Anneaux et corps

Polynômes cyclotomiques

Définition. Si $n \geq 1$, $\Phi_n(X) = \prod_{\substack{k=1 \\ k \wedge n = 1}}^{n} \left(X - e^{\frac{2ik\pi}{n}}\right) = \prod_{\substack{z \in \mathbb{C}^* \\ z \text{ d'ordre } n}} (X - z) \in \mathbb{C}[X]$

(polynôme cyclotomique)

ex: $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = (X-j)(X-j^2) = X^2 + X + 1$, $\Phi_4 = X^2 + 1$

$\forall p$ premier, $\Phi_p = X^{p-1} + X^{p-2} + \cdots + 1$

Propriétés : i) $X^n - 1 = \prod_{d \mid n} \Phi_d$ $\quad (\forall n \geq 1)$

ii) $\forall n \geq 1 \quad \Phi_n = \prod_{d \mid n} (X^d - 1)^{\mu\left(\frac{n}{d}\right)}$

où $\mu(k) = \begin{cases} (-1)^s & \text{si } k = p_1 \cdots p_s \text{ avec } p_i \text{ premiers distincts} \\ 0 & \text{sinon} \end{cases}$

ex. $\Phi_6 = \dfrac{(X^6 - 1)(X - 1)}{(X^2 - 1)(X^3 - 1)}$

iii) $\forall n \geq 1$, $\Phi_n \in \mathbb{Z}[X]$

(dl à coeff. entiers)

iv) $\deg \Phi_n = \varphi(n)$

Théorème $\forall n \geq 1$, $\Phi_n(X)$ irréductible sur $\mathbb{Q}$.

Démo. Si $P(X) = (X - a_1) \cdots (X - a_N) \in \mathbb{C}[X]$,

on note $\Delta_P = \prod_{1 \le i < j \le N} (a_i - a_j)^2$ discriminant

[Si $P = X^2 + \alpha X + \beta$, $\Delta_P = (a_1 - a_2)^2 = (a_1 + a_2)^2 - 4 a_1 a_2$
$= \alpha^2 - 4\beta$]

Par exemple $\Delta_{X^n - 1} = \pm n^n$

car $\Delta_P = \pm \prod_{1 \le i \le N} P'(a_i)$ (car $P'(a_i) = \prod_{\substack{j=1 \\ j \neq i}}^{N} (a_i - a_j)$)

or $P'(X) = N \prod_{i=1}^{N-1} (X - \xi_i)$

$\Rightarrow \Delta_P = \pm \left(\prod_{i=1}^{N} \prod_{j=1}^{N-1} (a_i - \xi_j) \right) N^N$

$= \pm N^N \prod_{j=1}^{N-1} \underbrace{\prod_{i=1}^{N} (\xi_j - a_i)}_{P(\xi_j)}$

$= \pm N^N \prod_{j=1}^{N-1} P(\xi_j)$

(ξ_j : racines de P')

si $P = X^N - 1$, $P' = N X^{N-1} \Rightarrow \xi_1 = \cdots = \xi_{N-1} = 0$

$\Rightarrow \Delta_{X^N - 1} = \pm N^N \prod_{j=1}^{N-1} (0^N - 1) = \pm N^N$.

Soit $z = e^{\frac{2 i \ell \pi}{n}}$ $\quad \ell \wedge n = 1$

Soit $P \in \mathbb{Q}[X]$ le polynôme minimal unitaire de z sur $\mathbb{Q}$.

P irréductible sur $\mathbb{Q}$.

$P \in \mathbb{Z}[X]$.

En effet, $P \in \mathbb{Q}[X]$, $\exists Q \in \mathbb{Q}[X]$, $PQ = X^n - 1$

$\exists \alpha, \beta$ entiers $\neq 0$, αP, $\beta Q \in \mathbb{Z}[X]$

Alors $\alpha P \beta Q = \alpha\beta(X^n - 1)$

$\Rightarrow$ (lemme de Gauss) $c(\alpha P)\, c(\beta Q) = \alpha\beta$

[$c(a_0 + \dots + a_d X^d) = \text{pgcd}(a_0, \dots, a_d)$ contenu]

$\Rightarrow \quad \underbrace{\frac{\alpha P}{c(\alpha P)}}_{\in \mathbb{Z}[X]} \underbrace{\frac{\beta Q}{c(\beta Q)}}_{\in \mathbb{Z}[X]} = \underbrace{X^n - 1}_{\text{unitaire}}$

$\Rightarrow$ coeff. dominant de $\frac{\alpha P}{c(\alpha P)} = 1 \quad \Rightarrow \alpha = c(\alpha P) \Rightarrow P = \frac{\alpha P}{\alpha} \in \mathbb{Z}[X]$.

$= \frac{\alpha}{c(\alpha P)}$ (car P unitaire)

Si p premier, $P(X^p) \equiv P(X)^p \mod p$ (dans $\mathbb{Z}[X]$)

(car dans $\mathbb{Z}/p\mathbb{Z}[X]$, $P(X)^p = P(X^p)$)

($\forall a \in \mathbb{Z}/p\mathbb{Z}$, $a^p = a$)

En particulier $P(z^p) = P(z)^p = 0 \mod p\mathbb{Z}[z]$

$p \mid P(z^p)$ dans l'anneau $A = \mathbb{Z}[z]$

Si $p \nmid n$ $\quad P(z^p) = 0$

Par l'absurde : si $P(z^p) \neq 0$

$P(X) = \prod_j (X - z_j)$ où z_j racines n ièmes de 1.

$\Rightarrow P(z^p) = \prod_j (z^p - z_j) =$ produit de différences de racines nièmes de 1

$\Rightarrow$ divise $\prod_{1 \le \alpha < \beta \le n} (z_\alpha - z_\beta)^2 = \Delta_{X^n - 1} = \pm n^n$ dans $A = \mathbb{Z}[z]$

($\forall \alpha \; z_\alpha = z^{m_\alpha}$ pour un $m_\alpha \in \mathbb{N}$)

donc $p \mid P(\zeta^p) \mid n^n$ dans A

$\Rightarrow \frac{n^n}{p} \in A \cap \mathbb{Q} = \mathbb{Z}$

[en effet si $\deg P = d$, alors $\mathbb{Q}(\zeta) = \mathbb{Q} \oplus \mathbb{Q}\zeta \oplus \cdots \oplus \mathbb{Q}\zeta^{d-1}$

$A = \mathbb{Z}[\zeta] = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}\zeta^{d-1}$

$\Rightarrow A \cap \mathbb{Q} = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}\zeta^{d-1} \cap \mathbb{Q} = \mathbb{Z}$]

donc $p \mid n^n$ dans $\mathbb{Z}$ $\Rightarrow p \mid n$.

Conclusion si p premier $\nmid n$, $P(\zeta^p) = 0$.

On en déduit que si $\alpha \wedge n = 1$ alors $\alpha = p_1 \cdots p_\ell$ où p_i premiers $\nmid n$

et $\zeta^\alpha = \left((\zeta^{p_1})^{p_2 \cdots} \right)^{p_\ell} \Rightarrow P(\zeta^\alpha) = 0$.

donc $\forall \alpha \wedge n = 1$, ζ^α racine de P donc $\Phi_n = \prod_{\alpha \wedge n = 1} (X - \zeta^\alpha) \mid P$

$\Rightarrow \Phi_n = P$ irréductible.

Corollaire

Théorème de Gauss sur les nombres constructibles

Définition. $z \in \mathbb{C}$ constructible si

$\exists a_0, \ldots, a_N \in \mathbb{C}$, $z \in \mathbb{Q}(\sqrt{a_0}, \sqrt{a_1}, \ldots, \sqrt{a_N})$

et $\forall i$, $a_i \in \mathbb{Q}(\sqrt{a_0}, \ldots, \sqrt{a_{i-1}})$ $\quad (a_0 \in \mathbb{Q})$

ex. $\cos \frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4} \in \mathbb{Q}(\sqrt{5})$, $e^{2i\pi/5} \in \mathbb{Q}\left(\sqrt{5}, \sqrt{\frac{-5-\sqrt{5}}{2}}\right)$

Théorème. Le nombre $e^{\frac{2i\pi}{n}}$ constructible

$\Leftrightarrow$ $n = 2^\alpha F_{i_1} \cdots F_{i_k}$

où $\alpha \in \mathbb{N}$, $F_{i_1}, \dots, F_{i_k}$ nombres premiers de Fermat $\neq$.

[$F_n = 2^{2^n} + 1$ $\quad F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$ premiers

$F_5 = 641 \times 6700437$ non premier]

démo de $\Rightarrow$: z constructible $\Rightarrow z \in \mathbb{Q}(\sqrt{a_0})(\sqrt{a_1}) \cdots (\sqrt{a_N})$

$\mathbb{Q} \subset \underbrace{\mathbb{Q}(\sqrt{a_0})}_{\text{degré 1 ou 2}} \subset \underbrace{\mathbb{Q}(\sqrt{a_0})(\sqrt{a_1})}_{\text{degré 1 ou 2}} \subset \cdots \subset \mathbb{Q}(\sqrt{a_0}) \cdots (\sqrt{a_N})$

$X^2 - a_0 \in \mathbb{Q}[X]$

$\Rightarrow$ (multiplicativité des degrés) $\quad [\mathbb{Q}(\sqrt{a_0}, \dots, \sqrt{a_N}) : \mathbb{Q}] = 2^\alpha$

$\Rightarrow \quad [\mathbb{Q}(z) : \mathbb{Q}] = 2^\gamma \quad (\gamma \in \mathbb{N})$ $\quad \alpha \leq N+1$.

$\forall n$ si $z = e^{2i\pi/n}$, $\quad [\mathbb{Q}(z) : \mathbb{Q}] = \deg \Phi_n = \varphi(n)$

$\varphi(n) = 2^\gamma \Rightarrow \quad n = 2^p \times$ un produit de nombres premiers $p_i \neq$

où $\varphi(p_i) = 2^{n_i} \Rightarrow p_i = 2^{n_i} + 1 \Rightarrow n_i = 2^{\lambda_i} \cdots$
$\quad = p_{i-1}$

]

Exo. Soit p premier, soit $N = p^d - 1$

Alors les facteurs irréductibles de Φ_N dans $\mathbb{F}_p[X]$ sont de degré d.

[En particulier, $\forall d$, $\exists$ un pol. irréductible de degré d sur $\mathbb{F}_p$]

Analyse fonctionnelle

Fonctions höldériennes

Définition. Soit $f : \mathbb{R} \longrightarrow \mathbb{C}$ tq f 2π-périodique
On dit que f est α-Höldériennes avec $0 < \alpha \leq 1$ si

$$|f|_{C^\alpha} = \sup_{x \neq y} \frac{|f(x) - f(y)|}{|x-y|^\alpha} < \infty$$

$$\left[\Rightarrow |f(x) - f(y)| \leq |f|_{C^\alpha} |x-y|^\alpha \right]$$

Théorème 1) Si $f : \mathbb{R} \to \mathbb{C}$ 2π périodique α-Höldérienne, $0 < \alpha \leq 1$
alors $S_n f \xrightarrow[n \to \infty]{} f$ uniformément

2) si de plus $\frac{1}{2} < \alpha$, alors $S_n f$ converge normalement

Rappel : $S_n f(x) = \sum_{k=-n}^{n} c_k(f)\, e^{ikx}$

où $c_k(f) = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(y) e^{-iky}\, dy$

démo 1) $S_n f(x) - f(x) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \sum_{k=-n}^{n} f(y) e^{-iky} e^{ikx}\, dx - f(x)$

$$= \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x-y) \underbrace{\sum_{k=-n}^{n} e^{iky}}_{D_n(y)}\, dy - f(x)$$

$$= \frac{1}{2\pi} \int_{-\pi}^{\pi} \left(f(x-y) - f(x) \right) D_n(y)\, dy$$

où $D_n(y) = \dfrac{\sin\left(n + \frac{1}{2}\right) y}{\sin y/2}$

$$S_n f(x) - f(x) = \underbrace{\frac{1}{2\pi}\int_{|y|<\delta}}_{A} + \underbrace{\frac{1}{2\pi}\int_{|y|\geq\delta}}_{B} \quad \text{où } 0<\delta<\pi$$

$$|A| \leq \frac{1}{2\pi}\int_{-\delta}^{\delta} \left|\frac{f(x-y)-f(x)}{\sin y/2}\right| \left|\sin\left(n+\tfrac{1}{2}\right)y\right| dy$$

$$\leq \frac{1}{2\pi} 2\int_0^{\delta} \frac{y^\alpha}{\sin(y/2)}\, dy \qquad \text{car } \forall\ 0\leq t\leq \frac{\pi}{2},\ \frac{\sin t}{t} \geq \frac{2}{\pi}$$

$$\leq \frac{1}{\pi}\cdot\pi\int_0^{\delta} y^{\alpha-1}\, dy = \frac{\delta^\alpha}{\alpha}$$

B_1 :

$$\frac{1}{2\pi}\int_{\delta}^{\pi} \underbrace{\frac{f(x-y)-f(x)}{\sin(y/2)}}_{h_x(y)} \sin\left(n+\tfrac{1}{2}\right)y\ dy$$

$$B_1 = \frac{1}{2}(B_1+B_1) = \frac{1}{4\pi}\left[\int_{\delta}^{\pi} h_x(y)\sin\left(n+\tfrac{1}{2}\right)y\ dy - \int_{\delta}^{\pi} h_x(y)\sin\left(n+\tfrac{1}{2}\right)\left(y+\frac{\pi}{n+\frac{1}{2}}\right)dy\right]$$

$$\tau := \frac{\pi}{n+\frac{1}{2}} \qquad = \frac{1}{4\pi}\left[\int_{\delta}^{\pi} h_x(y)\sin\left(n+\tfrac{1}{2}\right)y\, dy - \int_{\delta+\tau}^{\pi+\tau} h_x(y-\tau)\sin\left(n+\tfrac{1}{2}\right)y\, dy\right]$$

$$= \frac{1}{4\pi}\left[\underbrace{\int_{\delta}^{\pi}\left(h_x(y)-h_x(y-\tau)\right)\sin\left(n+\tfrac{1}{2}\right)y\, dy}_{I} + \int_{\delta}^{\delta+\tau} h_x(y-\tau)\sin\left(n+\tfrac{1}{2}\right)y\, dy - \int_{\pi}^{\pi+\tau} h_x(y-\tau)\sin\left(n+\tfrac{1}{2}\right)y\, dy\right]$$

$$\text{Or } \left|\int_{\delta}^{\delta+\tau} h_x(y-\tau)\sin\left(n+\tfrac{1}{2}\right)y\, dy\right| \leq \pi\tau\,|\delta|^{\alpha-1} \qquad 0<\tau<\frac{\delta}{2}$$

$$|h_x(y)| = \left|\frac{f(x-y)-f(x)}{\sin y/2}\right| \le \frac{|y|^\alpha}{\frac{2}{\pi}|y|/2} = \pi |y|^{\alpha-1}$$

$$h_x(y) - h_x(y-\tau) = \frac{f(x-y)-f(x)}{\sin y/2} - \frac{f(x-y+\tau)-f(x)}{\sin \frac{y-\tau}{2}}$$

$$= \frac{f(x-y)-f(x)}{\sin y/2} - \frac{f(x-y+\tau)-f(x-y)}{\sin\left(\frac{y-\tau}{2}\right)} - \frac{f(x-y)-f(x)}{\sin\left(\frac{y-\tau}{2}\right)}$$

$$= \left(f(x-y)-f(x)\right)\left(\frac{\sin\left(\frac{y-\tau}{2}\right)-\sin y/2}{\sin y/2 \sin\left(\frac{y-\tau}{2}\right)}\right) - \frac{f(x-y+\tau)-f(x-y)}{\sin\frac{y-\tau}{2}}$$

$$I \le \pi\left[2\|f\|_\infty \frac{\tau/2}{\frac{2}{\pi}\frac{\delta}{2}\,\frac{2}{\pi}\frac{\delta}{4}} + \frac{\tau^\alpha}{\frac{2}{\pi}\frac{\delta}{4}}\right]$$

$$\le C\left(\frac{\tau}{\delta^2} + \frac{\tau^\alpha}{\delta}\right)$$

$$B_1 \le C'\left(\frac{\tau}{\delta^2} + \frac{\tau^\alpha}{\delta} + \tau\delta^{\alpha-1}\right) \qquad \tau = \frac{\pi}{n+\frac{1}{2}}$$

Soit $\varepsilon > 0$. Soit $\delta > 0$ tq $\frac{\delta^\alpha}{\alpha} < \varepsilon$

Soit $n > 0$ tq $\frac{\tau}{\delta^2} + \frac{\tau^\alpha}{\delta} + \tau\delta^{\alpha-1} < \varepsilon$

$|S_n f(x) - f(x)| \le \varepsilon + 2C'\varepsilon$ $(\forall x)$.

...

Probabilités

Théorème Loi forte des grands nombres

Soient (X_n) v.a. i.i.d de même loi X_1 tq $E(|X_1|) < \infty$

alors $\dfrac{X_1 + \cdots + X_n}{n} \xrightarrow[n\infty]{p.s.} E(X_1)$

démo. si $E(|X_1|^4) < \infty$

Supposons $E(X_1) = 0$

Alors $\left(\dfrac{X_1 + \cdots + X_n}{n}\right)^4 = \dfrac{X_1^4 + \cdots + X_n^4}{n^4} + \sum_{i<j} \dfrac{1}{n^4} 6 X_i^2 X_j^2$

$+ \sum_{i \neq j} \dfrac{4}{n^4} X_i^3 X_j$

$+ \sum_{\substack{i_1, i_2, i_3 \\ 2 \text{ à } 2 \neq}} 12 \dfrac{X_{i_1}^2 X_{i_2} X_{i_3}}{n^4} + 24 \sum_{i_1 < i_2 < i_3 < i_4} \dfrac{X_{i_1} X_{i_2} X_{i_3} X_{i_4}}{n^4}$

$\Rightarrow E\left(\left(\dfrac{X_1 + \cdots + X_n}{n}\right)^4\right) = \dfrac{n E(X_1^4)}{n^4} + 3 \dfrac{n(n-1)}{n^4} E(X_1^2 X_2^2)$

$\leq \dfrac{E(X_1^4)}{n^3} + \dfrac{3}{n^2} E(X_1^4)$

$\leq \dfrac{C}{n^2}$

$\Rightarrow \sum_{n=1}^{\infty} E\left(\left(\dfrac{X_1 + \cdots + X_n}{n}\right)^4\right) < \infty$

$E\left(\sum_{n=1}^{\infty} \left(\dfrac{X_1 + \cdots + X_n}{n}\right)^4\right)$

donc p.s. $\lim_{n\infty} \left(\frac{X_1+\cdots+X_n}{n}\right)^4 = 0$

p.s. $\lim_{n\infty} \frac{X_1+\cdots+X_n}{n} = 0$ □

Théorème central limite

Soient X_n, $n \in \mathbb{N}$, des v.a. i.i.d tq $E(|X_1|^2) < \infty$

alors $\sqrt{n}\left(X_1+\cdots+X_n - nE(X_1)\right) \xrightarrow{\text{loi}} \mathcal{N}(0,\sigma^2)$

où $\forall m \in \mathbb{R}, \forall \sigma > 0$ $\mathcal{N}(m,\sigma^2)$ est la loi :

$$P(X \le t) = \int_{-\infty}^{t} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\left(\frac{t-m}{\sigma}\right)^2} dt$$

remarques. Si X de loi $\mathcal{N}(m,\sigma^2)$, alors $E(X) = m$

$$\text{var}(X) = \sigma^2$$

Définitions

1) fonctions caractéristiques

Si X v.a. dans $\mathbb{R}^d$ on pose

$$\forall \xi \in \mathbb{R}^d, \quad \Phi_X(\xi) = E\left(e^{i\,\xi\cdot X}\right)$$

ex. si $X \sim \mathcal{N}(m,\sigma^2)$ alors

$$\Phi_X(\xi) = \int_{-\infty}^{\infty} e^{i\xi t} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{1}{2}\left(\frac{t-m}{\sigma}\right)^2} dt$$

$s = i\xi$ $\quad g(s) = \int_{-\infty}^{\infty} e^{st} \frac{1}{\sqrt{2\pi}\sigma} e^{-1/2\left(\frac{t-m}{\sigma}\right)^2} dt$

$$= \int_{-\infty}^{\infty} e^{s(\sigma y + m)} \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}y^2} dy \quad \overset{y = \frac{t-m}{\sigma}}{=}$$

$$= \frac{e^{sm}}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{(y-s\sigma)^2}{2}} e^{+\frac{s^2\sigma^2}{2}} dy$$

$$= \sqrt{2\pi}$$

$$= e^{sm} e^{\frac{-s\sigma^2}{2}} \qquad (s \in \mathbb{R})$$

g holomorphe en $s \Rightarrow \forall s \in \mathbb{C}$, $g(s) = e^{sm} e^{+\frac{s^2\sigma^2}{2}}$

$$\Rightarrow \Phi_X(\xi) = g(i\xi) = e^{i\xi m} e^{-\frac{\xi^2\sigma^2}{2}} \qquad \square$$

2) $X = (X_1, \dots, X_d)$ est un vecteur gaussien

si $\forall i$ X_i v.a. réelle et $\forall a_1, \dots, a_d \in \mathbb{R}$, $a_1 X_1 + \dots + a_d X_d$ suit une loi gaussienne $\mathcal{N}(m, \sigma^2)$

Dans ce cas on note $\operatorname{var}(X) = \left(E\big((X_i - E(X_i))(X_j - E(X_j))\big) \right)_{1 \le i,j \le d}$

$\in \mathcal{S}_d(\mathbb{R})$ (symétrique)

$$\operatorname{var}_{ij}(X) = E(X_i X_j) - E(X_i) E(X_j)$$

Théorème. $X_1, \dots, X_d$ 2à2 indépendantes $\Leftrightarrow$ $\operatorname{var}(X)$ diagonale.

Exo.

Exercice 1.
Soit X, Y deux variables aléatoires indépendantes de loi $\mathcal{N}(0,1)$. Montrer que $X+Y$ et $X-Y$ sont indépendantes.

(TD 8)

(X, Y) vecteur gaussien

car $aX + bY$ est de loi $\mathcal{N}(0, a+b)$

$$\operatorname{var}(X+Y, X-Y) = \begin{pmatrix} E((X+Y)^2) - E(X+Y)^2 & E(X^2-Y^2) - E(X+Y)E(X-Y) \\ E(X^2-Y^2) - E(X+Y)E(X-Y) & E((X-Y)^2) - E(X-Y)^2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

$$E(X^2 - Y^2) = E(X^2) - E(Y^2) = \operatorname{var}(X) - \operatorname{var}(Y) = 1 - 1 = 0$$

$$E(X+Y)\,E(X-Y) = E(X)^2 - E(Y)^2 = 0$$

rem $\operatorname{var}(X+Y) = E((X+Y)^2) - E(X+Y)^2 = \operatorname{var}(X) + \operatorname{var}(Y)$

$= 2$

Exercice. Vérifier que si $X = \mathcal{N}(m, \sigma^2)$ alors

$$E(X) = m \text{ et } \operatorname{var}(X) = \sigma^2$$

c-à-d : $E(X) = \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} t\, e^{-\frac{1}{2}\left(\frac{t-m}{\sigma}\right)^2} dt$

$$\operatorname{var}(X) = \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} t^2 e^{-\frac{1}{2}\left(\frac{t-m}{\sigma}\right)^2} dt - E(X)^2$$

$$E(X) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} (\sigma y + m) e^{-\frac{y^2}{2}} dy = m \underbrace{\frac{\int_{-\infty}^{\infty} e^{-y^2/2}\, dy}{\sqrt{2\pi}}}_{=1} + \frac{\sigma}{\sqrt{2\pi}} \underbrace{\int_{-\infty}^{\infty} y e^{-y^2/2} dy}_{=0}$$

$y = \frac{t-m}{\sigma}$

$= m$

$$E(X^2) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} (\sigma y + m)^2 e^{-y^2/2}\, dy$$

$$= m^2 + \frac{\sigma^2}{\sqrt{2\pi}} \int_{-\infty}^{\infty} y^2 e^{-y^2/2}\, dy$$

$$y \cdot \left| \begin{array}{l} y e^{-y^2/2} \\ u = y \quad v' = y e^{-y^2/2} \\ u' = 1 \quad v = -e^{-y^2/2} \end{array} \right.$$

$$\underbrace{\text{i.p.p.} \left[-y e^{-y^2/2} \right]_{-\infty}^{+\infty}}_{0} + \underbrace{\int_{-\infty}^{\infty} e^{-y^2/2}\, dy}_{\sqrt{2\pi}}$$

$$= m^2 + \sigma^2 \implies \mathrm{Var}(X) = \sigma^2.$$