TD : Polynômes cyclotomiques

1.1

a) Soit n un nombre premier

$$\Phi_n(X) = \prod_{1 \le k \le n-1} \left(X - e^{\frac{2ik\pi}{n}}\right)$$

$$= \frac{1}{X-1} \prod_{1 \le k \le n} \left(X - e^{\frac{2ik\pi}{n}}\right)$$

$$= \frac{1}{X-1} (X^n - 1) = \sum_{k=0}^{n-1} X^k$$

b)

$$X^n - 1 = \prod_{1 \le k \le n} \left(X - e^{\frac{2ik\pi}{n}}\right)$$

Il suffit de montrer que $U_n = \bigsqcup_{d \mid n} P_d$

En effet, un élément de P_d est d'ordre d.
Donc $\bigsqcup_{d \mid n} P_d$ est une partition de U_n selon l'ordre de l'élément.

c) Pour m premier, $\Phi_m(X) \in \mathbb{Z}[X]$.
$m = 1 \sim 3$, O.K.
Supposons qu'au rang m, $\Phi_m(X) \in \mathbb{Z}[X]$.
Pour $m+1$,

$$X^{m+1} - 1 = \Phi_{m+1}(X) \underbrace{\prod_{\substack{d \mid m+1 \\ d \neq m+1}} \Phi_d(X)}_{P(X)} \rightarrow \text{unitaire}$$

On effectue une D.E. dans $\mathbb{Z}[X]$.

$$X^{m+1} - 1 = P(X) \times Q(X) + R(X) \quad \text{avec } Q, R \in \mathbb{Z}[X]$$

$\deg R < \deg P$

$$\Phi_{m+1} P = PQ + R$$

$$P(\underbrace{\Phi_{m+1} - Q}_{=0}) = R \quad \text{car } \deg R < \deg P$$

Donc, $\Phi_{m+1} = Q \in \mathbb{Z}[X]$.

1.2 $\quad m \wedge n = 1$

$$P_m \sqcup P_n \qquad P_{mn}$$

Soit $z \in P_n$, k, $\quad z = e^{\frac{2ik\pi}{m}}$ avec $k \wedge m = 1$

$$e^{\frac{2ik\pi}{m}} = e^{\frac{2ikn\pi}{mn}}, \quad z \notin P_{mn}$$

Inversement, si $z \in P_{mn}$, $z \notin P_m$.

~~Cependant~~ $\cancel{|P_m \sqcup P_n|}$

Donc, $\Phi_{mn}(X) \wedge \Phi_m(X)\Phi_n(X) = 1$.

2.1

a) $\quad P = \sum_{i=0}^{N} a_i X^i \in \mathbb{Z}[X]$

$$P(n+kP(n)) = \sum_{i=0}^{N} a_i \,(n+kP(n))^i$$

Mq: $P(n) \mid P(n+kP(n))$

$$\sum_{i=0}^{N} a_i (n+kP(n))^i = \sum_{i=0}^{N} a_i\, n^i \quad [P(n)]$$

$$= P(n) \; [P(n)] \quad = 0 \; [P(n)]$$

$$P(n+kP(n)) = \sum_{i=0}^{N} a_i \sum_{j=0}^{i} \binom{i}{j} n^j (kP(n))^{i-j}$$

$$= P(n) + \sum_{i=1}^{N} a_i \sum_{j=0}^{i-1} \binom{i}{j} n^j (kP(n))^{i-j}$$

$$= P(n) + kP(n) \underbrace{\sum_{i=1}^{N} a_i \sum_{j=0}^{i-1} \binom{i}{j} n^j (kP(n))^{i-1-j}}_{\text{divisible par } P(n)}$$

$$\sum_{i=1}^{N} a_i \sum_{j=0}^{i-1} \binom{i}{j} n^{j} (kP(n))^{i-1-j}$$

$$= \sum_{i=1}^{N} a_i \times i\, n^{i-1} \, [P(n)]$$

$P(X)-P(X)$
$=(Y-X)\,Q(X,Y)$

$$P(n+kP(n)) = P(n) + P'(n)\,kP(n) + \dots + \underbrace{\frac{P^{(d)}(n)}{d!}}_{\in \mathbb{Z}} k^d P(n)^d$$

T en n

b) Par l'absurde notons Π le produit des facteurs premiers distincts intervenant dans les $P(n)$.

Soit $n \in \mathbb{N}^*$ t.q. $P(n)$ non nul.

Pour $k \in \mathbb{N}^*$.

$$P(n+k\Pi P(n)) = P(n)\,(1 + k\Pi \quad m(k))$$

Comme $|P(x)| \xrightarrow[x \to +\infty]{} +\infty$

Soit k suffisament grand t.q. $|P(n+k\Pi P(n))| > |P(n)|$

Donc $\cancel{k\Pi P(n) m(k) \neq 0}$ $|1+k\Pi m(k)| \geq 2$

Soit p un facteur premier de $1+k\Pi P(n) m(k)$.

mais $p \nmid \Pi$ ↯.

Donc cet ensemble est infini.

2.2

a) D'après 1.1. $X^m - 1 = \Phi_m(X) \prod_{\substack{d|m \\ d<m}} \Phi_d(X)$ car les polynômes Φ_k sont dans $\mathbb{Z}[X]$.

$$a^m - 1 \equiv 0 \ [p] \Rightarrow a^m \equiv 1 \ [p]$$

b) On note $d = \omega(\bar{a})$

Avec a), $\bar{a}^m = 1$ donc $d \mid m$.

et par définition, $a^d - 1 \equiv 0 \ [p]$

$0 = \prod_{\delta | d} \Phi_\delta(\bar{a})$ donc comme $\mathbb{Z}/p\mathbb{Z}$ est un corps !

donc $\exists\, \delta$ diviseur de d, $\Phi_\delta(\bar{a}) = 0$.

c) Si $d < m$. $X^m - 1 = \Phi_m(X) \prod_{\substack{d|m \\ d<m}} \Phi_d(X)$

$\Rightarrow m X^{m-1} = \Phi'_m(X) \prod_{\substack{d|m \\ d<m}} \Phi_d(X) + \Phi_m(X) \left(\prod_{\substack{d|m \\ d<m}} \Phi_d(X) \right)'$

donc a est racine double de $X^m - 1$

donc $p \mid m a^{m-1}$

mais $p \wedge m = 1$ et a est non nul. $\lightning$

$\Rightarrow d = m$.

$a \in (\mathbb{Z}/p\mathbb{Z})^* \Rightarrow a^{p-1} \equiv 1 \; [p]$

$\Rightarrow \omega(a) = d = m \quad , \quad m \mid p-1$

Bref, $p = 1 \; [m]$

d) Appliquons 2.1 avec $P = \Phi_m(X) \in \mathbb{Z}[X]$.
On peut alors trouver une infinité de nombres premiers pour lesquels il existe a, $\Phi_m(a) = 0 \; [p]$.
Chacun de ces premiers p est congru à $1 \; [m]$.
<u>Conclusion</u> : $\exists$ une infinité de premiers de la forme $1 + km$.

3.1

a) $m = \omega(\zeta)$

$p = \omega(\eta)$

<u>premier cas</u> : $m \wedge p = 1$ $\quad \omega(\zeta\eta) = mp$.

<u>2ème cas</u> : $m = pq$ $\quad l = \omega(\zeta\eta)$

$(\zeta\eta)^l = e \Rightarrow \zeta^l = \eta^{-l}$

$p \mid l$: $\zeta^l = e$, $\quad l = m$

$p \nmid l$: $\omega(\eta^{-l}) = p$ $\quad \omega(a^n) = \dfrac{\omega(a)}{n \wedge \omega(a)}$

donc $\omega(\zeta^l) = p$ or $\omega(\zeta^l) = \dfrac{m}{m \wedge l} = \dfrac{m}{q}$

Or $l \mid m$: $l = q$

b) $p \nmid m$. $\Phi_n(X)\Phi_m(X) = \Phi_m(X^p)$ (?)

1) pas de racine commune car $n > m$ + DEF

2) Si $\begin{cases} \Phi_m(\zeta)=0 \\ \Phi_n(\zeta)=0 \end{cases}$ $\omega(\zeta) = m \Rightarrow \omega(\zeta^p) = \frac{m}{m \wedge p} = m$

$\Rightarrow \Phi_m(\zeta^p) = 0$

$\omega(\zeta) = n \Rightarrow \omega(\zeta^p) = \frac{n}{n \wedge p} = \frac{n}{p} = m$

$\Rightarrow \Phi_m(\zeta^p) = 0$.

3) $\deg(\Phi_n \Phi_m) = \varphi(mp) + \varphi(m)$

$= \varphi(m)\varphi(p) + \varphi(m)$

$= \varphi(m)(p-1+1) = \varphi(m)\, p$

$= \deg \phi_m(X^p)$

4) Normalisés.

Si $p \mid m$, même méthode.

$\phi_n(X) = \phi_m(X^p)$ (?)

$\Rightarrow \deg \Phi_{mp} = p\varphi(m) = \deg \Phi_n(X^p)$

$l = p_1^{\alpha_1} \dots p_r^{\alpha_r}$

$\varphi(l) = l\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right)$

$\varphi(p_i l) = p_i \varphi(l)$

Si $\omega(\zeta) = mp$, $\omega(\zeta^p) = m$ et $\phi_m(\zeta^p) = 0$

$\Rightarrow \Phi_{mp}(X) \mid \Phi_m(X^p)$

$\Rightarrow \Phi_{mp}(X) = \Phi_m(X^p)$

Φ_n ne vérifie pas (S) dans $\mathbb{Z}/p\mathbb{Z}[X]$

$\Phi(X^p) = \Phi(X)^p$

$\frac{\Phi_m(X^p)}{\Phi_m(X)} = \Phi_m(X)^{p-1}$ non (S)

c) Si $n \mid p-1$,

$$X^{p-1} - \bar{1} = \prod_{a \in \mathbb{Z}/p\mathbb{Z}^*} (X - a)$$

$$= \prod_{d \mid p-1} \Phi_d(X)$$

il y a Φ_n

d) Si Φ_n est dissocié, on a $p \nmid n$ (c.f. a))

$\exists\, a,\quad \phi_n(\bar{a}) = \bar{0}$

Avec 2), $\omega(\bar{a}) = n$, car $\bar{a}^{p-1} = \bar{1}$

$n \mid p-1$.

2.2

a) $$X^m - 1 = \Phi_m(X) \prod_{\substack{d|m \\ d \neq m}} \Phi_d(X)$$

$$a^m - 1 = \Phi_m(a) \prod \Phi_d(a) \equiv 0 \ [p]$$

Donc, $a^m \equiv 1 \ [p]$.

b) $$\cancel{\bar{a}^d = \bar{1} \iff a^d \equiv 1 \ [p]}$$

$\bar{a}^m = \bar{1}$, donc $d \mid m$.

$$X^d - 1 = \prod_{\delta | d} \Phi_\delta(X)$$

$$a^d - 1 \equiv 0 \ [p]$$

p divise $\prod_{\delta | d} \Phi_\delta(a)$

Comme p est un premier, il existe δ diviseur de d t.q. $\Phi_\delta(a) \equiv 0 \ [p]$

c) Si $d < m$. $\delta \leq d < m$

$$X^m - 1 = \Phi_m(X) \, \Phi_\delta(X) \prod_{\substack{d|m \\ d \neq m, \delta}} \Phi_d(X)$$

$\frac{d}{dX}$

$$m X^{m-1} = \Phi_m'(X) \Phi_\delta(X) \prod \Phi_d(X) + \Phi_\delta'(X) \Phi_m(X) \prod \Phi_d(X) + \Phi_m(X) \Phi_\delta(X) \left(\prod \Phi_d\right)'$$

$$m\bar{a}^{m-1} = \Phi_\delta(\bar{a}) (\quad) + \Phi_m(\bar{a}) (\quad) + \Phi_m(\bar{a}) (\quad)$$

$$= 0 + 0 + 0 = 0 \quad \text{dans } \mathbb{Z}/p\mathbb{Z}$$

Donc, $\bar{a}$ annule la dérivée de $X^m - 1$.

Ainsi, $p \mid m a^{m-1}$, $p \mid a$

Mais, $a^m \equiv 1\ [p]$. Contradiction !

$\Rightarrow d = m$.

$a \wedge p = 1 \Rightarrow a^{p-1} \equiv 1\ [p]$

$\Rightarrow m \mid p-1$

$\Rightarrow p-1 \equiv 0\ [m]$

$\Rightarrow p \equiv 1\ [m]$.

d) Appliquons 2.1 avec $P = \Phi_m(X) \in \mathbb{Z}[X]$

Alors, il existe une infinité de nombres premiers p t.q. $\exists\, a \in \mathbb{N}^*$ $p \mid P(a)$.

$\Phi_m(a) \equiv 0\ [p]$

Donc, $p \equiv 1\ [m]$.

Alors $p = 1 + km$ avec $k \in \mathbb{N}^*$.

Donc, cet ensemble est infini.

3.1

a) Si $p \nmid m$, l'ordre de $\zeta\eta$ est mp.

Si $p \mid m$, on note $m = lp$.

On note $\zeta = e^{i2\pi \frac{kp+r}{m}}$ $\quad (kp+r) \wedge m = 1$ $\quad \begin{cases} k_1 < l \\ r < p \end{cases}$

$\eta = e^{i2\pi \frac{k_2}{p}}$ $\quad k_2 < p$

$\zeta\eta = e^{i2\pi \frac{kp+r+lk_2}{lp}}$

$\zeta^d = \eta^{-d}$

On note $d = \omega(\zeta\eta)$. On sait déjà $d \mid m$.

$p \mid d$: $\zeta^d = 1 \Rightarrow m \mid d \Rightarrow m = d$

$p \nmid d$: $\omega(\eta^{-d}) = p$

donc, $\omega(\zeta^d) = p$ car $\omega(\zeta^d) = \dfrac{m}{d \wedge m} = \dfrac{m}{d}$

$m = pd \Rightarrow d = l$.

b) $n = mp$

$p \nmid m$: On veut mq $\Phi_n(X)\Phi_m(X) = \Phi_m(X^p)$

$\rightarrow \deg \Phi_m(X^p) = p \times \deg \Phi_m(X) = p\,\varphi(m)$

$\deg \Phi_n(X)\Phi_m(X) = \deg \Phi_n + \deg \Phi_m$

$= (p-1) \times \varphi(m) + \varphi(m) = p\,\varphi(m)$

$\rightarrow$ Soit η t.q. $\Phi_n(\eta) = 0$, $\Phi_m(\eta) = 0$.

$\eta = e^{i2\pi \frac{k_1}{n}} = e^{i2\pi \frac{k_2}{m}}$

$\frac{k_1}{n} = \frac{k_2}{m} \Rightarrow k_1 = pk_2 \Rightarrow p \mid k_1 \wedge n$ ↯

Donc, $\Phi_n(X)$ et $\Phi_m(X)$ n'ont pas de racine commune.

$\rightarrow$ Soit η une racine de $\Phi_n(X)$.

$\eta = e^{i2\pi \frac{k_1}{n}}$ avec $k_1 \wedge n = 1$

$\Phi_m(\eta^p) = \Phi_m\left(e^{i2\pi \frac{k_1}{m}}\right) = 0 \qquad k_1 \wedge m = 1$

Soit η une racine de $\Phi_m(X)$

$\eta = e^{i2\pi \frac{k}{m}}$ avec $k \wedge m = 1$

$\Phi_m(X^p) = \Phi_m\left(e^{i2\pi \frac{kp}{m}}\right) = 1. \quad kp \wedge m = 1$

Donc, par degré, $\Phi_n(X)\Phi_m(X) = \Phi_m(X^p)$

$p \mid m$: On a toujours $\Phi_n(X) \mid \Phi_m(X^p)$.

$\deg \Phi_n(X) = \varphi(n) \qquad \Phi_m(X^p) = p\,\varphi(m)$

$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = pm \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = p\,\varphi(m)$.

car $p \mid n$

Dans $\mathbb{Z}/p\mathbb{Z}[X]$, $(A+B)^p = A^p + B^p$

$(a_d X^d + \dots + a_1 X + a_0)^p$

$= (a_d X^d)^p + \dots + (a_1 X)^p + a_0^p$

$= a_d X^{pd} + \dots + a_1 X^p + a_0$

$\rightarrow \overline{\Phi}_n(X) = \dfrac{\overline{\Phi}_m(X^p)}{\overline{\Phi}_m(X)} = \dfrac{\overline{\Phi}_m(X)^p}{\overline{\Phi}_m(X)} = \overline{\Phi}_m(X)^{p-1}$

D'où $\overline{\Phi}_n(X)$ n'est pas scindé dans $\mathbb{Z}/p\mathbb{Z}$.

$\rightarrow \overline{\Phi}_n(X) = \overline{\Phi}_m(X^p) = \overline{\Phi}_m(X)^p$

D'où, $\overline{\Phi}_n(X)$ n'est pas scindé dans $\mathbb{Z}/p\mathbb{Z}$.

c) Si $n \mid p-1$,

$$X^{p-1} - 1 = \prod_{d \mid p-1} \Phi_d(X) = \Phi_n(X)\, P(X)$$

$X^{p-1} - \overline{1}$ est scindé à racines simples dans $\mathbb{Z}/p\mathbb{Z}$

Donc, $\overline{\Phi}_n(X)$ aussi. Φ_n vérifie (S).

d) Si Φ_n est dissocié, $p \nmid n$. (d'après b))

$\exists\, a \in \mathbb{Z}/p\mathbb{Z}$ t.q. $\overline{\Phi}_n(a) = 0$.

Alors, d'après 2.2., $p \equiv 1\ [n]$.

n divise $p-1$.