UJF - M1 Maths 2014-2015
M4211: Algèbre 2

Travaux dirigés 3

Dans ce qui suit on désigne par G un groupe fini, non réduit au neutre ; G est de plus supposé **abélien**, à l'exception des exercices 3, et 5.

Exercice 1. Expliciter le groupe dual $\widehat{G}$ des groupes suivants : $\mathbb{Z}/5\mathbb{Z}$, $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/8\mathbb{Z})^\times$.

Exercice 2. On note p un nombre premier ≥ 3 et $\mathbb{F}_p$ le corps à p éléments.

1) Quels sont les éléments d'ordre 2 de $\widehat{\mathbb{F}_p^\times}$? Quel en est le noyau ? Montrer (deux manières) que le *symbole de Legendre* défini sur $\mathbb{F}_p^\times$ par $x \mapsto 1$ si x est un carré dans $\mathbb{F}_p^\times$ et $x \mapsto -1$ sinon, est multiplicatif.

2) Si $x, y \in \mathbb{F}_p^\times$ ne sont pas des carrés dans $\mathbb{F}_p$, qu'en est-il de leur produit xy ?

Exercice 3. Soient $n \geq 1$ le cardinal du groupe G (pas forcément abélien), et $\widehat{G}$ le groupe dual, formé des caractères multiplicatifs de G. Soit $\mathbb{U}_n$ le groupe des racines complexes $n^{\text{ièmes}}$ de l'unité : $\mathbb{U}_n = \{e^{2\pi i\ell/n}\,;\ \ell \in \{0, \ldots, n-1\}\}$.

1) Rappeler pourquoi $\widehat{G}$ est l'ensemble des morphismes de G dans $\mathbb{U}_n$. On a ainsi, pour tous $g \in G$ et $\chi \in \widehat{G}$, on a $|\chi(g)| = 1$ et $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)} = \chi^{-1}(g)$.
On rappelle que $\mathbb{C}[G]$ est muni du produit hermitien : $\langle f_1, f_2\rangle = \frac{1}{n}\sum_{g\in G} \overline{f_1(g)} f_2(g)$.

2) Pour $g \in G$, soit $\delta_g \in \mathbb{C}[G]$ défini par $\delta_g(g) = 1$ et $\delta_g(h) = 0$ si $h \neq g$. Montrer que la famille $\{\delta_g\,;\ g \in G\}$ est une base orthogonale de $\mathbb{C}[G]$.

3) Montrer que pour $\chi \in \widehat{G}$ on a $\displaystyle\sum_{g\in G} \chi(g) = \begin{cases} 0 & \text{si } \chi \neq 1 \\ n & \text{si } \chi = 1 \end{cases}$. En déduire que les éléments de $\widehat{G}$ forment une famille orthonormée de $\mathbb{C}[G]$; en appliquant la théorie générale des représentations, on obtient que cette famille est une base si G est abélien.

Dans la suite on suppose G abélien.

4) Soient $g, h \in G$ tels que $\chi(g) = \chi(h)$ pour tout $\chi \in \widehat{G}$. Montrer que $g = h$.

5) Montrer que pour tous $g, h \in G$ on a $\displaystyle\sum_{\chi\in\widehat{G}} \overline{\chi(g)}\chi(h) = \begin{cases} 0 & \text{si } g \neq h \\ n & \text{si } g = h\,. \end{cases}$

Exercice 4. Soit H un sous–groupe de G.

1) Montrer que tout caractère multiplicatif de H se prolonge en un caractère multiplicatif de G, de $[G : H]$ façons. (`Indication:` commencer par construire les prolongements dans le cas où G/H est cyclique.)

2) En déduire une preuve (sans théorie des représentations) de ce que $|\widehat{G}| = |G|$.

3) Réciproquement, montrer comment déduire le résultat de prolongement ci-dessus du fait que tout groupe abélien fini a même ordre que son groupe dual. (`Indication:` identifier le noyau du morphisme de restriction ρ: $\widehat{G} \to \widehat{H}$ à un groupe dual.)

4) Trouver tous les caractères multiplicatifs de $(\mathbb{Z}/4\mathbb{Z})^2$ qui prolongent $\chi \in \widehat{H}$, où H est le sous–groupe cyclique engendré par $(\overline{2},\overline{2})$ et $\chi(\overline{2},\overline{2}) = -1$.

5) Ce résultat de prolongement reste–t–il vrai si G n'est pas abélien ? (considérer le cas $G = \mathfrak{S}_3$, $H = \mathfrak{A}_3$.)

6) Soit x dans G d'ordre N maximal, et soit $\chi : \langle x\rangle \to \mathbb{C}^*$ un caractère injectif de $\langle x\rangle$. Montrer que χ se prolonge en $\widetilde{\chi} : G \to \mathbb{U}_N$, et qu'on a un morphisme de groupe $G \simeq \langle x\rangle \times \operatorname{Ker}\widetilde{\chi}$.

7) Trouver un x dans $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, tel que G n'est pas isomorphe à $\langle x\rangle \times K$.

Exercice 5. Soit H un sous–groupe distingué de G (G pas forcément abélien). On note $H^\perp = \{\chi \in \widehat{G}\,;\ \chi_{|H} = 1\}$.

1) Montrer que $H^\perp$ est un sous–groupe de $\widehat{G}$, isomorphe à $\widehat{(G/H)}$. Qu'obtient-on pour $H = D(G)$?

Dans la suite on suppose que G est abélien.
2) Calculer $\operatorname{card} H^\perp$.

3) À quels groupes s'identifient canoniquement $\widehat{G}/H^\perp$ et $(H^\perp)^\perp$?

4) Montrer que l'application $H \mapsto H^\perp$ est une bijection de l'ensemble des sous–groupes de G dans l'ensemble des sous–groupes de $\widehat{G}$.

5) En déduire qu'étant donné un sous–groupe H de G, le nombre de sous–groupes de G isomorphes à H est égal au nombre de sous–groupes H' de G tels que $G/H' \simeq H$. Donner un contre-exemple si G n'est pas abélien.

Exercice 6. Démontrer l'unicité des facteurs invariants de G, *i.e.* des entiers $s \in \mathbb{N}^*$ et $q_1, \ldots, q_s$ tels que $G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_s\mathbb{Z}$, $2 \leq q_1$ et $q_i \mid q_{i+1}$ pour tout i entre 1 et $s-1$: si $(q'_i), 1 \leq i \leq s'$ est une autre telle suite, justifier d'abord que $q_s = q'_{s'}$, puis montrer par récurrence descendante que $q_{s-j} = q'_{s'-j}$ pour tout $j \leq i$, $0 \leq i \leq s-1$. (`Indication:` considérer dans les deux groupes produits le noyau de $x \mapsto q_{s-i}x$ puis raisonner par symétrie).

Exercice 7. Énumérer tous les groupes abéliens d'ordre 8, resp. 100, à isomorphisme près (donner leurs facteurs invariants).

Exercice 8. Donner les facteurs invariants du groupe $(\mathbb{Z}/55\mathbb{Z})^\times$. Ce groupe est–il isomorphe à $(\mathbb{Z}/75\mathbb{Z})^\times$?

Exercice 9. Soit n l'ordre de G. Montrer que pour tout diviseur d de n, G admet au moins un sous–groupe d'ordre d. (Est–ce vrai pour les groupes non abéliens ?)

Exercice 10. On reprend les notations de l'exercice 4. G désigne un groupe abélien d'ordre n. Pour $f \in \mathbb{C}[G]$, la transformée de Fourier $\widehat{f} = \mathcal{F}(f)$ est l'élément de $\mathbb{C}[\widehat{G}]$ défini par $\widehat{f}(\chi) = \sum_{g\in G} f(g)\chi(g)$.

1) Soient $\chi, \chi' \in \widehat{G}$. Calculer $\chi * \chi'$. Puis calculer $\widehat{\chi}$, et retrouver ainsi $\chi * \chi'$.

2) Déduire de 1) que les χ/n ($\chi \in \widehat{G}$) sont des idempotents deux à deux orthogonaux de l'algèbre $\mathbb{C}[G]$, dont la somme est 1. Qu'obtient–on par l'isomorphisme d'algèbres $\mathcal{F}$?

Donner tous les idempotents de $\mathbb{C}[G]$.

Exercice 11. *Sommes de Gauss.* Soit p un nombre premier. On note $\zeta = e^{2\pi i/p}$. Partant du corps $\mathbb{F}_p$ on considérera son groupe additif encore noté $\mathbb{F}_p$, et son groupe multiplicatif $\mathbb{F}_p^\times$ (cyclique). On étend tout élément χ de $\widehat{\mathbb{F}_p^\times}$ en un élément $\tilde{\chi}$ de $\mathbb{C}[\mathbb{F}_p]$, en posant $\tilde{\chi}(0) = 0$. Si de plus on a $\varphi \in \widehat{\mathbb{F}_p}$, on définit la *somme de Gauss* $G(\chi, \varphi)$ comme la valeur $\mathcal{F}_{add}(\tilde{\chi})(\varphi)$.

1) Donner l'expression de $G(\chi, \varphi)$. Exprimer $\tilde{\chi}$ dans la base $\widehat{\mathbb{F}_p}$.

On rappelle que les éléments de $\widehat{\mathbb{F}_p}$ sont exactement les $\varphi_k := \varphi_1^k$, où $0 \leq k \leq p-1$ et φ_1 est le morphisme $\bar{l} \mapsto e^{2\pi i l/p} = \zeta^l$. On note encore $\varphi_{\bar{k}} = \varphi_k$ ($\bar{k} \in \mathbb{F}_p$).

2) Pour x, y dans $\mathbb{F}_p$, $x \neq 0$, montrer que $G(\chi, \varphi_{xy}) = \overline{\chi(x)} G(\chi, \varphi_y)$.

3) Montrer que $G(\chi, \overline{\varphi}) = \chi(-1) G(\chi, \varphi)$ et que $G(\overline{\chi}, \varphi) = \chi(-1)\overline{G(\chi, \varphi)}$.

4) Évaluer $G(\chi, \varphi)$ si χ ou φ est le caractère trivial.

5) On suppose χ et φ non triviaux. En utilisant la formule de Plancherel, montrer que $|G(\chi, \varphi)| = \sqrt{p}$, puis que $G(\chi, \varphi) G(\overline{\chi}, \varphi) = p\chi(-1)$.

6) On prend $p \geq 3$ et $\chi = \eta$ le symbole de Legendre (cf. exo 2.). Déduire de la 2^e formule de 5) que $G(\eta, \varphi_1)^2 = (\sum_{x \in \mathbb{F}_p^\times} \eta(x)\zeta^x)^2 = (-1)^{\frac{p-1}{2}} p$. Interpréter en terme d'extensions du corps $\mathbb{Q}$.

Exercice 12. Soit H un sous–groupe de G. On note $H^\perp = \{\chi \in \widehat{G};\ \chi_{|H} = 1\}$. Le *support* $\mathrm{supp}(f)$ d'une fonction f est l'ensemble $f^{-1}(\mathbb{C}^\times)$.

1) Donner la transformée de Fourier de la fonction indicatrice $\mathbf{1}_H$. Que vaut $|\mathrm{supp}(\mathbf{1}_H)| \cdot |\mathrm{supp}(\widehat{\mathbf{1}_H})|$? (On pourra utiliser 5.1).)

2) Montrer la *formule sommatoire de Poisson* : si $g \in G$ et $f \in \mathbb{C}[G]$, on a

$$\sum_{h \in H} f(gh) = \frac{|H|}{|G|} \sum_{\chi \in H^\perp} \hat{f}(\bar{\chi}) \chi(g)\,.$$

(`Indication` : on pourra introduire la formule d'inversion dans le terme de gauche.)

Exercice 13. *L'endomorphisme* transformée de Fourier. On suit les notations du cours : Ω désigne la matrice de la TF $\mathcal{F}$ dans les bases naturelles, ET on note encore $\mathcal{F}$ l'endomorphisme de $\mathbb{C}^n$ associé. Que dire de la matrice $\frac{1}{\sqrt{n}}\Omega$? Montrer que l'endomorphisme $\mathcal{F}$ est diagonalisable en base orthonormée. En supposant de plus que Ω est symétrique, que dire des valeurs propres de $\mathcal{F}$? Examiner le cas de la TW et la TFD.

Exercice 14. *TF discrète.* Soit $n \geq 2$. On note $\zeta = e^{2\pi i/n}$. On considère $\mathcal{F}$ l'endomorphisme *transformée de Fourier discrète* de $\mathbb{C}^n$: si $a = (a_l)_{0 \leq l \leq n-1}$, $\mathcal{F}(a) = \big(\sum_{0 \leq k \leq n-1} a_k \zeta^{-lk}\big)_{0 \leq l \leq n-1}$. On note Ω sa matrice et $\mathcal{F}^-$ l'endomorphisme de $\mathbb{C}^n$ défini comme $\mathcal{F}$ mais en remplaçant ζ par son inverse ($\mathcal{F}^- = \mathcal{F} \circ \mathcal{I}$, où on rappelle que $\mathcal{I}$ désigne ici l'endomorphisme $a \mapsto (a_{[n-l]})_l$ de $\mathbb{C}^n$). On note $\tilde{a}$ la fonction $\mathbb{Z} \to \mathbb{C}$ définie par $\tilde{a}(m) = a_{[m]}$, où $[m]$ est le reste de la division euclidienne de m par n.

1) Traduire les conditions suivantes sur $a \in \mathbb{C}^n$ en terme de son image $\mathcal{F}(a)$:
i) On a $\mathcal{I}(a) = a$, (*i.e.* la fonction $\tilde{a}$ est paire)
ii) On a $\mathcal{I}(a) = -a$, (*i.e.* la fonction $\tilde{a}$ est impaire)
iii) $a \in \mathbb{R}^n$ et $\tilde{a}$ est paire.
iv) $\tilde{a}$ est réelle impaire.

2) Si $a, b \in \mathbb{C}^n$, rappeler la définition de $a * b$. Exprimer $\mathcal{F}(a) * \mathcal{F}(b)$ et $\mathcal{F}^-(a) * \mathcal{F}^-(b)$ en fonction de $a \cdot b$.

Exercice 15. Soient p un nombre premier (par exemple $p = 2$) et n un entier ≥ 1. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; on utilise la notation $\underline{x} = (x_i)_{1 \leq i \leq n}$ pour préciser les éléments de $\mathbb{F}_p^n$.

1) Au moyen de la forme bilinéaire $\langle \underline{x}, \underline{y} \rangle = \sum_{i=1}^n x_i y_i$ sur $\mathbb{F}_p^n$, expliciter un isomorphisme d'espaces vectoriels entre $\mathbb{F}_p^n$ et son dual $(\mathbb{F}_p^n)^*$.

2) En déduire un isomorphisme de groupes $\iota \colon g \mapsto \chi_g$ de $G := (\mathbb{F}_p^n, +)$ sur $\widehat{\mathbb{F}_p^n}$, qui vérifie $\chi_g(g') = \chi_{g'}(g)$, $(g, g' \in G)$.

3) Montrer que les sous–groupes de G sont exactement les $\mathbb{F}_p$–sous–espaces vectoriels de $\mathbb{F}_p^n$. Pour un tel sous–groupe H, on note ici $H^{\perp gr} := \{\chi \in \widehat{\mathbb{F}_p^n} \,;\ \chi_{|H} = 1\}$, sous–groupe de $\widehat{\mathbb{F}_p^n}$, et $H^{\perp b} \subset \mathbb{F}_p^n$ l'orthogonal de H pour la *forme bilinéaire* $\langle\ ,\ \rangle$.Décrire $H^{\perp gr}$ en terme de ι et $H^{\perp b}$.

4) *Formule de Poisson vectorielle* Soient H un sous–espace vectoriel de $\mathbb{F}_p^n$ et $f \in \mathbb{C}[\mathbb{F}_p^n]$. Montrer les deux formules (cf. 12.2) :

$$\sum_{h \in H} f(h) = \frac{|H|}{p^n} \sum_{u \in H^{\perp b}} \hat{f}(\chi_u) \tag{1}$$

$$\sum_{u \in H^{\perp b}} f(u) = \frac{1}{|H|} \sum_{h \in H} \hat{f}(\chi_h)\,. \tag{2}$$

L'écriture en base p fournit la bijection $\underline{x} = (x_i)_i \mapsto x := \sum_{i=1}^n x_i p^{i-1}$ (où pour tout i on identifie $x_i \in \mathbb{F}_p$ et son représentant dans $[0, p-1]$), entre $\mathbb{F}_p^n$ et l'ensemble *ordonné* E des entiers compris entre 0 et $p^n - 1$; en composant avec ι on obtient aussi une bijection entre $\widehat{\mathbb{F}_p^n}$ et E. Cet ordre sur les bases naturelles de $\mathbb{C}[\mathbb{F}_p^n]$ et $\mathbb{C}[\widehat{\mathbb{F}_p^n}]$ étant choisi, on note $\Omega = \Omega_{[p^n]}$ la matrice de $\mathcal{F}$ correspondante ; Ω est aussi la table des caractères de $\mathbb{F}_p^n$ pour ces ordres d'énumération. Par 2), c'est une matrice symétrique.

5) Écrire la matrice $\Omega_{[9]}$ associée au groupe $\mathbb{F}_3^2$. Comment l'obtenir à partir de la matrice $\Omega := \Omega_{[3]}$ de la TFD sur $\mathbb{Z}/3\mathbb{Z}$?

6) Quelle est l'inverse de $\Omega_{[9]}$?

Exercice 16. 1) Écrire la matrice W_8 de la transformée de Walsh associée à $(\mathbb{Z}/2\mathbb{Z})^3$. Vérifier la formule en terme de la matrice de taille 4 W_4.

2) On identifie les éléments de $G = (\mathbb{Z}/2\mathbb{Z})^3$ à leur numéro, de 0 à 7 (cf. exo 15). Vérifier que le produit de convolution sur $\mathbb{C}[G]$ n'est *pas* celui sur l'algèbre du groupe cyclique $\mathbb{Z}/8\mathbb{Z}$. Calculer $\mathcal{W}(\delta_2)\mathcal{W}(\delta_3)$. En déduire que la TW n'a *pas* un bon comportement vis-à-vis de ce qui serait le produit de convolution modulo $n = 8$.

3) Déterminer le nombre de changements de signe de chaque caractère, vu comme une fonction sur $\{0,\dots,7\}$. Interprétation ?

Exercice 17. Soient $k,n \geq 2$. On appelle *fonction booléenne* à k arguments toute fonction $\tilde{f}\colon (\mathbb{F}_2)^k \to \mathbb{F}_2$. En pratique, la donnée de $\tilde{f}$ équivaut à celle de la fonction réelle $f := (-1)^{\tilde{f}}$ à valeurs dans $\{-1,1\} \subset \mathbb{C}$, qu'on peut voir comme élément de $\mathbb{C}[\mathbb{F}_2^k]$. On peut ainsi considérer sa transformée de Walsh

$$\forall a \in \mathbb{F}_2^k,\ \mathcal{W}(f)(a) := \sum_{x\in\mathbb{F}_2^k} f(x)(-1)^{\langle x,a\rangle}\,.$$

Dans l'exercice on jongle entre les deux types de représentations f et $\tilde{f}$. Les fonctions booléennes *affines* sont les fonctions $\tilde{f}_{a,b}\colon x \mapsto \langle x,a\rangle + b$, où on a $a \in \mathbb{F}_2^k$ et $b \in \mathbb{F}_2$. On définit la distance $d(f,g)$ entre deux fonctions booléennes comme le nombre de $x \in \mathbb{F}_2^k$ tels que $\tilde{f}(x) \neq \tilde{g}(x)$ (c'est la *distance de Hamming* entre les deux vecteurs-valeurs de $\mathbb{F}_2^k$ associés ; en effet il est facile de vérifier l'inégalité triangulaire pour d). On définit la *non-linéarité* de $\tilde{f}$ comme l'entier

$$N(f) = \inf\{d(f,f_{a,b}) \,|\, a \in \mathbb{F}_2^k, b \in \mathbb{F}_2\}\,.$$

1) Soit $a \in \mathbb{F}_2^k$. Montrer que $\min\big(d(f,f_{a,0}), d(f,f_{a,1})\big) = \frac{1}{2}(2^k - |\mathcal{W}(f)(a)|\,)$.
En déduire que $N(f) = 2^{k-1} - \frac{1}{2}\max\{\,|\mathcal{W}(f)(x)|\,;\, x \in \mathbb{F}_2^k\}$. Donner une méthode de calcul rapide de $N(f)$.

2) Montrer que $N(f) \leq 2^{k-1} - 2^{\frac{k}{2}-1}$ (`Indication:` on pourra utiliser la formule de Plancherel).

3) On suppose que k est pair. Montrer qu'une fonction $\tilde{f}$ atteint la borne donnée en 2) si et seulement si $|\mathcal{W}(f)|$ est la constante $2^{\frac{k}{2}}$; on dira que $\tilde{f}$ est une *fonction courbe* (*bent function* en anglais).

4) Pour $u \in \mathbb{F}_2^k$ et $v \in \mathbb{F}_2^l$, on pose $w = (u,v) \in \mathbb{F}_2^{k+l}$. Soient $\tilde{f}$ et $\tilde{g}$ des fonctions booléennes à k resp. l arguments. On définit $\tilde{h}$ une fonction à $k+l$ arguments par $\tilde{h}(w) = \tilde{f}(u) + \tilde{g}(v)$. Calculer $\mathcal{W}(h)$. Montrer que $\tilde{h}$ est courbe si et seulement si $\tilde{f}$ et $\tilde{g}$ le sont.
Montrer que $\widetilde{f_0}\colon (u_0,u_1) \mapsto u_0u_1$ de $\mathbb{F}_2^2$ dans $\mathbb{F}_2$ est courbe. En déduire l'existence de fonctions courbes pour k pair.

On nomme *code de Reed-Muller* d'ordre 1 en n variables (noté $R(1,n)$), le sous–espace vectoriel de l'espace des fonctions booléennes à n arguments formé des fonctions affines $f_{a,b}$ ($a \in \mathbb{F}_2^n$).

5) Quelle est sa dimension ? que vaut la distance minimale d entre deux éléments distincts de $R(1,n)$ (dite la *distance minimale* du code) ? [1]

6) La procédure de codage consiste, à partir du couple (a,b) de $\mathbb{F}_2^n \times \mathbb{F}_2$, à produire le vecteur-valeurs $F_{a,b} := \big(f_{a,b}(x)\big)_{x\in\mathbb{F}_2^n}$. Donner une méthode de codage rapide.

7) Soit $F \in \mathbb{F}_2^{2^n}$ vecteur-valeurs de $\tilde{f}$ booléenne, tel que $N(f) \leq (d-1)/2$. Quel est le couple (a,b) (unique !) tel que $d(f,f_{a,b})$ soit minimale ? En déduire une méthode de décodage rapide.

1. Historiquement, le code $R(1,5)$, qui a 64 mots de longueur 32 et corrige 7 erreurs, a été utilisé par les sondes Mariner lancées par la NASA entre 1969 et 1973 pour transmettre des photos de Mars.

Exercice 18. Utiliser la transformée de Fourier discrète pour trouver les polynômes complexes P de degré au plus 3 tels que P vaut : 0 en 1, 1 en i, 2 en -1 et 3 en $-i$.

Exercice 19. Soit $n \geq 2$ un entier pair.
1) On considère les polynômes trigonométriques $p(t) = \sum_{k=-n/2}^{n/2-1} a_k e^{ikt}$. Utiliser la TFD pour montrer que les a_k s'expriment de manière unique en fonction des n valeurs $p(2l\pi/n)$, $0 \leq l \leq n-1$; donner cette expression.

2) On suppose que $n = 2n'$. On considère les polynômes trigonométriques $f(t) = \sum_{k=0}^{n'} b_k \cos(kt)$. Utiliser ce qui précède pour montrer que les $n'+1$ valeurs $y_l = f(l\pi/n')$, $0 \leq l \leq n'$, déterminent les coefficients b_k de f de manière unique, et donner l'expression correspondante.

Exercice 20. Soient les éléments $P_a = -10 + X - X^2 + 7X^3$ et $P_b = 3 - 6X + 8X^3$ de l'algèbre $\mathbb{C}[X]/(X^n - 1)$ $(n \geq 4)$; ils sont associés aux éléments a et b de $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}]$.

1) Si $n = 4$, calculer leur produit P_{a*b}.

2) Si $n = 8$, utiliser la FFT pour calculer les transformées de Fourier de P_a et P_b, et en déduire le produit $P_a P_b$ dans $\mathbb{C}[X]$.

FIN.