# 表紙について

表紙中央の図式は、ご覧の通り有名なメビウスの帯を表したもので、$R^3$内の曲面としてパラメータ表示を行うと変数r,θ$\left(-\frac{1}{2} \le r \le \frac{1}{2}, 0 \le \theta \le 2\pi\right)$を用いて$x = (1 + r\,cos(\theta/2))\,cos\,\theta\,, y = (1 + r\,cos(\theta/2))\,sin\,\theta\,, z = r\,sin(\theta/2)$と表すことができる。

また、$R^3$内の曲面 S が$C^1$-級の関数$\boldsymbol{x} = \boldsymbol{X}(s,t) = \big(X(s,t), Y(s,t), Z(s,t)\big)\ \big((s,t) \in \Omega\big)$で表されているとし、$\mathbf{f}(\boldsymbol{x}) = \big(f(\boldsymbol{x}), g(\boldsymbol{x}), h(\boldsymbol{x})\big)$を S 上で与えられた 3 次元ベクトル値関数とするとき、二重積分

$$\iint_{\Omega} \left\{ f(\boldsymbol{X}) \frac{\partial(y,z)}{\partial(s,t)} + g(\boldsymbol{X}) \frac{\partial(z,x)}{\partial(s,t)} + h(\boldsymbol{X}) \frac{\partial(x,y)}{\partial(s,t)} \right\} ds\,dt$$

を S 上の$\mathbf{f}(\boldsymbol{x})$の面積分といい、

$$\iint_{S} f(\boldsymbol{x}) dy_{\wedge} dz + g(\boldsymbol{x}) dz_{\wedge} dx + h(\boldsymbol{x}) dx_{\wedge} dy$$

と表す。

ベクトル$(\partial(y,z)/\partial(s,t)\,, \partial(z,x)/\partial(s,t)\,, \partial(x,y)/\partial(s,t))$は$\partial\boldsymbol{X}/\partial s$と$\partial\boldsymbol{X}/\partial t$の外積なので、曲面 S の法線ベクトルを表す。

この単位法線ベクトルは、

$$\mathbf{n} = \mathbf{n}(s,t) = \frac{1}{\left\{ \left(\frac{\partial(y,z)}{\partial(s,t)}\right)^2 + \left(\frac{\partial(z,x)}{\partial(s,t)}\right)^2 + \left(\frac{\partial(x,y)}{\partial(s,t)}\right)^2 \right\}^{1/2}} \left( \frac{\partial(y,z)}{\partial(s,t)}, \frac{\partial(z,x)}{\partial(s,t)}, \frac{\partial(x,y)}{\partial(s,t)} \right)$$

であり、$\mathbf{f}(\boldsymbol{x})$の面積分は、

$$\iint_{S} f dy_{\wedge} dz + g dz_{\wedge} dx + h dx_{\wedge} dy = \iint_{S} (\mathbf{f}, \mathbf{n}) dS$$

と表され、S の面積は$\iint_S (\mathbf{f}, \mathbf{n}) dS$によって与えられる。ここで、$dS = \{(\partial(y,z)/\partial(s,t))^2 + (\partial(z,x)/\partial(s,t))^2 + (\partial(x,y)/\partial(s,t))^2\}^{1/2} ds dt$は S の面要素である。

また、$\mathbf{n} = \mathbf{n}(s,t)$の方向を S の表側とし、上の式は S の表側に関する面積分とする。

これをメビウスの帯について適応する。$0 \le \theta \le 2\pi$によって定義される面要素は、メビウスの帯を$(\theta = 0, 0 \le r \le 1)$の像で定義される線分によって切り離した帯の面要素と同じである。

よって、面積分は$-2\pi \le \theta \le 0$で定義した値と、$0 \le \theta \le 2\pi$で定義した値の絶対値を付けた上での和である。(S を表す関数が連続ではないので$-2\pi \le \theta \le 2\pi$とは出来ない。)

S を、上述の方法で定義されたメビウスの帯とすると、

$$\begin{cases} x = f(r,\theta) = \left(1 + r\,cos\left(\frac{\theta}{2}\right)\right) cos\,\theta \\ y = g(r,\theta) = \left(1 + r\,cos\left(\frac{\theta}{2}\right)\right) sin\,\theta \\ z = h(r,\theta) = r\,sin\left(\frac{\theta}{2}\right) \end{cases}$$

であり、

$$\frac{\partial \mathrm{x}}{\partial \mathrm{r}} = \cos\left(\frac{\theta}{2}\right)\cos\theta \quad \frac{\partial x}{\partial \theta} = -\left(1 + r\cos\left(\frac{\theta}{2}\right)\right)\sin\theta - \frac{r}{2}\sin\left(\frac{\theta}{2}\right)\cos\theta$$
$$\frac{\partial \mathrm{y}}{\partial \mathrm{r}} = \cos\left(\frac{\theta}{2}\right)\sin\theta \quad \frac{\partial y}{\partial \theta} = \left(1 + r\cos\left(\frac{\theta}{2}\right)\right)\cos\theta - \frac{r}{2}\sin\left(\frac{\theta}{2}\right)\sin\theta$$
$$\frac{\partial \mathrm{z}}{\partial \mathrm{r}} = \sin\left(\frac{\theta}{2}\right) \qquad \frac{\partial z}{\partial \theta} = \frac{r}{2}\cos\left(\frac{\theta}{2}\right)$$

である。そして、

$$\frac{\partial(y,z)}{\partial(r,\theta)} = \det\begin{pmatrix} \frac{\partial y}{\partial r} & \frac{\partial y}{\partial \theta} \\ \frac{\partial z}{\partial r} & \frac{\partial z}{\partial \theta} \end{pmatrix} = \frac{\partial \mathrm{y}}{\partial \mathrm{r}}\frac{\partial z}{\partial \theta} - \frac{\partial y}{\partial \theta}\frac{\partial z}{\partial r} = \frac{r}{2}\sin\theta - \cos\theta\left(\frac{r}{2}\sin\theta + \sin\left(\frac{\theta}{2}\right)\right)$$
$$\frac{\partial(z,x)}{\partial(r,\theta)} = \det\begin{pmatrix} \frac{\partial z}{\partial r} & \frac{\partial z}{\partial \theta} \\ \frac{\partial x}{\partial r} & \frac{\partial x}{\partial \theta} \end{pmatrix} = \frac{\partial \mathrm{z}}{\partial \mathrm{r}}\frac{\partial x}{\partial \theta} - \frac{\partial z}{\partial \theta}\frac{\partial x}{\partial r} = -\frac{r}{2}\cos\theta - \sin\theta\left(\frac{r}{2}\sin\theta + \sin\left(\frac{\theta}{2}\right)\right)$$
$$\frac{\partial(x,y)}{\partial(r,\theta)} = \det\begin{pmatrix} \frac{\partial x}{\partial r} & \frac{\partial x}{\partial \theta} \\ \frac{\partial y}{\partial r} & \frac{\partial y}{\partial \theta} \end{pmatrix} = \frac{\partial \mathrm{x}}{\partial \mathrm{r}}\frac{\partial y}{\partial \theta} - \frac{\partial x}{\partial \theta}\frac{\partial y}{\partial r} = \cos\left(\frac{\theta}{2}\right) + r\cos^2\left(\frac{\theta}{2}\right)$$

である。

これを、面積分の式、$\iint_S (\mathbf{f},\mathbf{n})dS$に代入すると、

$$\iint_S (\mathbf{f},\mathbf{n})dS = \iint_S \left\{\left(\frac{r}{2}\sin\theta - \cos\theta\left(\frac{r}{2}\sin\theta + \sin\left(\frac{\theta}{2}\right)\right)\right)^2 + \left(-\frac{r}{2}\cos\theta - \sin\theta\left(\frac{r}{2}\sin\theta + \sin\left(\frac{\theta}{2}\right)\right)\right)^2 \right.$$
$$\left. + \left(\cos\left(\frac{\theta}{2}\right) + r\cos^2\left(\frac{\theta}{2}\right)\right)^2\right\}^{1/2} drd\theta = \iint_S \left\{\left(r\cos\left(\frac{\theta}{2}\right) + 1\right)^2 + \left(\frac{r}{2}\right)^2\right\}^{1/2} drd\theta$$

となり、これの表す値が面積となる。

## 参考文献

(笠原皓司著)『微分積分学』

# Contents

# 楕円曲線上の点の位数

中学 3 年　田代新之助

2018 年 5 月 2 日，3 日　第 73 回灘校文化祭

この記事では、楕円曲線と呼ばれる曲線上の点同士に演算を定義し，それによって成る群について考えていく．

3 次曲線 $y^2 = x^3 + ax^2 + bx + c$ の複素零点が全て異なるとき，このような曲線を楕円曲線という (正確には有理的な座標変換によって，このような曲線になる曲線が楕円曲線とよばれる)．

## 1　楕円曲線上の点がなす群

射影幾何学の基礎的な事項は文献 [2] を参考にした．

楕円曲線 $C : y^2 = f(x) = x^3 + ax^2 + bx + c$ をとる．$x = \dfrac{X}{Z}, y = \dfrac{Y}{Z}$ とおき，$y^2 = f(x)$ を同次化すると，

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3 \tag{1}$$

が得られる．無限遠直線 $Z = 0$ と $C$ は，$Z = 0$ を (1) に代入することで $X^3 = 0$ が得られるので，同次座標 $[0 : 1 : 0]$ で交わる．ゆえに，(1) の曲線は同次座標 $[0 : 1 : 0]$ である無限遠点を持つ．この点を $O$ とする．$C$ は，無限遠直線と点 $O$ で 3 重に交わり，垂直線 ($x =$ 定数) と $xy$ 平面上の 2 点と $O$ で交わり，垂直線でない直線と $xy$ 平面上の 3 点で交わる．

$C$ 上の 2 点 $P, Q$ が与えられたとき，$P$ と $Q$ を通る直線 ($P_1 = P_2$のときはその点の接線) との曲線の交点のうち $P, Q$ でないほうを $P * Q$ と表すことにする．このとき，$P * Q$ と $O$ を通る直線 ($P * Q$ を通る垂直線) とこの曲線の交点のうち $P * Q$ でないほうを $P + Q$ と定義する．

$P_1 = (x_1, y_1), P_2 = (x_2, y_2)(P_1 \neq P_2)$ を $C$ 上の点とし、$P_1 * P_2 = (x_3, y_3), P_1 + P_2 = (x_3, -y_3)$ とする．$P_1$ と $P_2$ を通る直線の方程式は，

$$y = \lambda x + \nu (\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2)$$

これを曲線の方程式に代入して，

$$(\lambda x + \nu)^2 = x^3 + ax^2 + bx + c$$

左辺を移項して整理すると，

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0$$

この $x$ についての 3 次方程式の解は $x_1, x_2, x_3$ なので，解と係数の関係より，

$$\lambda - a = x_1 + x_2 + x_3$$

ゆえに，

$$x_3 = \lambda^2 - a - x_1 - x_2, y_3 = \lambda x_3 + \nu \tag{2}$$

以降，点 $P$ の $x$ 座標を $x(P)$ と書くことにする．

**命題 1.1.** $P(x_0, y_0)$(ただし，$y_0 \neq 0$) を $C$ 上の点としたとき，$2P = P + P$ の $x$ 座標 $x(2P)$ は

$$\frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c}$$

で与えられる．

**証明.** 陰関数の微分法により $\dfrac{dy}{dx} = \dfrac{f'(x)}{2y}$ なので，$P(x_0, y_0)$ における $C$ の接線の傾き $\lambda$ は，

$$\lambda = \frac{f'(x_0)}{2y_0} = \frac{3x_0^2 + 2ax_0 + b}{2y_0}$$

よって, (2) と同様に

$$\begin{aligned} x(2P) &= \lambda^2 - a - 2x_0 \\ &= \frac{(3x_0^2 + 2ax_0 + b)^2 - 4y_0^2(a + 2x_0)}{4y_0^2} \\ &= \frac{(3x_0^2 + 2ax_0 + b)^2 - 4(x_0^3 + ax_0^2 + bx_0 + c)(a + 2x_0)}{4(x_0^3 + ax_0^2 + bx_0 + c)} \\ &= \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c} \end{aligned}$$

が得られる． □

**定理 1.2.** 上の定義で定義された演算 $+$ により，$C$ 上の点全体の集合は $O$ を単位元とする群をなす．

**証明.** $P, Q$ を $C$ 上の点とする．

$$P + O = (P * O) * O = P$$

より，$O$ が単位元であるとわかる．$P = (x, y)$ ならば，

$$P + (x, -y) = O * O = O$$

より，$-P = (x, -y)$ が $P$ の逆元であることがわかる． □

## 2　位数 2, 3 の点

1 と同様に，楕円曲線 $C$ をとる．

**定理 2.1.** $C$ 上の点 $P=(x,y)\neq O$ の位数が 2 であることと $y=0$ は同値．

**証明.** $P$ の位数が 2 であると仮定する．$2P=O$ であるから，$P=-P$．すなわち，$(x,y)=-(x,-y)$ であるので，$y=0$．逆も同様． □

**定理 2.2.** $C$ 上の点 $P=(x,y)\neq O$ の位数が 3 であることと

$$3x^4+4ax^3+6bx^2+12cx+(4ac-b^2)=0 \tag{3}$$

は同値．

**証明.** $P$ の位数が 3 であるとすると，$3P=O$ より $2P=-P$．よって，$x(2P)=x(-P)=x(P)$．逆に $x(2P)=x(P)$ を満たせば，$2P=\pm P$ であるので，$P=O$ または $3P=O$．しかし，仮定より $P\neq O$ なので，$3P=O$．よって，$P$ の位数が 3 であることと $x(2P)=x(P)$ は同値．また，定理 2.1 より $y\neq 0$ なので命題 1.1 より $x(2P)=x(P)$ と

$$x=\frac{x^4-2bx^2-8cx+b^2-4ac}{4x^3+4ax^2+4bx+4c}$$

すなわち (3) は同値． □

## 3　有限位数の有理点

楕円曲線 $C: y^2=f(x)=x^3+ax^2+bx+c(a,b,c\in\mathbb{Q})$ をとる．$X=d^2x, Y=d^3y$ とすれば，$C$ の方程式は，

$$Y^2=X^3+d^2aX^2+d^4bX+d^6c$$

これにより $a,b,c$ の分母を払うことができるので，以降は $a,b,c\in\mathbb{Z}$ と仮定する．

$f(x)$ の判別式は，

$$D=-4a^3c+a^2b^2+18abc-4b^3-27c^2$$

で与えられる．

**命題 3.1.** $f(x)$ の判別式を $D$，$\phi(x)=x^4-2bx^2-8cx+b^2-4ac$ とすると，

$$D=(3x^3-5ax^2-5bx+2ab-7c)f(x)+(-3x^2-2ax+a^2-4b)\phi(x)$$

**補題 3.2.** $P=(x,y)$ を $C$ 上の点とする．$P$ と $2P$ がともに整座標をもつ ($x$ 座標, $y$ 座標が両方整数) とき，$y=0$ または $y^2|D$

**証明.** $y\neq 0$ とする．定理 2.1 より，$2P\neq O$．$x(2P)$ が整数なので，命題より，$y^2|\phi(x)$．また，$y^2=f(x)$ であり，$3x^3-5ax^2-5bx+2ab-7c$, $-3x^2-2ax+a^2-4b$ はともに整数であるので，命題より $y^2|D$. □

$p$ を素数，$m,n(n>0,m,n$ は互いに素) を $p$ で割り切らない整数とする．このとき，任意の有理数 $a$ は一意に $\dfrac{m}{n}p^\nu$ と書ける．この $\nu$ を $a$ の位数とよび，$\mathrm{ord}(a)=\nu$ と書く．

以降，「分母」「分子」と表記したときは，既約分数におけるものであるとする．

$p$ を素数，$m,n,u,w,\mu,\sigma$ を整数 (ただし，$p\not|m,n,u,w$) としたとき，$x=\dfrac{m}{np^\mu},y=\dfrac{u}{wp^\sigma}$ と表せる $C$ 上の点 $(x,y)$ を考える．この点の座標を，$C$ の方程式に代入して，

$$\frac{u^2}{w^2p^{2\sigma}}=\frac{m^3+am^2np^\mu+bmn^2p^{2\mu}+cn^3p^{3\mu}}{n^3p^{3\mu}}$$

$p\not|u^2$ かつ $p\not|w^2$ であるので，

$$\mathrm{ord}(\frac{u^2}{w^2p^{2\sigma}})=-2\sigma$$

$\mu>0$ とする．$p\not|m$ なので，

$$p\not|m^3+am^2p^\mu+bmn^2p^2\mu+cn^3p^{3\mu}$$

よって，

$$\mathrm{ord}(\frac{m^3+am^2np^\mu+bmn^2p^{2\mu}+cn^3p^{3\mu}}{n^3p^{3\mu}})=-3\mu$$

であるから，$2\sigma=3\mu$．ゆえに，$\sigma>0$ なので，$p|w^2p^{2\sigma}$．また，$2|\mu$, $3|\sigma$ なので，ある正整数 $\nu$ を用いて，$\mu=2\nu$,$\sigma=3\nu$ と書ける．$\sigma>0$ としたときも同様に $\mu=2\nu$,$\sigma=3\nu$ と書けることが得られる．

$C(p^\nu)$ を，$p^{2\nu}$ が $x$ の分母を割り切り，$p^{3\nu}$ が $y$ を割り切る集合，すなわち，

$$C(p^\nu)=\{(x,y)\in C(\mathbb{Q})|\mathrm{ord}(x)\leq -2\nu\text{かつ }\mathrm{ord}(y)\leq -3\nu\}$$

と定義する．

$t=\dfrac{x}{y},s=\dfrac{1}{y}$ とおき，$C$ に対応する $(t,s)$ 平面上の曲線を $C_{ts}$ とすると，$C_{ts}$ の方程式は

$$s=t^3+at^2s+bts^2+cs^3$$

である．$x=\dfrac{t}{s},y=\dfrac{1}{s}$ なので，$y\neq 0$ である $C$ 上の点と $s\neq 0$ である $C_{ts}$ 上の点は 1 対 1 対応する．$(x,y)$ 平面上の直線 $y=\lambda x+\nu$ は，この方程式の両辺を $\nu y$ で割ると

$$\frac{1}{\nu}=\frac{\lambda}{\nu}\frac{x}{y}+\frac{1}{y}$$

よって，この直線は $(t,s)$ 平面上の直線 $s=-\dfrac{\lambda}{\nu}t+\dfrac{1}{\nu}$ に対応している．よって，$(t,s)$ 平面上では，原点を単位元として $(x,y)$ 平面上と同じように演算が定義できる．

**命題 3.3.** $R$ を素数 $p$ に関して $\mathrm{ord}(x)\geq 0$ を満たすような有理数全体の集合とすると，$R$ は環である．

**証明.** $a,b\in R$ とすると，$p$ で割り切れない $m,n,u,w$ と正の整数 $\mu,\sigma$ を用いて，$a=\dfrac{m}{n}p^{\mu}, b=\dfrac{u}{w}p^{\sigma}$ と書ける．このとき，

$$a+b=\frac{m}{n}p^{\mu}+\frac{u}{w}p^{\sigma}=\frac{mwp^{\mu}+nup^{\sigma}}{nw}$$

$p\not| nw$ で $mwp^{\mu}+nup^{\sigma}$ は整数なので，$a+b\in R$. また，

$$ab=\frac{m}{n}p^{\mu}\frac{u}{w}p^{\sigma}=\frac{mup^{\mu+\sigma}}{nw}$$

$p\not| nw$ で $mup^{\mu+\sigma}$ は整数なので，$ab\in R$. $0,1\in R$ であるので，$R$ は $\mathbb{Q}$ の部分環. □

**命題 3.4.** 任意の $\nu\geq 1$ に対して，$C(p^{\nu})$ は $C(\mathbb{Q})$ の部分群.

**証明.** $(x,y)$ を $C(p^{\nu})$ の元とする．このとき，ある $i\leq 0$ を用いて，$x=\dfrac{m}{np^{2(\nu+i)}}, y=\dfrac{u}{wp^{3(\nu+i)}}$ と書ける．そのとき，

$$t=\frac{x}{y}=\frac{mw}{nu}p^{\nu+i}, s=\frac{1}{y}=\frac{w}{u}p^{3(\nu+i)}$$

なので $(x,y)\in C(p^{\nu})$ であるための必要十分条件は $t\in p^{\nu}R$ かつ $s\in p^{3\nu}R$. $P_1=(t_1,s_1)$ と $P_2=(t_2,s_2)$(ただし，$P_1\neq P_2$) とする．$t_1=t_2$ のとき，原点は $O$ に対応するので，$t(P_1+P_2)=-t_1$ だから，$P_1+P_2\in C(p^{\nu})$. $t_1\neq t_2$ のとき，$s=\alpha t+\beta$ を $P_1$ と $P_2+$. $\alpha$ は $\alpha=\dfrac{s_2-s_1}{t_2-t_1}$ で与えられる．

$$\begin{aligned}s_2-s_1&=(t_2^3-t_1^3)+a(t_2^2s_2-t_1^2-t_1^2s_1)+b(t_2s_2^2-t_1s_1^2)+c(s_2^3-s_1^3)\\&=(t_2^3-t_1^3)+a\{(t_2^2-t_1^2)s_2+t_1^2(s_2-s_1)\}+b\{(t_2-t_1)s_2^2+t_1(s_2^2-s_1^2)\}+c(s_2^3-s_1^3)\end{aligned}$$

よって，

$$(t_2^3-t_1^3)+a(t_2^2-t_1^2)s_2+b(t_2-t_1)s_2^2=(s_2-s_1)-at_1^2(s_2-s_1)-bt_1(s_2^2-s_1^2)-c(s_2^3-s_1^3)$$

これを整理して，

$$(t_2-t_1)\{t_2^2+t_2t_1+t_1^2+a(t_1+t_2)s_2+bs_2^2\}=(s_2-s_1)\{1-t_1^2-bt_1(s_2+s_1)-c(s_2^2+s_2s_1+s_1^2)\}$$

ゆえに，

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_2 t_1 + t_1^2 + a(t_2 + t_1)s_2 + bs_2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_2 s_1 + s_1^2)} \tag{4}$$

陰関数の微分法より，

$$\frac{ds}{dt} = \frac{3t^2 + 2at_s + bs^2}{1 - at^2 - 2bts - 3cs^2}$$

よって，$C_{ts}$ 上の点 $P_0 = (x_0, y_0)$ の接線の傾きは，

$$\alpha = \frac{3t_1^2 + 2at_1 s + bs_1^2}{1 - at_1^2 - 2bt_1 s_1 - 3cs_1^2}$$

これは，(4) の右辺に $t_1 = t_2 = t_0$ を代入した形であるので，(4) はすべての場合に適用できる．$P_3 = (t_3, s_3)$ を $s = \alpha t + \beta$ と $C_{ts}$ の交点とする．$s = \alpha t + \beta$ を $C$ の方程式に代入して，

$$\alpha t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3$$

これを整理して，

$$(1 + a\alpha + b\alpha^2 + c\alpha^3)t^3 + (a\beta + 2b\alpha\beta + 3c\alpha^2\beta)t^2 + (b\beta^2 + 3ca\beta^2)t + c\beta = 0$$

この 3 次方程式の解は，$t_1, t_2, t_3$ なので，解と係数の関係より，

$$t_1 + t_2 + t_3 = -\frac{a\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3} \tag{5}$$

$P_1 + P_2$ は $(t_3,\ s_3)$ と $(0, 0)$ を通る直線と $C_{ts}$ の交点のうちこの 2 点でない点であるので，$(-t_3, -s_3)$ であることは明らか．$t_1, s_1, t_2, s_2 \in p^\nu R$ であるので，$\alpha$ の分子は $p^{2\nu}R$ の元．同様に

$$-at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_2 s_1 + s_1^2) \in p^{2\nu}R$$

も得られる．よって，$\alpha$ の分母は $R$ の単数．ゆえに，$\alpha \in p^{2\nu}R$.

また，$s_1 \in p^{3\nu}R, \alpha \in p^{2\nu}R, t_1 \in p^\nu R$ なので，$\beta = s_1 - \alpha t_1$ より $\beta \in p^{3\nu}R$ となる．$t_1 + t_2 + t_3$ の分母が $R$ の単数．よって，(5) より

$$t_1 + t_2 + t_3 \in p^{3\nu}R \tag{6}$$

$t_1, t_2 \in p^\nu R$ なので，$t_3 \in p^\nu R$ となり，$-t_3 \in p^\nu R$ である．これで，$C(p^\nu)$ が加法について閉じていることが示された．$O \in C(p^\nu)$ なので，$C(p^\nu)$ は $C(\mathbb{Q})$ の部分群である． □

$A - B \in p^\nu R$ であることを，$A \equiv B \pmod{p^\nu R}$ と表すことにする．このように，合同式を有理数の範囲に拡張しても同値関係であることが認められる．このとき，(6) より

$$t(P_1) + t(P_2) \equiv t(P_1 + P_2) \pmod{p^{3\nu}R}$$

よって，次の命題が得られる．

**命題 3.5.** 写像

$$C(p^\nu)/C(p^{3\nu}) \longrightarrow p^\nu R/p^{3\nu}R, P=(x,y) \longmapsto t(P)=\frac{x}{y}$$

は 1 対 1 の準同型．ただし，$O \longmapsto 0$.

**系 3.6.** 任意の素数 $p$ に対して，部分群 $C(p)$ は $O$ 以外の有限位数の点を含まない．

**証明.** $P=(x,y)$(ただし $\neq O$) を位数 $m$ の $C$ 上の点とする．このとき，$m \neq 1$．$P \in C(p)$ と仮定して矛盾を導く．

$x$ の分母が $p$ の任意の冪で割り切れることはないので，$P \in (p^\nu)$ かつ $P \notin C(p^\nu+1)$ であるような $\nu \geq 1$ が存在する．

$p \not| m$ とする．合同式

$$t(P_1+P_2) \equiv t(P_1)+t(P_2) \pmod{p^{3\nu}R}$$

を繰り返し適用すれば，

$$t(mP) \equiv mt(P) \pmod{p^{3\nu}R}$$

が得られる．$mP=O$ より，$t(mP)=t(O)=0$ である．$m$ と $p$ は互いに素なので，$m$ は $R$ の単数．よって，

$$t(P) \equiv 0 \pmod{p^{3\nu}R}$$

よって，$P \in C(p^{3\nu})$．しかし，$\nu \geq 1$ より $3\nu > \nu+1$ なので，$C(p^{3\nu}) \subset C(p^{\nu+1})$ であるから，$P \notin C(p^{\nu+1})$ に矛盾．

$p|m$ とする．このとき，$m=np$ と書ける．$P'=nP$ とすると，$P$ は位数 $m$ であるから，$P$ の位数は $p$．$C(p)$ は群なので，$P' \in C(p)$ となる．上と同様に $P' \in (p^\nu)$ かつ $P' \notin C(p^\nu+1)$ であるような $\nu > 0$ が存在する．$p \not| m$ のときと同じように

$$0=t(O)=t(pP') \equiv pt(P') \pmod{p^{3\nu}R}$$

が得られる．よって，$t(P') \equiv 0 \pmod{p^{3\nu-1}R}$．このとき，$\nu \geq 1$ より $3\nu-1 \geq \nu+1$ なので，$p \not| m$ のときと同様にして矛盾が導ける． □

**定理 3.7** (Nagell, Lutz)**.** $D$ を $f(x)$ の判別式，$P=(x,y)$ を有限位数の有理点とする．そのとき $x$ と $y$ は整数で，$y=0$ または $y^2|D$ である．

**証明.** $P$ の位数を $m$ とする．系より，$x,y$ はどんな素数でも割り切れないので，$x,y$ は整数．$2P=(X,Y)$ とすると，$2P$ の位数は $\dfrac{m}{\gcd(m,2)}$，すなわち有限位数なので，同様にして $X,Y$ が整数であることが得られる．よって，補題 3.2 より $y=0$ または $y^2|D$. □

## 4　おわりに

3 次曲線上の点の集合に群構造が表れていることが分かった．ちなみに，Nagell-Lutz の定理というと，$y^2|D$ の部分が $y|D$ である定理をさすことも多いが，補題 3.2 の段階でより強い結果が得られたので，ここでは $y^2|D$ とした．

## 参考文献

[1] J.H.Silverman, J.Tate『楕円曲線論入門』(足立恒雄・木田雅成・小松啓一・田谷久雄訳) 丸善出版，2012

[2] 川又雄二郎『射影空間の幾何学』朝倉書店，2001

# 素数定理

高校 1 年 2 組 33 番　小林晃一良

平成 31 年 4 月 10 日

## 1　はじめに

素数定理の主張は以下のとおりである.
定理 1.1(素数定理) 与えられた 自然数 $x$ 以下に存在する素数の個数を$\pi(x)$ とおいたとき

$$\pi(x) \sim \frac{x}{logx}(x \to \infty)$$

が成り立つ.($\pi(x)$ は今後同様の定義のもと用いる.)
この定理は 1792 年に当時 15 歳であった $Gauss$ によって初めて予想された. この記事ではこの定理を証明するが, 多数存在する証明法のうち今回は Newman-Zaiger による複素解析を用いたもので示す.

## 2　解析

前提知識を述べる.
定義 2.1 $\forall\epsilon > 0, \exists N, n \geq N$ となる $n$ に対して $|f_n(z) - f(z)| < \epsilon(z \in E)$ となるとき, $f_n$ は $f$ に $E$ 上で一様収束するという. また $f_n$が $f$ に $E$ 上で広義一様収束するとは $E$ に含まれる任意のコンパクト集合で $f_n$が $f$ に一様収束することをいう.
命題 2.2($Weierstrass$ の $M$ 判定法)$E$ 上の関数項級数 $\sum_{n=0}^{\infty} f_n(z)$ に対し $M_n \geq 0$ で $\forall z \in E, |f_n(z)| \leq M_n$かつ $\sum_{n=0}^{\infty} M_n < \infty$ となる数列があれば $\sum_{n=0}^{\infty} f_n(z)$ は $E$ 上で一様収束する.(但し関数項級数 $\sum_{n=0}^{\infty} f_n(z)$ が一様収束するとは部分和 $\sum_{n=0}^{n} f_n(z)$ が $\sum_{n=0}^{\infty} f_n(z)$ に一様収束することをいう.)
定理 2.3($Cauchy$ の積分定理)$f(z)$ が連結開領域 $D$ で正則であるとき $D$ 内の任意の区分的に滑らかな閉曲線 $C$ に対し

$$\int_C f(z)dz = 0$$

定理 2.4($Morera$ の定理)連結開領域 $D$ に含まれる任意の閉三角形 $T$ に対し

$$\int_{\partial T} f(z)dz = 0$$

が成り立てば $f(z)$ は $D$ で正則である.
定理 2.5($Taylor$ 展開)連結開領域 $D$ で正則な関数 $f(z)$ は領域 $D$ 内の任意の点 $c$ を定めると $z$ が $D$ に含まれる最大の円板 $U(c)$ に含まれるとき

$$f(z) = \sum_{n=0}^{\infty} a_n(z-c)^n (a_n = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n)$$

が成り立ちこれを点 $c$ を中心とした $Taylor$ 展開 という.
補題 2.6 $C$ が長さ有限の区分的 $C^1$級曲線のとき $C$ 上の連続関数 $fn$ が $f$ に一様収束していれば $lim_{n\to\infty} \int_C f_n(z)dz = \int_C f(z)dz$
(証明)$\forall \epsilon > 0, \exists N, n \geq N \Rightarrow \forall z \in C, |f_n(z) - f(z)| < \epsilon$ となる. よって

$$|\int_C f_n(z)dz - \int_C f(z)dz| \leq \int_C |f_n(z) - f(z)||dz| \leq \epsilon l(C)$$

. よって示された.
命題 2.7 領域 $D$ 上で正則な複素関数列 $(f_n)$ が $D$ で広義一様収束すれば広義一様収束極限 $f = lim_{n\to\infty} fn$ は $D$ で正則.
(証明)$\int_{\partial\Delta} f_n(z)dz$ は $D$ で正則なので $Cauchy$ の積分定理より $\int_{\partial\Delta} f_n(z)dz = 0$.また領域 $D$ 内の任意の閉三角形$\Delta$ の辺 $\partial\Delta$ はコンパクトなので $f_n$　は$\partial\Delta$上で一様収束するので補題 2.6 より $\int_{\partial\Delta} f(z)dz = lim_{n\to\infty} \int_{\partial\Delta} f_n(z)dz = 0$. よって $Morera$ の定理より $f$ は $D$ で収束.
定理 2.8(ローラン展開) $0 < r < R$ とする. このとき $f(z)$ が円環 $\{r < |z-a| < R\}$ で正則であるとき f(z) は

$$f(z) = \sum_{n=-\infty}^{\infty} c_n(z-a)^n$$

と表される.
定義 2.9(留数) $Res(f, a)$ とは関数 $f(z)$ を $a$ 周りでローラン展開した時の $c_{-1}$ の値のことである.
定義 2.10 $\sum_{n=-\infty}^{-1} c_n(z-a)^n$を $f(z)$ の $z = a$ における主要部と呼ぶ.$a$ 周りでローラン展開したときその主要部が有限和 ($c_{-k-1} = c_{-k-2} = \cdots = 0$ かつ $c_{-k} \neq 0$) で表されるとき a を位数 k の極という.
命題 2.11 $z = a$ が $f(z)$ の 1 位の極であるとき $Res(f, a) = lim_{z\to a}(z-a)f(z)$ である.
(ローラン展開をしたのち両辺に $z - a$ をかければ示される.)
定理 2.12(一致の定理)連結開領域 $D \in \mathbb{C}$ で正則な関数 $f(z), g(z)$ について $D$ の部分集合 $D'$ で $f(z) = g(z)(\forall z \in D')$ が成り立ち, $D'$が集積点をもつとき $f(z) = g(z)(\forall z \in D)$

## 3　素数定理の証明

まず関数を定義する.
定義 3.1 次の 3 つの関数を

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\Phi(s)=\sum_{p}\frac{logp}{p^s},\vartheta(x)=\sum_{p\leq x}logp$$

と定める.(但し $p$ は素数で $s\in\mathbb{C}$,$x\in\mathbb{R}$)

補題 3.2 $\alpha>0$ のとき

$$\sum_{n=1}^{\infty}\frac{1}{n^{1+\alpha}},\sum_{p}\frac{logp}{p^{1+\alpha}}$$

(但し $p$ は素数) は収束する.

(証明)

$$\sum_{n=1}^{\infty}\frac{1}{n^{1+\alpha}}=1+\sum_{n=2}^{\infty}\frac{1}{n^{1+\alpha}}\leq 1+\int_1^{\infty}\frac{1}{x^{1+\alpha}}dx=1+[-\frac{1}{\alpha x^{\alpha}}]_1^{\infty}=1+\frac{1}{\alpha}$$

よって

$$\sum_{p}\frac{logp}{p^{1+\alpha}}=\frac{2}{\alpha}\sum_{p}\frac{logp^{\frac{\alpha}{2}}}{p^{1+\alpha}}\leq\frac{2}{\alpha}\sum_{p}\frac{p^{\frac{\alpha}{2}}}{p^{1+\alpha}}\leq\frac{2}{\alpha}\sum_{n=2}^{\infty}\frac{1}{n^{1+\frac{\alpha}{2}}}\leq\frac{2}{\alpha}\frac{1}{\frac{\alpha}{2}}=\frac{4}{\alpha^2}$$

も成り立ち, これらと $\frac{1}{n^{1+\alpha}},\frac{logp}{p^{1+\alpha}}>0$ より示された.

命題 3.3 $n$ 番目に小さい素数を $P(n)$ とおき, $f_n(s)=\frac{1}{n^s},g_n(s)=\frac{logP(n)}{P(n)^s}$ としたとき関数項級数 $\sum_{n=1}^{\infty}f_n(s),\sum_{n=1}^{\infty}g_n(s)$ は $Re(s)>1$ で広義一様収束する.

(証明)$D=\{s\in\mathbb{C};Re(s)>1\}$ とおくと $D$’ $\subset D$ となるコンパクト集合 $D'$ は有界なので ($\because$ コンパクト集合 $\Leftrightarrow$ 有界閉集合)$\forall s\in D',k\leq Re(s)$ となる最大の $k$ がとれ (下限), $s\in D'$のとき $|\frac{1}{n^s}|=\frac{1}{n^{|s|}}\leq\frac{1}{n^k}$ と $|\frac{logP(n)}{P(n)^s}|=\frac{logP(n)}{P(n)^{Re(s)}}\leq\frac{logP(n)}{P(n)^k}$ が成り立つ. また $k>1$ より補題 3.2 から $\sum_{n=1}^{\infty}\frac{1}{n^k}$と $\sum_p\frac{logp}{p^k}$ は収束する. よって命題 2.2 より $\zeta(s),\Phi(s)$ は $s\in D'$ で一様収束. よってこれが $\forall D'\subset D$($D'$はコンパクト集合) に対して成立するので示された.

命題 2.7 と命題 3.3 より次が分かる.

定理 3.4 $\zeta(s),\Phi(s)$ は $Re(s)>1$ において正則関数である.

定理 3.5(Eular 積)$Re(s)>1$ のとき$\zeta(s)=\prod_p\frac{1}{1-p^{-s}}$(但し $p$ は素数)

(証明) 素因数分解の一意性より

$$\zeta(s)=\sum_{r_2,r_3,\cdots\geq 0}\frac{1}{(2^{r_2}3^{r_3}\cdots)^s}=\prod_p(\sum_{r=0}^{\infty}p^{-rs})=\prod_p\frac{1}{1-p^{-s}}$$

定理 3.6 $\zeta(s)-\frac{1}{s-1}$は $Re(s)>0$ において正則関数となるように定義できる.

(証明)$Re(s)>1$ のとき $\int_1^{\infty}\frac{1}{x^s}dx=[\frac{1}{(1-s)x^{s-1}}]_1^{\infty}=\frac{1}{s-1}$ なので

$$\zeta(s)-\frac{1}{s-1}=\sum_{n=1}^{\infty}\frac{1}{n^s}-\sum_{n=1}^{\infty}\int_n^{n+1}\frac{1}{x^s}dx=\sum_{n=1}^{\infty}\int_n^{n+1}(\frac{1}{n^s}-\frac{1}{x^s})dx$$

. また

$$|\int_n^{n+1}(\frac{1}{n^s}-\frac{1}{x^s})dx|=|\int_n^{n+1}\int_n^x\frac{s}{u^{s+1}}dudx|\leq\int_n^{n+1}\int_n^x|\frac{s}{u^{s+1}}|dudx\leq max_{n\leq u\leq n+1}|\frac{s}{u^{s+1}}|=\frac{|s|}{n^{Re(s)+1}}$$

となりこれと補題3.2より$\sum_{n=1}^{\infty}\frac{|s|}{n^{Re(s)+1}}<\infty$となることから命題2.2より$\sum_{n=1}^{\infty}\int_n^{n+1}(\frac{1}{n^s}-\frac{1}{x^s})dx$は$Re(s)>0$で一様収束する. 後は定理 3.4 の導出過程と同じようにすればよい.
定理 3.7 (Schwarz の鏡像の原理) 複素平面上の領域 $D$ が実軸上の線分を含み, 実軸に対して対称であるとする. このとき $f(z)$ が $D$ で正則で $D$ に含まれる実軸上で実数値をとるとき

$$f(\overline{z})=\overline{f(z)}(\forall z\in D)$$

が成り立つ.
(証明)$z=x+yi, f(z)=u(x,y)+iv(x,y)$ とおき,

$$F(z)=\overline{f(\overline{z})}=U(x,y)+iV(x,y)$$

とおくと,$\overline{f(\overline{z})}=u(x,-y)-iv(x.-y)$ から

$$U(x,y)=u(x,t)V(x,y)=-v(x,t)(t=-y)$$

$D$ が実軸に対して対称な形をしているので $f(x+it)=u(x,t)+iv(x,t)$ は正則関数. よって 実部 $u(x,t)$, 虚部 $v(x,t)$ は $D$ で連続な一回偏導関数を持ち $Cauchy-Riemann$ の方程式 を満たす. ここで上の関係式を用いると

$$\frac{\partial U}{\partial x}=\frac{\partial u}{\partial x}=\frac{\partial u}{\partial v}=\frac{\partial V}{\partial y}$$

$$\frac{\partial U}{\partial y}=-\frac{\partial u}{\partial t}=\frac{\partial v}{\partial x}=-\frac{\partial V}{\partial x}$$

が成り立つ. これは $U(x,y), V(x,y)$ に対する $Cauchy-Riemann$ の方程式であり $U,V$ の一回偏導関数は $u,y$ の一回偏導関数で表せるので,$D$ で連続でありよって $F(z)$ は $D$ で正則である. よって $z$ が $D$ に含まれる実軸上にある時条件より $F(z)=\overline{f(\overline{z})}=\overline{f(z)}=f(z)$ が成り立つことから一致の定理より $F(z)=f(z)(\forall z\in D)$. よって $D$ が実軸に対して対称な形をしているので $f(\overline{z})=F(\overline{z})=\overline{f(z)}$ が成り立つ.
定理 3.8 $Re(s)\geq 1$ に対して $\zeta(s)\neq 0$ である.
(証明) $Re(s)>1$ のときは定理 3.5 より従うので $Re(s)=1$ の場合を考える.$\exists t\in\mathbb{R}, \zeta(1+it)=0$ と仮定する. $|z|<1$ ならば $Re(log(1-z))=Re(-\sum_{k=1}^{\infty}\frac{z^k}{k})$ としてよく $Re(s)>1$ のとき

$$log|\zeta(s)|=log\prod_p|1-p^{-s}|^{-1}=-\sum_p log|1-p^{-s}|=\sum_p Re(-log(1-p^{-s}))=Re(\sum_p\sum_{k=1}^{\infty}\frac{1}{kp^{ks}})$$

. したがって数列 $\{c_n\}$ を

$$c_n=\begin{cases}\frac{1}{k} & (n=p^k, p\text{ は素数})\\ 0 & (otherwise)\end{cases}$$

によって定義すると,$c_n\geq 0$ であり

$$log|\zeta(s)|=Re(\sum_{n=1}^{\infty}\frac{c_n}{n^s})$$

が成立.$s=\sigma+ti$ ならば

$$\frac{c_n}{n^s}=\frac{c_n}{n^\sigma}n^{-it}=\frac{c_n}{n^\sigma}(cos(tlogn)-isin(tlogn))$$

. よって

$$log|\zeta(s)|=\sum_{n=1}^{\infty}\frac{c_n}{n^\sigma}cos(tlogn).$$

したがって補題 3.2 から $\zeta(\sigma)$ が収束することを踏まえ

$$log|\zeta(\sigma)^3\zeta(\sigma+ti)^4\zeta(\sigma+2ti)|=3log|\zeta(\sigma)|+4log|\zeta(\sigma+ti)|+log|\zeta(\sigma+2ti)|$$

$$=\sum_{n=1}^{\infty}\frac{c_n}{n^\sigma}(3+4cos(tlogn)+cos(2tlogn))=\sum_{n=1}^{\infty}\frac{c_n}{n^\sigma}2(1+cos(tlogn))^2\geq 0$$

これより $\sigma>1$ ならば

$$|\zeta(\sigma)^3\zeta(\sigma+ti)^4\zeta(\sigma+2ti)|\geq 1$$

となる. また

$$Z(\sigma)=\zeta(s)^3|\zeta(\sigma+ti)|^4|\zeta(\sigma+2ti)|^2$$

とおくと $lim\sigma\to 1+Z(\sigma)=0$. これらは $Z(\sigma)$ の連続性に矛盾.
命題 3.9 $f(t)(t\geq 0)$ を有界で局所可積分な関数とし

$$g(z)=\int_0^{\infty}f(t)e^{-zt}dt(Re(z)>0)$$

が $Re(z)\geq 0$ に正則に拡張されるとする. このとき $\int_0^{\infty}f(t)dt$ は収束し $g(0)$ に等しい.
この定理は証明なしで認めるものとする.
命題 3.10 $Re(s)\geq 1$ のとき $\Phi(s)-\frac{1}{s-1}$ は正則である.
(証明)$Re(s)>0$ のとき定理 3.5 の式の両辺の対数をとって微分すると

$$\frac{\zeta'(s)}{\zeta(s)}=\sum_p\frac{logp}{p^s-1}=\Phi(s)+\sum_p\frac{logp}{p^s(p^s-1)}\cdots(1)$$

右辺の第 2 項は $Re(s)>\frac{1}{2}$ で絶対収束し正則である. 定理 3.6 より $\frac{-\zeta'(s)}{\zeta(s)}$ は $Re(s)>0$ で有理型関数でその極は $s=1$ と$\zeta(s)$ の零点のみ. よって上の式より $\Phi(s)$ は $Re(s9>\frac{1}{2}$ で有理型関数として拡張されその極は $s=1$ と$\zeta(s)$ の零点のみ. また,$\psi=\zeta(s)-\frac{1}{s-1}$ とおくと定理 3.6 よりこれは $Re(s)>0$ において正則で

$$-\frac{\zeta'(s)}{\zeta(s)}=-\frac{-(s-1)^2+\psi'(s)}{(s-1)^{-1}+\psi(s)}=\frac{1-(s-1)^2\psi'(s)}{(s-1)(1+(s-1)\psi(s))}\cdots(2)$$

なので $lim_{s\to 1}-(s-1)\frac{\zeta'(s)}{\zeta(s)}=1\cdots(3)$ である.$\zeta(s)$ が $s=1+\alpha(\alpha\neq 0)$ で $n$ 位 の零点を持ち $s=1+2i\alpha$ で $m$ 位の零点を持つとすると定理 3.6 よりテイラー展開可能だから $n,m\geq 0$. また定理 3.7 より $s=1-i\alpha$ は $n$ 位の零点,$s=1-2i\alpha$ は $m$ 位 の零点.(1),(2) より $s=1,s=1\pm i\alpha,s=1\pm 2i\alpha$ は 1 位の極であり命題 2.9 よりこれらの留数は (3) を用いるとそれぞれ $1,-n,-m$ となる. よって

$$lim_{\epsilon\to+0}\Phi(1+\epsilon)=1,lim_{\epsilon\to+0}\epsilon\Phi(1+\epsilon\pm i\alpha)=-n,lim_{\epsilon\to+0}\epsilon\Phi(1+\epsilon\pm 2i\alpha)=-m$$

これと

$$\sum_{r=-2}^{2}\binom{4}{2+r}\Phi(1+\epsilon+ir\alpha)=\sum_{p}\frac{logp}{p^{1+\epsilon}}(p^{\frac{i\alpha}{2}}+p^{\frac{-i\alpha}{2}})^4\geq 0$$

より $6\leq 8n+m\leq 8n$ なので $n=0$. つまり $\zeta(1+i\alpha)\neq 0$ となり (1) より $\Psi(s)-\frac{1}{s-1}$ は $Re(s)\geq 1$ で正則.
命題 3.11 $\vartheta(x)=O(x)$
(証明) 自然数 $n$ に対して

$$2^{2n}=(1+1)^{2n}=\sum_{r=0}^{2n}\binom{2n}{r}\geq\binom{2n}{r}$$

$n<p\leq 2n$ ならば $p|\binom{2n}{n}$ より $\binom{2n}{n}$ は $\prod=n<p\leq 2np$ で割り切れる. よって $\binom{2n}{n}\geq\prod n<p\leq 2np$. また,

$$log(\prod_{n<p\leq 2n}p)=\sum_{n<p\leq 2n}logp=\vartheta(2n)-\vartheta(n)$$

なので

$$2nlog2\geq log\binom{2n}{n}\geq log(\prod_{n<p\leq 2n}p)=\sum_{n<p\leq 2n}logp=\vartheta(2n)-\vartheta(n)$$

$[\frac{x}{2}]=n$ とおくと $[x]$ は $2n$ または $2n+1$ したがって

$$\vartheta(x)-\vartheta(\frac{x}{2})=\vartheta([x])-\vartheta([\frac{x}{2}])=\begin{cases}\vartheta(2n)-\vartheta(n)\\ \vartheta(2n+1)-\vartheta(n)\end{cases}$$

よって

$$\vartheta(x)-\vartheta(\frac{x}{2})\leq\vartheta(2n)-\vartheta(n)+logx\leq 2nlog2+logx\leq xlog2+logx$$

任意の $C>log2$ に対して, すべての $x\geq x_0=x_0(C)$ について,$logx\leq(C-log2)x$ が成り立つので結局 $\vartheta(x)-\vartheta(\frac{x}{2})\leq Cx(\forall x\geq x_0)$ が成り立つ.$x\geq x_0$ とし $r\geq 0$ を $\frac{x}{2^r}\geq x_0\geq\frac{x}{2^{r+1}}$ となるように定める.

$$\vartheta(\frac{x}{2^{k-1}})-\vartheta(\frac{x}{2^k}0\leq C\frac{x}{2^{k-1}}(k=1,2,\cdots r+1)$$

について加えると

$$\vartheta(x)-\vartheta(\frac{x}{2^{r+1}})\leq C\sum_{k=1}^{r+1}\frac{x}{2^{k-1}}\leq C\sum k=1^{\infty}\frac{x}{2^{k-1}}=2Cx$$

$$\vartheta(x)\leq 2Cx+\vartheta(\frac{x}{2^{r+1}}\leq 2Cx+\vartheta(x_0)=2Cx+0(1)$$

命題 3.12 $\int_1^\infty \frac{\vartheta(x)-x}{x^2}dx$ は収束する.
(証明)自然数 $n$ に対して数列

$$\lambda(n) = \begin{cases} logn & (n \text{ が素数}) \\ 0 & (otherwise) \end{cases}$$

と定義すると $\lambda(n) = \vartheta(n) - \vartheta(n-1)$. $Re(s) > 1$ に対して

$$\Phi(s) = \sum_p \frac{logp}{p^s} = \sum_{n=1}^\infty \frac{\lambda(n)}{n^s} = \sum_{n=2}^\infty \frac{\vartheta(n)-\vartheta(n-1)}{n^s} = \sum_{n=2}^\infty \frac{\vartheta(n)}{n^s} - \sum_{n=1}^\infty \frac{\vartheta(n)}{(n+1)^s}$$

$$= \sum_{n=1}^\infty \vartheta(n) \int_n^{n+1} \frac{s}{x^{s+1}}dx = \sum n = 1\infty s \int_n^{n+1} \frac{\vartheta(x)}{x^{s+1}}dx = s\int_1^\infty \frac{\vartheta(x)}{x^{s+1}}dx(x = e^t \text{とおく}) = s\int_0^\infty e^{-st}\vartheta(e^t)dt.$$

ここで

$$f(t) = \vartheta(e^t)e^{-t} - 1(t \geq 0), g(z) = \frac{\Phi(z+1)}{z+1} - \frac{1}{z}(Re(z) > 0)(f(t) \text{ は命題 3.11 より収束})$$

とおく. 命題 3.10 より $\Phi(z+1) - \frac{1}{z} = h(z)$ は $Re(z) \geq 0$ で正則. したがって,

$$g(z) = \frac{h(z)+z^{-1}}{z+1} - \frac{1}{z} = \frac{h(z)}{z+1} - \frac{1}{z+1}$$

は $Re(z) \geq 0$ で正則である. さらに,$Re(z) > 0$ において,

$$\int_0 \infty f(t)e^{-zt}dt = \int_0^\infty (\vartheta(e^t)e^{-t} - 1)e^{-zt}dt = \int_0^\infty \vartheta(e^t)e^{-(z+1)t}dt - \int_0^\infty e^{-zt}dt$$

$$= \frac{\Phi(z+1)}{z+1} - [-\frac{1}{z}e^{-zt}]_0^\infty = \frac{\Phi(z+1)}{z+1} - \frac{1}{z} = g(z).$$

よって定理 3.9 より積分

$$\int_0^\infty f(t)dt = \int_0^\infty (\vartheta(e^t)e^{-t} = 1)dt = \int_1^\infty (\vartheta(x)x^{-1} - 1)x^{-1}dx$$

は収束する.
命題 3.13 $\vartheta(x) \sim x$
(証明) $\forall\lambda > 1, \int_1^\lambda \frac{\lambda-u}{u^2}dt > 0$ より $\forall\lambda > 1, 0 < \epsilon < \int_1^\lambda \frac{\lambda-u}{u^2}du$ となる $\epsilon$ が存在しこれに対し
命題 3.12 より $\exists R > 0, \forall y' > y > R$,

$$-\epsilon < \int_y^{y'} \frac{\vartheta(t)-t}{t^2}dt < \epsilon \cdots (1)$$

ここで $limsup_{x\to\infty}\frac{\vartheta(x)}{x} > 1$ と仮定すると $\exists\lambda' > 1, \vartheta(x) \geq \lambda' x$. この$\lambda'$ に対し (1) より特に $x > R$ のとき $y = x, y' = \lambda' x$ とすると

$$\int_x^{\lambda' x} \frac{\vartheta(t)-t}{t^2}dt < \epsilon \cdots (2)$$

また,

$$\epsilon < \int_1^{\lambda'} \frac{\lambda' - u}{u^2} du \cdots (3)$$

が成り立つ. $\vartheta(x)$ は広義単調増加関数なので $t \geq x$ ならば $\vartheta(t) \geq \vartheta(x) \geq \lambda' x$ なので ($t = xv$ として)

$$\int_x^{\lambda' x} \frac{\vartheta(t) - t}{t^2} dt \geq \int_x^{\lambda' x} \frac{\lambda' x - t}{t^2} dt = \int_1^{\lambda'} \frac{\lambda' - v}{v^2} dv$$

これと (2),(3) より

$$\epsilon < \int_1^{\lambda'} \frac{\lambda' - u}{u^2} du \leq \int_x^{\lambda' x} \frac{\vartheta(t) - t}{t^2} dt < \epsilon$$

よって矛盾. 同様に $liminf_{x\to\infty} \frac{\vartheta(x)}{x} \geq 1$ も成り立つ. よってこれらより示された.
定理 1.1(素数定理) $lim_{x\to\infty} \frac{\pi(x)logx}{x} = 1$
(証明)$\forall \epsilon > 0$,

$$\vartheta(x) \leq \sum_{p \leq x} logx = \pi(x)logx,$$

$$\vartheta(x) \geq \sum_{x^{1-\epsilon} < p \leq x} logp \geq \sum_{x^{1-\epsilon} < p \leq x} (1-\epsilon)logx = (1-\epsilon)(\pi(x) - \pi(x^{1-\epsilon})logx$$

が成り立つので

$$\frac{\vartheta(x)}{x} \leq \frac{\pi(x)logx}{x} \leq \frac{1}{1-\epsilon}\frac{\vartheta(x)}{x} + \frac{\pi(x^{1-\epsilon})logx}{x} = \frac{1}{1-\epsilon}\frac{\vartheta(x)}{x} + \frac{logx}{x^{\epsilon}}$$

これらと命題 3.13 より

$$1 = lim_{x\to\infty} \frac{\vartheta(x)}{x} \leq liminf_{x\to\infty} \frac{\pi(x)logx}{x} \leq limsup_{x\to\infty} \frac{\pi(x)logx}{x}$$

$$\leq lim_{x\to\infty} (\frac{1}{1-\epsilon}\frac{\vartheta(x)}{x} + \frac{logx}{x^{\epsilon}}) = \frac{1}{1-\epsilon} lim_{x\to\infty} \frac{\vartheta(x)}{x} + 0 = \frac{1}{1-\epsilon}$$

これは $\forall \epsilon > 0$ に対して成り立つので

$$liminf_{x\to\infty} \frac{\pi(x)logx}{x} = limsup_{x\to\infty} \frac{\pi(x)logx}{x} = 1$$

よって示された.

## 4 参考文献


1. 微分積分学 (サイエンス社, 笠原晧司著)
2. 複素関数論 (朝倉書店, 加藤昌英著)
3.Newman's short proof of the prime number theorem （American mathematical monthly, D.Zagier)

# 素数定理の初等的証明

高校 2 年　平山楓馬

2019 年 5 月 2, 3 日　第 73 回灘校文化祭

## はじめに

自然数の中に素数がどれほどの「割合」で分布しているかという問題は人類にとって永らく重要な関心であったが、18 世紀末には Legendre や Gauss により形式的で簡明な以下の予想が提示された。

**予想.** $x$ 以下の素数の個数を $\pi(x)$ とおくと、$\lim_{x\to\infty}\dfrac{\pi(x)\log x}{x}=1$

すなわち $x$ 以下での素数の「割合」は $1/\log x$ で近似できると主張しており、この近似は $x$ が小さくても比較的正確であることが具体的計算で確認できる。この予想は 19 世紀末に Hadamard と Poissin によりゼータ関数を用いて独立に証明され、**素数定理** との輝かしい名称が与えられた。20 世紀になると Selberg と Erdös により技巧的な初等的証明が提示され、驚きをもって迎えられた。今回は彼らのアイディアを基にした初等的証明の一例を最短経路で紹介する。大きな行間や前提知識は極力排除したので、微積の基本的な扱いが出来る読者は容易く議論を追えるであろう。

## 1　Dirichlet 積

まずこの記事で頻繁に用いる *Landau* **の記号**について説明する。関数 $f(x),\ g(x)$ に対し、$\lim_{x\to\infty}\left|\dfrac{f(x)}{g(x)}\right|$ が存在し有限値をとるとき $f(x)=O(g(x))$、$\lim_{x\to\infty}\left|\dfrac{f(x)}{g(x)}\right|=0$ であるとき特に $f(x)=o(g(x))$ と表す。

正整数 $n$ が $n=p_1^{a_1}\cdots p_k^{a_k}$ と素因数分解されるとき、*Möbius* **関数**を以下で定義する。ただし $\mu(1)=1$ とする。

$$\mu(n)=\begin{cases}(-1)^k & (a_1=\cdots a_k=1)\\ 0 & (\text{otherwise})\end{cases}$$

**定理 1.1.** $\displaystyle\sum_{d|n}\mu(d)=\left[\frac{1}{n}\right]=\begin{cases}1 & (n=1)\\ 0 & (n>1)\end{cases}$

**証明.** $n=1$ の場合は明らかより、$n>1$ とする。$n=p_1^{a_1}\cdots p_k^{a_k}$ と素因数分解されるとすると

$$\sum_{d|n}\mu(d)=\mu(1)+\mu(p_1)+\cdots+\mu(p_k)+\cdots+\mu(p_1\cdots p_k)=1+\binom{k}{1}(-1)+\cdots+\binom{k}{k}(-1)^k=(1-1)^k=0$$

□

(数論的) 関数 $f,g$ に対し *Dirichlet* **積**を $(f*g)(n)=\displaystyle\sum_{d|n}f(d)g\left(\frac{n}{d}\right)$ で定義する。可換性と結合性が容易に確認できる。

**定理 1.2.** $I(n)=\left[\dfrac{1}{n}\right]=\begin{cases}1 & (n=1)\\ 0 & (n>1)\end{cases}$ とおくと、$f*I=I*f=f$

**証明.** $(f*I)(n)=\displaystyle\sum_{d|n}f(d)I\left(\frac{n}{d}\right)=\sum_{d|n}f(d)\left[\frac{d}{n}\right]=f(n)$ □

**定理 1.3** (Möbius の反転公式)**.** $f(n)=\displaystyle\sum_{d|n}g(d)\Longleftrightarrow g(n)=\sum_{d|n}f(d)\mu\left(\frac{n}{d}\right)$

**証明.** $u$ を恒等的に 1 をとる関数とすると、定理 1.1 は $\mu * u = I$ と書ける。したがって $f = g * u$ のとき

$$f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g$$

逆も同様に示される。 □

Dirichlet 積の一般化として関数 $\alpha, F$ に対し *Dirichlet* **の畳み込み**を $(\alpha \circ F)(x) = \sum_{n \le x} \alpha(n) F\left(\frac{x}{n}\right)$ で定義する。

**定理 1.4.** $\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F$

**証明.** $(\alpha \circ (\beta \circ F))(x) = \sum_{n \le x} \alpha(n) \sum_{n \le x/n} \beta(m) F\left(\frac{x}{mn}\right) = \sum_{mn \le x} \alpha(n)\beta(m) F\left(\frac{x}{mn}\right) = \sum_{k \le x} \left( \sum_{n|k} \alpha(n)\beta\left(\frac{k}{n}\right) \right) F\left(\frac{x}{k}\right)$
$= \sum_{k \le x} (\alpha * \beta)(k) F\left(\frac{x}{k}\right) = ((\alpha * \beta) \circ F)(x)$ □

**定理 1.5.** $h = f * g$ のとき、$F, G, H$ を $F(x) = \sum_{n \le x} f(n)$ などで定めると $H(x) = \sum_{n \le x} f(n) G\left(\frac{x}{n}\right) = \sum_{n \le x} g(n) F\left(\frac{x}{n}\right)$

**証明.** $U(x) = \begin{cases} 0 & (0 < x < 1) \\ 1 & (x \ge 1) \end{cases}$ とすると $F = f \circ U$ などと書ける。したがって定理 1.4 より

$$f \circ G = f \circ (g \circ U) = (f * g) \circ U = H = (g * f) \circ U = g \circ (f \circ U) = g \circ F$$

□

**系 1.6.** $F(x) = \sum_{n \le x} f(n)$ のとき $\sum_{n \le x} \sum_{d|n} f(d) = \sum_{n \le x} f(n) \left[\frac{x}{n}\right] = \sum_{n \le x} f\left(\frac{x}{n}\right)$

**証明.** 定理 1.5 において $g(n) \equiv 1,\ G(x) = [x]$ とすればよい。 □

## 2 Abel の総和法

**定理 2.1** (Abel)**.** 数列 $\{c_n\}$ に対し $C(x) = \sum_{n \le x} c_n$ とおくと $\sum_{n \le x} c_n f(n) = \sum_{n \le x-1} C(n)\{f(n) - f(n+1)\} + C(x) f([x])$
特に $f$ が $[y, x]$ の範囲で連続な導関数を持つとき $\sum_{y < n \le x} c_n f(n) = C(x)f(x) - C(y)f(y) - \int_y^x C(t) f'(t)\ dt$

**証明.** $k = [x],\ m = [y]$ とおく。$C(k) = C(x),\ C(m) = C(y)$ であることに留意すると、

$$\begin{aligned}
\sum_{y < n \le x} c_n f(n) &= \sum_{n=m+1}^{k} \{C(n) - C(n-1)\} f(n) = \sum_{n=m+1}^{k} C(n) f(n) - \sum_{n=m}^{k-1} C(n) f(n+1) \\
&= \sum_{n=m+1}^{k-1} C(n)\{f(n) - f(n+1)\} + C(k)f(k) - C(m)f(m+1) \\
&= -\sum_{n=m+1}^{k-1} C(n) \int_n^{n+1} f'(t)\ dt + C(k)f(k) - C(m)f(m+1) \\
&= -\int_{m+1}^{k} C(t) f'(t)\ dt + C(x)f(x) - \int_k^x C(t)f'(t) - C(y)f(y) - \int_y^{m+1} C(t) f'(t)\ dt \\
&= C(x)f(x) - C(y)f(y) - \int_y^x C(t) f'(t)\ dt
\end{aligned}$$

□

**系 2.2** (Euler)**.** $\sum_{y < n \le x} f(n) = \int_y^x f(t)\ dt + \int_y^x (t - [t]) f'(t)\ dt + f(x)([x] - x) - f(y)([y] - y)$

**証明.** 定理 2.1 で $c_n = 1$ とすると $C(x) = [x]$ である。$\int tf'(t)\ dt = tf(t) - \int f(t)\ dt$ に注意して変形すると

$$\begin{aligned}\sum_{y<n\le x} f(n) &= [x]f(x) - [y]f(y) - \int_y^x [t]f'(t)\ dt \\ &= [x]f(x) - [y]f(y) - \int_y^x [t]f'(t)\ dt + \int_y^x tf'(t)\ dt + \int_y^x f(t)\ dt - (xf(x) - yf(y)) \\ &= \int_y^x f(t)\ dt + \int_y^x (t-[t])f'(t)\ dt + f(x)([x]-x) - f(y)([y]-y)\end{aligned}$$

□

**定理 2.3.** $x \ge 1$ および正数 $s \ne 1$ に対し (a) $\displaystyle\sum_{n\le x}\frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$　　(b) $\displaystyle\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O\left(\frac{1}{x^s}\right)$

ただし (a) における $\gamma$ は *Euler* **定数**である。また (b) における $\zeta(s)$ は $s > 1$ では *Riemann* **ゼータ関数** $\displaystyle\sum_{n=1}^{\infty}\frac{1}{n^s}$ に一致する。

**証明.** $f(t) = 1/t$ について系 2.2 を適用して

$$\begin{aligned}\sum_{n\le x}\frac{1}{n} &= \int_1^x \frac{1}{t}\ dt - \int_1^x \frac{t-[t]}{t^2}\ dt + 1 - \frac{x-[x]}{x} \\ &= \log x + 1 - \int_1^\infty \frac{t-[t]}{t^2}\ dt + \int_1^\infty \frac{t-[t]}{t^2}\ dt + O\left(\frac{1}{x}\right)\end{aligned}$$

ここで $0 \le \displaystyle\int_x^\infty \frac{t-[t]}{t^2}\ dt \le \int_x^\infty \frac{1}{t^2}\ dt = \frac{1}{x}$ より、$\gamma = 1 - \displaystyle\int_1^\infty \frac{t-[t]}{t^2}\ dt$ とおくと (a) を得る。

同様に $f(t) = t^{-s}$ について系 2.2 を適用して

$$\begin{aligned}\sum_{n\le x}\frac{1}{n^s} &= \int_1^x \frac{1}{t^s}\ dt - s\int_1^x \frac{t-[t]}{t^{s+1}}\ dt + 1 - \frac{x-[x]}{x^s} \\ &= \frac{x^{1-s}}{1-s} - \frac{1}{1-s} + 1 - s\int_1^\infty \frac{t-[t]}{t^{s+1}}\ dt + O(x^{-s})\end{aligned}$$

$\zeta(s) = 1 - \dfrac{1}{1-s} - s\displaystyle\int_1^\infty \frac{t-[t]}{t^{s+1}}\ dt$ とすることで (b) を得る。 □

## 3 Chebyshev 関数

正整数 $n$ に対し *von Mangoldt* **関数**を以下で定義する。

$$\Lambda(n) = \begin{cases}\log p & (n = p^m) \\ 0 & (\text{otherwise})\end{cases}$$

正数 $x$ に対し**第一** *Chebyshev* **関数**を $\vartheta(x) = \displaystyle\sum_{p\le x}\log p$ で定義する。ただし総和は $x$ 以下の素数全体を渡る。また von Mangoldt 関数を用いて**第二** *Chebyshev* **関数**を $\psi(x) = \displaystyle\sum_{n\le x}\Lambda(n)$ で定義する。これらには以下の性質がある。

**定理 3.1.** $0 \le \psi(x) - \vartheta(x) \le \dfrac{\sqrt{x}\log^2 x}{2\log 2}$

**証明.** $\psi(x) = \displaystyle\sum_{m\le\log_2 x}\vartheta(x)$ と書けることが容易にわかり、これより $0 \le \psi(x) - \vartheta(x) = \displaystyle\sum_{2\le m\le\log_2 x}\vartheta(x^{1/m})$

ここで明らかに $\vartheta(x) \le x\log x$ より、

$$0 \le \psi(x) - \vartheta(x) \le \sum_{2\le m\le\log_2 x} x^{1/m}\log(x^{1/m}) \le (\log_2 x)\sqrt{x}\log\sqrt{x} = \frac{\log x}{\log 2}\cdot\frac{\sqrt{x}}{2}\log x = \frac{\sqrt{x}\log^2 x}{2\log 2}$$

□

**定理 3.2.** $x \leq 2$ に対し $\vartheta(x) = \pi(x)\log x - \displaystyle\int_2^x \frac{\pi(t)}{t}\,dt$ および $\pi(x) = \frac{\vartheta(x)}{\log x} + \displaystyle\int_2^x \frac{\vartheta(t)}{t\log^2 t}\,dt$

**証明.** $a(n) = \begin{cases} 1 & (n \text{ が素数のとき}) \\ 0 & (\text{otherwise}) \end{cases}$ とおくと、$\pi(x) = \displaystyle\sum_{1<n\leq x} a(n)$ および $\vartheta(x) = \sum_{1<n\leq x} a(n)\log x$ と書ける。$f(x) = \log x$ として定理 2.1 を適用すると

$$\vartheta(x) = \sum_{1<n\leq x} a(n)\log x = \pi(x)\log x - \pi(1)\log 1 - \int_1^x \frac{\pi(t)}{t}\,dt$$

より第 1 式を得る。また $b(n) = a(n)\log n$ とおくと $\pi(x) = \displaystyle\sum_{3/2<n\leq x} \frac{b(n)}{\log n}$ および $\vartheta(x) = \sum_{n\leq x} b(n)$ で、$f(x) = \dfrac{1}{\log x}$ として再び定理 2.1 を適用すると

$$\pi(x) = \sum_{3/2<n\leq x} \frac{b(n)}{\log n} = \frac{\vartheta(x)}{\log x} - \frac{\vartheta(3/2)}{\log 3/2} + \int_{3/2}^x \frac{\vartheta(t)}{t\log^2 t}\,dt$$

より第 2 式を得る。 □

**定理 3.3.** $\displaystyle\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1 \iff \lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1 \iff \lim_{x\to\infty} \frac{\psi(x)}{x} = 1$

**証明.** 2 つ目の同値は定理 3.1 より直ちに従うから、以下 1 つ目の同値を示す。
($\Longrightarrow$) 仮定より $\dfrac{\pi(t)}{t} = O\left(\dfrac{1}{\log t}\right)$ であるから $\displaystyle\int_y^x \frac{\pi(t)}{t}\,dt = O\left(\int_y^x \frac{dt}{\log t}\right)$ で、これより

$$\int_2^x \frac{\pi(t)}{t}\,dt \leq \int_2^{\sqrt{x}} \frac{dt}{\log t} + \int_{\sqrt{x}}^x \frac{dt}{\log t} \leq \frac{\sqrt{x}}{\log 2} + \frac{x-\sqrt{x}}{\log\sqrt{x}}$$

したがって $\displaystyle\lim_{x\to\infty} \frac{1}{x}\int_2^x \frac{\pi(t)}{t}\,dt = 0$ であるから定理 3.2 より示される。
($\Longleftarrow$) 仮定より $\vartheta(t) = O(t)$ であるから $\displaystyle\int_y^x \frac{\vartheta(t)}{t\log^2 t}\,dt = O\left(\int_y^x \frac{dt}{\log^2 t}\right)$ で、これより

$$\int_2^x \frac{\vartheta(t)}{t\log^2 t}\,dt \leq \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t} \leq \frac{\sqrt{x}}{\log^2 2} + \frac{x-\sqrt{x}}{\log^2\sqrt{x}}$$

したがって $\displaystyle\lim_{x\to\infty} \frac{\log x}{x}\int_2^x \frac{\vartheta(t)}{t\log^2 t}\,dt = 0$ であるから定理 3.2 より示される。 □

**定理 3.4** (Shapiro)**.** 非負実数からなる数列 $\{a_n\}$ が $\displaystyle\sum_{n\leq x} a_n\left[\frac{x}{n}\right] = x\log x + O(x)$ をみたすとする。このとき、

(a) $\displaystyle\sum_{n\leq x} a_n \leq Bx$ なる定数 $B$ が存在する。 (b) $\displaystyle\sum_{n\leq x} a_n \geq Ax$ なる定数 $A$ が存在する。 (c) $\displaystyle\sum_{n\leq x} \frac{a_n}{n} = \log x + O(1)$

**証明.** $S(x) = \displaystyle\sum_{n\leq x} a_n$, $T(x) = \sum_{n\leq x} a_n\left[\frac{x}{n}\right]$ とおく。まず $S(x) - S\left(\dfrac{x}{2}\right) \leq T(x) - 2T\left(\dfrac{x}{2}\right)$ を示す。

$$T(x) - 2T\left(\frac{x}{2}\right) = \sum_{n\leq x}\left[\frac{x}{n}\right]a_n - 2\sum_{n\leq x/2}\left[\frac{x}{2n}\right]a_n = \sum_{n\leq x/2}\left(\left[\frac{x}{n}\right] - 2\left[\frac{x}{2n}\right]\right)a_n + \sum_{x/2<n\leq x}\left[\frac{x}{n}\right]a_n$$

ここで $[2y] - [y]$ は 0 または 1、特に非負であるから

$$T(x) - 2T\left(\frac{x}{2}\right) \geq \sum_{x/2<n\leq x}\left[\frac{x}{n}\right]a_n = \sum_{x/2<n\leq x} a_n = S(x) - S\left(\frac{x}{2}\right)$$

ところで仮定より $T(x) - 2T\left(\dfrac{x}{2}\right) = x\log x + O(x) - 2\left(\dfrac{x}{2}\log\dfrac{x}{2} + O(x)\right) = O(x)$ であるから、上の不等式と合わせて $S(x) - S\left(\dfrac{x}{2}\right) = O(x)$、すなわちある定数 $K > 0$ が存在して $S(x) - S\left(\dfrac{x}{2}\right) \leq Kx$ である。これを $x/2,\ x/4, \cdots$ について順に足し合わせれば、$B = 2K$ とすることで (a) を得る。

次に (c) を示す。(a) の結果より

$$T(x)=\sum_{n\le x}\left[\frac{x}{n}\right]a_n=\sum_{n\le x}\left(\frac{x}{n}+O(1)\right)a_n=x\sum_{n\le x}\frac{a_n}{n}+O\left(\sum_{n\le x}a_n\right)=x\sum_{n\le x}\frac{a_n}{n}+O(x)$$

これより仮定と合わせて $\displaystyle\sum_{n\le x}\frac{a_n}{n}=\frac{1}{x}T(x)+O(1)=\log x+O(1)$ を得る。

最後に (b) を示す。いま $\displaystyle A(x)=\sum_{n\le x}\frac{a_n}{n}$ とおくと (c) は $A(x)=\log x+R(x)$ と書ける。ただし剰余項 $R(x)$ は $O(1)$、すなわちある定数 $M>0$ が存在して $|R(x)|\le M$ である。$0<\alpha<1$ について

$$\begin{aligned}A(x)-A(\alpha x)&=\log x+R(x)-(\log\alpha x+R(\alpha x))=-\log\alpha+R(x)-R(\alpha x)\\&\ge-\log\alpha-|R(x)|-|R(\alpha x)|\ge-\log\alpha-2M\end{aligned}$$

特に $-\log\alpha-2M=1$ すなわち $\alpha=e^{-2M-1}$ とおくと $A(x)-A(\alpha x)\ge1$ となる。ところで

$$A(x)-A(\alpha x)=\sum_{\alpha x<n\le x}\frac{a_n}{n}\le\frac{1}{\alpha x}\sum_{n\le x}a_n=\frac{S(x)}{\alpha x}$$

であるから $S(x)\ge\alpha x$ で、$A=\alpha$ とすることで (b) を得る。 □

**定理 3.5.** (a) $Ax\le\psi(x)\le Bx$ なる定数 $A,B$ が存在する。 (b) $\displaystyle\sum_{n\le x}\frac{\Lambda(n)}{n}=\log x+O(1)$

**証明.** $\displaystyle\sum_{n\le x}\Lambda(n)\left[\frac{x}{n}\right]=x\log x+O(x)$ を示せば定理 3.4 より結論を得る。$f(t)=\log t$ について系 2.2 を適用し

$$\begin{aligned}\sum_{n\le x}\log n&=\int_1^x\log t\ dt+\int_1^x\frac{t-[t]}{t}\ dt-(x-[x])\log x\\&=x\log x-1+x+O\left(\int_1^x\frac{1}{t}\ dt\right)+O(\log x)=x\log x-x+O(\log x)\end{aligned}$$

また系 1.6 より $\displaystyle\sum_{n\le x}\Lambda(n)\left[\frac{x}{n}\right]=\sum_{n\le x}\sum_{d|n}\Lambda(d)=\sum_{n\le x}\log n$ であるから結論を得る。 □

**系 3.6.** $\displaystyle\sum_{n\le x}\psi\left(\frac{x}{n}\right)=x\log x-x+O(\log x)$

**証明.** 系 1.6 より $\displaystyle\sum_{n\le x}\Lambda(n)\left[\frac{x}{n}\right]=\sum_{n\le x}\psi\left(\frac{x}{n}\right)$ である。また定理 3.5 の証明より $\displaystyle\sum_{n\le x}\Lambda(n)\left[\frac{x}{n}\right]=x\log x-x+O(\log x)$ であるから、これらより結論を得る。 □

## 4 Selberg の恒等式

**定理 4.1.** $G(x)=\log x\displaystyle\sum_{n\le x}F\left(\frac{x}{n}\right)$ のとき、$\displaystyle F(x)\log x+\sum_{n\le x}F\left(\frac{x}{n}\right)\Lambda(n)=\sum_{d\le x}\mu(d)G\left(\frac{x}{d}\right)$

**証明.** 定理 1.1 より

$$F(x)\log x=\sum_{n\le x}\left[\frac{1}{n}\right]F\left(\frac{x}{n}\right)\log\frac{x}{n}=\sum_{n\le x}F\left(\frac{x}{n}\right)\sum_{d|n}\mu(d)\log\frac{x}{n}$$

また $\displaystyle\log n=\sum_{d|n}\Lambda(d)$ が容易にわかるので、$f(x)=\log x,\ g(x)=\Lambda(x)$ に対し定理 1.3 を適用して

$$\sum_{n\le x}F\left(\frac{x}{n}\right)\Lambda(n)=\sum_{n\le x}F\left(\frac{x}{n}\right)\sum_{d|n}\mu(d)\log\frac{n}{d}$$

これらを足し合わせて、$n=qd$ とおくと

$$F(x)\log x+\sum_{n\le x}F\left(\frac{x}{n}\right)\Lambda(n)=\sum_{n\le x}\sum_{d|n}F\left(\frac{x}{n}\right)\mu(d)\log\frac{x}{d}=\sum_{d\le x}\mu(d)\log\frac{x}{d}\sum_{q\le x/d}F\left(\frac{x}{qd}\right)=\sum_{d\le x}\mu(x)G\left(\frac{x}{d}\right)$$

ただし最後の等号は $G(x)$ の定義において $x = x/d,\ n = q$ とした。 □

**定理 4.2** (Selberg)**.** $\psi(x)\log x + \sum_{n\le x}\Lambda(n)\psi\left(\frac{x}{n}\right) = 2x\log x + O(x)$

**証明.** $F_1(x) = \psi(x)$ について系 3.6 より

$$G_1(x) = \log x \sum_{n\le x}\psi\left(\frac{x}{n}\right) = x\log^2 x - x\log x + O(\log^2 x)$$

また $F_2(x) = x - \gamma - 1$ について定理 2.3(a) より

$$G_2(x) = \log x \sum_{n\le x}\left(\frac{x}{n} - \gamma - 1\right) = x\log x\left(\log x + \gamma + O\left(\frac{1}{x}\right)\right) - (\gamma+1)\log x(x+O(1)) = x\log^2 x - x\log x + O(\log x)$$

これらより $G_1(x) - G_2(x) = O(\log^2 x)$ である。ここでは $G_1(x) - G_2(x) = O(\sqrt{x})$ として利用する。いま $F_1(x)$ および $F_2(x)$ についてそれぞれ定理 4.1 を適用する。定理 2.3(b) より右辺の差は

$$\sum_{d\le x}\mu(d)\left\{G_1\left(\frac{x}{d}\right) - G_2\left(\frac{x}{d}\right)\right\} = O\left(\sum_{d\le x}\sqrt{\frac{x}{d}}\right) = O\left(\sqrt{x}\sum_{d\le x}\frac{1}{\sqrt{d}}\right) = O(x)$$

これより左辺の差も $O(x)$ である。この結果を書き換えて定理 3.5(b) を用いると

$$\psi(x)\log x + \sum_{n\le x}\psi\left(\frac{x}{n}\right)\Lambda(n) = (x-\gamma-1)\log x + \sum_{n\le x}\left(\frac{x}{n} - \gamma - 1\right)\Lambda(n) + O(x) = 2x\log x + O(x)$$

□

**系 4.3.** $\sum_{n\le x}\Lambda(n)\log n + \sum_{mn\le x}\Lambda(m)\Lambda(n) = 2x\log x + O(x)$

**証明.** $c_n = \Lambda(n),\ f(x) = \log x$ について定理 2.1 を適用すると、定理 3.5(a) より

$$\sum_{n\le x}\Lambda(n)\log n = \psi(x)\log x - \int_2^x \frac{\psi(t)}{t}\,dt = \psi(x)\log x + O(x)$$

また $\sum_{n\le x}\Lambda(n)\psi\left(\frac{x}{n}\right) = \sum_{n\le x}\Lambda(n)\sum_{m\le x/n}\Lambda(m) = \sum_{mn\le x}\Lambda(m)\Lambda(n)$ であるから、定理 4.2 より結論を得る。 □

## 5 素数定理の本証明

$R(x) = \psi(x) - x$ とおくと、定理 3.3 より素数定理は $\lim_{x\to\infty} R(x) = 0$ と同値であるからこれを目標とする。

定理 4.2 および定理 3.5(b) より $R(x)\log x + \sum_{n\le x}\Lambda(n)R\left(\frac{x}{n}\right) = O(x)$ で、これより

$$\log x\left(R(x)\log x + \sum_{n\le x}\Lambda(n)R\left(\frac{x}{n}\right)\right) - \sum_{n\le x}\Lambda(n)\left(R\left(\frac{x}{n}\right)\log\frac{x}{n} + \sum_{m\le x/n}\Lambda(m)R\left(\frac{x}{mn}\right)\right) = O(x\log x) + O\left(x\sum_{n\le x}\frac{\Lambda(n)}{n}\right)$$
$$= O(x\log x)$$

ただし 2 つ目の等号で定理 3.5(b) を用いた。整理して

$$R(x)\log^2 x = -\sum_{n\le x}\Lambda(n)R\left(\frac{x}{n}\right)\log n + \sum_{mn\le x}\Lambda(m)\Lambda(n)R\left(\frac{x}{mn}\right) + O(x\log x)$$

ここで $a_n = \Lambda(n)\log n + \sum_{hk=n}\Lambda(h)\Lambda(k)$ とおけば $|R(x)|\log^2 x \le \sum_{n\le x}a_n\left|R\left(\frac{x}{n}\right)\right| + O(x\log x)$ と書け、また系 4.3 より $\sum_{n\le x}a_n = 2x\log x + O(x)$ である。

**補題 5.1.** $\sum_{n\le x}a_n\left|R\left(\frac{x}{n}\right)\right| = 2\int_1^x\left|R\left(\frac{x}{t}\right)\right|\log t\,dt + O(x\log x)$

**証明.** $F(x)=\psi(x)+x=O(x)$ とおくと、$t>t'\geq 0$ に対し

$$||R(t)|-|R(t')||\leq |R(t)-R(t')|=|\psi(t)-\psi(t')-t+t'|\leq \psi(t)-\psi(t')+t-t'=F(t)-F(t')$$

また定理 2.3(a) より

$$\sum_{n\leq x-1} n\left(F\left(\frac{x}{n}\right)-F\left(\frac{x}{n-1}\right)\right)=\sum_{n\leq x}F\left(\frac{x}{n}\right)-[x]F\left(\frac{x}{[x]}\right)=O\left(x\sum_{n\leq x}\frac{1}{n}\right)=O(x\log x)$$

$c_1=0,\ c_n=a_n-2\displaystyle\int_{n-1}^{n}\log t\ dt,\ f(n)=\left|R\left(\frac{x}{n}\right)\right|$ について定理 2.1 を適用すると、$C(x)=\displaystyle\sum_{n\leq x}a_n-2\int_1^{[x]}\log t\ dt$ で

$$\begin{aligned}\sum_{n\leq x}a_n\left|R\left(\frac{x}{n}\right)\right|-2\sum_{2\leq n\leq x}\left|R\left(\frac{x}{n}\right)\right|\int_{n-1}^{n}\log t\ dt&=\sum_{n\leq x-1}c_n\left(\left|R\left(\frac{x}{n}\right)\right|-\left|R\left(\frac{x}{n+1}\right)\right|\right)-C(x)R\left(\frac{x}{[x]}\right)\\&=O\left(\sum_{n\leq x-1}n\left(F\left(\frac{x}{n}\right)-F\left(\frac{x}{n+1}\right)\right)\right)+O(x)=O(x\log x)\end{aligned}$$

次に、

$$\begin{aligned}\left|\left|R\left(\frac{x}{n}\right)\right|\int_{n-1}^{n}\log t\ dt-\int_{n-1}^{n}\left|R\left(\frac{x}{n}\right)\right|\log t\ dt\right|&\leq\int_{n-1}^{n}\left|\left|R\left(\frac{x}{n}\right)\right|-\left|R\left(\frac{x}{t}\right)\right|\right|\log t\ dt\\&\leq\int_{n-1}^{n}\left(F\left(\frac{x}{n}\right)-F\left(\frac{x}{n}\right)\right)\log t\ dt\leq(n-1)\left(F\left(\frac{x}{n-1}\right)-F\left(\frac{x}{n}\right)\right)\end{aligned}$$

したがって、

$$\sum_{2\leq n\leq x}\left|R\left(\frac{x}{n}\right)\right|\int_{n-1}^{n}\log t\ dt-\int_1^x\left|R\left(\frac{x}{t}\right)\right|\log t\ dt=O\left(\sum_{n\leq x-1}n\left(F\left(\frac{x}{n}\right)-F\left(\frac{x}{n+1}\right)\right)\right)+O(x\log x)=O(x\log x)$$

以上より示された。 □

補題 5.1 を用いると $|R(x)|\log^2 x\leq 2\displaystyle\int_1^x\left|R\left(\frac{x}{t}\right)\right|\log t\ dt+O(x\log x)$ である。

ここで $V(\xi)=e^{-\xi}R(e^\xi)=e^{-\xi}\psi(e^\xi)+1$ とおく。$x=e^\xi,\ t=xe^\eta$ と置換すると、簡単な重積分の交換により

$$\int_1^x\left|R\left(\frac{x}{t}\right)\right|\log t\ dt=x\int_0^\xi|V(\eta)|\,(\xi-\eta)\ d\eta=x\int_0^\xi|V(\eta)|\int_\eta^\xi d\zeta d\eta=x\int_0^\xi\int_0^\zeta|V(\eta)|\ d\eta d\zeta$$

これより $\xi^2|V(\xi)|\leq 2\displaystyle\int_0^\xi\int_0^\zeta|V(\eta)|\ d\eta d\zeta+O(\xi)$ と書ける。

ここで $\alpha=\limsup_{\xi\to\infty}|V(\xi)|,\ \beta=\limsup_{\xi\to\infty}\frac{1}{\xi}\displaystyle\int_0^\xi|V(\eta)|d\eta$ とおくと ($\psi(x)=O(x)$ よりこれらの極限値は存在する)、素数定理は $\alpha=0$ を示すことに帰着される。いま $\xi^2|V(\xi)|\leq 2\displaystyle\int_0^\xi(\beta\zeta+o(\zeta))\ d\zeta+O(\zeta)=\beta\xi^2+o(\xi^2)$ すなわち $|V(\xi)|\leq\beta+o(1)$ より $\alpha\leq\beta$ を得る。以下 $\alpha>0$ と仮定し、$\beta<\alpha$ を示すことで矛盾を導く。

**補題 5.2.** 任意の $\xi_1,\xi_2>0$ に対し $\left|\displaystyle\int_{\xi_1}^{\xi_2}V(\eta)\ d\eta\right|<A_1$ なる定数 $A_1$ が存在する。

**証明.** $c_n=\Lambda(n),\ f(x)=\dfrac{1}{x}$ について定理 2.1 を適用して $\displaystyle\sum_{n\leq x}\frac{\Lambda(n)}{n}=\frac{\psi(x)}{x}+\int_2^x\frac{\psi(t)}{t^2}\ dt$ で、定理 3.5 より $\displaystyle\int_2^x\frac{\psi(t)}{t^2}\ dt=\log x+O(1)$ これより $x=e^\xi,\ t=e^\eta$ の置換によって $\displaystyle\int_0^\xi V(\eta)\ d\eta=\int_1^x\left(\frac{\psi(t)}{t^2}-\frac{1}{t}\right)dt=O(1)$ □

**補題 5.3.** $\eta_0>0$ について $V(\eta_0)=0$ のとき $\displaystyle\int_0^\alpha|V(\eta_0+\tau)|d\tau\leq\frac{1}{2}\alpha^2+O\left(\frac{1}{\eta_0}\right)$

**証明.** $x > x_0 \geq 1$ について定理 4.2 より $\psi(x)\log x - \psi(x_0)\log x_0 + \sum_{x_0 < mn \leq x} \Lambda(m)\Lambda(n) = 2(x\log x - x_0 \log x_0) + O(x)$
特に $\Lambda(n) \geq 0$ より $0 \leq \psi(x)\log x - \psi(x_0)\log x_0 \leq 2(x\log x - x_0\log x_0) + O(x)$ で、これより $|R(x)\log x - R(x_0)\log x_0| \leq x\log x - x_0 \log x_0 + O(x)$ である。いま $x = e^{\eta_0+\tau},\ x_0 = e^{\eta_0}$ とおき $R(x_0) = 0$ とすると、$0 \leq \tau \leq \alpha$ について

$$|V(\eta_0+\tau)| \leq 1 - \left(\frac{\eta_0}{\eta_0+\tau}\right)e^{-\tau} + O\left(\frac{1}{\eta_0}\right) = 1 - e^{-\tau} + O\left(\frac{1}{\eta_0}\right) \leq \tau + O\left(\frac{1}{\eta_0}\right)$$

ただし最後の不等号は $1 + x \leq e^x$ による。最左辺および最右辺を $\tau$ について 0 から $\alpha$ まで積分することで結論を得る。 □

いま $V(\eta)$ は不連続点を除いて単調減少し、不連続点で増加することが定義より直ちにわかる。これより、ある区間において $V(\eta)$ に零点が存在しないとき、その区間における $V(\eta)$ の符号変化は高々 1 度である。$\delta > \alpha$ および $\zeta > 0$ に対し、区間 $[\zeta, \zeta+\delta-\alpha]$ における零点の有無で場合分けを行う。

(1) $\eta_0$ で零点を持つとき、$\alpha' = \alpha\left(1 - \dfrac{\alpha}{2\delta}\right)$ とおくと補題 5.3 より

$$\begin{aligned}\int_\zeta^{\zeta+\delta} |V(\eta)|d\eta &= \int_\zeta^{\eta_0} |V(\eta)|d\eta + \int_{\eta_0}^{\eta_0+\alpha} |V(\eta)|d\eta + \int_{\eta_0+\alpha}^{\zeta+\delta} |V(\eta)|d\eta \\ &\leq \alpha(\eta_0 - \zeta) + \frac{1}{2}\alpha^2 + \alpha(\zeta+\delta-\eta_0-\alpha) + o(1) = \alpha\left(\delta - \frac{1}{2}\alpha\right) + o(1) = \alpha'\delta + o(1)\end{aligned}$$

(2) 零点を持たないとき、$\eta_1$ でのみ符号変化があるとすると補題 5.2 より

$$\int_\zeta^{\zeta+\delta-\alpha} |V(\eta)|d\eta = \left|\int_\zeta^{\eta_1} V(\eta)\ d\eta\right| + \left|\int_{\eta_1}^{\zeta+\delta-\alpha} V(\eta)\ d\eta\right| < 2A_1$$

また符号変化がない場合も

$$\int_\zeta^{\zeta+\delta-\alpha} |V(\eta)|d\eta = \left|\int_\zeta^{\zeta+\delta-\alpha} V(\eta)\ d\eta\right| < A_1 < 2A_1$$

したがって $\alpha'' = \dfrac{2A_1 + \alpha^2}{\delta}$ とおけば

$$\int_\zeta^{\zeta+\delta} |V(\eta)|d\eta = \int_\zeta^{\zeta+\delta-\alpha} |V(\eta)|d\eta + \int_{\zeta+\delta-\alpha}^{\zeta+\delta} |V(\eta)|d\eta < 2A_1 + \alpha^2 + o(1) = \alpha''\delta + o(1)$$

特に $\delta = \dfrac{3\alpha^2 + 4A_1}{2\alpha} > \alpha$ とおくと、$\alpha' = \alpha\left(\dfrac{4A_1 + 2\alpha^2}{4A_1 + 3\alpha^2}\right) = \alpha''$ となる。したがって $M = \left[\dfrac{\xi}{\zeta}\right]$ とおくと

$$\int_0^\xi |V(\eta)|\ d\eta = \sum_{m=0}^{M-1} \int_{m\delta}^{(m+1)\delta} |V(\eta)|\ d\eta + \int_{M\delta}^{\xi} |V(\eta)|\ d\eta \leq \alpha' M\delta + o(M) + O(1) = \alpha'\xi + o(\xi)$$

よって $\beta = \limsup_{\xi\to\infty} \dfrac{1}{\xi}\displaystyle\int_0^\xi |V(\eta)|\ d\eta \leq \alpha' < \alpha$ より矛盾が導かれ、素数定理が示された。

## 参考文献


[1] Tom M.Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer

[2] G.H.Hardy & E.M.Wright, *An Introduction to the Theory of Numbers*, 4th Edition, Oxford University Press

[3] Norman Levinson, *A Motivated Account of an Elementary Proof of the Prime Number Theorem*, The American Mathematical Monthly, Mathrmatical Assosiation of America, 1969

# 可換群と可換環

高校 3 年　黒木 亮汰

以下, 可換群, 可換環を単に群, 環ということにします. この記事では, まず群, 環, アを定義し, それらの関係を調べます. アが実は群と環の組と同等であることを証明する事 (定理 7,...,11) が本記事の目的です. 群や環について予備知識を仮定します. この記事で使われる用語は一般的なものと異なる場合があります.

## 1　群, 環, ア

群と環の両方に関わる対象を考えようと思うと, 幾つか障害がある. 厄介なのは, 群は演算が一つしかないのに, 環には二つあるという事である. 最も自然な解決法は, 群にもう一つ演算を付け足すことである.

**定義** (群)**.** 集合 $G$, $+,\cdot : G\times G\to G$, $v : G\to G$, $0\in G$ が以下の条件を全て満たすとき, 組 $(G,+,v,0)$ を群という (以下 $(G,+,v,0)$ を $G$ と略す). 以下, $a,b,c$ は $G$ の元を表し, $v(a)$ を $(-a)$ で, $a+(-b)$ を $a-b$ で表す.

(i) $0+a=a$
(ii) $a-a=0$
(iii) $(a+b)+c=a+(b+c)$
(iv) $a+b=b+a$

以下 $G$ を群とする. □

**定義** (環)**.** 集合 $R$, $+,\cdot : R\times R\rightrightarrows R$, $v : R\to R$, $0,1\in R$ が以下の条件を全て満たすとき, 組 $(R,+,\cdot,v,0,1)$ を環という (以下 $(R,+,\cdot,v,0,1)$ を $R$ と略す). 以下, $a,b,c$ は $R$ の元を表し, $a\cdot b$ を $ab$ で表す.

(i) $(R,+,v,0)$ は群
(ii) $1a=a$
(iii) $a(b+c)=ab+ac$
(iv) $(ab)c=a(bc)$
(v) $ab=ba$

以下 $R$ を環とする. □

**定義** (ア)**.** 集合 $A$, $+,\cdot : A\times A\rightrightarrows A$, $v : A\to A$, $0,1\in A$ が以下の条件を全て満たすとき, 組 $(A,+,\cdot,v,0,1)$ をアという (以下 $(A,+,\cdot,v,0,1)$ を $A$ と略す). 以下, $a,b,c$ は $A$ の元を表す.

(i) $(A,+,v,0)$ は群
(ii) $0a+a1=a$

(iii) $a(b+c) = ab + ac$
(iv) $(ab)c = a(bc)$
(v) $abc = bac$

以下 $A$ をアとする. □

**命題 1.** $a \in A$ について,

(i) $a0 = 0$
(ii) $01 = 0$
(iii) $11 = 1$
(iv) $1a = a$

**証明.** 以下の計算による.

(i) $a0 = a0 + a0 - a0 = a(0+0) - a0 = a0 - a0 = 0$
(ii) $01 = 0 + 01 = 00 + 01 = 0$ $(0a + a1 = a$ の使用に注意)
(iii) $11 = 0 + 11 = 01 + 11 = 1$ $(0a + a1 = a$ の使用に注意)
(iv) $1a = 1(0a + a1) = 10a + 1a1 = 0a + a11 = 0a + a1 = a$

□

**命題 2.** 群 $(G, +, v, 0)$ に $1 = 0$, $ab = b$ と定めたものはア.

**証明.** 以下の計算による.

(i) $0a + a1 = a + 1 = a + 0 = a$
(ii) $a(b+c) = b + c = ab + ac$
(iii) $(ab)c = c = bc = a(bc)$
(iv) $abc = c = bac$

このように定まるアも群という事にする. アについて, $1 = 0$ が成立するならば,

$$ab = a1b = a0b = 0b = 1b = b$$

となり, 群であることが示される. □

**命題 3.** 乗算が可換なアは環.

**証明.** 命題 1 より. □

アに関する基本概念を定義する.

**定義** (アの積)**.** ア $A, B$ について, $A \times B$ には自然にアの構造が入る. 具体的には以下の通り.

(i) $(a, b) + (c, d) := (a + c, b + d)$
(ii) $(a, b) \cdot (c, d) := (ac, bd)$
(iii) $-(a, b) := (-a, -b)$

こう定義すると (結局成分ごとに計算しているので) アの公理を満たすことは明らかなのでその計算は省く. □

**定義** (準同型)**.** ア $A, B$ について, 以下を満たす写像 $f : A \to B$ を準同型という.

(i) $f(a+b) = f(a) + f(b)$
(ii) $f(ab) = f(a)f(b)$
(iii) $f(1_A) = 1_B$

□

準同型の例を二つ挙げる.

**命題 4.** $(A, +, \cdot, v, 0_A, 1_A)$ について, $A \xrightarrow{f} A$ を $f(a) = 0a$ で定めると, $f(A) := \{x \in A : \exists a \in A \text{ s.t. } x = f(a)\}$ には群構造 $(f(A), +, \cdot, v, 0_A, 0_A)$ が入り, $f : A \to f(A)$ は準同型.

**証明.** まず準同型性 (といっても $f(A)$ がアである事すら示していないのでまだ準同型ではないが, $f(A)$ の演算は $A$ の演算と一致するように入れるので問題ない). $a, b \in A$ について,

(i) $f(a+b) = 0(a+b) = 0a + 0b = f(a) + f(b)$
(ii) $f(ab) = 0ab = 00ab = 0a0b = f(a)f(b)$
(iii) $f(1_A) = 0_A 1_A = 0_A = 1_{f(A)}$

次に $f(A)$ の群構造 ($f(A)$ の演算は $A$ の演算と一致するように入れる). $x, y \in f(A)$ とすると, $a, b \in A$ が存在して $(x, y) = (f(a), f(b))$ なので,

(i) $x + y = f(a) + f(b) = f(a+b) \in f(A)$
(ii) $0 = 01 = f(1) \in f(A)$
(iii) $-x = -f(a) = f(-a) - f(-a) - f(a) = f(-a) - f(0) = f(-a) \in f(A)$

より $f(A)$ は $0$ を含み, $+, v$ で閉じているので, $A$ のア性から $(f(A), +, v, 0)$ は群. さらに, $f(A)$ において

(i) $1_{f(A)} = 0_A = 0_{f(A)}$
(ii) $xy = f(a)f(b) = 0a0b = 0b = f(b) = y$

より示せた. □

以後 $g(a) = a1$ とおいて同様の議論をするが, $g$ についての議論は (分配律が片側しか成り立たないために) そのままだと面倒なので, $f$ と $g$ についてまとめておく.

**命題 5.** $a \in A$ について

(i) $f(g(a)) = g(f(a)) = 0$
(ii) $f(a) + g(a) = a$
(iii) $f(f(a)) = f(a)$
(iv) $g(g(a)) = g(a)$

**証明.** $f(g(a)) = 0a1 = a01 = 0$, $g(f(a)) = 0a1 = 0$. 後は定義や命題 1 から従う. □

**命題 6.** $(A,+,\cdot,v,0_A,1_A)$ について, $g(a)=a1$ とおくと, $g(A)=\{x\in A:\exists a\in A \text{ s.t. } x=g(a)\}$ には環構造 $(g(A),+,\cdot,v,0_A,1_A)$ が入り, $g:A\to g(A)$ は準同型.

**証明.** まず準同型性 (といっても $g(A)$ がアである事すら示していないのでまだ準同型ではないが, $g(A)$ の演算は $A$ の演算と一致するように入れるので問題ない). $a,b\in A$ について,

(i) $g(a+b)=a+b-f(a+b)=a+b-f(a)-f(b)=g(a)+g(b)$
(ii) $g(ab)=ab1=a1b1=g(a)g(b)$
(iii) $g(1_A)=1_A1_A=1_A=1_{g(A)}$

次に $g(A)$ の環構造 ($g(A)$ の演算は $A$ の演算と一致するように入れる). $x,y\in g(A)$ とすると, $a,b\in A$ が存在して $(x,y)=(g(a),g(b))$ なので,

(i) $x+y=g(a)+g(b)=g(a+b)\in g(A)$
(ii) $0=01=g(0)\in g(A)$
(iii) $1=11=g(1)\in g(A)$
(iv) $-x=-g(a)=-a+f(a)=(-a)-f(-a)=g(-a)\in g(A)$

より $g(A)$ は 0 を含み, $+,v$ で閉じているので, $A$ のア性から $(g(A),+,\cdot,v,0)$ は群. さらに, $g(A)$ において

(i) $1_{g(A)}=0_A=0_{g(A)}$
(ii) $xy=g(a)g(b)=0a0b=0b=g(b)=y$

より示せた. □

**定理 7.** $A\cong f(A)\times g(A)$

**証明.** $F:A\to f(A)\times g(A)$ を $a\mapsto(f(a),g(a))$ で定め, $G:f(A)\times g(A)\to A$ を $(x,y)\mapsto x+y$ で定めればよい. 準同型性は明らか. 同型性は以下 ($GF,FG$ が恒等写像であるということ). $(x,y)\in f(A)\times g(A)$ について, 定義より $(x,y)=(f(a),g(b))$ となる $a,b\in A$ が取れて,

(i) $f(a)+g(a)=a$
(ii) $f(x+y)=f(f(a))+f(g(b))=f(a)=x$
(iii) $g(x+y)=x+y-f(x+y)=y$

より示せた. □

**定理 8.** $G\cong f(G\times R)$, $R\cong g(G\times R)$

**証明.** $H:G\to f(G\times R)$ を $x\mapsto(x,0)$ で定め, $I:f(G\times R)\to G$ を $(x,y)\mapsto x$ で定めて, $J:R\to g(G\times R)$ を $y\mapsto(0,y)$ で定め, $K:g(G\times R)\to R$ を $(x,y)\mapsto y$ で定めればよい. 準同型性は明らか. 同型性は以下 ($IH$, $HI$, $KJ$, $JK$ が恒等写像であるということ). $IH$, $KJ$ は明らかに恒等写像. $HI$, $JK$ については,

(i) $(x,y)\in f(G\times R)\Rightarrow y=0_R$
(ii) $(x,y)\in g(G\times R)\Rightarrow x=0_G$

を示せばよい.

(i) $(0_G, 0_R)(x, y) = (0_G x, 0_R y) = (x, 0_R)$
(ii) $(x, y)(1_G, 1_R) = (x0_G, y1_R) = (0_G, y)$

より示せた. □

**定理 9.** アの準同型 $h : A \to B$ は, 群, 環の準同型 $h_f : f(A) \to f(B)$, $h_g : g(A) \to g(B)$ を誘導する ($f, g$ の関手性).

**証明.** $h$ を制限すると, 準同型 $h_f : f(A) \to B$, $h_g : g(A) \to B$ が定まる. 後はこれらの像がそれぞれ $f(B)$, $g(B)$ におさまることを言えばよい.

(i) $h_f f(a) = h(0a) = fh(a) \in f(B)$
(ii) $h_g g(a) = h(a1) = gh(a) \in g(B)$

この割り当ては $h$ を制限しているだけなので, 合成や恒等射を保つ. よってこの割り当ては関手的である. □

**定理 10.** 群, 環の準同型 $i : G \to H$, $j : R \to S$ はアの準同型 $i \times j : G \times R \to H \times S$ を誘導する.

**証明.** 成分ごとに $i \times j : (x, y) \mapsto (i(x), j(y))$ と定めればよい. 準同型性は明らか. □

**定理 11.** $hf \times hg = h$, $i = (i \times j)f$, $j = (i \times j)g$ (但し, domain, codomain を, 定理 7, 8 の同型で同一視している)

**証明.** 定義と以上の議論から明らか. □

まとめると, [ア] と [群と環の組 (積)] が関手的に対応しており, 左から右は $f, g$ を取ることで割り当て, 右から左は積を取ることで割り当てると, 圏同値が構成できる.

**注 12** (AT category)**.** 群の圏と環の圏に対するアの圏の立場は, Abelian category と pretopos に対する AT category の立場に似ているように思える (但し, opposite な状況になっている). AT category に関する事は参考文献 [1] をご覧ください. 以下はこの analogy の基本的な部分の表である (断りが無い限り, 対象や射, lim, colim は表の最上段の圏の物とみなす).

| $\mathcal{A}$: アの圏 | $\mathcal{C}$: AT category |
|---|---|
| 1 (アとみなした自明環又は自明群) | 0 (initial object) |
| $G$ が群 $\iff 1 \to G$ が存在する | $X$ が type A $\iff$ 射 $X \to 0$ が存在する |
| $R$ が環 $\iff (\forall G : \text{群} \quad \hom(R, G) = \{0\})$ | $Y$ が type T $\iff (\forall X : \text{type A} \quad \hom(X, Y) = \{0\})$ |
| $f(A) \cong 1 \amalg A$ は群 | $A(Z) := 0 \times Z$ は type A |
| $g(A) \cong 1 \times_{f(A)} A$ は環 | $T(Z) := 0 \amalg_{A(Z)} Z$ は type T |
| $A \cong f(A) \times g(A)$ | $Z \cong A(Z) \amalg T(Z)$ |

このように $f(A), g(A)$ を categorical に定めることもできる. 以上の議論も categorical に進めればもう少し見通しが良かったかもしれない. □

## 2　イデアル, Torsion theory

以下ではアの概念の応用として, アに対するイデアルを考え, 群や環の (正規) 部分群, イデアルとの類似を見る (正規部分群とイデアルの関係については congruence として圏論的に見るのが一般的である). その後, Abelian category における Torsion theory などとの類似を見る. まずイデアルについて, イデアルでアを割る操作をうまく定義できる事を地道に計算で確かめる.

**定義** (イデアル)**.** 以下を満たす $A$ の部分集合 $I$ を $A$ のイデアルという.

(i) $I$ は $A$ の部分群.
(ii) $a \in A$, $x \in I$ について $ax \in I$.

以下 $I$ をイデアルとする. □

$A$ が群の時, $I$ は (正規) 部分群 (可換群については実質部分群なので以下部分群と書く事にする) で, $A$ が環の時, $I$ はイデアルである.

**命題 13.** $A$ にはイデアル $I$ による同値関係が入り, その同値関係で $A$ を割ったものはアになる.

**証明.** $a \sim b :\iff a - b \in I$ で関係を入れると, これは同値関係であることは容易に示せる. この同値関係で $A$ を (集合として) 割ったものを $A/I$ で表す. $a \in A$ で代表される $A/I$ の元を $a + I$ で表すことにする. $(a + I) + (b + I) := (a + b) + I$ と定めると, これが代表元の取り方によらず well-defined であることは容易に示せる. $(a + I)(b + I) := (ab) + I$ と定める. これが代表元の取り方によらず well-defined であることは以下の計算による. $c \in a + I$, $d \in b + I$ について, $cd \sim ab$ を示せばよい. $c = a + x$, $d = b + y$ $(x, y \in I)$ とおけて,

$$\begin{aligned} cd &\sim (a + x)b + (a + x)y \\ &\sim (a + x)b \\ &\sim (a + x)0b + (a + x)b1 \\ &\sim 0b + g(ba) + g(bx) \\ &\sim a0b + ab1 + bx1 \\ &\sim 0ab + ab1 + bx - 0bx \\ &\sim ab \end{aligned}$$

この加法と乗法によって $A/I$ にア構造が入る事は, $A$ のア構造から容易に従う. □

**例 14.** $f(A), g(A)$ は $A$ のイデアルで, 定理 7 より $A/f(A) \cong g(A)$, $A/g(A) \cong f(A)$. □

次に torsion theory について, (opposite な意味での) analogy の中で基本的な物を表としてまとめる. アの圏には零対象はないが, ここに書いていない事でも, きちんと対応した命題が成り立っているはずである. $B \rightarrowtail A \twoheadrightarrow C$ が完全列であるとは, $B \rightarrowtail A$ による $A$ の商が $A \twoheadrightarrow C$ と同型であることを意味する. Torsion theory については参考文献 [2] をご覧ください.

| $\mathcal{A}$: アの圏 | $\mathcal{C}$: Abelian category | 左側の証明について |
|---|---|---|
| $G$ が群 | $T$ が torsion (以下 $T \in \mathcal{T}$ で表す) | |
| $R$ が環 | $F$ が torsion free (以下 $F \in \mathcal{F}$ で表す) | |
| $\hom(R, G) \cong \{0\}$ | $\hom(T, F) \cong \{0\}$ | 0,1 共に $0_G$ に写るので零射のみ |
| 任意の $A$ について,<br>$g(A) \rightarrowtail A \twoheadrightarrow f(A)$ は完全列 | 任意の $C$ について, $T \in \mathcal{T}$, $F \in \mathcal{F}$ と<br>完全列 $T \rightarrowtail C \twoheadrightarrow F$ が存在 | 例 14 より |
| $A \to G$ が単射ならば $A$ は群 | $T \to C$ が epi ならば $C \in \mathcal{T}$ | $0_A, 1_A$ 共に 0 に写るから等しい |
| $R \to A$ が全射ならば $A$ は環 | $C \to F$ が mono ならば $C \in \mathcal{F}$ | $R$ の可換性が $A$ に遺伝する |
| 1 は環でも群でもある | $0 \in \mathcal{F}$, $0 \in \mathcal{T}$ | 自明環, 自明群 |

表に入りきらなかったものが二つあるので, その証明を書く (上の対応によって読み替えたものが torsion theory においても成り立つ).

**命題 15.** $R$ が環 $\iff$ 任意の群 $G$ に対して $\hom(R, G) = \{0\}$

**証明.** 左から右は, $0_R, 1_R$ が $R \to G$ によって共に $0_G$ に写るので零射のみ. 右から左は, $G = f(R)$ とすると, $0, f : R \rightrightarrows f(R)$ が一致するので, $f(R) \cong 1$ で, 定理 7 より $R$ は環. □

**命題 16.** $G$ が群 $\iff$ 任意の環 $R$ に対して $\hom(R, G) = \{0\}$

**証明.** 左から右は, 命題 15 と同様. 右から左は, $R = g(G)$ とすると, $0, g : G \rightrightarrows g(G)$ が一致するので, $g(G) \cong 1$ で, 定理 7 より $G$ は群. □

## 3 終わりに

地味な議論になってしまったが, たまにはこのような計算力の確認をするのも良いと思った. 終わりに書いても意味がないですが, この記事は証明を読むというより, 主張を読んで計算練習すると腕の筋肉がつきます. 準同型定理などが群や環の場合と同様にアでも成立する (様な気がする) が, 教科書の焼き直しになるので詳しくは触れなかった. 非可換な場合についてもアと同様の対象が考えられないか, また一般に二つの代数的対象のクラスについてアのような役割を果たす物が具体的に ((i),...,(v) のような公理のレベルで) どの様に作られるのか, 今後調べたい. 読んでいただきありがとうございました.

## 参考文献

[1] Peter Freyd : Abelian-Topos Categories (Category Theory Mailing List)
[2] Francis Borceux : Handboook of Categorical Algebra 2

# クラブ紹介

現在、灘校数学研究部では以下の活動を行っています。

・ゼミ（週 4 回）

数人のグループで大学以降で扱う数学書を輪読しています。聞き手は数学的に不完全な点を指摘したり、関連する情報を共有したりしています。

・顧問の先生による講義（週 1 回）

顧問の先生に大学以降で学ぶ数学をかみ砕いて講義していただいています。数学的なモチベーションが分かりやすい等、好評です。

・中一講義（週 2 回）

中 3 生が新中 1 生に中学、高校数学、競技数学を教えます。

他にも、数学の問題を作ったり解いたり、遊んだりするなど、自由に活動しています。

# 編集後記

高校 1 年　山中 優輝

本日は灘校文化祭、及び灘校数学研究部にお越しいただきありがとうございます。そして何より、この部誌を読んで頂きありがとうございます。

部員がだんだん LaTeX に慣れて、後輩などもこれで部誌を書き始めているのはとても喜ばしいことなのですが、当の本人、この私がいまだに慣れておらずまだ Word に頼っていることに関しては誠にふがいなく思っております。まあ、来年には LaTeX で統一された、綺麗にまとまった部誌をご覧いただくことができるでしょう。(というかやります)

最後になりましたが、黒木部長や顧問の先生にアドバイスを頂きながら、無事完成させることができましたこと心より感謝しております。　今後とも灘校数学研究部をよろしくお願いいたします。

# Contact　us

Blog

https://nada-mathclub.jimdo.com

Twitter

Twitter@nada_mathclub