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

CORRIGÉ DU PARTIEL DU VENDREDI 15 NOVEMBRE 2013

Problème

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

(1) On note $j := 2^6 \in \mathbf{F}_{19}$. Montrer que $j^3 = 1$.

2 appartient au groupe $\mathbf{F}_{19}^\times$ qui est d'ordre 18, donc $j^3 = 2^{18} = 1$.

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

Dans $\mathbf{F}_{19}$, on a $j = 2^6 = 64 = 64 - 3 \cdot 19 = 7 \neq 1$. Comme $j^3 = 1$ et $j \neq 1$, l'ordre de j dans $\mathbf{F}_{19}^\times$ est 3. Ainsi, $1, j = 7, j^2 = 49 = 11$ sont trois racines distinctes du polynôme $X^3 - 1$ dans $\mathbf{F}_{19}$, et ce sont les seules parce que ce polynôme est de degré 3.

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

Les lignes de codes suivantes permettent d'obtenir que $2^6 = 7 \neq 1$ et $2^9 = -1 \neq 1$:

```
F19=GF(19)
F19(2)^6,F19(2)^9
```

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

Les diviseurs de 18 autres que 18 sont $1, 3, 9, 2, 6$. Tous divisent 6 ou 9, donc pour vérifier qu'un élément de $\mathbf{F}_{19}^\times$ en est un générateur, il suffit de vérifier que son ordre ne divise ni 6 ni 9. Comme $2^6 \neq 1$ et $2^9 \neq 1$, on obtient que 2 engendre $\mathbf{F}_{19}^\times$.

(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.

$a^6 = 2^{6i} = (2^6)^i = j^i$. Comme j est d'ordre 3, j^i ne dépend que de la classe de congruence de i modulo 3. Ainsi, si $i \equiv 0 \mod 19$, $j^i = 1$, si $i \equiv 1 \mod 19$, $j^i = j = 7$ et si $i \equiv 2 \mod 19$, $j^i = j^2 = 11$.

(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.

Si 3 divise i, on peut écrire $i = 3j$ avec $j \in \mathbf{Z}$, poser $b = 2^j$ et alors $a = b^3$. S'il existe $b \in \mathbf{F}_{19}^\times$ tel que $a = b^3$, il vient $a^6 = b^{18} = 1$, donc $i \equiv 0 \mod 3$ d'après la question précédente.

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

On peut écrire a sous la forme $a = 2^i$ puisque 2 est un générateur de $\mathbf{F}_{19}^\times$. Raisonnons par contraposition, le polynôme de degré 3 $X^3 - 1$ n'est pas irréductible si et seulement s'il admet une racine, c'est-à-dire qu'il existe $b \in \mathbf{F}_{19}^\times$ tel que $a = b^3$, c'est-à-dire 3 divise i ou encore que $a^6 = 1$ d'après les deux questions précédentes.

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

On applique le résultat de la question précédente avec $a = 2$. Comme $2^6 = j = 7 \neq 1$, on obtient que P 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 $K[X]$.

Si $x \in K$, notons $y := \frac{x}{u}$. Du fait de l'identité $u^3 = 1$, l'équation $x^3 = 2$ équivaut à $y^3 = 1$. Les racines troisième de l'unité étant $1, j, j^2$, on en déduit que $X^3 - 2$ est scindé sur K et que ses racines sont u, ju, j^2u.

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

Le groupe $K^\times$ est d'ordre 19^3-1. En utilisant la commande `factor(19^3-1)`, on obtient que $19^3-1 = 2\cdot 3^3\cdot 127$. L'ordre d'un élément $x\in K^\times$ est un diviseur de cet entier et s'il ne lui est pas égal, il existe un nombre premier $p\in\{2,3,127\}$ tel que $x^{\frac{19^3-1}{p}}=1$. Le code suivant construit le corps de rupture K de X^3-2 et teste ce critère :

```
A.<X>=F19[]
q=19**3
K.<u>=GF(q,modulus=X^3-2)
for p in [2,3,127]:
        print u^((q-1)/p)
```

Pour $p=127$, on obtient $u^{54}=1$, donc u n'est pas un générateur de $K^\times$.

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

Appliqué à $1+u$, le critère de la question précédente donne que $1+u$ engendre $K^\times$.

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 $(v^q)^2=u$.

On a $(v^q)^2=v^{2q}=(v^2)^q=u^q=u$, la dernière égalité venant du fait que $u\in K$ et que le corps K soit de cardinal q.

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

$\varepsilon=\frac{v^q}{v}$, donc $\varepsilon^2=\frac{(v^q)^2}{v^2}=\frac{u}{u}=1$ d'après la question précédente.

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

Comme q est impair, $\frac{q-1}{2}$ est un entier, et $u^{\frac{q-1}{2}}=(v^2)^{\frac{q-1}{2}}=v^{q-1}=\varepsilon$.

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

(Ici, on ne sait pas encore que X^2-u est irréductible dans $K[X]$, donc on ne peut pas encore se permettre de construire son corps de rupture dans Sage et d'y calculer v^q.) Le calcul $u^{\frac{q-1}{2}}=-1$ peut se faire avec la commande `u^((q-1)/2)`. D'après la question précédente, on obtient ainsi $\varepsilon=-1$, puis $v^q=\varepsilon\cdot v=-v\neq v$.

(16) En déduire que $v\notin K$.

Les éléments $x\in K$ vérifient $x^q=x$, ce qui n'est pas le cas de v, donc $v\notin K$.

(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.

On vient de montrer que les racines de Q n'appartenaient pas à K. Le polynôme Q étant de degré 2, il est irréductible dans $K[X]$. Le corps de rupture de Q sur K s'identifie au sous-corps $K[v]$ de L engendré par une racine v de Q. Comme les racines de Q sont v et $-v$, on obtient que $L=K[v]$, donc L s'identifie au corps de rupture de Q sur K, l'extension L/K est donc de degré 2.

(18) Quel est le cardinal de L ?

Comme $[L\colon K]=2$, on a $\#L=\#K^2=q^2=19^6$.

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

On sait que pour tout entier naturel d divisant 6, il existe un unique sous-corps de L de cardinal 19^d que l'on note $\mathbf{F}_{19^d}$ et que l'on obtient ainsi tous les sous-corps de L. Les valeurs possibles pour d sont $1,2,3,6$ qui correspondent respectivement aux sous-corps $\mathbf{F}_{19},\mathbf{F}_{19^2},K,L$. (Si on pose $w:=v^3$, on remarque que $w^2=2$ et que $w^{19}=-w\neq w$, ce qui permet de montrer que $\mathbf{F}_{19^2}$ est le sous-corps de L engendré par w.)

(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 $\deg R_w$?

Le degré du polynôme R_w est égal au degré de l'extension $\mathbf{F}_{19}[w]/\mathbf{F}_{19}$ qui est égal 1, 2, 3 ou 6 d'après la question précédente.

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

$L = K[v] = \mathbf{F}_{19}[u, v] = \mathbf{F}_{19}[v]$ puisque $u = v^2$. Le sous-corps engendré par v est donc L tout entier.

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

D'après la question précédente, le degré du polynôme minimal $R_v \in \mathbf{F}_{19}[X]$ de v sur $\mathbf{F}_{19}$ est 6. Comme v est racine du polynôme $X^6 - 2$, on en déduit que $R_v = X^6 - 2$. Le polynôme minimal d'un élément d'une extension de corps étant irréductible, on en déduit que $X^6 - 2 \in \mathbf{F}_{19}[X]$ est irréductible.

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

```
B.<Y>=PolynomialRing(K)
L.<v>=K.extension(Y^2-u)
```

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

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

En posant `e=q^2` et en faisant `factor(e-1)`, on obtient que $e - 1 = 2^3 \cdot 3^3 \cdot 5 \cdot 7^3 \cdot 127$, donc les nombres premiers divisant le cardinal de $L^\times$ sont 2, 3, 5, 7 et 127.

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

```
z=1+v+v^3
for p in [2,3,5,7,127]:
      print (z^(e/p))
```

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

Comme dans la question (4), si z n'était pas un générateur de $L^\times$, son ordre est un diviseur de $e-1$ différent de $e-1$, donc diviseur de $\frac{e-1}{p}$ pour p un diviseur premier de $e-1$, ce qui n'est pas le cas.

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

```
C.<Z>=PolynomialRing(L)
prod([Z-z^(19^i) for i in range(6)])
```

On obtient $R = X^6 + 13X^5 + 9X^4 + 4X^3 + 17X^2 + 18X + 15$. On constate que ce polynôme appartient à $\mathbf{F}_{19}[X]$.

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

L'élément z engendre le groupe multiplicatif $L^\times$. *A fortiori*, il engendre le corps L. Le polynôme minimal (irréductible) R_z est donc de degré 6. La question précédente fournissant un polynôme unitaire annulateur de z à coefficients dans $\mathbf{F}_{19}$ et de degré 6, il vient que $R = R_z$ et donc 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 $\mathbf{F}_7$.

```
F7=GF(7)
D.<T>=PolynomialRing(F7)
P=T^5+T+3
for i in range(7):
    print P(i)
```

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

Calculer le reste de la division euclidienne d'un polynôme par P revient à calculer son représentant canonique dans le quotient $\mathbf{F}_7[X]/(P)$. On peut ainsi obtenir le résultat cherché en utilisant l'algorithme d'exponentiation rapide dans l'anneau $\mathbf{F}_7[X]/(P)$.

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

L'élévation à la puissance n par exponentiation rapide demande $O(\log n)$ multiplications dans $\mathbf{F}_7[X]/(P)$, chacune d'entre elle ayant un coût borné en opérations arithmétiques dans $\mathbf{F}_7$. Le coût cherché est donc $O(\log n)$.

(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 $A.quotient(P)$.)

```
def puissance(n):
        E=D.quotient(T^5+T+3)
        return (E(T)^n).lift()
```

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

En faisant `puissance(7**5)`, on obtient que $X^{7^5} \equiv X \mod P$.

(34) En déduire que P est irréductible.

D'après la question précédente, P divise $X^{7^5} - X$ qui est le produit des polynômes irréductibles unitaires de degrés divisant 5 (c'est-à-dire de degré 5). Comme P ne possède pas de racine, P est un produit de polynômes irréductibles de degré 5. Comme $\deg P = 5$, on obtient que P est irréductible.