

19 juin 2019
Master 1 M.F., Orsay

Corrigé de l'examen de M.A.O. Calcul Formel
Durée : 3 heures

Exercice 1

1. On calcule la fraction rationnelle $2x(t)y(t)^2 + x(t) + 5y(t) = 0$, multipliée par $(t^2+1)^2$ pour que ce soit un polynôme. On cherche ensuite les racines complexes de ce polynôme ; il est clair par construction que i et $-i$ ne sont pas des racines. On trouve 6 racines, qui sont toutes simples ; il faut ensuite vérifier qu'elles correspondent à 6 points $(x(t), y(t))$ deux à deux distincts (car on n'a pas démontré que le paramétrage est injectif). Il suffit pour cela d'afficher les 6 abscisses et de constater qu'elles sont distinctes.

```
sage: AnneauPolynomes.<T> = QQ[]
sage: X = T^2 + T + 1
sage: Ynum = T^2 - 1
sage: Ydenom = T^2 + 1
sage: Polynome = 2 * X * Ynum^2 + Ydenom^2 * X +  5 * Ynum * Ydenom^2
sage: Racines = Polynome.roots(CC)
sage: len(Racines)
6
sage: [X(Racines[i][0]) for i in range(len(Racines))]
[0.859336859842480, 1.74552134527429, -1.34934601843553 + 0.610859817210298*I,
-1.34934601843553 - 0.610859817210298*I, 1.04691691587715 - 1.19844578212008*I,
1.04691691587715 + 1.19844578212008*I]
```

2. Considérons les polynômes $P_1(X,Y,T) = T^2+T+1-X$ et $P_2(X,Y,T) = (T^2-1) - (T^2+1)Y$ de $\mathbb{Q}[X,Y][T]$. Le code ci-dessous montre que leur résultant est

$$P(X,Y) = X^2Y^2 - 2X^2Y + X^2 + 4XY + Y^2 - 4X + 3.$$

Montrons que ce polynôme convient. Soit $(x,y) \in \mathcal{C}$. Alors il existe $t \in \mathbb{C} \setminus \{-i, i\}$ tel que $P_1(x,y,t) = P_2(x,y,t) = 0$: les polynômes $P_1(x,y,T)$ et $P_2(x,y,T)$ ont une racine complexe commune. Donc leur résultant est nul. Considérons la spécialisation $\varphi : \mathbb{Q}[X,Y] \to \mathbb{C}$ définie par $\varphi(S) = S(x,y)$. Comme P_1 est unitaire (vu comme élément de $\mathbb{Q}[X,Y][T]$), l'image par φ de son coefficient dominant ne s'annule pas et on a donc $\mathrm{Res}(P_1(x,y,T), P_2(x,y,T)) = \varphi(P) = P(x,y)$. Finalement on a donc $P(x,y) = 0$. Réciproquement, si $P(x,y) = 0$ alors le résultant de $P_1(x,y,T)$ et $P_2(x,y,T)$ est nul (par le même argument). Comme $\mathbb{C}$ est algébriquement clos, $P_1(x,y,T)$ et $P_2(x,y,T)$ ont une racine commune $t \in \mathbb{C}$. Comme $P_2(x,y,i) = P_2(x,y,-i) = -2 \neq 0$, on a $t \in \mathbb{C} \setminus \{-i, i\}$ et finalement $(x,y) \in \mathcal{C}$.

```
sage: PXY.<X, Y> = PolynomialRing(QQ)
sage: PXYT.<T> = PolynomialRing(PXY)
sage: PolX = T^2 + T + 1 - X
sage: PolY = (T^2 - 1) - (T^2 + 1) * Y
sage: PolX.resultant(PolY)
X^2*Y^2 - 2*X^2*Y + X^2 + 4*X*Y + Y^2 - 4*X + 3
```

3. D'après la question 1 il s'agit de démontrer que $\mathcal{C}' = \mathcal{C} \cap \mathbb{R}^2$; l'inclusion $\mathcal{C}' \subset \mathcal{C} \cap \mathbb{R}^2$ est triviale. Soit $(x, y) \in \mathcal{C} \cap \mathbb{R}^2$. Il existe $t \in \mathbb{C} \setminus \{-i, i\}$ tel que le système (1) soit vérifié. On a $(t^2+1)y = t^2 - 1$ donc $y \neq 1$ et $t^2 = \frac{1+y}{1-y}$. On en déduit que $t = x - t^2 - 1 \in \mathbb{R}$, donc $(x, y) \in \mathcal{C}'$.

Exercice 2

1. Notons $F : \mathbb{K} \to \mathbb{K}$, $x \mapsto x^2$ le morphisme de Frobenius, qui est $\mathbb{F}_2$-linéaire puisque $\mathbb{K}$ est de caractéristique 2. Alors pour tous $x \in \mathbb{K}$ et $i \in \mathbb{N}$ on a $x^{2^i} = F^i(x)$ donc l'application $\widetilde{T} : \mathbb{K} \to \mathbb{K}$, $x \mapsto T(x)$ (qu'on pourrait encore noter T) vérifie $\widetilde{T} = \sum_{i=0}^{m-1} F^i$: elle est $\mathbb{F}_2$-linéaire.
2. On a $T(X)^2 = T(X^2)$ car $T \in \mathbb{F}_2[X]$, d'où (en posant $j = i + 1$ dans la deuxième somme)

$$T(X)(1 + T(X)) = T(X) + T(X^2) = \sum_{i=0}^{m-1} X^{2^i} + \sum_{j=1}^{m} X^{2^j} = X^{2^m} + X.$$

   On peut aussi démontrer cette identité à partir d'un produit de Cauchy, même si c'est plus long. En effet en notant $T(X)(1 + T(X)) = \sum_{k=1}^{2^m} c_k X^k$ on a pour tout $k \in \{1, \ldots, 2^m\}$:

$$c_k = \sum_{\substack{0 \leq i,j \leq m-1 \\ 2^i + 2^j = k}} 1 + \sum_{\substack{0 \leq i \leq m-1 \\ 2^i = k}} 1.$$

   Si $k = 1$ ou $k = 2^m$ alors l'une des deux sommes vaut 1 et l'autre 0, donc $c_k = 1$. Si $k = 2^a$ avec $1 \leq a \leq m-1$ alors chacune des deux sommes vaut 1, en prenant $i = j = a - 1$ dans la première, donc $c_k = 0$. Enfin si $2 \leq k \leq 2^m - 1$ n'est pas une puissance de 2 alors la deuxième somme est nulle, et le première aussi car le nombre de couples (i, j) tels que $2^i + 2^j = k$ est pair (on a en effet $i \neq j$ donc on peut apparier (i, j) et (j, i)) : on a $c_k = 0$.
3. Soit $x \in \mathbb{F}_{2^m}$. Alors $x^{2^m} = x$ donc $x^{2^m} + x = 0$. D'après la question 2 on en déduit $T(x)(1+T(x)) = 0$: on a $T(x) = 0$ ou $T(x) = 1$, donc $T(x) \in \mathbb{F}_2$. L'application $\widetilde{T}$ de la question 1 est donc une forme linéaire sur le $\mathbb{F}_2$-espace vectoriel $\mathbb{F}_{2^m}$: son noyau est un hyperplan ou bien $\mathbb{F}_{2^m}$ tout entier. Comme $\deg T = 2^{m-1} < \operatorname{Card} \mathbb{F}_{2^m}$ ce n'est pas $\mathbb{F}_{2^m}$ tout entier. C'est donc un sous-espace vectoriel de $\mathbb{F}_{2^m}$ de dimension $m-1$: son cardinal est égal à 2^{m-1}. Les éléments $x \in \mathbb{F}_{2^m}$ qui n'appartiennent pas à cet hyperplan sont exactement ceux tels que $T(x) = 1$; il y en a $2^m - 2^{m-1} = 2^{m-1}$. Au

lieu de s'intéresser au noyau de cette forme linéaire, on pouvait aussi conclure grâce à la relation $T(X)(1+T(X)) = X^{2^m} + X$. En effet le polynôme $X^{2^m} + X$ est scindé à racines simples sur $\mathbb{F}_{2^m}$. On en déduit que $T(X)$ et $1+T(X)$ le sont également : ils ont chacun 2^{m-1} racines dans $\mathbb{F}_{2^m}$.

4. (a) On a $[\mathbb{F}_2(x) : \mathbb{F}_2] = d$ donc $\operatorname{Card} \mathbb{F}_2(x) = 2^d$. Comme $\mathbb{F}_2(x)$ est un sous-corps de $\mathbb{F}_{2^m}$, on en déduit que d divise m.

   (b) Comme $\deg P = m$, on a $P(X) = \prod_{i=0}^{m-1}(X - x^{2^i})$. Comme P est unitaire, le coefficient de X^{m-1} est l'opposé de la somme des racines : c'est $T(x)$, puisque $1 = -1$ en caractéristique 2.

   (c) On a $P(X) = \prod_{i=0}^{d-1}(X - x^{2^i})$ donc (comme à la question précédente) le coefficient de X^{d-1} est $\sum_{i=0}^{d-1} x^{2^i}$. Par ailleurs on a $x^{2^d} = x$ donc $x^{2^{dq+r}} = x^{2^r}$ pour tous $q, r \in \mathbb{N}$. Comme d divise m d'après la question (a), on peut écrire $m = dQ$ et on a
   $$T(x) = \sum_{i=0}^{dQ-1} x^{2^i} = \sum_{r=0}^{d-1}\sum_{q=0}^{Q-1} x^{2^{dq+r}} = Q\sum_{r=0}^{d-1} x^{2^r}.$$
   Si $Q = m/d$ est pair on a donc $T(x) = 0$; dans le cas contraire, $T(x)$ est égal au coefficient de X^{d-1} dans P.

   (d) Pour $x \in \mathbb{F}_{2^m}$, $T(x)$ est la trace de x relativement à l'extension $\mathbb{F}_{2^m}/\mathbb{F}_2$ (voir le TD 7 d'arithmétique, exercice 3, pour l'analogue dans une extension de corps de nombres).

Problème

1. Il s'agit de l'algorithme d'Euclide. Son coût est $O((1+\deg A)(1+\deg B))$ opérations arithmétiques dans $\mathbb{F}_q$. *La réponse $O((\deg A)(\deg B))$, valable lorsque A et B sont non constants, a été considérée comme juste.*

2.
```
def Euclide(A,B):
    a=A
    b=B
    while b<>0:
        r=a%b
        a=b
        b=r
    return a
```

3. (a)
```
sage: F = GF(13)
sage: Polynomes.<Y> = F[]
sage: P = Y^4 + 5*Y + 1
sage: P.is_irreducible()
True
```

   (b) Comme $\deg P = 4$ on a $\operatorname{Card} \mathbb{K} = 13^4$ (ce qui fait 28561).

(c)
```
sage: K.<y> = GF(13^4, modulus = P)
sage: R.<X> = K[]
sage: A = X^4 - X^2 - y^2 - y
sage: B = X^4 - (y + 3)*X^2 + 2*y + 2
sage: Euclide(A,B)
(y + 2)*X^2 + 12*y^2 + 10*y + 11
sage: A.gcd(B)
X^2 + 12*y + 12
sage: A.gcd(B)*(y+2)
(y + 2)*X^2 + 12*y^2 + 10*y + 11
```
Le pgcd unitaire de A et B est $X^2 - y - 1$. L'algorithme d'Euclide renvoie bien un pgcd, mais pas forcément celui qui est unitaire. Dans cet exemple il renvoie le pgcd de coefficient dominant $y + 2$.

4. Les éléments de $\mathcal{P}$ sont de deux sortes : d'une part les polynômes constants égaux à un nombre premier, et d'autre part les polynômes non constants, primitifs, de coefficient dominant strictement positif, qui sont irréductibles dans $\mathbb{Q}[X]$. Les premiers sont inversibles dans $\mathbb{Q}[X]$ alors que les seconds y restent irréductibles. La décomposition de S en produit d'irréductibles dans $\mathbb{Q}[X]$ est donc $c\prod_P P^{v_S(P)}$ où le produit porte sur les $P \in \mathcal{P}$ non constants ; ici c est un entier non nul, égal à $\varepsilon\prod_P P^{v_S(P)}$ où le produit porte sur les $P \in \mathcal{P}$ constants. Le pgcd de S et T est donc, à association près, $\prod_P P^{\min(v_S(P),v_T(P))}$. Le produit peut porter, au choix, sur tous les $P \in \mathcal{P}$ ou seulement sur ceux qui ne sont pas constants : cela ne change le pgcd que par un scalaire multiplicatif non nul.

5. Posons $S = X$ et $T = X + 2$. On a $\mathrm{pgcd}_{\mathbb{Z}[X]}(S, T) = 1$ car S et T appartiennent à $\mathcal{P}$. Mais pour tous $U, V \in \mathbb{Z}[X]$ le polynôme $US + VT$ prend une valeur paire en 0 (égale à $2V(0)$), donc il ne peut pas être égal à 1. Évidemment il existe de tels polynômes U et V dans $\mathbb{Q}[X]$: c'est une relation de Bezout.

6. Notons $\mathrm{cd}(R)$ le coefficient dominant d'un polynôme R. Alors $\mathrm{cd}(D) = \prod_P \mathrm{cd}(P)^{\min(v_S(P),v_T(P))}$ divise $\mathrm{cd}(S) = \prod_P \mathrm{cd}(P)^{v_S(P)}$, et aussi $\mathrm{cd}(T)$. Donc $\mathrm{cd}(D)$ divise $\mathrm{pgcd}(\mathrm{cd}(S), \mathrm{cd}(T))$. Par hypothèse sur p, on en déduit que p ne divise pas $\mathrm{cd}(D)$. Donc les polynômes D et $\overline{D}$ ont le même degré.

7. Il est clair que D divise S dans $\mathbb{Z}[X]$, c'est-à-dire qu'il existe $A \in \mathbb{Z}[X]$ tel que $S = DA$: en effet il suffit de poser $A = \prod_{P\in\mathcal{P}} P^{v_S(P)-\min(v_S(P),v_T(P))}$. En réduisant modulo p il vient $\overline{S} = \overline{D}\,\overline{A}$ donc $\overline{D}$ divise $\overline{S}$. De même $\overline{D}$ divise $\overline{T}$, donc $\overline{D}$ divise le pgcd de $\overline{S}$ et $\overline{T}$.

8. D'après la proposition 6.12 du poly, comme p ne divise ni le pgcd des coefficients dominants de S/D et T/D ni leur résultant, les polynômes $\overline{S}/\overline{D} = \overline{S/D}$ et $\overline{T}/\overline{D}$ sont premiers entre eux dans $\mathbb{F}_p[X]$. Donc $\overline{D}$ est (à association près) le pgcd de $\overline{S}$ et $\overline{T}$.

9. Notons $d = \min(\deg S, \deg T)$ et $M = 2^d \min(\|S\|_2, \|T\|_2)$. Comme D divise S et T dans $\mathbb{Z}[X]$, on a $\|D\|_\infty \leq 2^{\deg D} \min(\|S\|_2, \|T\|_2) \leq M$. *Dans cette question toute réponse similaire était admise, par exemple* $M = 2^{\deg S}\|S\|_2$.

10. A la question 6 on a montré que le coefficient dominant de D divise ℓ, donc il existe un tel entier c.
11. Pour tout $i \in \{1, \dots, k\}$ notons $\overline{R_i} \in \mathbb{F}_{p_i}[X]$ le pgcd unitaire des réductions modulo p_i de S et T ; la question 1 montre comment calculer $\overline{R_i}$. Les hypothèses faites sur p_i (et le fait que S et T soient primitifs) permettent d'appliquer la question 8 : la réduction de D modulo p_i est égale (à association près) à $\overline{R_i}$. Or $\overline{cD}$ et $\overline{\ell R_i}$ ont en outre le même coefficient dominant (d'après la question 10), donc $\overline{cD} = \overline{\ell R_i}$. On connaît donc la réduction de cD modulo chacun des nombres premiers p_i. Grâce au théorème chinois on peut calculer un polynôme $Q \in \mathbb{Z}[X]$, à coefficients compris entre $-p_1 \dots p_k/2$ et $p_1 \dots p_k/2$, dont la réduction modulo chaque p_i est égale à celle de cD. Comme $p_1 \dots p_k/2 > \ell M \geq \|\ell D\|_\infty \geq \|cD\|_\infty$ d'après la question 9, on en déduit que $cD = Q$.
12. Comme D est primitif (car S et T le sont), cD est le contenu de D (c'est-à-dire le pgcd des coefficients de D) : on le trouve facilement, et on en déduit D.