

NOM : DURAND

Prénom : Romain

Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi : 110. Caractères d'un groupe abélien fini et transformée de Fourier discrète.
Applications.

Autre sujet :

Ref: REYRE

Δ_{VP}
1
(17+19)

<u>I) Espace de fonctions sur G</u> Quand non précisé, G est un groupe fini quelconque. <u>Def 1:</u> On note $\mathcal{C}[G] = \{f: G \rightarrow \mathbb{C}\}$. C'est un $\mathbb{C}$-ev que l'on peut munir d'une structure hermitienne par $\langle f, g \rangle = \frac{1}{ G } \sum_{x \in G} f(x) \overline{g(x)}$. <u>Rq 2:</u> Analogie avec $\langle f, g \rangle = \int_{\mathbb{R}} f(x) \overline{g(x)} dx$ dans $L^2(\mathbb{R})$. <u>Prop 3:</u> (Invariance par translation). Si, pour $g \in G$, $T_g f(x) = f(xg)$. Alors on a $\langle T_g f, T_g g \rangle = \langle f, g \rangle \quad \forall f, g \in \mathcal{C}[G]$. <u>Prop 4:</u> Pour $g \in G$, on pose $\delta_g: h \mapsto 1$ si $h=g$ sinon $0 \in \mathcal{C}[G]$. Alors $\{\delta_g\}_{g \in G}$ forme une base de $\mathcal{C}[G]$. <u>Cor 5:</u> $\dim_{\mathbb{C}} \mathcal{C}[G] = G$. <u>Rq 6:</u> La multiplication $f, g \mapsto f \cdot g$ confère à $\mathcal{C}[G]$ une structure d'algèbre, mais celle-ci ne prend pas en compte la structure de groupe de G. <u>Def 7:</u> (Produit de convolution). On définit * par $\delta_g \cdot \delta_h = \delta_{gh}$ pour $g, h \in G$, que l'on étend par bilinéarité à $\mathcal{C}[G]$. Pour $f_1, f_2 \in \mathcal{C}[G]$ et $g \in G$ $f_1 * f_2(g) = \sum_{h+k=g} f_1(h) f_2(k) = \sum_{h \in G} f_1(h) f_2(h^{-1}g)$. <u>Prop 8:</u> * est commutatif, associatif, $(f_1, f_2) \mapsto f_1 * f_2$ est bilinéaire. On a donc une autre structure d'algèbre sur $\mathcal{C}[G]$ héritée de la structure de groupe de G. <u>II) Caractères et dualité</u> <u>Def 9:</u> Un caractère χ de G est un morphisme de $G \rightarrow \mathbb{C}^*$. On note $\hat{G}$ l'ensemble des caractères et on l'appelle le dual de G. <u>Prop 10:</u> $\hat{G}$ est un groupe abélien muni de $\chi_1 \chi_2: x \mapsto \chi_1(x) \chi_2(x)$.	<u>Prop 11:</u> Si $G =n$, $\hat{G}$ est constitué des morphismes de $G \rightarrow \mathbb{C}^*$. <u>Cor 12:</u> $\forall g \in G, \chi(g) =1$ et $\chi(g^{-1}) = \overline{\chi(g)}$. <u>1) Cas cyclique</u> <u>Prop 13:</u> Si $G \simeq \mathbb{Z}/n\mathbb{Z}$, et ω est une racine primitive n-ième de l'unité, les éléments de $\hat{G}$ sont donnés par $\chi_j: k \mapsto (\omega^j)^k$. <u>Cor 14:</u> On a $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}$. <u>Rq 15:</u> L'isomorphisme $G \simeq \hat{G}$ n'est pas canonique: il dépend du choix de la racine primitive ω. <u>2) Cas d'un groupe abélien quelconque</u> <u>lemme 16:</u> Si G, H sont finis abéliens, $\widehat{G \times H} \simeq \hat{G} \times \hat{H}$. <u>lemme 17:</u> (Prolongement des caractères). Soit G abélien et H un sous-groupe de G et $\chi \in \hat{H}$. Alors il existe $\tilde{\chi} \in \hat{G}$ tq $\tilde{\chi} _H = \chi$. <u>lemme 18:</u> Si G est abélien fini, il existe x d'ordre tel que l'élément de tout y de G divise celui de x. <u>Thm 19</u> (Structure des groupes abéliens finis) Si G est un groupe abélien fini, il existe $n_1, \dots, n_r$ avec $n_1 n_2 \dots n_r = G$ et tels que $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$. <u>Cor 20:</u> On a $G \simeq \hat{G}$, mais l'isomorphisme n'est pas canonique. <u>Def 21:</u> On définit $\hat{\hat{G}}$ le bidual de G. <u>Prop 22:</u> On a un isomorphisme canonique $G \simeq \hat{\hat{G}}$ donné par $\Phi: g \mapsto (\chi \mapsto \chi(g))$. <u>3) Orthogonalité:</u> <u>lemme 23:</u> Soit G abélien fini. Alors $\forall \chi \in \hat{G}, \sum_{g \in G} \chi(g) = G$ si $\chi = \chi_0$ (le caractère trivial) et 0 sinon. <u>Prop 24:</u> $\forall (\chi_1, \chi_2) \in \hat{G}^2, \langle \chi_1, \chi_2 \rangle = 1$ si $\chi_1 = \chi_2$ et 0 sinon. <u>Cor 25:</u> $\{\delta_g\}_{g \in G}$ est une base orthogonale de $\mathcal{C}[G]$.
--	---

NOM :

Prénom :

Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi :

Autre sujet :

<u>Cor 26</u>: Pour $g, h \in G$, $\sum_{x \in G} \chi(g) \chi(h) = G$ si $g \neq h$. <u>III</u> - Transformée de Fourier discrète (G est abélien fini) <u>Def 27</u>: $\mathcal{F}: \ell^1(G) \rightarrow \ell^\infty(\hat{G})$ ou $\hat{f}(\chi) = \sum_{x \in G} f(x) \chi(x) = G ^{-1} \sum_{x \in G} f(x) \chi(x)$ <u>Ex 28</u>: Si $(f(x))_{x \in \mathbb{Z}/n\mathbb{Z}} \in \mathbb{C}^n$ est un signal $f(x) = \sum_{j \in \mathbb{Z}/n\mathbb{Z}} \hat{f}(j) e^{\frac{2\pi i j x}{n}}$, où $\hat{f} \in \ell^1(\mathbb{Z}/n\mathbb{Z})$ ($i \rightarrow \hat{f}(i)$) et $x \in \mathbb{Z}/n\mathbb{Z}$ ($j \rightarrow e^{\frac{2\pi i j x}{n}}$) <u>Prop 29</u>: (Inversion de Fourier). $\forall f \in \ell^1(G)$, $f = \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi$ et $\hat{f}(\chi) = \frac{1}{ G } \sum_{x \in G} f(x) \chi(x)$. <u>Cor 30</u>: $\mathcal{F}$ est un isomorphisme de $\mathbb{C}$-ev entre $\ell^1(G)$ et $\ell^\infty(\hat{G})$. <u>Prop 31</u> (Formule de Plancherel). Soient f et g dans $\ell^1(G)$. Alors $\langle f, g \rangle_{\ell^1(G)} = \frac{1}{ G } \langle \hat{f}, \hat{g} \rangle_{\ell^\infty(\hat{G})}$, i.e. $\ f\ _2 = \frac{1}{ G } \ \hat{f}\ _2$ <u>Application 32</u>: Si $\mathbb{P}$ est une mesure de proba sur G, on a $\forall g \in G$, $\hat{P}(g) ^2 = \frac{1}{ G } \sum_{\chi \in \hat{G}} \hat{P}(\chi) ^2$ <u>Thm fondamental 33</u>: $\hat{f} * \hat{g} = \widehat{f \cdot g}$: $\mathcal{F}$ est un isomorphisme d'algèbres de $(\ell^1(G), *) \rightarrow (\ell^\infty(\hat{G}), \cdot)$ <u>Rq 34</u>: Le produit de convolution correspond à la somme de 2 variables aléatoires indépendantes: $\mathbb{P}_{X+Y} = \mathbb{P}_X * \mathbb{P}_Y$ <u>Application 35</u>: Si n impair, la marche aléatoire biaisée sur $\mathbb{Z}/n\mathbb{Z}$ converge vers la mesure uniforme. <u>Prop 36</u>: (lien avec le continu). Pour $f \in L^1$, on pose $\hat{f}(\xi) = \int_{\mathbb{R}} f(x) e^{-2\pi i x \xi} dx$. Les seuls morphismes de $(\mathbb{R}, +) \rightarrow (\mathbb{C}, \cdot)$ sont les $\chi_\xi: x \rightarrow e^{2\pi i x \xi}$ pour $\xi \in \mathbb{R}$: $\hat{f}(\xi) = \int_{\mathbb{R}} f(x) \chi_\xi(x) dx$. <u>IV</u> - Transformée de Fourier rapide <u>Rq 37</u>: Si $P = a_n X^n + \dots + a_0 \in \mathbb{C}[X]$, on peut définir $\hat{P} \in \ell^1(\mathbb{Z}/n\mathbb{Z})$ par $\hat{P}(i) = a_i$. Avec cette notation, pour $P, Q \in \mathbb{C}[X]$, on a $\widehat{PQ} = \hat{P} * \hat{Q}$. Dans la suite, on confondra P et $\hat{P}$.	<u>Prop 38</u>: (Transformée de Fourier rapide) Soit $G = \mathbb{Z}/n\mathbb{Z}$, $S = e^{\frac{2\pi i}{n}}$ et $H = \mathbb{Z}/\frac{n}{2}\mathbb{Z}$. Pour $f \in \ell^1(G)$ et $\chi \in \hat{G}$, on note $\tilde{f} = f _H \in \ell^1(H)$ et $\tilde{\chi} = \chi _H = f _H(u+1)$ Alors pour tout j, on a $\hat{f}(\chi_j) = \hat{\tilde{f}}(\tilde{\chi}_j) + S^{-1} \hat{f}(\chi_j)$ et $\Delta(j) \geq 2^{n-1}$ et $k = j - 2^{n-1}$. $\hat{f}(\chi_j) = \hat{\tilde{f}}(\tilde{\chi}_j) - S^{-k} \hat{f}(\tilde{\chi}_k)$. Ainsi, par cette méthode, le calcul de $\hat{f}$ est en $\mathcal{O}(n \log n) = \mathcal{O}(N \log N)$. <u>Application 39</u>: (Multiplication de polynômes) Avec l'identification de $\mathbb{Z}/n\mathbb{Z}$, comme $\hat{f}(\chi_j) = \hat{f}(\chi_j)$ et $\hat{g}(\chi_j) = \hat{g}(\chi_j)$ $\hat{P}, \hat{Q} \in \ell^1(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\mathcal{F}} \hat{P}, \hat{Q} \in \ell^1(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\mathcal{F}} \widehat{PQ} \in \ell^1(\mathbb{Z}/n\mathbb{Z})$ On peut calculer le produit en $\mathcal{O}(N \log N)$ opérations au lieu de $\mathcal{O}(N^2)$ du calcul direct. <u>Cor 40</u>: Calcul d'un produit d'entiers en base 2. <u>V</u> Application aux corps finis: Soit p premier et $q = p^r$. <u>1</u> Description des caractères additifs <u>Prop 41</u>: $\mathbb{F}_q^*$ est cyclique <u>Def 42</u>: Les éléments de $(\mathbb{F}_q, +)$ sont les caractères additifs, notés ψ. <u>Def 43</u>: Pour $\alpha \in \mathbb{F}_q$, on définit $\text{Tr}(\alpha) = \alpha + \alpha^p + \dots + \alpha^{p^{r-1}}$. <u>lemme 44</u>: $x \in \mathbb{F}_q$. Alors $x \in \mathbb{F}_p \Leftrightarrow x^p = x$. <u>Prop 45</u>: Tr est une forme linéaire sur $\mathbb{F}_p$, à valeurs dans $\mathbb{F}_p$, et non triviale.
--	---

NOM : DURAND

Prénom :

Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi : 110

Autre sujet :

<u>Prop 46</u>: (Description des caractères additifs). On définit le morphisme canonique $\psi: \mathbb{F}_q \rightarrow \mathbb{C}^\times$ puis, pour $a \in \mathbb{F}_q$, $\psi_a: (x \rightarrow \psi(ax)) \in \widehat{\mathbb{F}_q}$. Alors $\mathbb{F}_q = (\psi_a)_{a \in \mathbb{F}_q}$. <u>2) Sommes de Gauss et équation de Fermat dans $\mathbb{F}_q$</u> <u>Def 47</u>: Pour $\chi \in \widehat{\mathbb{F}_q}^\times$ et $\psi \in \widehat{\mathbb{F}_q}$, on définit la somme de Gauss: $G(\chi, \psi) = \sum_{x \in \mathbb{F}_q} \chi(x) \psi(x)$ <u>Rq 48</u>: (lien avec la TFD) $G(\chi, \psi) = \overline{F_{\text{mult}}(\psi)}(\chi) = \overline{F_{\text{mult}}(\chi)}(\psi)$ où $\chi \in \widehat{\mathbb{F}_q}^\times$ est le prolongement de χ avec $\chi(0) = 0$. <u>Prop 49</u>: i) $G(\chi, \psi_{ab}) = \overline{\chi(a)} G(\chi, \psi_b)$ ii) $G(\chi, \overline{\psi}) = \chi(-1) G(\chi, \psi)$ iii) $G(\overline{\chi}, \psi) = \chi(-1) \overline{G(\chi, \psi)}$ <u>Prop 50</u>: On a $G(\chi, \psi) = \begin{cases} q-1 & \text{si } (\chi, \psi) = (\chi_0, \psi_0) \\ -1 & \text{si } \chi = \chi_0, \psi \neq \psi_0 \\ 0 & \text{si } \chi \neq \chi_0, \psi = \psi_0 \end{cases}$ et si $\chi \neq \chi_0, \psi \neq \psi_0$, $G(\chi, \psi) = \sqrt{q}$ <u>lemme 51</u>: Soit G additif abélien fini, et $A_1, A_2, \dots, A_n$ des parties de G, et $h \in G$. Alors $E = \{ (x_1, \dots, x_n) \in A_1 \times \dots \times A_n; x_1 + \dots + x_n = h \}$ est de cardinal $\frac{ A_1 \dots A_n }{ G } + R$, où $R = \frac{1}{ G } \sum_{\psi \neq \psi_0} \chi_\psi(h)$. <u>Thm 52</u>: Soit $k \geq 2$ et $q = p^r$, $d = \text{pgcd}(k, q-1)$. Alors si $q \geq d^4 + 4$, $x^k + y^k = z^h$ a des solutions dans $\mathbb{F}_q^\times$.	<u>Cor 53</u>: $x^3 + y^3 = z^3$ a des solutions non triviales dans $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.
---	---

3/11/15

Leçon 110: Caractères d'un gpe abélien fini et transformée de Fourier discrète. Application

Ex 2

$$\mathbb{F}_q \quad x^k = y^k = g^k \quad d = \text{pgcd}(k, q-1)$$

Remarquons que $\{x^k, x \in \mathbb{F}_q^*\} = \{x^d, x \in \mathbb{F}_q^*\}$ car si $k = kd'$ $x^k = (x^{k'})^d$ et si $d = vk + r(q-1)$, $x^d = (x^k)^v$

Il suffit de mg $x^d + y^d = g^d$ a des solutions

$$\mathcal{H}_d := \{x^d, x \in \mathbb{F}_q^*\}, d \text{ divise } d$$

$$\mathcal{Y}_d := \{X \in \mathbb{F}_q^*, X^d = X_0\} \sim \mathbb{F}_q^* / \mathcal{H}_d$$

Pour $A_1, A_2 \subset \mathbb{F}_q$ $E := \{(x, y, z) \in A_1 \times A_2 \times \mathcal{H}_d, x+y-z=0\}$

On veut mg pour $A_1 = A_2 = \mathcal{H}_d$ E est non vide

$$\frac{|E| - |A_1||A_2|}{q} \leq R = \frac{1}{|G|} \sum_{\Psi \neq \Psi_0} |\widehat{\mathbb{1}}_{A_1}(\Psi)| |\widehat{\mathbb{1}}_{A_2}(\Psi)|$$

$$\text{Pour } r=3: R \leq \frac{1}{|G|} \sum_{\Psi \neq \Psi_0} |\widehat{\mathbb{1}}_{A_1}(\Psi)| |\widehat{\mathbb{1}}_{A_2}(\Psi)| |\widehat{\mathbb{1}}_{A_3}(\Psi)|$$

$$\text{Posons } \Phi(A) = \max_{\Psi \neq \Psi_0} |\widehat{\mathbb{1}}_A(\Psi)|$$

$$|R| \leq \Phi(A_3) \langle \mathbb{1}_{A_1}, \mathbb{1}_{A_2} \rangle$$

$$\leq \Phi(A_3) \|\mathbb{1}_{A_1}\|_2 \|\mathbb{1}_{A_2}\|_2 \text{ par ?}$$

$$\text{Par Plancherel, } |R| \leq \Phi(A_3) \|\mathbb{1}_{A_1}\|_2 \|\mathbb{1}_{A_2}\|_2 |G|$$

$$\text{Or } \|\mathbb{1}_A\|_2^2 = \frac{1}{|G|} \sum_{x \in G} \mathbb{1}_A(x) = \frac{|A|}{|G|}$$

$$\text{Donc } |R| \leq \Phi(A_3) \sqrt{|A_1||A_2|}$$

$$\text{Pour } \Psi \neq \Psi_0: \frac{1}{d} \sum_{x \in G} G(x, \Psi) = \frac{1}{d} \sum_{x \in G} \sum_{x \in \mathcal{H}_d} \chi(x) \psi(x)$$

$$\text{Or } \sum_{x \in G} \chi(x) = \begin{cases} |G| & \text{si } x=e, x \in \mathcal{H}_d = d \mathbb{1}_{\mathcal{H}_d}(x) \\ 0 & \text{sinon} \end{cases}$$

$$\text{Donc } \frac{1}{d} \sum_{x \in G} G(x, \Psi) = \frac{1}{d} \sum_x d \mathbb{1}_{\mathcal{H}_d}(x) \psi(x) = \widehat{\mathbb{1}_{\mathcal{H}_d}}(\Psi)$$

$$|\widehat{\mathbb{1}_{\mathcal{H}_d}}(\Psi)| \leq \frac{1}{d} \sum_{x \in G} |G(x, \Psi)| = \frac{1}{d} (1 + (d-1)\sqrt{q}) < \sqrt{q}$$

$$R \leq \sqrt{q} |A_1| |A_2|$$

Cherchons des conditions sur $f_i = \frac{q-1}{|A_i|}$

[--]

II Exercices

① Dans $\mathbb{F}_p^*$ $\mathbb{F}_p^*$ cyclique est d'ordre 2 ? (ds)

$$\chi^2 = \chi_0$$

$$\forall x \in \mathbb{F}_p^*, \chi(x) \in \{ -1, 1 \} \text{ et } \exists x, \chi(x) = -1$$

$$\chi_p: x \mapsto \begin{cases} 1 & \text{si } x \text{ est un carré} \\ 0 & \text{sinon} \end{cases}$$

$$x^{p-1} = 1 \quad x^{p-1/2} \in \{ -1, 1 \} \quad \text{Si } x \text{ d'ordre } p-1, x^{p-1/2} = -1$$

$\forall \chi, \chi_p$ est un morph.

$\chi_p(\chi_y)$ est pdt de 2 non carrés et un carré.

$$\text{Si } x \text{ est un carré, } x = y^2, x^{p-1/2} = y^{p-1} = 1$$

Et réciproquement $x^{p-1/2} = 1$ a $\frac{p-1}{2}$ racines de ce sont les carrés.

$$\text{Donc } x \text{ carré} \Leftrightarrow x^{p-1/2} = 1$$

