DS 3 de mathématiques

Durée : 4 heures. Les calculatrices et autres technologies sont interdites.

Si vous repérez une possible erreur d'énoncé, vous êtes invité(e) à venir le signaler.

1 Structure des groupes abéliens finis

1.1 Ordres et exposant

Soit G un groupe abélien fini de cardinal n ; la loi de groupe est notée multiplicativement et l'élément neutre est noté 1.
On rappelle que l'ordre d'un élément $x \in G$, qu'on note $\omega(x)$, est le plus petit entier naturel $k \in \mathbb{N}^*$ tel que $x^k = 1$. On rappelle la propriété suivante :

$$\forall k \in \mathbb{Z}, x^k = 1 \iff \omega(x) \mid k.$$

1. Soit a un élément de G.
   Montrer que l'application $\tau_a : G \to G, x \mapsto ax$ est une permutation de G.
2. En considérant le produit[1] $P = \prod_{x \in G} x$, en déduire que $\omega(a) \mid n$.
3. On note[2] $e = \max_{x \in G} \omega(x)$ l'*exposant* de G. On cherche à montrer que, pour tout x dans G, $\omega(x)$ divise e.
   (a) Soient a, b deux éléments de G tels que $\omega(a) \wedge \omega(b) = 1$.
   Montrer que $\omega(ab) = \omega(a)\omega(b)$.
   (b) On fixe un élément y d'ordre e. Soit $x \in G$, soit p un nombre premier. On écrit $\omega(x) = p^\alpha r$ et $e = p^\beta s$ où $\alpha, \beta \in \mathbb{N}$ et où p ne divise pas les entiers r et s.
   Montrer que $\omega(x^r) = p^\alpha$, $\omega(y^{p^\beta}) = s$ et $\omega(x^r y^{p^\beta}) = p^\alpha s$.
   (c) Conclure.
4. **Un exemple.** Soit p un nombre premier, soit G un groupe de cardinal p^3. Montrer que l'exposant de G ne peut prendre que 3 valeurs. Dans chacun des 3 cas, donner un exemple de groupe ayant cet exposant.

[1] Bien défini car indépendant de l'ordre choisi pour les facteurs

[2] Rien à voir avec l'élément neutre.

1.2 Prolongement de caractères

Un *caractère* d'un groupe abélien fini G est un morphisme de groupes $\chi : G \to \mathbb{U}$.

Soient G un groupe abélien fini, H un sous-groupe strict de G et $\chi : H \to \mathbb{U}$ un caractère de H. On souhaite montrer qu'il existe un caractère $\hat{\chi} : G \to \mathbb{U}$ tel que $\chi = \hat{\chi}_{|H}$.

5. On fixe un élément $a \in G \setminus H$. Montrer que l'ensemble $\{k \in \mathbb{N}^* \mid a^k \in H\}$ admet un élément minimal d et montrer qu'on a la propriété suivante :
$$\forall k \in \mathbb{Z}, a^k \in H \iff d \mid k.$$

6. On note K le sous-groupe de G engendré par $H \cup \{a\}$.
   (a) Montrer que $K = \{ha^k, h \in H \text{ et } k \in \mathbb{Z}\}$.
   (b) On note $h_0 = a^d \in H$. Montrer qu'il existe $\omega \in \mathbb{U}$ tel que $\omega^d = \chi(h_0)$.

   On fixe un tel ω dans la suite.

   (c) On définit $\chi' : K \to \mathbb{U}, ha^k \mapsto \chi(h)\omega^k$, pour tout h.
   Justifier que χ' est bien défini, que c'est un caractère de K et que $\chi'_{|H} = \chi$.

7. Conclure quant à l'existence d'un caractère $\hat{\chi}$ de G tel que $\hat{\chi}_{|H} = \chi$.

1.3 Théorème de structure

Soient G un groupe abélien fini de cardinal n et d'exposant e. On note x un élément de G d'ordre e.

8. Montrer que le sous-groupe $\langle x \rangle$ de G est isomorphe au groupe additif $\mathbb{Z}/e\mathbb{Z}$.

9. En déduire l'existence d'un caractère χ de $\langle x \rangle$ tel que $\mathrm{Im}(\chi) = \mathbb{U}_e$ et tel que $\chi : \langle x \rangle \to \mathbb{U}_e$ est un isomorphisme de groupes.

D'après la partie précédente, on peut alors considérer un caractère $\hat{\chi}$ de G tel que $\hat{\chi}_{|\langle x \rangle} = \chi$. On note H le noyau de $\hat{\chi}$.

10. Montrer que $\hat{\chi}(G) = \mathbb{U}_e$. En déduire que tout élément g de G s'écrit de façon unique $g = x^k h$, où $k \in [\![0, e-1]\!]$ et $h \in H$.

11. En déduire qu'il existe un isomorphisme de groupes de G dans $\mathbb{Z}/e\mathbb{Z} \times H$.

12. En déduire la partie *existence* du théorème de structure des groupes abéliens finis :
Soit G un groupe abélien fini de cardinal $n \geq 2$. Il existe une unique suite finie $(d_1, \ldots, d_r)$ d'entiers supérieurs à 2 telle que
   - $\forall k \in [\![1, r-1]\!], d_{k+1} \mid d_k$
   - *G est isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \mathbb{Z}/d_r\mathbb{Z}$.*

2 Convolution de Dirichlet et fonction de Möbius

2.1 Anneau des fonctions arithmétiques

On appelle *fonction arithmétique* une fonction $f : \mathbb{N}^* \to \mathbb{C}$ et on note $\mathcal{A}$ l'ensemble des fonctions arithmétiques. On munit l'ensemble $\mathcal{A}$ de deux lois de composition interne $+$ et $*$ définies ainsi, pour tous $f, g \in \mathcal{A}$:

- $+$ est l'addition usuelle des fonctions :

$$\forall n \in \mathbb{N}^*, (f+g)(n) = f(n) + g(n).$$

- $*$ est un *produit de convolution* défini par :

$$\forall n \in \mathbb{N}^*, (f * g)(n) = \sum_{\substack{(a,b)\in(\mathbb{N}^*)^2 \\ ab=n}} f(a)g(b) = \sum_{\substack{d\in\mathbb{N}^* \\ d|n}} f(d)g(\frac{n}{d}).$$

1. Montrer que $(\mathcal{A}, +)$ est un groupe abélien.
2. Montrer que la loi $*$ est commutative et associative.
3. On note $\delta_1 \in \mathcal{A}$ la fonction définie par $\delta_1(1) = 1$ et $\delta_1(n) = 0$ si $n \geq 2$.
   Montrer que δ_1 est élément neutre pour $*$.
4. Montrer que $(\mathcal{A}, +, *)$ est un anneau commutatif.
5. On note $(\mathcal{A}^\times, *)$ le groupe des inversibles de $\mathcal{A}$. Montrer que $f \in \mathcal{A}^\times \iff f(1) \neq 0$.

2.2 Fonctions multiplicatives

Une fonction $f \in \mathcal{A}$ est *multiplicative* si $\forall m, n \in \mathbb{N}^*, m \wedge n = 1 \implies f(mn) = f(m)f(n)$.
On note $\mathcal{M}$ l'ensemble des fonctions multiplicatives .
Pour tout $k \in \mathbb{N}^*$, on note $\mathrm{Div}(k)$ l'ensemble des diviseurs strictement positifs de k.

6. Soient $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$. Montrer que l'application

$$\begin{cases} \phi : \mathrm{Div}(m) \times \mathrm{Div}(n) & \to & \mathrm{Div}(mn) \\ (d_1, d_2) & \mapsto & d_1 d_2 \end{cases}$$

   est bien définie et est une bijection.
7. En déduire que $\mathcal{M}$ est stable par $*$.
8. Montrer que $\mathcal{M} \setminus \{0\} \subset \mathcal{A}^\times$.
9. Soit $f \in \mathcal{M} \setminus \{0\}$. On cherche à montrer que $f^{-1} \in \mathcal{M}$.

(a) Montrer qu'il existe une unique fonction $g \in \mathcal{M}$ telle que

$$\forall p \in \mathbb{P}, \forall k \in \mathbb{N}^*, g(p^k) = f^{-1}(p^k).$$

(b) Montrer que $\forall p \in \mathbb{P}, \forall k \in \mathbb{N}^*, (g * f)(p^k) = 0$.

(c) Conclure.

Ainsi, on a montré que $\mathcal{M} \setminus \{0\}$ est un sous-groupe des inversibles de $\mathcal{A}$, pour la loi $*$.

2.3 Fonction de Möbius

On définit la fonction $\mu \in \mathcal{A}$ par

$$\mu(n) = \begin{cases} (-1)^r & \text{si } n \text{ est le produit de } r \text{ nombres premiers distincts} \\ 0 & \text{sinon.} \end{cases}$$

10. Montrer que $\mu \in \mathcal{M}$.

11. On note $\mathbb{1} \in \mathcal{M}$ la fonction constante égale à 1.

(a) Montrer que $\forall p \in \mathbb{P}, \forall k \in \mathbb{N}^*, (\mu * \mathbb{1})(p^k) = \sum_{i=0}^{k} \mu(p^i) = 0$.

(b) En déduire que μ est l'inverse de $\mathbb{1}$ et qu'on a la relation :

$$\forall n \in \mathbb{N}^*, \sum_{d|n} \mu(d) = \begin{cases} 0 & \text{si } n \geq 2 \\ 1 & \text{si } n = 1 \end{cases}$$

12. Soit $f \in \mathcal{A}$. On définit $g \in \mathcal{A}$ par $\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} f(d)$.

Montrer la *formule d'inversion de Möbius* : $\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$.

2.4 Produits eulériens

Soient S un ensemble fini de nombres premiers et N un entier naturel. On note $\mathbb{N}_{S,N}$ l'ensemble des $n \in \mathbb{N}^*$ tels que, si p est un diviseur premier de n, alors $p \in S$ et $\nu_p(n) \leq N$.

13. Montrer que si $f \in \mathcal{M}$, alors $\sum_{k \in \mathbb{N}_{S,N}} f(k) = \prod_{p \in S} \left(\sum_{k=0}^{N} f(p^k) \right)$.

On admet que si $\lim\limits_{n\to+\infty}\sum\limits_{k=1}^{n}|f(k)|$ existe, alors on peut *passer à la limite* dans l'identité précédente et montrer l'identité : $\lim\limits_{n\to+\infty}\sum\limits_{k=1}^{n}f(k) = \lim\limits_{r\to+\infty}\prod\limits_{j=1}^{r}\left(\lim\limits_{N\to+\infty}\sum\limits_{k=0}^{N}f(p_j^k)\right)$, où pour tout $j\in\mathbb{N}^*$, on a noté p_j le j-ème nombre premier.

Pour les questions qui suivent, on ne demande pas de vérifier l'existence de $\lim\limits_{n\to+\infty}\sum\limits_{k=1}^{n}|f(k)|$, pour les fonctions $f\in\mathcal{M}$ qu'on utilisera.

Si s est un entier naturel supérieur à 2, on note $\zeta(s) = \lim\limits_{n\to+\infty}\sum\limits_{k=1}^{n}\dfrac{1}{k^s}$.

14. Montrer que $\zeta(s) = \lim\limits_{r\to+\infty}\prod\limits_{j=1}^{r}\dfrac{1}{1-p_j^{-s}}$.

15. Montrer que $\dfrac{1}{\zeta(s)} = \lim\limits_{n\to+\infty}\sum\limits_{k=1}^{n}\dfrac{\mu(k)}{k^s}$.

2.5 Probabilité que deux entiers soient premiers entre eux

Pour tous entiers $1\leq d\leq n$, on note $H_d^n = \big\{(u,v)\in [\![1,n]\!]^2 \mid u\wedge v = d\big\}$.

16. Soient $1\leq d\leq n$ des entiers.
    Montrer que $\lfloor\dfrac{n}{d}\rfloor^2 = \sum\limits_{\substack{1\leq k\leq n\\ d\mid k}}|H_k^n|$, où $|H_k^n|$ désigne le nombre d'éléments de H_k^n.

17. En déduire que $|H_1^n| = \sum\limits_{k=1}^{n}\mu(k)\lfloor\dfrac{n}{k}\rfloor^2$.

18. Montrer que, pour tout $n\geq 1$, on a les majorations suivantes :

$$\left||H_1^n| - n^2\sum_{k=1}^{n}\frac{\mu(k)}{k^2}\right| \leq 2n\sum_{k=1}^{n}\frac{1}{k} \leq 2n(\ln n + 1).$$

La probabilité que deux entiers soient premiers entre eux est définie comme la limite de $\dfrac{|H_1^n|}{n^2}$, quand $n\to+\infty$ (sous réserve d'existence).

19. Déterminer cette probabilité.