 の再記）　p, q を奇素数とし, $p \neq q$ とする. このとき,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$
$$= \begin{cases} 1, & p \equiv 1 \pmod 4 \text{ または } q \equiv 1 \pmod 4 \text{ のとき}, \\ -1, & p \equiv q \equiv 3 \pmod 4 \text{ のとき} \end{cases}$$

が成り立つ.

証明　奇素数 p に対して $p^* = (-1)^{\frac{p-1}{2}} p$ とおく.

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

を示せば十分である. なぜなら, 第 1 補充法則より

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

となって, 求める等式が得られるからである.

Gauss 和 $\tau(\chi)$ の χ として Legendre 記号 $\left(\frac{*}{p}\right)$ をとる. ここで, $x \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ に対し, x_0 を x の代表元とするとき,

$$\left(\frac{x}{p}\right) = \left(\frac{x_0}{p}\right)$$

とおく. この定義は代表元 x_0 の選び方に依存しない. なぜなら, x の別の代表元 x_1 をとると, $x_0 \equiv x_1 \pmod{p}$ と命題 3.3 より $\left(\dfrac{x_0}{p}\right) = \left(\dfrac{x_1}{p}\right)$ が成り立つからである. $\mathbb{F}_p^\times$ から $\mathbb{C}^\times$ への準同型写像になることも系 3.5.2 からいえるので, $\left(\dfrac{*}{p}\right)$ は $\mathbb{F}_p^\times$ の指標になる.

Legendre 記号の値は常に実数なので, $\overline{\chi} = \chi$ である. よって, 命題 2.6 と第 1 補充法則より,

$$\tau(\chi)^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p. \tag{3}$$

ゆえに,

$$\tau(\chi)^{q-1} = \tau(\chi)^{\frac{2(q-1)}{2}} = (p^*)^{\frac{q-1}{2}}.$$

Euler の規準により,

$$\tau(\chi)^{q-1} \equiv \left(\frac{p^*}{q}\right) \pmod{q\mathbb{Z}}.$$

系 4.1.1 より, $\mathbb{Z}[\zeta_p]$ において q を法として考えると,

$$\tau(\chi)^{q-1} \equiv \left(\frac{p^*}{q}\right) \pmod{q\mathbb{Z}[\zeta_p]}.$$

両辺に $\tau(\chi)$ を掛ければ,

$$\tau(\chi)^q \equiv \left(\frac{p^*}{q}\right) \tau(\chi) \pmod{q\mathbb{Z}[\zeta_p]}. \tag{4}$$

一方, 補題 4.2 より,

$$\tau(\chi)^q \equiv \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \zeta_p^{iq} = \tau_q(\chi) \pmod{q\mathbb{Z}[\zeta_p]}.$$

これと命題 2.1 を合わせれば,

$$\tau(\chi)^q \equiv \left(\frac{q}{p}\right) \tau(\chi) \pmod{q\mathbb{Z}[\zeta_p]}. \tag{5}$$

ゆえに, 2 つの式 (4), (5) から,

$$\left(\frac{q}{p}\right)\tau(\chi) \equiv \left(\frac{p^*}{q}\right)\tau(\chi) \pmod{q\mathbb{Z}[\zeta_p]}.$$

両辺に $\tau(\chi)$ を掛けると, 式 (3) より,

$$(-1)^{\frac{p-1}{2}}p\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}}p\left(\frac{p^*}{q}\right) \pmod{q\mathbb{Z}[\zeta_p]}.$$

系 4.1.1 より, $\mathbb{Z}$ において

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

p, q は異なる素数だから, $\gcd(p, q) = 1$ である. よって, 上式の両辺を $(-1)^{\frac{p-1}{2}}p$ で割ることができて,

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod{q\mathbb{Z}}.$$

q は奇数であり, Legendre 記号の値は ± 1 であるから,

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

である. □