UFR de Mathématiques et Informatique
Université Bordeaux I Année 2000–2001

Licence de Mathématiques et Informatique

Module d'Algorithmique Arithmétique

Corrigé de l'épreuve du 22 janvier 2001

Exercice I

1) Question préliminaire.

a) Les seuls problèmes de convergence sont en 0 et à l'infini. A l'infini, e^{-x} décroit plus rapidement vers 0 que toute puissance de x, donc l'intégrale converge. En 0, e^{-x} tend vers 1 donc l'intégrale est de même nature que celle de x^α, qui converge si et seulement si $\alpha > -1$.

b) Si $\alpha > 0$, on a

$$I(\alpha) = -x^\alpha e^{-x}\Big|_0^\infty + \int_0^\infty \alpha x^{\alpha-1}e^{-x}\,dx = \alpha I(\alpha-1)\ ,$$

d'où le résultat.

c) Si k est entier, on a donc

$$I(k) = kI(k-1) = k(k-1)I(k-2) = \cdots k!I(0) = k!\ .$$

On peut donc poser $\alpha! = I(\alpha)$. Noter que $I(\alpha-1)$ est en fait appelée la fonction gamma, et notée $\Gamma(\alpha)$.

d) Par récurrence sur k, il est clair que la dérivée k-ième de X^α est égale à $\alpha(\alpha-1)\cdots(\alpha-k+1)X^{\alpha-k}$. D'après la récurrence $\alpha! = \alpha(\alpha-1)!$, ceci est bien égal à $(\alpha!/(\alpha-k)!)X^{\alpha-k}$.

2) a) D'après la question 1a), l'intégrale définissant $< P, Q >$ est combinaison linéaire finie d'intégrales du type $I(a+k)$ avec $k \geq 0$ entier, donc converge. De plus, il est clair que $< P, Q >$ est une forme bilinéaire, que cette forme est symétrique, et que $< P, P >= \int_0^\infty P(x)^2 x^a e^{-x}\,dx$ est bien positif ou nul. Le point le plus important est de noter que puisque $P^2(x)x^a e^{-x}$ est une fonction *continue* sur $]0,\infty[$, on ne peut avoir $< P, P >= 0$ que si $P^2(x)x^a e^{-x}$ est identiquement nul sur $]0,\infty[$, ce qui n'est pas possible pour un polynôme non identiquement nul. Répétons encore une fois le raisonnement, en posant $f(x) = P^2(x)x^a e^{-x}$. Si $f(x)$ n'était pas identiquement nulle sur $]0,\infty[$, il existerait $x_0 > 0$ avec $f(x_0) > 0$. Choisissons $\varepsilon = f(x_0)/2$. Par continuité de f, il existe $\eta > 0$ tel

que pour tout x tel que $|x-x_0| < \eta$ on ait $|f(x)-f(x_0)| < \varepsilon = f(x_0)/2$. En particulier, on a $f(x) \geq f(x_0)/2$ dans l'intervalle $[x_0, x_0+\eta[$, donc l'intégrale de x_0 à $x_0+\eta$ est supérieure ou égale à $\eta f(x_0)/2$. Comme $f(x) \geq 0$ sur $]0, \infty[$, l'intégrale de 0 à l'infini est supérieure ou égale à celle de x_0 à $x_0+\eta$, donc à $\eta f(x_0)/2 > 0$, contradiction puisqu'on a supposé qu'elle est nulle.

Il en résulte donc bien que $< P, Q >$ est un produit scalaire.

b) D'après les formules de Gram–Schmidt et l'intégrale calculée dans la question préliminaire, on a $P_0(X) = 1$,

$$P_1(X) = X - \frac{< X, 1 >}{< 1, 1 >} = X - \frac{(a+1)!}{a!} = X - (a+1) \ ,$$

$$\begin{aligned} P_2(X) &= X^2 - \frac{< X^2, X-(a+1) >}{< X-(a+1), X-(a+1) >}(X-(a+1)) - \frac{< X^2, 1 >}{< 1, 1 >} \\ &= X^2 - \frac{(a+3)! - (a+1)(a+2)!}{(a+2)! - 2(a+1)(a+1)! + (a+1)^2 a!}(X-(a+1)) - \frac{(a+2)!}{a!} \\ &= X^2 - 2(a+2)X + (a+1)(a+2) \ . \end{aligned}$$

3) a) Nous allons calculer tous les coefficients de $Q_n(X)$, ce qui nous permettra d'économiser des calculs ultérieurement. D'après la formule de Leibnitz, la formule de la question 1d) et en posant pour simplifier les notations $D = d/dx$, on a

$$D^n(X^{n+a}e^{-X}) = \sum_{k=0}^{n} \binom{n}{k} D^{n-k}(X^{n+a}) D^k(e^{-X}) = \sum_{k=0}^{n} \binom{n}{k} \frac{(n+a)!}{(k+a)!} X^{k+a} (-1)^k e^{-X} \ .$$

On a donc

$$Q_n(X) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \frac{(n+a)!}{(k+a)!} X^k \ .$$

En particulier, il est clair que Q_n est un polynôme en X de degré n, le coefficient de X^n étant égal à $(-1)^n$.

b) On a

$$\begin{aligned} < Q_n, R > &= \int_0^\infty D^n(x^{n+a}e^{-x}) R(x)\, dx \\ &= D^{n-1}(x^{n+a}e^{-x}) R(x) \Big|_0^\infty - \int_0^\infty D^{n-1}(x^{n+a}e^{-x}) DR(x)\, dx \ . \end{aligned}$$

Il est facile de voir par récurrence sur k, et on a également vu ceci dans le calcul de $Q_n(X)$ effectué ci-dessus, que la dérivée k-ième de $x^{n+a}e^{-x}$ est de la forme $x^{n+a-k}S_k(x)e^{-x}$ pour un polynôme $S_k(X)$ de degré k. En particulier, ceci s'annule à l'infini, et si $k <= n-1$, aussi en 0 puisque $a > -1$. Le terme tout intégré est donc nul, et on peut poursuivre les intégrations par parties, pour obtenir finalement

$$< Q_n, R >= (-1)^n \int_0^\infty x^{n+a} e^{-x} D^n R(x)\, dx \ .$$

Or $R(X) = rX^{n+1} + sX^n + \cdots$. Il en résulte que

$$D^n R = r(n+1)!X + sn! = n!(r(n+1)X + s) \ ,$$

et donc que

$$< Q_n, R >= (-1)^n n!(r(n+1)(n+a+1)! + s(n+a)!) = (-1)^n n!(n+a)!(r(n+1)(n+a+1)+s) \ .$$

En particulier, si $r = s = 0$, c'est à dire si R est de degré inférieur ou ègal à $n-1$, on a $< Q_n, R >= 0$.

c) On sait qu'à une constante multiplicative près, le polynôme P_n est l'unique polynôme de degré n qui soit orthogonal à tous les polynômes de degré inférieur ou égal à $n-1$. Comme c'est le cas de Q_n, on en déduit que $P_n(X) = c_n Q_n(X)$ pour une certaine constante c_n. Comme le coefficient dominant de Q_n est égal à $(-1)^n$, on a $c_n = (-1)^n$, donc $P_n(X) = (-1)^n Q_n(X)$.

4) Grâce au calcul fait ci-dessus, on obtient immédiatement

$$P_n(X) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \frac{(n+a)!}{(k+a)!} X^k \ .$$

5) a) La formule ci-dessus donne $P_n(X) = X^n - n(n+a)X^{n-1} + \cdots$. D'après la question 3b), si $R(X) = rX^{n+1} + sX^n + \cdots$, on a

$$< P_n, R >= (-1)^n < Q_n, R >= n!(n+a)!(r(n+1)(n+a+1)+s) \ .$$

Appliquant ceci à $R(X) = XP_n(X)$ et à $R(X) = P_n(X)$, on en déduit que

$$u_n =< P_n, XP_n >= n!(n+a)!((n+1)(n+a+1) - n(n+a)) = n!(n+a)!(2n+a+1)$$

et que $v_n =< P_n, P_n >= n!(n+a)!$.

b) On a donc

$$a_n = -\frac{n!(n+a)!(2n+a+1)}{n!(n+a)!} = -(2n+a+1) \ ,$$

et

$$b_n = -\frac{n!(n+a)!}{(n-1)!(n-1+a)!} = -n(n+a) \ .$$

Les polynômes P_n vérifient donc la récurrence

$$P_{n+1}(X) = (X - (2n+a+1))P_n(X) - n(n+a)P_{n-1}(X) \ .$$

Par exemple, sachant que $P_0(X) = 1$ et $P_1(X) = X - (a+1)$, on obtient

$$P_2(X) = (X - (a+3))(X - (a+1)) - (a+1) = X^2 - 2(a+2)X + (a+1)(a+2) \ ,$$

et on retrouve la formule trouvée ci-dessus.

Exercice II

On calcule que

$$AA^t = \begin{pmatrix} a^2+1 & a & 0 \\ a & a^2+1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Le polynôme caractéristique de cette matrice se calcule facilement et est égal à

$$X(X^2 - 2(a^2+1)X + (a^4+a^2+1)) \, .$$

Les racines du polynôme du second degré ci-dessus sont égales à

$$a^2+1 \pm \sqrt{(a^2+1)^2 - (a^4+a^2+1)} = a^2+1 \pm a \, .$$

Comme $a > 0$, les valeurs propres de AA^t sont, en ordre décroissant, a^2+a+1, a^2-a+1 et 0. En particulier, on a

$$D = \begin{pmatrix} \sqrt{a^2+a+1} & 0 & 0 \\ 0 & \sqrt{a^2-a+1} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

La norme de A est égale à sa plus grande valeur singulière, donc à $\sqrt{a^2+a+1}$.

2) Pour $a = 2$, on a

$$D = \begin{pmatrix} \sqrt{7} & 0 & 0 \\ 0 & \sqrt{3} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Si $A = UDV^t$, on a $AA^t = UD^2U^t$, donc U est une matrice de vecteurs propres orthonormés de AA^t. Tous calculs faits, on trouve par exemple

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & \sqrt{2} \end{pmatrix}$$

Pour trouver la matrice V, il faut faire attention. On calcule que

$$A^tA = \begin{pmatrix} 4 & 2 & 0 \\ 2 & 5 & 2 \\ 0 & 2 & 1 \end{pmatrix}$$

et la matrice V est *une* matrice de vecteurs propres orthonormés de A^tA. Comme toutes les valeurs propres sont simples, les dimensions des sous-espaces propres sont égales à 1, donc il n'y a que deux choix pour chaque vecteur propre, mais il faut faire le bon choix.

Plus précisément, puisque $AV = UD$, si V_i désigne la i-ième colonne de V, c'est à dire le i-ième vecteur propre, AV_i doit être égal à la i-ième colonne de

$$UD = \begin{pmatrix} \sqrt{7/2} & \sqrt{3/2} & 0 \\ \sqrt{7/2} & -\sqrt{3/2} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

On trouve donc $V_1 = \pm(2,3,1)^t/\sqrt{14}$, donc $AV_1 = \pm\sqrt{7/2}(1,1,0)^t$, donc on doit choisir le signe $+$, c'est à dire $V_1 = (2,3,1)^t/\sqrt{14}$. De même $V_2 = \pm(-2,1,1)^t/\sqrt{6}$, donc $AV_2 = \pm\sqrt{3/2}(-1,1,0)^t$, donc cette fois-ci on doit choisir le signe $-$, c'est à dire $V_2 = (2,-1,-1)^t/\sqrt{6}$. Enfin, la troisième colonne de UD est nulle, donc on peut prendre $V_3 = \pm(1,-2,4)^t/\sqrt{21}$ avec un signe $\pm$ indifférent. On a donc finalement (par exemple)

$$V = \frac{1}{\sqrt{42}} \begin{pmatrix} 2\sqrt{3} & 2\sqrt{7} & \sqrt{2} \\ 3\sqrt{3} & -\sqrt{7} & -2\sqrt{2} \\ \sqrt{3} & -\sqrt{7} & 4\sqrt{2} \end{pmatrix}$$

3) On a par définition

$$D^\dagger = \begin{pmatrix} 1/\sqrt{7} & 0 & 0 \\ 0 & 1/\sqrt{3} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

et $A^\dagger = VD^\dagger U^t$. Tous calculs faits, on trouve

$$D^\dagger U^t = \frac{1}{\sqrt{42}} \begin{pmatrix} \sqrt{3} & \sqrt{3} & 0 \\ \sqrt{7} & -\sqrt{7} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

puis

$$A^\dagger = \frac{1}{21} \begin{pmatrix} 10 & -4 & 0 \\ 1 & 8 & 0 \\ -2 & 5 & 0 \end{pmatrix}$$

Exercice III

1) Il est clair que $\omega^2 = \omega - 2$ et que $\overline{\omega} = 1 - \omega$.

2) Si $\alpha = a + b\omega$ et $\beta = c + d\omega$, il est clair que si α et β sont dans K alors $\alpha - \beta \in K$, et s'ils sont dans A alors $\alpha - \beta \in A$. Il en résulte que K et A sont des sous-groupes additifs de $\mathbb{C}$. De plus, on a $\alpha\beta = ac + (ad + bc)\omega + bd\omega^2$. Mais d'après la question précédente (et c'est le point essentiel), on a $\omega^2 = \omega - 2$, donc $\alpha\beta = (ac - 2bd) + (ad + bc + bd)\omega$, et ceci appartient bien à K si α et β y appartiennent, ou à A si α et β y appartiennent. La multiplication est donc stable, et bien entendu $1 \in A \subset K$, donc A est un sous-anneau de K qui est lui-même un sous-anneau de $\mathbb{C}$. Enfin, pour voir que K est un corps, il faut

montrer que tout élement non nul est inversible. En effet si $\alpha = a + b\omega \neq 0$, on a tout d'abord

$$\alpha\overline{\alpha} = (a+b\omega)(a+b\overline{\omega}) = (a+b\omega)(a+b-b\omega) = a(a+b) + b^2\omega - b^2\omega^2 = a^2 + ab + 2b^2$$

d'après la première question. On a donc

$$\frac{1}{\alpha} = \frac{\overline{\alpha}}{\alpha\overline{\alpha}} = \frac{a+b\overline{\omega}}{a^2+ab+2b^2} = \frac{a+b}{a^2+ab+2b^2} - \frac{b}{a^2+ab+2b^2}\omega$$

et ceci est donc bien dans K puisque les coefficients sont dans $\mathbb{Q}$.

3) Nous venons de montrer que $\phi(\alpha) = a^2 + ab + 2b^2$. Mais en considérant b comme la variable prioritaire, on peut aussi écrire $\phi(\alpha) = 2(b + a/4)^2 + 7a^2/8$, ce qui est le résultat demandé.

4) On a $\phi(\alpha - (u + v\omega)) = \phi(\beta)$ avec $\beta = (a-u) + (b-v)\omega$. On a donc

$$\phi(\alpha - (u+v\omega)) = 2(b - v + (a-u)/4)^2 + 7(a-u)^2/8\ .$$

Comme u est l'entier le plus proche de a, on a $|a - u| \leq 1/2$ donc $(a-u)^2 \leq 1/4$. De même, comme v est l'entier le plus proche de $b + (a-u)/4$, on a $|b + (a-u)/4 - v| \leq 1/2$ donc $(b - v + (a-u)/4)^2 \leq 1/4$. En remplaçant, on obtient

$$\phi(\alpha - (u+v\omega)) \leq 2/4 + 7/32 = 23/32 < 1\ .$$

5) Soient x et y deux éléments de A avec $y \neq 0$. Comme A est un sous-anneau de K et que K est un corps, $\alpha = x/y$ est un élément de K. D'après la question précédente, si on pose $q = u + v\omega$ on a $\phi(\alpha - q) < 1$ (en fait plus petit ou égal à 23/32). Comme ϕ a la propriété d'être multiplicative (ce qui n'est pas exigé pour un stathme Euclidien), on a donc $\phi(y(\alpha - q)) < \phi(y)$. Or $r = y(\alpha - q) = x - qy \in A$, et bien entendu $q \in A$. On a donc écrit $x = qy + r$ avec q et y dans A et $\phi(r) < \phi(y)$, ce qui montre bien que ϕ est un stathme Euclidien (les autres propriétés sont évidentes). Il en résulte bien que l'anneau A est Euclidien.

Si on prend plus généralement $\omega = (1 + i\sqrt{4k-1})/2$ avec $k \geq 0$ entier, on peut essayer de faire le même raisonnement. On a toujours $\overline{\omega} = 1 - \omega$, et ici $\omega^2 = \omega - k$. L'ensemble K est toujours un corps et A un sous-corps. Toutefois, l'inégalité de la quatrième question devient

$$\phi(\alpha - (u+v\omega)) \leq \frac{4k^2+4k-1}{16k}\ ,$$

et ceci est strictement inférieur à 1 si et seulement si $k = 1$, 2 et 3, c'est à dire $\omega = (1 + i\sqrt{d})/2$ avec $d = 3$, 7 et 11. Et de fait, pour $k = 4$ par exemple, c'est à dire pour $d = 15$, il n'est pas difficile de voir que l'anneau A n'est pas Euclidien pour le stathme ϕ, car il n'est même pas principal. En effet, on a par exemple

$$15 = 3 \cdot 5 = -(2\omega - 1)^2\ ,$$

et on vérifie que les éléments 3, 5 et $2\omega - 1$ sont irréductibles, ne sont pas inversibles ni associés, ce qui est impossible dans un anneau principal.