/CPGE Ibn Ghazi
MP*1 (Rabat)

Prof MAMOUNI
myismail.net

PREPARATION
CONCOURS

Algèbre Gle : Arithmétique
des Polynômes

IG $K = \mathbb{R}$ ou $\mathbb{C}$

Partie I Generalités

① Soit $P, Q \in \mathbb{C}(X)$ mq $P \wedge Q = 1 \iff P$ et Q n'ont pas de racine commune dans $\mathbb{C}$

② Soit $P \in \mathbb{R}(X)$ et $a \in \mathbb{C} \setminus \mathbb{R}$
mq a racine de P de mult α
$\iff \bar{a}$ " " "

③ Soit $P, Q \in \mathbb{R}(X)$ mq
$P \wedge Q = 1 \iff P$ et Q n'ont pas de racine commune dans $\mathbb{C}$

④ Soit $P, Q \in \mathbb{R}(X)$ premiers dans $\mathbb{R}$ mq
$P \wedge Q = 1 \iff$ " " " dans $\mathbb{R}$

dans $\mathbb{R}$

(5) Soit $P \in \mathbb{R}(X)$ scindé à racine simple dans $\mathbb{R}$
mq P' l'est aussi

(6) Soit $P \in \mathbb{R}[X]$ scindé dans $\mathbb{R}$
mq P' l'est aussi

(7) Mq P est scindé à racine simple dans $K = \mathbb{R}$ ou $\mathbb{C}$
$\Leftrightarrow P' \wedge P = 1$

Partie II — Irreductibilité dans $\mathbb{Z}[X]$ et $\phi(X)$

Soit $P \in \mathbb{Z}[X]$ non nul ie $P(X) = a_n X^n + \dots + a_0$ tq $a_k \in \mathbb{Z}$
on pose $c(P) = \text{pgcd}(a_0, \dots, a_n)$ contenu de P
si $c(P) = 1$, on dit que P est primitif

(1)(i) Soit $P \in \mathbb{Z}[X]$ primitif et irreductible dans $\mathbb{Q}[X]$
mq P est irreductible dans $\mathbb{Z}[X]$
Rappel : les seuls diviseurs de P dans $\mathbb{Z}[X]$ sont $\pm P$

(ii) Mq à l'aide d'un contre Exple l'hyp primitif est necessaire

(2) Soit $P, Q \in \mathbb{Z}[X]$ primitifs, mq PQ l'est aussi
Indic : Mq $\forall p$ premier, $\exists c_k$ coeff de PQ tq p ne divise pas c_k

(3) Soit $P \in \mathbb{Z}[X]$ et $a \in \mathbb{Z}$. Mq $c(aP) = a\,c(P)$

(4) Lemme de Gauss

Soit $P, Q \in \mathbb{Z}[X]$ non nul, Mq $c(PQ) = c(P) \cdot c(Q)$

Indic : Utiliser les polynômes $\frac{P}{c(P)}$ et $\frac{Q}{c(Q)}$

(5) Soit $P, Q \in \mathbb{Q}[X]$ unitaires $cd(P) = cd(Q) = 1$

Mq $PQ \in \mathbb{Z}[X] \Rightarrow P \in \mathbb{Z}[X]$ et $Q \in \mathbb{Z}[X]$

Indic : Utiliser $\alpha, \beta \in \mathbb{Z}$ tq $\alpha P \in \mathbb{Z}[X]$
$\beta Q \in \mathbb{Z}[X]$

(6) Soit $P, Q \in \mathbb{Z}[X]$ tq $cd(Q) = 1$

poser $P = BQ + R$ tq $B, R \in \mathbb{Q}[X]$
et $\deg R < \deg Q$

Mq $B, R \in \mathbb{Z}[X]$

indic : par récurrence sur $n = \deg P$

Partie III : Racine $n^{ème}$ de l'unité

(1) Soit $(G, \cdot)$ gpe et $a \in G$ d'ordre fini $o(a) = n$

Mq $\forall k \in \mathbb{N}$ a^k d'ordre fini avec $o(a^k) = \frac{n}{k \wedge n}$

(2) Soit $G = \langle a \rangle$ un gpe cyclique tq $\mathrm{Card}\, G = n$

(i) Mq $x = a^k$ est un générateur de $G \Leftrightarrow k \wedge n = 1$

(ii) En déduire que G admet exactement $\varphi(n)$ générateurs

Ce sont les a^k tq $k \wedge n = 1$

③ On pose $U_n = \{z \in \mathbb{C} \text{ tq } z^n = 1\}$

ⓐ Mq $(U_n, \cdot)$ est cyclique de cardinal $= n$
engendré par $\omega_n = e^{\frac{2i\pi}{n}}$

ⓐⓘ En déduire que U_n admet exact $\varphi(n)$ générateurs

ω_n^k tq $k \wedge n = 1$

ω_n^k s'appelle racine primitive n^e de l'unité

④ On pose $R_n = \{z = \omega_n^k \text{ tq } k \wedge n = 1\} = \{z \in U_n \text{ tq } o(z) = n\}$
de cardinal $\varphi(n)$

ⓐ Mq $\bar{R}_n = R_n$, En déduire que $\varphi(n)$ est pair

ⓐⓘ Mq $U_n = \bigcup_{d \mid n} R_d$. En déduire que $n = \sum_{d \mid n} \varphi(d)$

ⓐⓘⓘ Soit $m \wedge n = 1$ ⓐ Mq l'app $\varphi : R_n \times R_m \to R_{nm}$
$(x, y) \mapsto xy$
est bien défini et bij

indic :
Mq $o(x) \wedge o(y) = 1$
$\Downarrow$
$o(x \cdot y) = o(x) \cdot o(y)$

ⓑ En déduire que $\forall z \in R_{nm}$
$\exists! x \in R_n, \exists! y \in R_m$ tq $z = xy$

⑤ Mq $\prod_{z \in R_n} z = 1$

Partie IV — Polynômes Cyclotomiques

On pose $\Phi_n(X) = \prod_{z \in \mathcal{R}_n} (X - z)$, $\deg \Phi_n = \varphi(n)$

(1) Justifier que n premier $\Rightarrow \Phi_n(X) = \sum_{k=0}^{n-1} X^k$

(2) Mq $\forall n \geq 1$ $\prod_{d \mid n} \Phi_d(X) = X^n - 1$

(3) Fct de Moebius : $\mu(n) = \sum_{z \in \mathcal{R}_n} z$

(i) Vérifier que $\mu(1) = 1$

(ii) Établir que $\sum_{d \mid n} \mu(d) = 0 \quad \forall n \geq 2$

(iii) Soit p premier. Mq $\mu(p) = -1$
$\mu(p^\alpha) = 0 \quad \forall \alpha \geq 2$

(iv) Mq $m \wedge n = 1 \Rightarrow \mu(mn) = \mu(m)\mu(n)$
Indic : Utiliser II.4 - iii.b

(v) En déduire que $\mu(n) = 0$ si $\exists p$ premier tq p^2 divise n
$= \pm 1$ sinon

(4) Polynômes Cyclotomiques vs Fct de Möbius

on pose $F_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$

(i) Etablir que $F_n(X) = \prod_{d|n} \prod_{k|d} \phi_k(X)^{\mu(\frac{n}{d})}$

$$= \prod_{k|n} \phi_k(X)^{\alpha_k}$$

où $\alpha_k = \sum_{\substack{\alpha \in \mathbb{N} \\ \text{tq } \alpha k | n}} \mu\left(\frac{n}{\alpha k}\right)$

(ii) Justifier que $\alpha_k = \sum_{\beta | \frac{n}{k}} \mu(\beta)$

(iii) En déduire que $\boxed{\phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}}$

Indic : IV-3) i) et ii)

Partie V / Relations entre Poly Cyclotomiques /

(1) On suppose p et q premiers

Mq $\boxed{\Phi_{pq}(x) = \dfrac{\Phi_p(x^q)}{\Phi_p(x)}}$

(2) (i) Soit p, q, r nombres premiers

(ii) Mq $\Phi_{pqr}(x) = \dfrac{\Phi_{pq}(x^r)}{\Phi_{pq}(x)}$

(iii) Conclure que $\boxed{\Phi_{pqr}(x) = \dfrac{\Phi_p(x^{qr})\,\Phi_p(x)}{\Phi_p(x^r)\,\Phi_p(x^q)}}$

(3) En déduire $\Phi_{p_1 \cdots p_r}(x)$ où $p_1 \cdots p_r$ nbr premiers

(4) Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ tq p_i premier

on pose $m = p_1 \cdots p_r$

(a) Mq $\Phi_n(x) = \Phi_m(x^{n/m})$

(b) En déduire un algorithme pour le calcul de $\Phi_n(x)$

(c) Calculer $\Phi_{20}(x)$

FIN ET BONNE CHANCE

(7)