Université de Bretagne Occidentale
UFR Sciences et Techniques
LICENCE DE MATHEMATIQUES

ARITHMETIQUE ET APPLICATIONS, COMBINATOIRE ET GRAPHES

Examen terminal, le 7 mai 2015, 14h00–17h00

CORRIGE et BAREME

Question de cours. (2 pts) Soit G un groupe fini. Si $x \in G$, le sous-groupe $\langle x \rangle$ engendré par x est un sous-groupe cyclique de G. Le nombre de générateurs d'un groupe cyclique de cardinal m est $\varphi(m)$. En comptant les éléments de G en fonction des sous-groupes qu'ils engendrent, on obtient

$$|G| = \sum_{C \subseteq G} \varphi(|C|)$$

où C parcourt tous les sous-groupes cycliques de G.

Les sous-groupes cycliques de $\mathbb{Z}/n\mathbb{Z}$ sont les sous-groupes $\frac{n}{d}\mathbb{Z}/n\mathbb{Z}$, où d parcourt l'ensemble des diviseurs positifs de n. De plus, le sous-groupe $\frac{n}{d}\mathbb{Z}/n\mathbb{Z}$ est de cardinal d. En appliquant la formule ci-dessus à $G = \mathbb{Z}/n\mathbb{Z}$ on obtient donc

$$n = |\mathbb{Z}/n\mathbb{Z}| = \sum_{d|n} \varphi(|\tfrac{n}{d}\mathbb{Z}/n\mathbb{Z}|) = \sum_{d|n} \varphi(d).$$

Exercice 1. a. **(2 pts)** On a

$$DF = D\left(1 + X + \sum_{n=0}^{\infty} a_{n+2}X^{n+2}\right) = 1 + \sum_{n=0}^{\infty}(n+2)a_{n+2}X^{n+1} =$$
$$1 + \sum_{n=0}^{\infty}((n+1)a_{n+1} + na_n)X^{n+1} = 1 + \sum_{n=0}^{\infty}(n+1)a_{n+1}X^{n+1} + \sum_{n=1}^{\infty} na_nX^{n+1} =$$
$$1 + X\sum_{n=0}^{\infty}(n+1)a_{n+1}X^n + X^2\sum_{n=1}^{\infty} na_nX^{n-1} = 1 + XDF + X^2DF = 1 + (X + X^2)DF.$$

Du coup, $(1 - X - X^2)DF = 1$ et

$$DF = \frac{1}{1 - X - X^2}.$$

b. **(2 pts)** On décompose la fraction rationnelle $1/(1 - X - X^2)$ en éléments simples dans le corps des fractions rationnelles $\mathbb{C}(X)$. La décomposition en irréductibles de $1 - X - X^2$ dans $\mathbb{C}[X]$ est

$$1 - X - X^2 = (1 - aX)(1 - bX),$$

où $a, b = \frac{1}{2} \pm \frac{1}{2}\sqrt{5}$. En effet, pour ces valeurs de a et b on a $a + b = 1$ et $ab = -1$. Remarquons que $a - b = \sqrt{5}$. On a alors

$$DF = \frac{1}{1 - X - X^2} = \frac{1}{a-b}\left(\frac{a}{1-aX} - \frac{b}{1-bX}\right) = \frac{1}{\sqrt{5}}\left(a\sum_{n=0}^{\infty} a^n X^n - b\sum_{n=0}^{\infty} b^n X^n\right) = \sum_{n=0}^{\infty} \frac{1}{\sqrt{5}}(a^{n+1} - b^{n+1})X^n.$$

Du coup,

$$F = 1 + \sum_{n=1}^{\infty} \frac{1}{n\sqrt{5}}(a^n - b^n)X^n.$$

On en déduit que

$$a_n = \frac{1}{n\sqrt{5}}\left((\tfrac{1}{2} + \tfrac{1}{2}\sqrt{5})^n - (\tfrac{1}{2} - \tfrac{1}{2}\sqrt{5})^n\right)$$

pour tout $n \in \mathbb{N}^\star$.

Exercice 2. (4 pts) Notons $V = \{0, \ldots, 7\}$ l'ensemble des sommets de G. Rappelons que l'algorithme de Dijkstra construit une suite strictement croissante de sous-ensembles $S_0, S_1, \ldots, S_7$ de V telle que $S_0 = \{0\}$ et $S_7 = V$. De plus, il construit une application «prédécesseur»

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

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 $\ell\colon V \to \mathbb{R}$ 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 objects par récurrence.

A l'initialisation, on pose $S_0 = \{0\}$ et $\ell(0) = 0$. Afin de construire S_1, et les applications $p\colon S_1 \setminus \{0\} \to S_1$ et $\ell\colon S_1 \to \mathbb{R}$, on cherche un sommet v voisin de 0 tel que $d(0, v)$ est minimal. Les voisins de 0 sont $2, 3, 5, 6$ à distance pondérée $3, 2, 1, 4$, respectivement. On voit que $v = 5$ est le voisin le plus proche de 0 et se trouve à une distance 1 de 0. 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 $u \in S_1$ et $v \in V \setminus S_1$ tels que u et v sont voisins et tels que $\ell(u) + d(u, v)$ est minimale. Pour ce faire, on dresse la liste de tous les pairs (u, v) avec $u \in \{0, 5\}$ et $v \notin \{0, 5\}$ avec u voisin de v et on calcule $\ell(u) + d(u, v)$ pour chaque pair :

(u, v)	$\ell(u) + d(u, v)$
$(0, 2)$	0+3=3
$(0, 3)$	0+2=2
$(0, 6)$	0+4=4
$(5, 1)$	1+1=2
$(5, 6)$	1+2=3
$(5, 7)$	1+2=3

On constate que $\ell(u) + d(u, v)$ est minimale et vaut 2 pour $u = 0$ et $v = 3$, par exemple. On pose donc $S_2 = S_1 \cup \{3\} = \{0, 3, 5\}$ et on définit $p(3) = 0$ et $\ell(3) = 2$. Le chemin le plus court de 3 à 0 est le chemin $3, p(3) = 0$ qui est de longueur $\ell(3) = 2$. Le chemin le plus court de 0 à 3 est donc le chemin inverse $0, 3$ qui est de la même longueur.

Ensuite, on cherche $u \in S_2$ et $v \in V \setminus S_2$ tels que u et v sont voisins et tels que $\ell(u) + d(u, v)$ est minimale. Pour ce faire, on dresse la liste de tous les pairs (u, v) avec $u \in \{0, 5, 3\}$ et $v \notin \{0, 5, 6\}$ avec u voisin de v et on calcule $\ell(u) + d(u, v)$ pour chaque pair :

(u, v)	$\ell(u) + d(u, v)$
$(0, 2)$	0+3=3
$(0, 6)$	0+4=4
$(3, 2)$	2+1=3
$(3, 4)$	2+1=3
$(3, 6)$	2+1=3
$(3, 7)$	2+1=3
$(5, 1)$	1+1=2
$(5, 6)$	1+2=3
$(5, 7)$	1+2=3

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

Le tableau pour $S_3 = \{0, 1, 3, 5\}$ est

(u, v)	$\ell(u) + d(u, v)$
$(0, 2)$	0+3=3
$(0, 6)$	0+4=4
$(1, 6)$	2+1=3
$(1, 7)$	2+3=5
$(3, 2)$	2+1=3
$(3, 4)$	2+1=3
$(3, 6)$	2+1=3
$(3, 7)$	2+1=3
$(5, 6)$	1+2=3
$(5, 7)$	1+2=3

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

La tableau pour $S_4 = \{0, 1, 2, 3, 5\}$ est

(u,v)	$\ell(u)+d(u,v)$
$(0,6)$	0+4=4
$(1,6)$	2+1=3
$(1,7)$	2+3=5
$(2,6)$	3+2=5
$(2,7)$	3+1=4
$(3,4)$	2+1=3
$(3,6)$	2+1=3
$(3,7)$	2+1=3
$(5,6)$	1+2=3
$(5,7)$	1+2=3

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

Le tableau suivant est

(u,v)	$\ell(u)+d(u,v)$
$(1,7)$	2+3=5
$(2,7)$	3+1=4
$(3,4)$	2+1=3
$(3,7)$	2+1=3
$(5,7)$	1+2=3
$(6,4)$	3+3=6
$(6,7)$	3+2=5

On voit que $u=3$ et $v=4$ conviennent. On pose $S_6=S_5\cup\{4\}=\{0,1,2,3,4,5,6\}$ et on définit $p(4)=3$ et $\ell(4)=3$. Le chemin le plus court de 0 à 4 est donc $0,3,4$ qui est de longueur 3.

Le dernier tableau est

(u,v)	$\ell(u)+d(u,v)$
$(1,7)$	2+3=5
$(2,7)$	3+1=4
$(3,7)$	2+1=3
$(4,7)$	3+1=4
$(5,7)$	1+2=3
$(6,7)$	3+2=5

On voit que $u=3$ et $v=7$ conviennent. On a $S_7=S_6\cup\{7\}=\{0,1,2,3,4,5,6,7\}=V$ et on définit $p(7)=3$ et $\ell(7)=3$. Le chemin le plus court de 0 à 7 est donc $0,3,7$ qui est de longueur 3.

Exercice 3. a. **(0,5 pt)** Le petit Théorème de Fermat dit que le polynôme X^3-X s'annule sur tous les éléments de $\mathbb{F}_3$. On a donc $P_2(0)=P_2(1)=P_2(-1)=-1\neq 0$. Le polynôme P_2 n'a donc pas de racine dans $\mathbb{F}_3$. Comme il est de degré ≤ 3, cela suffit pour conclure qu'il est irréductible dans $\mathbb{F}_3[X]$.

b. **(0,5 pt)** Soit donc $Q=P_2$. Comme Q est irréductible, $\mathbb{F}_3[X]/(Q)$ est un corps.

c. **(0,5 pt)** D'après le Théorème de la division euclidienne dans $\mathbb{F}_3[X]$, toute classe dans $\mathbb{F}_3[X]/(Q)$ possède un représentant unique de degré ≤ 2. Du coup, $\overline{1},\overline{X},\overline{X}^2$ est une $\mathbb{F}_3$-base de K.

d. **(0,5 pt)** Comme K est de dimension 3 sur $\mathbb{F}_3$, il est isomorphe à $\mathbb{F}_3^3$ comme $\mathbb{F}_3$-espace vectoriel. En particulier, il y a une bijection entre K et $\mathbb{F}_3^3$. Comme ce dernier a $3^3 = 27$ éléments, il en est de même pour le premier.

e. **(0,5 pt)** Comme $\alpha^3 = \alpha + 1$, et donc aussi $\alpha^4 = \alpha^2 + \alpha$, et $2 = -1$ dans K, on a

$$\left(\overline{aX^2 + bX + c}\right)^2 = \left(a\overline{X}^2 + b\overline{X} + c\right)^2 = \left(a\alpha^2 + b\alpha + c\right)^2 =$$
$$a^2\alpha^4 - ab\alpha^3 - ac\alpha^2 + b^2\alpha^2 - bc\alpha + c^2 = a^2(\alpha^2 + \alpha) - ab(\alpha + 1) + (-ac + b^2)\alpha^2 - bc\alpha + c^2 =$$
$$(a^2 - ac + b^2)\alpha^2 + (a^2 - ab - bc)\alpha + (-ab + c^2).$$

f. **(0,5 pt)** D'après le d, le groupe $K^\star$ est de cardinal $27 - 1 = 26 = 2 \times 13$. D'après le Théorème de Cauchy, les éléments de $K^\star$ sont d'ordre $1, 2, 13, 26$. D'après le c, $\alpha \in K^\star$, $\alpha \neq 1$ et $\alpha^2 \neq 1$. L'élément α appartient donc à $K^\star$ et son ordre n'est pas égal à 1 ou 2. Calculons α^{13} en utilisant que $(x + y)^3 = x^3 + y^3$ dans un corps de caractéristique 3 :

$$\alpha^{13} = \alpha^{3^2+3+1} = (\alpha^3)^3\alpha^3\alpha = (\alpha + 1)^3(\alpha + 1)\alpha =$$
$$(\alpha^3 + 1)(\alpha + 1)\alpha = (\alpha + 1 + 1)(\alpha + 1)\alpha = (\alpha - 1)(\alpha + 1)\alpha =$$
$$(\alpha^2 - 1)\alpha = \alpha^3 - \alpha = \alpha + 1 - \alpha = 1.$$

Par conséquent, α est d'ordre 13 dans $K^\star$.

g. **(0,5 pt)** D'après le e, il faut résoudre dans $\mathbb{F}_3$ les équations

$$(-1)^2 - (-1)1 + b^2 = 0,\ (-1)^2 - (-1)b - b1 = 1,\ -(-1)b + 1^2 = 0,$$

i.e.,

$$1 + 1 + b^2 = 0,\ 1 + b - b = 1,\ b + 1 = 0.$$

On voit que $b = -1$ est la seule solution.

h[1]. **(0,5 pt)** Soit $\gamma = -\alpha^2 - \alpha + 1$. D'après le g, $\gamma^2 = \alpha$. Comme α est d'ordre 13, on a bien-sûr également $(\alpha^7)^2 = \alpha$. Or,

$$\alpha^7 = (\alpha^3)^2\alpha = (\alpha + 1)^2\alpha = (\alpha^2 - \alpha + 1)\alpha = \alpha^3 - \alpha^2 + \alpha = \alpha + 1 - \alpha^2 + \alpha = -\alpha^2 - \alpha + 1 = \gamma.$$

Comme 7 est premier avec 13, $\gamma = \alpha^7$ est d'ordre 13. Du coup, $-\gamma$ est d'ordre 26, i.e., $\beta = -\gamma$ est un générateur de $K^\star$.

i. **(1 pt)** Si L est un sous-corps de K, alors L est un sous-$\mathbb{F}_3$-espace vectoriel de K contenant le corps premier $\mathbb{F}_3$ de K. Il est donc de dimension $1, 2, 3$. Si $\dim(L) = 1$, L est égal à $\mathbb{F}_3$. Si $\dim(L) = 3$, L est égal à K. Supposons que $\dim(L) = 2$. Dans ce cas, le cardinal de L est de $3^2 = 9$. Le groupe $L^\star$ est donc un sous-groupe de cardinal 8 de $K^\star$ qui est de cardinal 26. Comme 8 ne divise pas 26, on a une contradiction avec le Théorème de Lagrange.

Un autre argument qui montre que K ne possède pas de sous-corps non trivial c'est le suivant. Supposons que L est un sous-corps de K avec $\mathbb{F}_3 \subsetneq L \subsetneq K$. Comme on a vu ci-dessus, $|L| = 9$. Comme K est une extension de L, on peut considérer K comme un L-espace vectoriel, forcément de dimension fini, disons n. Du coup, le cardinal de K est $|L|^n = 9^n = 3^{2n}$. Or, $|K| = 3^3$ et n est donc égal à $\frac{3}{2}$ ce qui est absurde.

Les seuls sous-corps de K sont donc les sous-corps triviaux $\mathbb{F}_3$ et K lui-même.

1. Si le but de l'exercice était de trouver un générateur de $K^\star$, on aurait pu argumenter aussi bien que $-\alpha$ est générateur de $K^\star$.

Exercice 4. a. **(3 pts)** Bob utilise le mot reçu r comme coefficients d'un polynôme et définit

$$R = X^{14} + X^5 + X^4 + X^3 + X^2 + 1 \in \mathbb{F}_2[X].$$

Rappelons que le BCH$[15, 7]$ est basé sur des calculs dans le corps $\mathbb{F}_{16}$ qu'on représente comme $\mathbb{F}_2[X]/(X^4 + X + 1)$. On note $\alpha = \overline{X}$ dans $\mathbb{F}_{16}$. On sait que α est un générateur de $\mathbb{F}_{16}^\star$. De plus, par construction, $1, \alpha, \alpha^2, \alpha^3$ est une $\mathbb{F}_2$-base de $\mathbb{F}_{16}$, et on a $\alpha^4 = \alpha + 1$.

Bob calcule $R(\alpha)$, $R(\alpha^2)$ et $R(\alpha^3)$. Notons que $\alpha^{14} = \alpha^{-1}$ car $\alpha^{15} = 1$. En multipliant $\alpha^4 + \alpha + 1 = 0$ par $\alpha^{-1} = \alpha^{14}$, on obtient $\alpha^3 + 1 + \alpha^{14} = 0$. Du coup,

$$R(\alpha) = \alpha^{14} + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1 = \alpha^5 + \alpha^4 + \alpha^2 = (\alpha + 1)\alpha + (\alpha + 1) + \alpha^2 = 1.$$

Il s'ensuit que $R(\alpha^2) = R(\alpha)^2 = 1$ car $R \in \mathbb{F}_2[X]$. Quant à $R(\alpha^3)$, on a

$$R(\alpha^3) = \alpha^{42}+\alpha^{15}+\alpha^{12}+\alpha^9+\alpha^6+1 = \alpha^{12}+1+\alpha^{12}+(\alpha^4)^2\alpha+\alpha^4\alpha^2+1 = (\alpha^2+1)\alpha+(\alpha+1)\alpha^2 = \alpha^2 + \alpha.$$

Puis, Bob définit $P \in \mathbb{F}_2[X]$ par

$$P = R(\alpha)X^2 + R(\alpha^2)X + (R(\alpha^3) + R(\alpha)R(\alpha^2)) = X^2 + X + \alpha^2 + \alpha + 1.$$

Comme ce polynôme n'est pas nul et ne possède pas 0 comme racine, il y a exactement deux erreurs de transmission.

b. **(2 pts)** On cherche les deux indices i pour lesquels $P(\alpha^i) = 0$. On calcule

$$\begin{aligned}
P(\alpha^0) &= 1 + 1 + \alpha^2 + \alpha = \alpha^2 + \alpha + 1 \neq 0,\\
P(\alpha^1) &= \alpha^2 + \alpha + \alpha^2 + \alpha + 1 = 1 \neq 0,\\
P(\alpha^2) &= \alpha^4 + \alpha^2 + \alpha^2 + \alpha + 1 = 0,\\
P(\alpha^3) &= \alpha^6 + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^2(\alpha^4 + \alpha + 1) + \alpha + 1 = \alpha + 1 \neq 0,\\
P(\alpha^4) &= \alpha^8 + \alpha^4 + \alpha^2 + \alpha + 1 = (\alpha + 1)^2 + \alpha^2 = 1 \neq 0,\\
P(\alpha^5) &= \alpha^{10} + \alpha^5 + \alpha^2 + \alpha + 1 = (\alpha + 1)^2\alpha^2 + (\alpha + 1)\alpha + \alpha^2 + \alpha + 1 = \alpha^2 + \alpha \neq 0,\\
P(\alpha^6) &= \alpha^{12} + \alpha^6 + \alpha^2 + \alpha + 1 = (\alpha + 1)^3 + (\alpha + 1)\alpha^2 + \alpha^2 + \alpha + 1 = \alpha^2 \neq 0,\\
P(\alpha^7) &= \alpha^{14} + \alpha^7 + \alpha^2 + \alpha + 1 = (\alpha^3 + 1) + (\alpha + 1)\alpha^3 + \alpha^2 + \alpha + 1 = \alpha^2 + 1 \neq 0,\\
P(\alpha^8) &= \alpha^{16} + \alpha^8 + \alpha^2 + \alpha + 1 = \alpha + (\alpha + 1)^2 + \alpha^2 + \alpha + 1 = 0.
\end{aligned}$$

Les erreurs se trouvent donc dans les coefficients devant X^2 et X^8 dans le polynôme R, i.e, le polynôme de code dont disposait Alice était

$$C = X^{14} + X^8 + X^5 + X^4 + X^3 + 1 \in \mathbb{F}_2[X].$$

Autrement dit, le mot de code envoyé par Alice était

$$c = (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1).$$