Gauss 和と Fourier 変換

@unaoya

2017 年 12 月 12 日

1　はじめに

http://people.cs.uchicago.edu/~laci/reu02/fourier.pdf に従って、次の定理の証明を紹介する。

定理 1. k を整数 q を素数 $q \geq k^4 + 4$ とする。このとき

$$x^k + y^k = z^k$$

は $\mathbb{F}_q$ に非自明な解を持つ。

2　有限巡回群の指標

G を有限巡回群とする。

定義 1 (指標)**.** G の指標とは群準同型 $\chi : G \to \mathbb{C}^\times$ のことをいう。

自明な指標を χ_0 と書くことにする。つまり任意の $x \in G$ について $\chi_0(x) = 1$ である。

χ_1, χ_2 が共に G の指標であるとき、$\chi_1\chi_2(x) = \chi_1(x)\chi_2(x)$ と定めることで指標の積を定義できる。このようにして定まる G の指標全体の群を $\hat{G}$ とかく。

G が有限巡回群 $\mathbb{Z}/n$ であるとき、指標は $\chi_k : x \mapsto \exp(2\pi i \frac{k}{n} x)$ で与えられるもので全て。これにより $\hat{G}$ も位数 n の巡回群になることがわかる。

G の元 x を一つ取ると、これは $\hat{G}$ の指標 $f_x : \hat{G} \to \mathbb{C}^\times$ を $f_x(\chi) = \chi(x)$ により定めることができる。

補題 1. G を巡回群で χ をその指標としたとき

$$\sum_{x \in G} \chi(x) = \begin{cases} 0 & (\chi \neq \chi_0) \\ |G| & (\chi = \chi_0) \end{cases}$$

証明. $S = \sum_{x \in G} \chi(x)$ とする。$\chi(y)S = \sum_{x \in G} \chi(y)\chi(x) = \sum_{x \in G} \chi(yx) = S$ より $\chi(y) \neq 1$ なら $S = 0$ となる。 □

上で見たことから

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} 0 & (\chi \neq \chi_0) \\ |G| & (\chi = \chi_0) \end{cases}$$

も成り立つ。

$\mathbb{C}^G$ を G 上の複素数値関数全体の集合とし、$\mathbb{C}$ 線形空間とみなす。この空間に内積を

$$(f,g) = \frac{1}{n}\sum_{x\in G} f(x)\overline{g(x)}$$

とすることでこれは有限次元の Hilbert 空間となる。特に Cauchy-Schwarz 不等式が成り立つ。

補題 2. G の指標は Hilbert 空間 $\mathbb{C}^G$ の正規直交基底となる。

証明. $\hat{G}$ は位数が n で $\mathbb{C}^G$ は n 次元なので個数はあう。直交することは

$$\begin{aligned}(\chi_1,\chi_2) &= \frac{1}{n}\sum_{x\in G}\chi_1(x)\overline{\chi_2(x)} \\ &= \frac{1}{n}\sum_{x\in G}\chi_1\chi_2^{-1}(x)\end{aligned}$$

と計算すれば、上の補題から証明できる。 □

3 Fourier 変換

G を位数 n の巡回群とする。

定義 2 (Fourier 変換)**.** $f \in \mathbb{C}^G$ の Fourier 変換 $\hat{f} : \hat{G} \to \mathbb{C}^\times$ を

$$\hat{f}(\chi) = \sum_{x\in G}\chi(x)f(x)$$

と定める。また $g \in \mathbb{C}^{\hat{G}}$ の Fourier 逆変換 $\hat{g} : G \to \mathbb{C}$ を

$$g(x) = \frac{1}{n}\sum_{\chi\hat{G}} g(\chi)\chi(-x)$$

と定める。

前の補題を用いると、Fourier 逆変換公式を証明することができる。$\delta_0 \in \mathbb{C}^G$ を 0 に台を持つ特性関数とすると、$\hat{\delta}_0(\chi) = 1$ であり、Fourier 逆変換公式から

$$\delta_0 = \sum_{\chi\in\hat{G}}\chi$$

となる。

定理 2 (Plancherel 公式)**.**

$$(\hat{f},\hat{g}) = n(f,g)$$

である。特に

$$||f|| = ||\hat{f}||$$

証明. 一点 a, b に台を持つ δ 関数 δ_a, δ_b を用いて確かめると

$$(\delta_a, \delta_b) = \begin{cases} \dfrac{1}{n} & a = b \\ 0 & a \neq b \end{cases}$$

であり、また

$$\hat{\delta}_a(\chi) = \sum_{x \in G} \delta_a(x)\chi(x) = \chi(a)$$

であることから

$$(\hat{\delta}_a, \hat{\delta}_b) = \frac{1}{n} \sum_{\chi \in \hat{G}} \chi(a)\chi(b) = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$$

と計算できる。 □

4 Gauss 和

ここでは q を素数とし、$\mathbb{Z}/q = \mathbb{F}_q$ と書く。また $\mathbb{F}_q$ のかけ算を考えることで $\mathbb{F}_q - \{0\} = \mathbb{F}_q^\times$ も巡回群になることがわかる。

定義 3 (Gauss 和)**.** 加法的指標 $\chi : \mathbb{F}_p \to \mathbb{C}^\times$ と乗法的指標 $\psi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ にたいし

$$S(\chi, \psi) = \sum_{a \in \mathbb{F}_p} \chi(a)\psi(a) = \sum_{a \in \mathbb{F}_p^\times} \chi(a)\psi(a)$$

$\psi(0) = 0$ とすることで $\psi : \mathbb{F}_p \to \mathbb{C}^\times$ とみなす。

命題 1 (Gauss 和の評価)**.** ψ が非自明な時

$$|S(\chi, \psi)| = \sqrt{q}$$

証明.

$$\begin{aligned} |S(\chi, \psi)| &= \sum_{x \in G} \chi(x)\psi(x) \sum_{y \in G} \overline{\chi(y)\psi(y)} \\ &= \sum_{x, y \in G} \chi(x)\chi(-y)\psi(x)\psi(y^{-1}) \\ &= \sum_{x, y \in G^\times} \chi(x - y)\psi(xy^{-1}) \end{aligned}$$

ここで $z = xy^{-1}$ と変数変換すると

$$\begin{aligned} |S(\chi, \psi)| &= \sum_{z, y \in G^\times} \chi(yz - y))\psi(z) \\ &= \sum_{z \in G^\times} \psi(z) \sum_{y \in G^\times} \chi((z - 1)y) \end{aligned}$$

となる。さらに $z=1$ かどうかで場合分けすると、$\chi : G \to \mathbb{C}^\times$ が指標なので

$$\sum_{y\in G^\times} \chi((z-1)y) = \begin{cases} q-1 & (z=1 \text{ or } \chi=\chi_0) \\ -1 & \text{それ以外} \end{cases}$$

となる。したがって、

$$\begin{aligned} |S(\chi,\psi)| &= (q-1)\psi(1) + \sum_{z\neq 1}\psi(z)(-1) \\ &= q-1+\sum_{z\in G^\times}\psi(z)(-1)+1 = q \end{aligned}$$

となる。 □

Gauss 和と Gauss 周期の関係について。Fourier 変換

$$\hat{1}_A(\chi) = \sum_{x\in A}\chi(x)$$

において $\chi(x)=\exp(2\pi ix/p)$ で A を部分群の coset とすればよい。

命題 2. $A\subset \mathbb{F}_q^\times$ を指数 k の部分群とし $\psi_0,\dots,\psi_{k-1}$ を $\mathbb{F}_q^\times/A$ の指標全体とする。この指標から誘導される $\mathbb{F}_q^\times$ の指標も同じく $\psi_0,\dots,\psi_{k-1}$ とする。$\mathbb{F}_q$ の指標 χ にたいし

$$\hat{1}_A(\chi) = \frac{1}{k}\sum_{i=0}^{k-1} S(\chi,\psi_i)$$

証明.

$$\begin{aligned} \sum_{i=0}^{k-1} S(\chi,\psi_i) &= \sum_{i=0}^{k-1}\sum_{x\in G}\chi(x)\psi_i(x) \\ &= \sum_{x\in G}\chi(x)(\sum_{i=0}^{k-1}\psi_i(x)) \end{aligned}$$

ここで指標の和に関する公式

$$\sum_{\psi\in\hat{H}}\psi(x) = \begin{cases} |H| & (x=0) \\ 0 & (x\neq 0) \end{cases}$$

を思い出すと、

$$\sum_{i=0}^{k-1}\psi_i(a) = \begin{cases} 0 \ (a\notin A \text{ もしくは } a=0) \\ k \ (a\in A) \end{cases}$$

となる。よって

$$\sum_{i=0}^{k-1} S(\chi,\psi_i) = \sum_{x\in G}\chi(x)k1_A(x) = \hat{1}_A(x)$$

とできる。 □

部分集合 $A \subset G$ に対し

$$\Phi(A) = \max_{\chi \neq \chi_0} |\hat{1}(\chi)|$$

とする。上の二つを合わせて

定理 3. 部分群 $A \subset G^\times$ について

$$\Phi(A) < \sqrt{q}$$

証明.

$$\begin{aligned}
|\hat{1}_A(\chi)| &\leq \frac{1}{k} \sum_{\psi} |S(\chi, \psi)| \\
&\leq \frac{1}{k}(|S(\chi, \psi_0)| + \sqrt{q}(k-1))
\end{aligned}$$

となる。前に示したように $|S(\chi, \psi)| = \sqrt{q}$ であり

$$S(\chi, \psi_0) = \sum_{x \in G^\times} \chi(x) = -1$$

であることから、

$$\frac{1}{k}(|S(\chi, \psi_0)| + \sqrt{q}(k-1)) \leq \frac{1}{k}(1 + \sqrt{q}(k-1)) \leq \sqrt{q}$$

となる。 □

5 方程式の解の個数

定理 4. 部分集合 $A_1, A_2, A_3 \subset G = \mathbb{Z}/n$ に対し、N を $x_1 + x_2 + x_3 = 0, x_i \in A_i$ の解の個数とする。この時

$$|N - \frac{|A_1||A_2||A_3|}{n}| < \Phi(A_3)\sqrt{|A_1||A_2|}$$

が成り立つ。

証明.

$$\begin{aligned}
N &= \sum_{x_i \in A_i} \delta(x_1 + x_2 + x_3) \\
&= \frac{1}{n} \sum_{x_i \in A_i} \sum_{\chi \in \hat{G}} \chi(x_1 + x_2 + x_3) \\
&= \frac{1}{n} \sum_{x_i \in A_i} \chi_0(x_1 + x_2 + x_3) + \frac{1}{n} \sum_{\chi \neq \chi_0} \sum_{x_i \in A_i} \chi(x_1 + x_2 + x_3)
\end{aligned}$$

となる。χ が指標であるから $\chi(x_1 + \cdots + x_k) = \chi(x_1) \cdots \chi(x_k)$ であり、和を因数分解すると

$$\sum_{x_i \in A_{11}} \chi_0(x_1 + x_2 + x_3) = \sum_{x_i \in A_i} \chi_0(x_1)\chi_0(x_2)\chi_0(x_3) = |A_1||A_2||A_3|$$

となる。

第二項も同様に計算でき、これを評価していく。

$$
\begin{aligned}
|\sum_{\chi\neq\chi_0}\sum_{x_i\in A_i}\chi(x_1)\chi(x_2)\chi(x_3)| &= |\sum_{\chi\neq\chi_0}(\sum_{x\in G}\chi 1_{A_1}(x))(\sum_{x\in G}\chi 1_{A_2}(x))(\sum_{x\in G}\chi 1_{A_3}(x))| \\
&= |\sum_{\chi\neq\chi_0}\hat{1}_{A_1}(\chi)\hat{1}_{A_2}(\chi)\hat{1}_{A_3}(\chi)| \\
&\leq \Phi(A_3)\sum_{\chi\in\hat{G}}|\hat{1}_{A_1}(\chi)||\hat{1}_{A_2}(\chi)|
\end{aligned}
$$

と計算できる。

さらに $\mathbb{C}^G$ が Hilbert 空間なので、Cauchy-Schwarz より

$$
\begin{aligned}
\sum_{\chi\in\hat{G}}|\hat{1}_{A_1}(\chi)||\hat{1}_{A_2}(\chi)| &\leq \sqrt{(\sum_{\chi\in\hat{G}}|\hat{1}_{A_1}(\chi)|^2)(\sum_{\chi\in\hat{G}}|\hat{1}_{A_2}(\chi)|^2)} \\
&= \sqrt{n^2|A_1||A_2|}
\end{aligned}
$$

と計算できる。 □

定理 5. $k|q-1$ および部分集合 $A_1, A_2 \subset \mathbb{F}_q$ に対し、N を方程式

$$x + y = z^k \ (x \in A_1, y \in A_2, z \in \mathbb{F}_q^\times)$$

の解の個数とする。

このとき

$$|N - \frac{|A_1||A_2|(q-1)}{q}| < k\sqrt{|A_1||A_2|q}$$

が成立する。

証明. $A_3 = \{z^k \mid z \in \mathbb{F}_q^\times\}$ とし、N' を

$$x + y = u \ (x \in A_1, y \in A_2, u \in A_3)$$

の解の個数とする。$k|q-1$ なので $z^k = u$ は k 個解を持つ。したがって $N = kN'$ となる。

$$|N - \frac{|A_1||A_2||A_3|}{n}| < \Phi(A_3)\sqrt{|A_1||A_2|}$$

であり、$\Phi(A_3) < \sqrt{q}$ を使えば証明できる。 □

参考文献

http://people.cs.uchicago.edu/~laci/reu02/fourier.pdf