CRYPTOGRAPHIE ALGÉBRIQUE **4M035** **Feuille 5**
P. V. Koseleff

Corps finis

Exercice 5.1. — Polynômes cyclotomiques
On utilise ici que les racines de Φ_n sont les $\varphi(n)$ racines primitives n-ème de 1 (dans $\mathbf{C}^*$).

1. Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$.
2. Montrer que $\Phi_n \in \mathbf{Z}[X]$ est unitaire, de degré $\varphi(n)$.
3. Montrer que si $n \geq 3$ est impair alors $\Phi_{2n} = \Phi_n(-X)$
4. Montrer que si n est pair alors $\Phi_{2n} = \Phi_n(X^2)$.
5. Montrer que si p premier divise n alors $\Phi_{np} = \Phi_n(X^p)$.
6. Montrer que si p premier ne divise pas n alors $\Phi_{np}\Phi_n = \Phi_n(X^p)$.
7. Montrer que si $n = p_1^{n_1} \cdots p_k^{n_k}$, alors $\Phi_n = \Phi_{n_0}(X^{n/n_0})$, où n_0 est le radical $r(n) = p_1 \cdots p_k$.
8. Calculer Φ_n, pour $1 \leq n \leq 20$.

Exercice 5.2. — Degré du polynôme minimal
Soit p un nombre premier, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ et K un corps de cardinal $q = p^n$, de sous-corps premier $\mathbf{F}_p$.

1. (a) Montrer que si $P \in K[X]$ alors $P(X^q) = P(X)^q$.
   (b) Montrer que si $P \in K[X]$, alors $P(X^p) = P(X)^p \Leftrightarrow P \in \mathbf{F}_p[X]$.
2. Soit $\alpha \in K^*$, d'ordre N.
   (a) Montrer que $(N, p) = 1$ et posons $d = \mathrm{ord}\,(p)$ dans $(\mathbf{Z}/N\mathbf{Z})^*$.
   (b) Montrer que $\alpha^{p^m} = 1$ ssi $d|m$.
   (c) En déduire que $P = (X-\alpha)(X-\alpha^p)\cdots(x-\alpha^{p^{d-1}})$ est le polynôme minimal de α et $d|n$.
   (d) Montrer que P divise $X^q - X$.
3. Soit P irréductible de degré d. Montrer que P divise $X^q - X$ si et seulement si d divise n.
4. En déduire que P de degré n est irréductible si et seulement P est premier avec $X^{p^e} - X$ pour tout $e \leq n/2$.

Exercice 5.3. —

1. Montrer que $\Phi_9 = X^6 + X^3 + 1 \in \mathbf{F}_2[X]$ est irréductible. On pose $\mathbf{K} = \mathbf{F}_2[X]/(\Phi_9)$ et $\alpha = X \pmod{\Phi_9} \in \mathbf{K}$.
2. Soit $\beta = \alpha^3$ et $\gamma = \alpha^2 + \alpha$. Montrer que α, β et γ sont respectivement d'ordre 9, 3 et 21 dans le groupe multiplicatif de $\mathbf{K}$.
3. Montrer que $\mathbf{K}$ est un $\mathbf{F}_2$-espace vectoriel et que $(1, \alpha, \ldots, \alpha^5)$ en est une base.
4. Déterminer les polynômes minimaux de β et γ.
5. Montrer que $1 + \alpha = \gamma/\alpha$ est un élément primitif de $\mathbf{K}$ et donner son polynôme minimal.
6. On considère σ l'automorphisme de Froebenius $x \mapsto x^2$. Déterminer $\ker \sigma^k - \mathbb{1}$, pour $k \geq 1$. On donnera une base en fonction de α.

Exercice 5.4. — (Algorithme de El Gamal)
Alice souhaite se faire envoyer des messages confidentiellement en utilisant cet algorithme. Elle considère pour cela le polynôme $P = X^6 + X + 1$ et $K = \mathbf{F}_2[X]/(P)$. Soit α la classe de X modulo Φ_9.

1. Justifier que K est un corps et montrer que α est un générateur de K^*.
2. Alice rend public le triplet $(K, \alpha, \alpha^2 + 1)$, et Bob envoie des messages à Alice en utilisant cette clé publique.
3. Bob veut coder le message $1 + \alpha$ pour l'envoyer à Alice. Conformément à l'algorithme, il choisit un entier x compris entre 2 et 62, par exemple $x = 3$. Que transmet-il à Alice ?
4. Vous interceptez le message $(\alpha^3, \alpha^3 + \alpha^2 + \alpha)$. Quel était le message envoyé par Bob ?

Exercice 5.5. — Polynôme Φ_5

1. (a) Montrer que le polynôme Φ_5 est irréductible dans $\mathbf{F}_3[X]$. Soit $\mathbf{K} = \mathbf{F}_3[X]/(\Phi_5)$ et $\alpha = X \pmod{\Phi_5} \in \mathbf{K}^*$.
   (b) Montrer que $\mathbf{K}$ est un corps et un $\mathbf{F}_3$-espace vectoriel et en donner une base.
   (c) Quel est l'ordre de α dans le groupe multiplicatif $\mathbf{K}^*$?
   (d) Soit $\beta = \alpha^2 + \alpha - 1 \in \mathbf{K}^*$. Quel est l'ordre de β dans $\mathbf{K}^*$? Quel est le polynôme minimal de β dans $\mathbf{F}_3[X]$.
   (e) Montrer que $\gamma = \alpha\beta$ est d'ordre 80. Donner le polynôme minimal de γ dans $\mathbf{F}_3[X]$.
2. (a) Dire suivant la congruence de $p \pmod 5$, quel sont les degrés des facteurs irréductibles de Φ_5 dans $\mathbf{F}_p[X]$.
   (b) Factoriser Φ_5 dans $\mathbf{Z}/19\mathbf{Z}[X]$. On pourra remarquer que les facteurs ont deux racines conjuguées donc inverses l'une de l'autre.

Exercice 5.6. — Factorisation de Φ_n dans $\mathbf{F}_p$
Soit p un nombre premier et $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$ et K un corps fini de caractéristique p.

1. On suppose que $(p, n) = 1$. Montrer qu'il existe un corps K contenant $\mathbf{Z}/p\mathbf{Z}$ dans lequel $X^n - 1$ est scindé.
   (a) Montrer que $X^n - 1$ n'a que des racines simples dans K.
   (b) En déduire que les racines de Φ_n dans K sont des racines primitives n-èmes de 1.
   (c) En déduire que les facteurs irréductibles de Φ_n dans $\mathbf{F}_p[X]$ sont tous de même degré r, où $r = \mathrm{ord}\,(p)$ est l'ordre de p dans $(\mathbf{Z}/n\mathbf{Z})^*$.
   (d) Montrer que les facteurs irréductibles de Φ_{p^n-1} sont de degré n.
   (e) Factoriser Φ_{15} dans $\mathbf{F}_2[X]$, dans $\mathbf{F}_4[X]$.
2. Factoriser Φ_{p^k} dans $\mathbf{Z}/p\mathbf{Z}[X]$.

Exercice 5.7. — Critères d'irréductibilité dans $\mathbf{F}_p[X]$

1. (a) Montrer que que si $(P, P') \neq 1$, alors P n'est pas irréductible.
   (b) Montrer que $P/(P, P')$ est sans facteur carré.
2. Soit $P \in \mathbf{F}_p[X]$ un polynôme sans facteur carré de degré n.
   (a) Montrer que P est irréductible si et seulement si $(P, X^{p^m} - X) = 1$ pour tout $m \leq n/2$.
   (b) Evaluer la complexité de ce test.
3. On définit $R_0 = P$, $Q_e = \mathrm{pgcd}(X^{q^e} - X, R_{e-1})$, $R_e = R_{e-1}/Q_e$.
   (a) Montrer que Q_e est le produit des polynômes irréductibles de degré e divisant P
   (b) Montrer que $P = Q_1 Q_2 \cdots Q_e$. Évaluer le coût de cet algorithme.