Université Paris-Sud 11 — M1 MFA
Année universitaire 2013/2014 — MAO Calcul formel

PARTIEL DU VENDREDI 15 NOVEMBRE 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 cette 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.

Ce partiel est une épreuve de mathématiques. Avant d'utiliser l'ordinateur, il convient de se demander s'il n'est pas possible d'obtenir par un raisonnement simple ce qui pourrait être obtenu par un calcul plus complexe fait par ordinateur. À titre indicatif, dans les questions signalées par le signe (⋆), on s'attend à une réponse utilisant de façon essentielle l'ordinateur ; pour les autres, on s'attend davantage à une réponse argumentée, utilisant éventuellement l'ordinateur mais de façon plus marginale.

Dans tous les cas, 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.

Dans ce partiel, on s'interdira d'utiliser les fonctions comme `factor` permettant de factoriser un polynôme, déterminer ses racines ou déterminer s'il est irréductible.

Problème

On considère le corps $\mathbf{F}_{19}$ à 19 éléments.

(En cas de blocage sur certaines questions, on pourra passer directement à la question (23) en admettant le résultat aux questions précédentes.)(1) On note $j := 2^6 \in \mathbf{F}_{19}$. Montrer que $j^3 = 1$.

(2) Déterminer l'ensemble des racines du polynôme $X^3 - 1$ dans $\mathbf{F}_{19}$.

(3) (⋆) Vérifier que dans $\mathbf{F}_{19}$, on a $2^6 \neq 1$ et $2^9 \neq 1$.

(4) En déduire que 2 est un générateur du groupe multiplicatif $\mathbf{F}_{19}^\times$.

(5) Soit $i \in \mathbf{Z}$. On note $a := 2^i$. Donner la valeur de a^6 en fonction de la classe de congruence de i modulo 3.

(6) Soit $i \in \mathbf{Z}$. On note $a := 2^i$. Montrer que a peut s'écrire $a = b^3$ pour $b \in \mathbf{F}_{19}$ si et seulement si 3 divise i.

(7) Soit $a \in \mathbf{F}_{19}^\times$. Montrer que $X^3 - a$ est irréductible si et seulement si $a^6 \neq 1$.

(8) Montrer que $P := X^3 - 2 \in \mathbf{F}_{19}$ est irréductible.

On note $K := \mathbf{F}_{19}[U]/(U^3 - 2)$ le corps de rupture de P sur $\mathbf{F}_{19}$. On note $u \in K$ la classe de U dans K : c'est la racine privilégiée de P dans K.

(9) Quelles sont les racines de $X^3 - 2$ dans K ? En déduire la factorisation complète de $X^3 - 2$ dans $K[X]$.

(10) (⋆) L'élément u est-il un générateur du groupe multiplicatif $K^\times$?

(11) (⋆) L'élément $1 + u$ est-il un générateur du groupe multiplicatif $K^\times$?

On note q le cardinal du corps K. On introduit un corps de décomposition L du polynôme $Q = X^2 - u \in K[X]$. On note $v \in L$ une racine du polynôme $X^2 - u$. (À ce stade, on ignore quel est le degré de l'extension L/K.)

(12) Montrer que $(v^q)^2 = u$.

(13) On pose $\varepsilon := v^{q-1} \in L$. Montrer que $\varepsilon^2 = 1$.

(14) Montrer que $\varepsilon = u^{\frac{q-1}{2}}$.

(15) ($\star$) Calculer ε et montrer que $v^q \neq v$.

(16) En déduire que $v \notin K$.

(17) Montrer que $Q = X^2 - u \in K[X]$ est irréductible et que L/K est une extension de degré 2 que l'on peut identifier au corps de rupture de Q sur K.

(18) Quel est le cardinal de L ?

(19) Donner la liste des sous-corps de L.

(20) Soit $w \in L$. Notons $\mathbf{F}_{19}[w] \subset L$ le sous-corps de L engendré par w. Notons $R_w \in \mathbf{F}_{19}[X]$ le polynôme minimal de w sur $\mathbf{F}_{19}$. *A priori*, quelles valeurs peut prendre l'entier $\deg R_w$?

(21) Quel est le sous-corps $\mathbf{F}_{19}[v]$ de L engendré par v ?

(22) En déduire que le polynôme $X^6 - 2 \in \mathbf{F}_{19}[X]$ est irréductible.

(23) ($\star$) Construire le corps L dans Sage. (On pourra le définir comme extension de K ou directement comme extension de $\mathbf{F}_{19}$.)

On note $z := 1 + v + v^3 \in L$.

(24) ($\star$) Quels sont les nombres premiers p divisant le cardinal e de $L^\times$?

(25) ($\star$) Vérifier que $z^{\frac{e}{p}} \neq 1$ pour tout nombre premier p divisant e.

(26) En déduire que z est un générateur du groupe $L^\times$.

(27) ($\star$) Calculer $R := \prod_{i=0}^{5}(X - z^{19^i}) \in L[X]$. Que constate-t-on ?

(28) Montrer que R est irréductible dans $\mathbf{F}_{19}[X]$.

Exercice

On considère le corps $\mathbf{F}_7$ à 7 éléments. Notons $P = X^5 + X + 3 \in \mathbf{F}_7[X]$.

(29) ($\star$) Vérifier que P n'a pas de racines dans $\mathbf{F}_7$.

(30) Soit $n \geq 0$. Proposer un algorithme pour calculer le reste de la division euclidienne de X^n par P.

(31) Donner une estimation en fonction de n du coût de votre algorithme en opérations arithmétiques dans $\mathbf{F}_7$.

(32) ($\star$) Définir dans Sage une fonction prenant en argument un entier n et renvoyant un représentant de la classe de X^n dans $\mathbf{F}_7[X]/(P)$. (On rappelle que si dans Sage A est l'anneau des polynômes $\mathbf{F}_7[X]$, alors le quotient $\mathbf{F}_7[X]/(P)$ peut être défini avec $A.quotient(P)$.)

(33) ($\star$) Calculer la classe de X^{7^5} dans $\mathbf{F}_7[X]/(P)$.

(34) En déduire que P est irréductible.

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 `GF?`, `Integers?` ou `matrix?`.