Université de Bretagne Occidentale
UFR Sciences et Techniques
LICENCE DE MATHEMATIQUES

ARITHMETIQUE ET APPLICATIONS, COMBINATOIRE ET GRAPHES

Examen terminal, le 12 mai 2014, 14h00–17h00

CORRIGE et BAREME

Question de cours. Soit $x \in L$. Soit n la dimension de L comme K-espace vectoriel. Comme la famille $1; x; x^2; \ldots; x^n$ est de cardinal $n+1$, elle est liée. Il existe donc $a_0; \ldots; a_n \in K$ non tous nuls tels que $a_0 \cdot 1 + a_1 \cdot x + \cdots + a_n \cdot x^n = 0$. Il s'ensuit que x est algébrique sur K. **(2 pts)**

Exercice 1. a. On calcule

$$X(D(XF)) = X \cdot D(X \cdot \sum_{n=0}^{1} a_n X^n) =$$
$$X \cdot D(\sum_{n=0}^{1} a_n X^{n+1}) = X \cdot \sum_{n=0}^{1} (n+1) a_n X^n =$$
$$\sum_{n=0}^{1} (n+1) a_n X^{n+1} = \sum_{n=1}^{1} n a_{n-1} X^n. \quad \textbf{(1 pt)}$$

Comme cette série est égale à

$$F - 1 = (a_0 - 1) + \sum_{n=1}^{1} a_n X^n;$$

on obtient $a_0 - 1 = 0$ et $a_n = n a_{n-1}$ pour $n \geq 1$. Il s'ensuit que $a_n = n!$. **(0,5 pt)**

b. Non, la suite (a_n) n'est pas a support fini, i.e., l'ensemble des n tels que $a_n \neq 0$ est infini. **(0,5 pt)**

c. Non. Montrons par l'absurde que F n'est pas une fraction rationnelle. Supposons que $F = P/Q$ où $P; Q \in \mathbb{C}[X]$ avec $Q \neq 0$. On peut supposer que P et Q sont premiers entre eux. Ecrivons $P = b_d X^d + \cdots + b_0$ et $Q = c_e X^e + \cdots + c_0$. Comme $FQ = P$, on a $a_0 c_0 = b_0$. Comme $a_0 = 1$, on a même $c_0 = b_0$. Si $c_0 = 0$, on a $b_0 = 0$ et les polynômes P et Q seraient tous les deux divisibles par X, ce qui est contradictoire à l'hypothèse $\mathrm{pgcd}(P; Q) = 1$. Du coup, $c_0 \neq 0$. Comme $P/Q = (P/c_0)/(Q/c_0)$, on peut supposer $c_0 = 1$, quitte à remplacer P par P/c_0 et Q par Q/c_0.

Identifions maintenant les coe□cients devant X^n des deux membres de l'égalité $FQ = P$, pour $n \geq \max\{d+1; e\}$. Celui de P est zéro car $n > d$. Celui de FQ est égal à

$$a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_e a_{n-e}$$

car $n \geq e$. On obtient donc la relation de récurrence

$$a_n = -c_1 a_{n-1} - c_2 a_{n-2} - \cdots - c_e a_{n-e}$$

pour $n \geq \max\{d+1; e\}$. Or, $a_k = k!$ pour tout $k \in \mathbb{N}$ d'après le a. Soit $n \geq \max\{d+1; e\}$ tel que $n > |c_1| + |c_2| + \cdots + |c_e|$. On a alors

$$\begin{aligned} n! = |a_n| = |-c_1 a_{n-1} - c_2 a_{n-2} - \cdots - c_e a_{n-e}| \leq \\ |c_1| \cdot |a_{n-1}| + |c_2| \cdot |a_{n-2}| + \cdots + |c_e| \cdot |a_{n-e}| = \\ |c_1| \cdot (n-1)! + |c_2| \cdot (n-2)! + \cdots + |c_e| \cdot (n-e)! \leq \\ |c_1| \cdot (n-1)! + |c_2| \cdot (n-1)! + \cdots + |c_e| \cdot (n-1)! \leq \\ (|c_1| + |c_2| + \cdots + |c_e|) \cdot (n-1)! < n \cdot (n-1)! = n!. \end{aligned}$$

Contradiction. **(1,5 pt)**

d. Oui, comme $a_0 \neq 0$, la série formelle F est inversible dans $\mathbb{C}[[X]]$, d'après le cours. **(0,5 pt)**

Exercice 2. a. On a la décomposition suivante dans $\mathbb{C}[[X]]$:

$$F = (1 + X^2 + X^4 + X^6 + \cdots) \cdot (1 + X^3 + X^6 + X^9 + \cdots).$$

Le premier facteur est égal à $1/(1-X^2)$, et le dernier à $1/(1-X^3)$. On a donc

$$F = \frac{1}{(1-X^2)(1-X^3)}$$

dans $\mathbb{C}[[X]]$. **(1 pt)**

b. Le dénominateur de la fraction rationnelle ci-dessus se décompose de plusieurs façons utiles pour la suite :

$$\begin{aligned} (1-X^2)(1-X^3) = (1-X)(1+X)(1-X)(1-jX)(1-j^2X) = \\ (1-X)^2(1+X)(1-jX)(1-j^2X) = (1-X)^2(1+X)(1+X+X^2) = \\ (1-X)^2(1+2X+2X^2+X^3). \end{aligned}$$

sur $\mathbb{C}$. En substituant $Y = 1 - X$ on obtient le polynôme

$$Y^2(1 + 2(1-Y) + 2(1-Y)^2 + (1-Y)^3) = Y^2(6 - 9Y + 5Y^2 - Y^3).$$

Puis on fait la division suivant les puissances croissantes de Y du numérateur 1 par le polynôme $6 - 9Y + 5Y^2 - Y^3$ à l'ordre 2 :

$$1 = (\tfrac{1}{6} + \tfrac{1}{4}Y)(6 - 9Y + 5Y^2 - Y^3) + Y^2(\tfrac{17}{12} - \tfrac{13}{12}Y + \tfrac{1}{4}Y^2).$$

Du coup,

$$\begin{aligned} \frac{1}{(1-X^2)(1-X^3)} = \frac{(\frac{1}{6} + \frac{1}{4}Y)(6 - 9Y + 5Y^2 - Y^3) + Y^2(\frac{17}{12} - \frac{13}{12}Y + \frac{1}{4}Y^2)}{Y^2(6 - 9Y + 5Y^2 - Y^3)} = \\ \frac{\frac{1}{6} + \frac{1}{4}Y}{Y^2} + \frac{\frac{17}{12} - \frac{13}{12}Y + \frac{1}{4}Y^2}{6 - 9Y + 5Y^2 - Y^3} = \\ \frac{\frac{1}{6}}{(1-X)^2} + \frac{\frac{1}{4}}{1-X} + \frac{\frac{7}{12} + \frac{7}{12}X + \frac{1}{4}X^2}{1 + 2X + 2X^2 + X^3} = \\ \frac{\frac{1}{6}}{(1-X)^2} + \frac{\frac{1}{4}}{1-X} + \frac{\frac{7}{12} + \frac{7}{12}X + \frac{1}{4}X^2}{(1+X)(1-jX)(1-j^2X)} \end{aligned}$$

La décomposition en éléments simples du dernier terme est de la forme

$$\frac{\frac{7}{12}+\frac{7}{12}X+\frac{1}{4}X^2}{(1+X)(1-jX)(1-j^2X)}=\frac{a}{1+X}+\frac{b}{1-jX}+\frac{c}{1-j^2X}$$

avec $a;b;c\in\mathbb{C}$. En multipliant de deux côtés par $1+X$, en simplifiant ensuite, et en évaluant en -1, on obtient

$$a=\frac{\frac{7}{12}-\frac{7}{12}+\frac{1}{4}}{(1+j)(1+j^2)}=\frac{1}{4}:$$

De même, pour trouver b, on multiplie par $1-jX$, on simplifie ensuite et on évalue en j^2 pour obtenir

$$b=\frac{\frac{7}{12}+\frac{7}{12}j^2+\frac{1}{4}j^4}{(1+j^2)(1-j^4)}=\frac{\frac{7}{12}+\frac{7}{12}(-j-1)+\frac{1}{4}j}{(1-j-1)(1-j)}=$$
$$\frac{-\frac{1}{3}j}{-j(1-j)}=\frac{-\frac{1}{3}j}{j^2-j}=\frac{-\frac{1}{3}j}{-i\sqrt{3}}=\frac{1}{6}+\frac{1}{6\sqrt{3}}i:$$

Comme la fraction rationnelle est à coe□cients réels, on a obligatoirement

$$c=\overline{b}=\frac{1}{6}-\frac{1}{6\sqrt{3}}i:$$

Au final, la décomposition en éléments simples de F est

$$F=\frac{\frac{1}{6}}{(1-X)^2}+\frac{\frac{1}{4}}{1-X}+\frac{\frac{1}{4}}{1+X}+\frac{\frac{1}{6}+\frac{1}{6\sqrt{3}}i}{1-jX}+\frac{\frac{1}{6}-\frac{1}{6\sqrt{3}}i}{1-j^2X}:\quad\textbf{(2 pt)}$$

c. Comme

$$\frac{1}{1-X}=\sum_{n=0}^{+\infty}X^n;$$

on a

$$\frac{1}{(1-X)^2}=D\left(\frac{1}{1-X}\right)=\sum_{n=0}^{+\infty}(n+1)X^n$$
$$\frac{1}{1+X}=\frac{1}{1-(-X)}=\sum_{n=0}^{+\infty}(-1)^nX^n$$
$$\frac{1}{1-jX}=\sum_{n=0}^{+\infty}j^nX^n$$
$$\frac{1}{1-j^2X}=\sum_{n=0}^{+\infty}j^{2n}X^n:$$

Du coup,

$$F=\sum_{n=0}^{+\infty}\left(\frac{1}{6}(n+1)+\frac{1}{4}+\frac{1}{4}(-1)^n+(\frac{1}{6}+\frac{1}{6\sqrt{3}}i)j^n+(\frac{1}{6}-\frac{1}{6\sqrt{3}}i)j^{2n}\right)X^n;$$

et donc

$$a_n = \frac{1}{6}(n+1) + \frac{1}{4} + \frac{1}{4}(-1)^n + (\tfrac{1}{6} + \tfrac{1}{6\sqrt{3}}i)j^n + (\tfrac{1}{6} - \tfrac{1}{6\sqrt{3}}i)j^{2n} =$$

$$\begin{cases} \frac{1}{6}(n+6) & \text{si } n \equiv 0 \pmod 6 \\ \frac{1}{6}(n-1) & \text{si } n \equiv 1 \pmod 6 \\ \frac{1}{6}(n+4) & \text{si } n \equiv 2 \pmod 6 \\ \frac{1}{6}(n+3) & \text{si } n \equiv 3 \pmod 6 \\ \frac{1}{6}(n+2) & \text{si } n \equiv 4 \pmod 6 \\ \frac{1}{6}(n+1) & \text{si } n \equiv 5 \pmod 6 \end{cases}$$

On peut vérifier pour quelques valeurs de n : Pour $n = 0$, il n'y a que $(x;y) = (0;0)$ comme solution à $2x+3y = 0$, et effectivement, $\frac{1}{6}(0+6) = 1$. Pour $n = 1$, il n'y a pas de solution à l'équation $2x + 3y = 0$ dans $\mathbb{N}^2$, et effectivement, $\frac{1}{6}(1-1) = 0$. Pour $n = 2$, il n'y a que la solution $(x;y) = (1;0)$ à l'équation $2x + 3y = 2$, et effectivement $\frac{1}{6}(2+4) = 1$. Pour $n = 3$, il n'y a que $(x;y) = (0;1)$ comme solution, et effectivement $\frac{1}{6}(3+3) = 1$, Pour $n = 4$, il n'y a que $(x;y) = (2;0)$ comme solution, et effectivement $\frac{1}{6}(4+2) = 1$. Pour $n = 5$, il n'y a que $(x;y) = (1;1)$ comme solution, et effectivement $\frac{1}{6}(5+1) = 1$. Pour $n = 6$, il y a deux solutions : $(3;0)$ et $(0;2)$, et effectivement $\frac{1}{6}(6+6) = 2$. **(1 pt)**

Exercice 3. D'après le cours, on a la formule récurrente

$$\Phi_n = \frac{X^n - 1}{\prod_d \Phi_d};$$

où le produit est pris sur tous les diviseurs positifs d de n différents de n **(1 pt)**. On en déduit que

$$\Phi_1 = X - 1; \quad \Phi_3 = X^2 + X + 1; \quad \text{et} \quad \Phi_5 = X^4 + X^3 + X^2 + X + 1:$$

Du coup,

$$\Phi_{15} = \frac{X^{15} - 1}{(X-1)(X^2+X+1)(X^4+X^3+X^2+X+1)}:$$

On a

$$\frac{X^{15} - 1}{(X-1)} = X^{14} + X^{13} + \cdots + 1:$$

Comme

$$X^{14} + X^{13} + \cdots + 1 = (X^4 + X^3 + X^2 + X + 1)(X^{10} + X^5 + 1);$$

on a

$$\frac{X^{15} - 1}{(X-1)(X^4+X^3+X^2+X+1)} = X^{10} + X^5 + 1:$$

Pour calculer Φ_{15}, il suffit donc d'effectuer la division longue de $X^{10} + X^5 + 1$ par $X^2 + X + 1$ et on obtient :

$$\Phi_{15} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1: \quad \textbf{(1 pt)}$$

Exercice 4. a. Supposons que P est réductible. Dans ce cas P est divisible par un polynôme irréductible de degré ≤ 2. Or, les seuls polynômes irréductibles de degré ≤ 2 dans $\mathbb{F}_2[X]$ sont X, $X+1$ et X^2+X+1. Si P était divisible par X ou $X+1$, il aurait eu une racine dans $\mathbb{F}_2$ ce qui n'est pas le cas. Du coup, P est divisible par $Q = X^2+X+1$. Ecrivons $P = QR$, avec $R \in \mathbb{F}_2[X]$. Comme P n'a pas de racine dans $\mathbb{F}_2$, le polynôme R n'en a pas non plus. Comme $\deg(R) = 2$, le polynôme R est irréducible. Or, comme on vient de dire, le seul polynôme irréductible de degré 2 dans $\mathbb{F}_2[X]$ est Q. Du coup, $R = Q$ et

$$P = QR = Q^2 = (X^2+X+1)^2 = X^4+X^2+1.$$

Contradiction. **(1 pt)**

b. D'après la division euclidienne dans $\mathbb{F}_2[X]$, tout élément A de $\mathbb{F}_2[X]$ est congru modulo P à un polynôme R de $\mathbb{F}_2[X]$ de degré ≤ 3. De plus, le polynôme R est le seul ayant cette propriété. Il s'ensuit que tout élément de K s'ecrit de façon unique sous la forme $a_0 \cdot 1 + a_1 \cdot \ + a_2 \cdot \ ^2 + a_3 \cdot \ ^3$ avec $a_0, \ldots, a_3 \in \mathbb{F}_2$. Autrement dit, la famille $1, \ , \ ^2, \ ^3$ est une $\mathbb{F}_2$-base de K. **(1 pt)**

c. D'après le b, K contient $2^4 = 16$ éléments. Le groupe multiplicatif $K^\star$ en contient donc 15. **(0,5 pt)**

d. Comme $K^\star$ est de cardinal 15, l'élément de $K^\star$ est d'ordre 1, 3, 5 ou 15. D'après le b, $\neq 1$ et l'ordre de n'est pas égal à 1. D'après le b encore, $^3 \neq 1$ et l'ordre de est différent de 3. Calculons ^{5} en utilisant que $^4 = \ + 1$:

$$^5 = \ \cdot \ ^4 = \ (\ + 1) = \ ^2 + \ .$$

Cet élément de $K^\star$ est encore différent de 1 d'après le b. Il s'ensuit que l'ordre de est égal a 15 et est donc générateur de $K^\star$. **(1 pt)**

e. Comme on vient de voir $^4 = \ + 1$. On a donc

$$^8 = (\ ^4)^2 = (\ + 1)^2 = \ ^2 + 1 = B.$$

Bob avait donc choisi l'entier $b = 8$. Du coup, la clé secrète partagée est

$$s = A^b = (\ ^3 + \ + 1)^8$$

qu'on calcule par carrés successifs :

$$\begin{aligned}
(\ ^3 + \ + 1)^2 &= \ ^6 + \ ^2 + 1 = \ ^2(\ + 1) + \ ^2 + 1 = \ ^3 + 1 \\
(\ ^3 + 1)^2 &= \ ^6 + 1 = \ ^3 + \ ^2 + 1 \\
(\ ^3 + \ ^2 + 1)^2 &= \ ^6 + \ ^4 + 1 = \ ^3 + \ ^2 + \ .
\end{aligned}$$

La clé secrète partagée est donc $^3 + \ ^2 + \ $. **(1,5 pt)**

Exercice 5. Notons $V = \{0, \ldots, 6\}$ l'ensemble des sommets de G. Rappelons que l'algorithme de Dijkstra construit une suite strictement croissante de sous-ensembles $S_0, S_1, \ldots, S_6$ de V telle que $S_0 = \{0\}$ et $S_6 = V$. De plus, il construit une application «prédécesseur»

$$p \colon S_6 \setminus \{0\} \to S_6$$

qui a la propriété que pour tout sommet v de G le chemin le plus court de v à 0 est $v, p(v), p^2(v), \ldots, p^d(v)$, où d est le plus petit entier naturel tel que $p^d(v) = 0$.

L'algorithme construit en outre une fonction $\ell : V \to \mathbb{R}$ qui a la propriété que $\ell(v) = d(v;0)$ dans le graphe pondéré, i.e., $\ell(v)$ est la longueur du chemin le plus court de v à 0. Rappelons encore que l'algorithme de Dijkstra construit tous ces object par récurrence.

A l'initialisation, on pose $S_0 = \{0\}$ et $\ell(0) = 0$. Afin de construire S_1, et les applications $p : S_1 \setminus \{0\} \to S_1$ et $\ell : S_1 \to \mathbb{R}$, on cherche un sommet w voisin de 0 tel que $d(0;w)$ est minimal. Les voisins de 0 sont $1;5;6$ à distance pondérée $4;1;2$, respectivement. On voit que $w = 5$ est le voisin le plus proche de 0 et se trouve à une distance de 1. On pose $S_1 = \{0;5\}$, et on définit $p(5) = 0$ et $\ell(5) = 1$. Le chemin le plus court de 5 à 0 est donc le chemin $5;p(5) = 0$ qui est de longueur $\ell(5) = 1$. Le chemin le plus court de 0 à 5 est donc le chemin inverse $0;5$ qui est de la même longueur.

Puis, on cherche $v \in S_1$ et $w \in V \setminus S_1$ tels que v et w sont voisins et tels que $\ell(v) + d(v;w)$ est minimale. Pour ce faire, on dresse la liste de tous les pairs $(v;w)$ avec $v \in \{0;5\}$ et $w \notin \{0;5\}$ avec w voisin de v et on calcule $\ell(v) + d(v;w)$ pour chaque pair :

$(v;w)$	$\ell(v) + d(v;w)$
$(0;1)$	4
$(0;6)$	2
$(5;2)$	3
$(5;3)$	3
$(5;4)$	4

On constate que $\ell(v) + d(v;w)$ est minimale et vaut 2 pour $v = 0$ et $w = 6$. On pose donc $S_2 = S_1 \cup \{6\} = \{0;5;6\}$ et on définit $p(6) = 0$ et $\ell(6) = 2$. Le chemin le plus court de 6 à 0 est le chemin $6;p(6) = 0$ qui est de longueur $\ell(6) = 2$. Le chemin le plus court de 0 à 6 est donc le chemin inverse $0;6$ qui est de la même longueur.

Ensuite, on cherche $v \in S_2$ et $w \in V \setminus S_2$ tels que v et w sont voisins et tels que $\ell(v) + d(v;w)$ est minimale. Pour ce faire, on dresse la liste de tous les pairs $(v;w)$ avec $v \in \{0;5;6\}$ et $w \notin \{0;5;6\}$ avec w voisin de v et on calcule $\ell(v) + d(v;w)$ pour chaque pair :

$(v;w)$	$\ell(v) + d(v;w)$
$(0;1)$	4
$(5;2)$	3
$(5;3)$	3
$(5;4)$	4
$(6;1)$	3

On voit que $v = 6$ et $w = 1$ conviennent (entre autres). On pose $S_3 = S_2 \cup \{1\} = \{0;1;5;6\}$, et on définit $p(1) = 6$ et $\ell(1) = 3$. Le chemin le plus court de 1 à 0 est donc $1;p(1) = 6;p^2(1) = p(6) = 0$ qui est de longueur 3. Le chemin le plus court de 0 à 1 est donc le chemin inverse $0;6;1$ qui est de la même longueur.

La liste pour $S_3 = \{0;1;5;6\}$ est

$(v;w)$	$\ell(v)+d(v;w)$
$(1;2)$	8
$(1;3)$	5
$(1;4)$	4
$(5;2)$	3
$(5;3)$	3
$(5;4)$	4

On voit que $v=5$ et $w=2$ conviennent. On pose $S_4=S_3\cup\{2\}=\{0;1;2;5;6\}$ et on définit $p(2)=5$ et $\ell(2)=3$. Le chemin le plus court de 0 à 2 est donc $0;5;2$ qui est de longueur 3.

La liste pour $S_4=\{0;1;2;5;6\}$ est

$(v;w)$	$\ell(v)+d(v;w)$
$(1;3)$	5
$(1;4)$	4
$(2;4)$	8
$(5;3)$	3
$(5;4)$	4

On voit que $v=5$ et $w=3$. On pose $S_5=S_4\cup\{3\}=\{0;1;2;3;5;6\}$ et on définit $p(3)=5$ et $\ell(3)=3$. Le chemin le plus court de 0 à 3 est donc $0;5;3$ qui est de longueur 3.

On a forcément $w=4$ et $S_6=V=S_5\cup\{4\}=\{0;1;2;3;4;5;6\}$. Cherchons $v\in S_5$ avec $\ell(v)+d(v;4)$ minimale :

$(v;w)$	$\ell(v)+d(v;w)$
$(1;4)$	4
$(2;4)$	8
$(3;4)$	6
$(5;4)$	4

On voit que $v=5$ convient. Le chemin le plus court de 0 à 4 est donc $0;5;4$ qui est de longueur 4. **(3 pts)**