Université Paris-Sud 11 — M1 MFA
Année universitaire 2012/2013 — MAO Calcul formel

EXAMEN DU LUNDI 21 JANVIER 2013, DURÉE : 3H

Les documents autres que des notes de cours manuscrites, imprimées ou en ligne (`http://www.math.u-psud.fr/~riou/enseignement/`), sujets et corrigés de TP compris, sont interdits. Il est également permis de consulter la documentation de Sage ; on pourra ainsi de suivre les liens vers l'aide indiqués en haut de la page `http://www.math.u-psud.fr/~riou/enseignement/`. L'utilisation d'autres dispositifs électroniques ou mécaniques (calculatrices, ordinateurs de poche, baladeurs, téléphones portables, bouliers, etc.) est interdite.

Si vous utilisez l'ordinateur, vous devez recopier les lignes de code Sage que vous avez utilisées (en faisant attention à l'indentation) et il est également indispensable d'expliquer les calculs que vous faites faire à l'ordinateur.

Le sujet comporte deux pages.

Exercice I

Pour tout entier $n \geq 1$, on note μ_n l'ensemble des $\zeta \in \mathbf{C}^\times$ tels que $\zeta^n = 1$. Muni de la loi $\times$, μ_n est le groupe des racines n-ièmes de l'unité. On note $\mu_n^{\text{prim}} \subset \mu_n$ l'ensemble des $\zeta \in \mu_n$ tels que l'ordre de ζ dans le groupe μ_n soit exactement n (on dit alors que ζ est une racine n-ième primitive de l'unité).

Pour tout $n \geq 1$, on note $\zeta_n = \exp(\frac{2\imath\pi}{n})$.

(1) Soit $n \geq 1$. Montrer que $\zeta_n \in \mu_n^{\text{prim}}$ et que que $\mu_n = \{\zeta_n^i, 0 \leq i \leq n-1\}$.

(2) Soit $n \geq 1$. Soit $i \in \mathbf{Z}$. Montrer que $\zeta_n^i \in \mu_n^{\text{prim}}$ si et seulement si $i \wedge n = 1$.

On définit le n-ième polynôme cyclotomique par la formule $\Phi_n = \prod_{\zeta \in \mu_n^{\text{prim}}}(X - \zeta) \in \mathbf{C}[X]$, ce qui revient à dire, d'après la question précédente que $\Phi_n = \prod_{0 \leq i \leq n-1, i \wedge n = 1}(X - \zeta_n^i)$.

(3) Montrer que $\deg \Phi_n = \varphi(n)$ où $\varphi(n)$ est la fonction indicatrice d'Euler ($\varphi(n) = \#\mathbf{Z}/n\mathbf{Z}^\times$).

(4) Soit p un nombre premier. Soit $\zeta \in \mu_p^{\text{prim}}$. Montrer que $\frac{\zeta^p - 1}{\zeta - 1} = 0$. En déduire que $\Phi_p = 1 + X + X^2 + \cdots + X^{p-1}$.

Soit $m \geq 1$ un nombre entier. Soit p un nombre premier ne divisant pas m. Soit $d \geq 1$. On conserve ces notations jusqu'à la question 8 incluse.

(5) Soit $z \in \mathbf{C}$ une racine du polynôme $\Phi_m(X^{p^d})$. Montrer que $z \in \mu_{mp^d}$ et plus précisément que l'ordre de z est de la forme mp^i pour $0 \leq i \leq d$.

(6) Montrer que $\Phi_m(X^{p^d})$ n'a que des racines simples dans $\mathbf{C}$. (Indication : compter le nombre de racines de ce polynôme.)

(7) En appliquant ce qui précède aux entiers d et $d-1$, montrer la relation $\Phi_m(X^{p^d}) = \Phi_{mp^d} \cdot \Phi_m(X^{p^{d-1}})$, autrement dit $\Phi_{mp^d} = \frac{\Phi_m(X^{p^d})}{\Phi_m(X^{p^{d-1}})}$.

(8) Si $m = 1$, que vaut Φ_m ? En déduire une formule pour Φ_{p^d} pour p un nombre premier et $d \geq 1$.

(9) Soit $n \geq 1$. On suppose connue la factorisation $n = p_1^{d_1} \dots p_k^{d_k}$ de n en produit de nombres premiers distincts. À partir des questions précédentes, imaginer un algorithme pour calculer Φ_n.

(10) Implémenter cet algorithme dans Sage sous la forme d'une fonction prenant en argument les deux suites d'entiers $P = [p_1, \dots, p_k]$ et $D = [d_1, \dots, d_k]$. (On admettra sans justification que Φ_n appartient à $\mathbf{Z}[X]$.)

(11) Implémenter une fonction Sage prenant en argument n et renvoyant Φ_n. (On utilisera la liste obtenue par la syntaxe `list(factor(n))`.)

(12) Calculer Φ_{20}.

Exercice II

Soit ℓ un nombre premier. Le polynôme cyclotomique $\Phi_\ell \in \mathbf{Z}[X]$ a été introduit dans l'exercice précédent. On aura ici uniquement besoin de savoir que $\Phi_\ell = \frac{X^\ell - 1}{X-1} = 1 + X + X^2 + \cdots + X^{\ell-1}$.

Soit p un nombre premier différent de ℓ. On note $P \in \mathbf{F}_p[X]$ la classe de Φ_ℓ dans $\mathbf{F}_p[X]$.

Soit K une extension finie de $\mathbf{F}_p$ de degré d. (On conservera ces notations jusqu'à la question 15.)

(13) Soit $x \in K^\times$. Montrer que x est racine de P si et seulement si l'ordre de x dans le groupe $K^\times$ est exactement ℓ.

(14) Montrer que si P admet une racine dans K alors ℓ divise $p^d - 1$.

(15) Montrer que si ℓ divise $p^d - 1$, alors P est scindé dans $K[X]$ (et à racines simples).

(16) On note d le plus petit entier ≥ 1 tel que ℓ divise $p^d - 1$. Justifier l'existence de cet entier et montrer que tous les facteurs irréductibles de P dans $\mathbf{F}_p[X]$ sont de degré d.

(17) Quels sont les degrés des diviseurs irréductibles $\sum_{i=0}^{30} X^i$ dans $\mathbf{F}_2[X]$? (Dans cette question et la suivante, on s'interdira d'utiliser la fonction `factor`.)

(18) Montrer que $\sum_{i=0}^{10} X^i$ est irréductible dans $\mathbf{F}_{13}[X]$. En déduire que $\sum_{i=0}^{10} X^i$ est irréductible dans $\mathbf{Q}[X]$.

Exercice III

Soit $P \in \mathbf{F}_2[X]$ un polynôme unitaire sans facteur carré. *On fait l'hypothèse que les facteurs (unitaires) irréductibles $P_1, \ldots, P_e$ de P sont tous d'un même degré d que l'on suppose connu.*

On note $A := \mathbf{F}_2[X]/(P)$. Pour $1 \leq i \leq e$, on note $K_i := \mathbf{F}_2[X]/(P_i)$. On suppose que $e \geq 2$.

(19) Montrer qu'il existe un isomorphisme canonique $\sigma\colon A \xrightarrow{\sim} K_1 \times K_2 \times \cdots \times K_e$.

(20) Supposons ici que l'on connaisse $Q \in \mathbf{F}_2[X]_{<de}$ dont la classe $b := [Q] \in A$ soit non nulle et telle qu'une des coordonnées de $\sigma(b)$ soit nulle. Expliquer comment il est possible d'utiliser Q pour déterminer un diviseur non trivial de P.

On cherche maintenant un moyen de déterminer un tel polynôme Q.

(21) Fixons $1 \leq i \leq e$. Soit $\alpha \in K_i$. On note $\beta = \sum_{k=0}^{d-1} \alpha^{2^k}$. Montrer que $\beta^2 = \beta$. En déduire que $\beta \in \mathbf{F}_2 \subset K_i$.

(22) Montrer que l'application $K_i \to \mathbf{F}_2$ qui à α associe $\sum_{k=0}^{d-1} \alpha^{2^k}$ est une application $\mathbf{F}_2$-linéaire non nulle. En déduire que si α est tiré uniformément au hasard dans K_i, la probabilité pour que $\sum_{k=0}^{d-1} \alpha^{2^k} = 0$ est $\frac{1}{2}$.

On considère l'algorithme suivant. On tire au hasard un polynôme $R \in \mathbf{F}_2[X]_{<de}$. On note $a := [R] \in A$. On calcule $b := \sum_{k=0}^{d-1} a^{2^k} \in A$ (c'est-à-dire que l'on détermine $Q \in \mathbf{F}_2[X]_{<de}$ tel que $[Q] = b = \sum_{k=0}^{d-1} a^{2^k}$). Si $b \neq 0$ et $b \neq 1$, alors Q vérifie la condition de la question 20 ce qui permet de déterminer un diviseur non trivial de P.

(23) Le polynôme R étant tiré au hasard de façon uniforme, quelle est la probabilité pour que $b \neq 0$ et $b \neq 1$ (autrement si que $\sigma(b)$ ne soit ni $(0, \ldots, 0)$ ni $(1, \ldots, 1)$.) ?

(24) En utilisant l'algorithme décrit ci-dessus, écrire une fonction dans Sage prenant en argument le polynôme P et l'entier d et renvoyant un facteur non trivial de P. (On tirera au hasard un polynôme R jusqu'à en obtenir un qui permette de déterminer un facteur non trivial de P.)

(25) Écrire une fonction dans Sage prenant en argument P et d et renvoyant la liste des facteurs irréductibles de P.

(26) En utilisant votre implémentation, factoriser $\sum_{i=0}^{30} X^i$ dans $\mathbf{F}_2[X]$.

Sage

On pourra utiliser les pages d'aide signalées en haut de la page `http://www.math.u-psud.fr/~riou/enseignement/`, et des informations utiles pourront aussi être obtenus dans l'aide de Sage, en tapant par exemple `len?`, `range?`, `GF?`, `ZZ?`, `Integers?` ou `ZZ.random_element?`. On rappelle que si `P` est un polynôme, son degré peut être calculé avec `P.degree()`.