*Téléchargé depuis http://www.math.u-psud.fr/~fischler/enseignement.html*

# Corrigé de l'examen de M.A.O. Calcul Formel

Lundi 18 juin 2018
Master 1 M.F.A., Orsay

**Exercice 1.**

1. ($\star$)

```
sage: PXY.<x, y> = PolynomialRing(QQ)
sage: A = 2*x*y^2 + 4*x*y + 5
sage: B = x*y - x - 1
sage: R = A.resultant(B, y)
sage: R
6*x^3 + 13*x^2 + 2*x
sage: R.factor()
x * (x + 2) * (6*x + 1)
```

2. Soit $(x, y) \in \mathcal{C}$. Notons $\varphi : \mathbb{Q}[X] \to \mathbb{Q}$ l'homomorphisme de $\mathbb{Q}$-algèbres consistant à évaluer en $x$. Pour tout $P = P(X, Y) \in \mathbb{Q}[X, Y]$, on note $P^\varphi(X) = P(x, Y) \in \mathbb{Q}[Y]$ l'image de $P$ par l'homomorphisme $\mathbb{Q}[X, Y] \to \mathbb{Q}[Y]$ consistant à appliquer $\varphi$ à chaque coefficient de $P$ vu dans $(\mathbb{Q}[X])[Y]$. Le coefficient dominant de $A$ dans $(\mathbb{Q}[X])[Y]$ est $2X$ ; celui de $B$ est $X$. Le cas $x = 0$ doit être traité séparément ; comme $R(0) = 0$ d'après la question 1, le résultat est trivial dans ce cas. Supposons désormais $x \neq 0$. Alors les coefficients dominants de $A$ et $B$ ont des images non nulles par $\varphi$ donc on a

$$\mathrm{Res}(A^\varphi, B^\varphi) = \varphi(\mathrm{Res}(A, B)) = \varphi(R) = R(x).$$

Or par hypothèse le réel $y$ vérifie $A(x, y) = B(x, y) = 0$ donc les polynômes $A^\varphi$ et $B^\varphi$ ont une racine commune $y$. Cela implique $\mathrm{Res}(A^\varphi, B^\varphi) = 0$, c'est-à-dire $R(x) = 0$. Géométriquement, notons $p$ la projection orthogonale sur l'axe des abscisses, dans le plan $\mathbb{R}^2$ muni de sa structure euclidienne canonique. On a montré que l'image de $\mathcal{C}$ par $p$ est contenue dans l'ensemble des points de la forme $(x, 0)$, où $x$ est une racine de $R$.

3. ($\star$) D'après la question 1, les racines réelles de $R$ sont 0, $-2$ et $-1/6$. Pour chacune de ces racines $x$, on factorise les polynômes $A(x, Y)$ et $B(x, Y)$ pour voir si ils ont une racine commune. Les lignes suivantes montrent que c'est le cas pour $-2$ et $-1/6$, mais pas pour 0. On obtient ainsi que $\mathcal{C}$ est l'ensemble formé par les deux points $(-2, 1/2)$ et $(-1/6, -5)$.

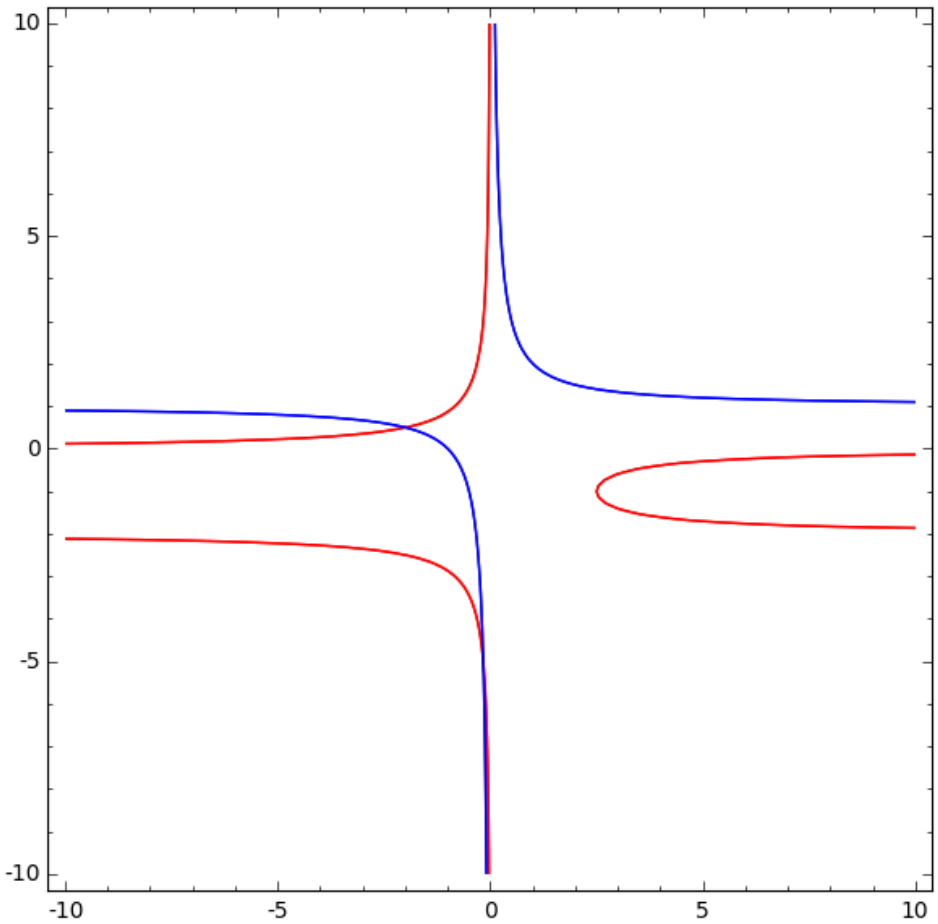
```
sage: A(-2, y).factor()
(-1) * (2*y - 1) * (2*y + 5)
```

```
sage: B(-2, y).factor()
(-1) * (2*y - 1)
sage: A(-1/6, y).factor()
(-1/3) * (y - 3) * (y + 5)
sage: B(-1/6, y).factor()
(-1/6) * (y + 5)
sage: A(0, y)
5
sage: B(0, y)
-1
```

4. On a vu à la question 3 que 0 est une racine de $R$ pour laquelle aucun réel $y$ ne vérifie $(x, y) \in \mathcal{C}$. Une première explication de ce phénomène est que 0 est une racine commune des coefficients dominants de $A$ et $B$ (voir le corrigé de la question 2). Ceci implique $R(0) = 0$, indépendamment de l'existence de $y \in \mathbb{R}$ tel que $(x, y) \in \mathcal{C}$. Une autre explication, plus géométrique et qui dépasse le cadre du cours, est la présence d'une asymptote verticale commune aux courbes définies par $A$ et $B$, d'équation $x = 0$. Intuitivement, il y a bien un point d'abscisse 0 sur $\mathcal{C}$, mais il est "à l'infini" dans la direction verticale.

5. ($\star$) Le calcul suivant montre que le résultant $S$ de $A$ et $B$, vus dans $(\mathbb{Q}[Y])[X]$, n'a que deux racines : $1/2$ et $-5$. Ce sont exactement les ordonnées des éléments de $\mathcal{C}$. Le phénomène évoqué à la question 4 ne se produit pas, car les coefficients dominants de $A$ et $B$ dans $(\mathbb{Q}[Y])[X]$ sont respectivement $2Y^2 + 4Y$ et $Y - 1$ : ils n'ont aucune racine commune. On peut donc raisonner comme à la question 2, sans distinguer de valeur particulière de $y$. Géométriquement, les deux courbes n'ont aucune asymptote horizontale commune. Même si ce n'était pas demandé, voici l'allure des courbes d'équations $A(x, y) = 0$ (en rouge) et $B(x, y) = 0$ (en bleu).

```
sage: a = implicit_plot(A, (x, -10, 10), (y, -10, 10), color='red')
sage: b = implicit_plot(B, (x, -10, 10), (y, -10, 10), color='blue')
sage: a + b
```




**Exercice 2.**

1. Il y a quatre polynômes de degré 2 à coefficients dans $\mathbb{F}_2$ : $X^2$, $X^2+1$, $X^2+X$, $X^2+X+1$. Les trois premiers ont au moins une racine (0 pour le premier et le troisième, 1 pour le deuxième et le troisième) donc ils ne sont pas irréductibles. Le dernier est irréductible car il est de degré 2 sans racine dans $\mathbb{F}_2$.

2. Soit $Q = X^3 + aX^2 + bX + c$ un polynôme irréductible de $\mathbb{F}_2[X]$ de degré 3 (son coefficient dominant étant non nul, il vaut forcément 1). Comme $Q$ est irréductible, il n'a aucune racine dans $\mathbb{F}_2$. On a donc $c = Q(0) = 1$, puis $a + b = Q(1) = 1$. Il y a donc deux possibilités, selon que $(a, b)$ est égal à $(1, 0)$ ou à $(0, 1)$. On trouve ainsi deux polynômes : $X^3+X^2+1$ et $X^3+X+1$. Réciproquement, ces deux polynômes sont bien irréductibles car, par construction, ils sont de degré 3 sans racine dans $\mathbb{F}_2$.

3. Si $P$ n'était pas irréductible, il pourrait se factoriser sous la forme $Q_1Q_2$ avec $1 \leq \deg Q_1 \leq \deg Q_2$. Comme $P$ est de degré 6, on aurait $\deg Q_1 \leq 3$. En considérant un facteur irréductible de $Q_1$, on voit que $P$ serait divisible par un polynôme irréductible de degré au plus 3. D'après les questions 1 et 2, ce polynôme serait $X$, $X+1$,

$X^2+X+1$, $X^3+X^2+1$ ou $X^3+X+1$. Or les lignes de code suivantes montrent que $P$ n'est divisible par aucun de ces 5 polynômes.

```
sage: F = GF(2)
sage: X = polygen(F)
sage: (X^6 + X + 1)%X
1
sage: (X^6 + X + 1)%(X + 1)
1
sage: (X^6 + X + 1)%(X^2 + X + 1)
x
sage: (X^6 + X + 1)%(X^3 + X^2 + 1)
x^2 + 1
sage: (X^6 + X + 1)%(X^3 + X + 1)
x^2 + x
```

4. Comme $P$ est irréductible de degré 6 sur $\mathbb{F}_2$, on a $[\mathbb{K}:\mathbb{F}_2]=6$ et $\operatorname{Card}\mathbb{K}=2^6=64$.

5. Les sous-corps de $\mathbb{K}$ sont en bijection avec les éléments de l'ensemble $\{1,2,3,6\}$ des diviseurs de 6 : il y en a donc quatre. Leurs cardinaux respectifs sont $2^1=2$, $2^2=4$, $2^3=8$ et $2^6=64$.

6. ($\star$) Les lignes de code suivantes montrent que $a^{21}=1+a^2+a^3+a^4+a^5$. On calcule ensuite $(a^{21})^4=a^{84}$, et on trouve $a^{21}$ : cela montre que $a^{21}$ appartient à l'unique sous-corps de $\mathbb{K}$ de cardinal 4. Comme $a^{21}\notin\mathbb{F}_2$ (comme le prouve son expression dans la base $(1,a,a^2,\dots,a^5)$), ce sous-corps est $\mathbb{F}_2(a^{21})$.

```
sage: K.<a> = GF(2^6, modulus=X^6 + X + 1)
sage: a^21
a^5 + a^4 + a^3 + a + 1
sage: (a^21)^4
a^5 + a^4 + a^3 + a + 1
```

7. ($\star$) On constate successivement que $b^2\neq b$ et $b^4\neq b$, donc $b$ n'appartient ni à $\mathbb{F}_2$ ni au sous-corps de $\mathbb{K}$ de cardinal 4. En revanche $b^8=8$ donc $b$ appartient sous-corps de $\mathbb{K}$ de cardinal 8. Il l'engendre car il n'appartient à aucun corps strictement contenu dans celui-ci.

```
sage: b = a + a^8
sage: b^2 - b
a^4 + a^3 + 1
sage: b^4 - b
a^4 + a^2 + a + 1
```

```
sage: b^8 - b
0
```

8. Les sous-corps de $\mathbb{K}$ sont donc $\mathbb{F}_2 = \mathbb{F}_2(1)$, $\mathbb{F}_2(a^{21})$ qui est de cardinal 4, $\mathbb{F}_2(b)$ qui est de cardinal 8, et $\mathbb{K} = \mathbb{F}_2(a)$.

9. On a $\deg R = [\mathbb{K} : \mathbb{F}_2(b)] = \frac{[\mathbb{K}:\mathbb{F}_2]}{[\mathbb{F}_2(b):\mathbb{F}_2]} = \frac{6}{3} = 2$.

10. ($\star$) Le morphisme de Frobenius relatif à $\mathbb{F}_2(b)$ est $x \mapsto x^8$. Comme $a$ est de degré 2 sur $\mathbb{F}_2(b)$ on a $R(X) = (X-a)(X-a^8)$. Par défaut les coefficients de $R$ sont écrits par Sage comme polynômes en $a$, mais ils appartiennent à $\mathbb{F}_2(b) = \mathrm{Vect}_{\mathbb{F}_2}(1, b, b^2)$ (puisque $[\mathbb{F}_2(b) : \mathbb{F}_2] = 3$) donc il n'est pas difficile de les écrire à vue comme polynômes de degré au plus 2 en $b$. On obtient ainsi $R(X) = X^2 + bX + b^2 + b + 1$.

```
sage: R = (X - a)*(X - a^8)
sage: R
x^2 + (a^3 + a^2 + a)*x + a^4 + a^3
sage: b
a^3 + a^2 + a
sage: b^2
a^4 + a^2 + a + 1
sage: R - (X^2 + b*X + b^2 + b + 1)
0
```

**Exercice 3.**

1. ($\star$)

```
sage: all((n^17 + 9).gcd((n + 1)^17 + 9) == 1 for n in range(1, 10^5))
True
```

2. Calculer $n^{17} + 9$ et $(n+1)^{17} + 9$ coûte $O(1)$ opérations arithmétiques dans $\mathbb{Z}$. On calcule ensuite leur pgcd par l'algorithme d'Euclide, pour un coût de $O(\log(n^{17}+9)) = O(\log n)$ opérations arithmétiques dans $\mathbb{Z}$.

3. Le coût est de $\sum_{n=1}^{N} O(\log n) = O(N \log N)$. Si on veut $N \log N \simeq 10^{12}$, on doit prendre $\log N \simeq \log(10^{12}) = 12 \log(10) \simeq 28$ donc $N \simeq \frac{10^{12}}{28} \simeq 3,6 \cdot 10^{10}$. On vérifie que pour $N = 3,6 \cdot 10^{10}$ on a $N \log N \simeq 8,8 \cdot 10^{11} < 10^{12}$.

4. Il semble contre-intuitif que $\mathcal{P}(n)$ soit vraie pour tout $n$, mais il est rare de voir une propriété vraie jusqu'à un tel rang puis fausse ensuite !

5. ($\star$)

```
sage: X = polygen(ZZ)
sage: p = (X^17 + 9).resultant((X + 1)^17 + 9)
sage: p
893658223791571665995096225335894563579345325693555 9
```

6. Si $p$ est premier alors pour tout $a \in \mathbb{Z}$ on a $a^p - a \equiv 0 \bmod p$ d'après le petit théorème de Fermat. Donc si le test réussit, alors $p$ n'est pas premier.

7. ($\star$) Le test est un échec. Cela ne démontre pas que $p$ est premier, mais cela corrobore cette hypothèse.

```
sage: Zmodp = Integers(p)
sage: echantillon = (Zmodp.random_element() for _ in range(100))
sage: any(a^p - a for a in echantillon)
False
```

8. Pour chaque $a \in \mathbb{Z}/p\mathbb{Z}$, on calcule $a^p$ par exponentiation rapide. Le coût est de $O(\log p)$ opérations ; comme $\log p \simeq 119$ on a besoin de 100 opérations (en ordre de grandeur). Ensuite tester si $a^p$ est égal à $a$ dans $\mathbb{Z}/p\mathbb{Z}$ ne coûte aucune opération. Comme on répète cela 100 fois, on effectue au total de l'ordre de $10^4$ opérations.

9. Supposons que $n^{17}+9$ et $(n+1)^{17}+9$ ne sont pas premiers entre eux : ils possèdent un facteur premier $p'$ en commun. Posons $P = X^{17}+9$ et $Q = (X+1)^{17}+9$. Notons $\varphi : \mathbb{Z} \to \mathbb{Z}/p'\mathbb{Z}$ la réduction modulo $p'$, et $T^\varphi \in (\mathbb{Z}/p\mathbb{Z})[X]$ le polynôme obtenu à partir de $T \in \mathbb{Z}[X]$ en appliquant $\varphi$ à tous les coefficients. Comme $P$ et $Q$ sont unitaires on a $\mathrm{Res}(P^\varphi, Q^\varphi) = \varphi(p)$. Or $\varphi(n)$ est une racine commune de $P^\varphi$ et $Q^\varphi$ dans $\mathbb{Z}/p\mathbb{Z}$, donc $\mathrm{Res}(P^\varphi, Q^\varphi) = 0$. On obtient donc $\varphi(p) = 0$, c'est-à-dire que $p'$ divise $p$. Comme $p$ et $p'$ sont des nombres premiers, on a donc $p' = p$ : le résultant $p$ divise $n^{17}+9$ et $(n+1)^{17}+9$.

10. On constate avec Sage que $p-1$ est divisible par 17, et que dans $\mathbb{Z}/p\mathbb{Z}$ on a $(-9)^{(p-1)/17} = 1$. Evidemment ce calcul doit être fait dans $\mathbb{Z}/p\mathbb{Z}$ : l'entier $(-9)^{(p-1)/17}$ est énorme, il n'est pas question de le calculer avant de réduire modulo $p$. Donc l'équation $x^{17} = -9$ a une solution $x_0$ dans $\mathbb{Z}/p\mathbb{Z}$ (en effet l'ensemble des éléments de la forme $x^{17}$ avec $x \in (\mathbb{Z}/p\mathbb{Z})^*$ est contenu dans l'ensemble des $y$ tels que $y^{(p-1)/17} = 1$, et ces deux ensembles sont de même cardinal $(p-1)/17$ donc égaux). En outre les éléments $x \in (\mathbb{Z}/p\mathbb{Z})^*$ tels que $x^{17} = 1$ forment un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$ qui est cyclique de cardinal 17 (car $(\mathbb{Z}/p\mathbb{Z})^*$ lui-même est cyclique). Donc l'équation $x^{17} = -9$ possède 17 solutions dans $\mathbb{Z}/p\mathbb{Z}$. Autrement dit, en gardant les notations de la question précédente (avec $p' = p$), le polynôme $P^\varphi$ est scindé sur $\mathbb{Z}/p\mathbb{Z}$. Comme $\mathrm{Res}(P^\varphi, Q^\varphi) = \varphi(p) = 0$, les polynômes $P^\varphi$ et $Q^\varphi$ ont une racine commune dans $\mathbb{Z}/p\mathbb{Z}$ : il existe $n \geq 1$ tel que $p$ divise $P(n)$ et $Q(n)$. Cette propriété reste vraie si on ajoute à $n$ un multiple quelconque de $p$, donc on obtient ainsi une infinité d'entiers $n \geq 1$ pour lesquels $\mathcal{P}(n)$ est fausse.

11. En combinant les deux questions précédentes on voit que $\mathcal{P}(n)$ est fausse si, et seulement si, la classe de $n$ modulo $p$ est une racine commune de $P^\varphi$ et $Q^\varphi$. Les lignes de code suivantes montrent que ces deux polynômes ont une et une seule racine commune dans $\mathbb{Z}/p\mathbb{Z}$, qui est $n_0 = 842443292559288932928819732230890067245942046079243 3$. Finalement $\mathcal{P}(n)$ est fausse si, et seulement si, $n \equiv n_0 \bmod p$.

```
sage: T = polygen(Zmodp)
sage: P = T^17 + 9
sage: Q = P(T + 1)
sage: [a for a in P.roots(multiplicities=False) if Q(a) == 0]
[842443292559288932928819732230890067245942046079243 3]
```